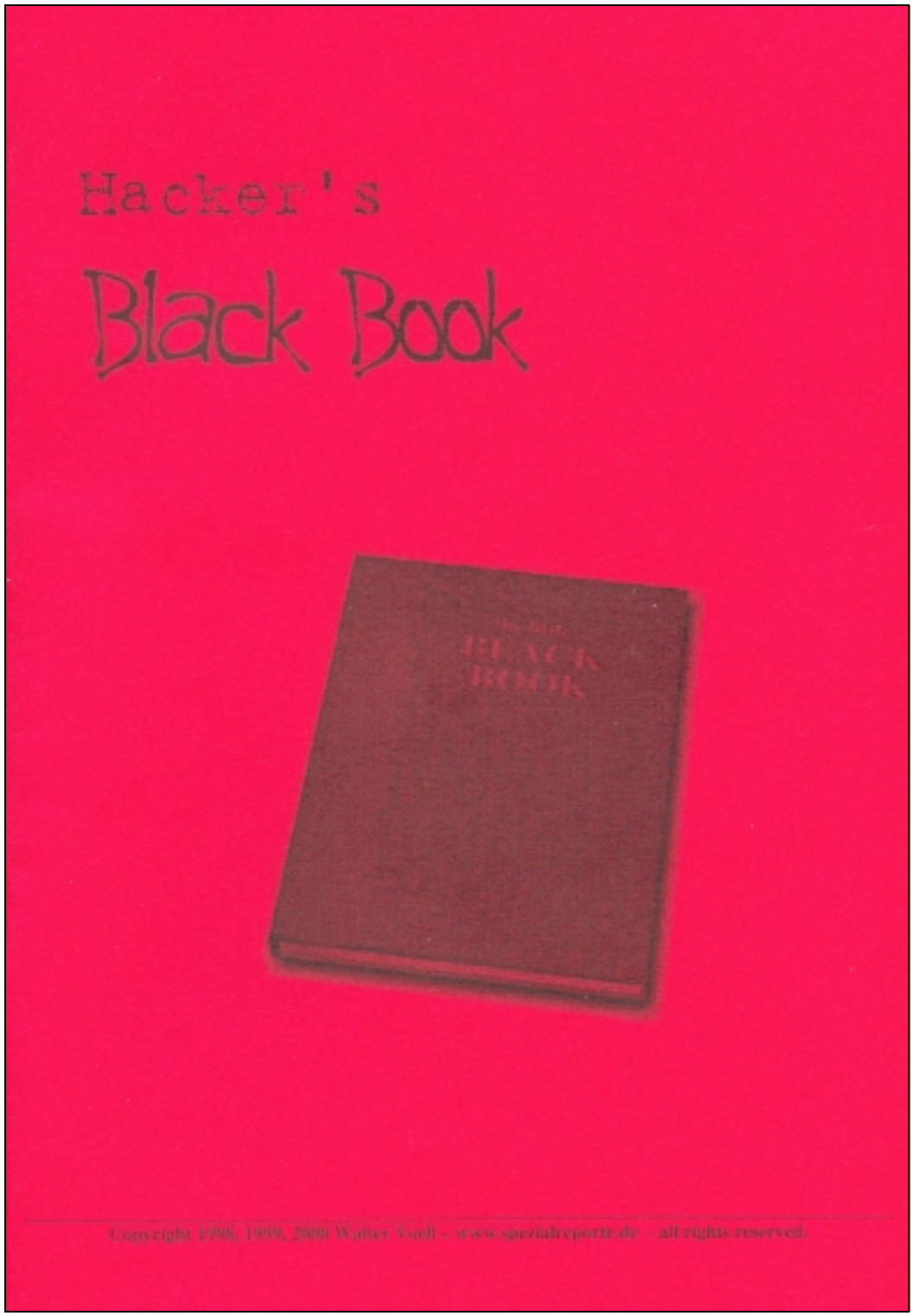
Hacker's Blackbook



Inhalt

Hacker's Blackbook

Dieser Report ist in zweierlei Hinsicht hilfreich. Er soll Menschen, die ihr Passwort verloren haben, die Möglichkeit geben, es durch Anwendung einfacher Techniken ohne lange Wartezeiten zurückzubekommen und Besitzern von Websites mit geschütztem Inhalt ermöglichen, diese Inhalte zu schützen.

Beachten Sie, dass Sie sich strafbar machen können, wenn Sie die angegebenen Techniken anwenden!

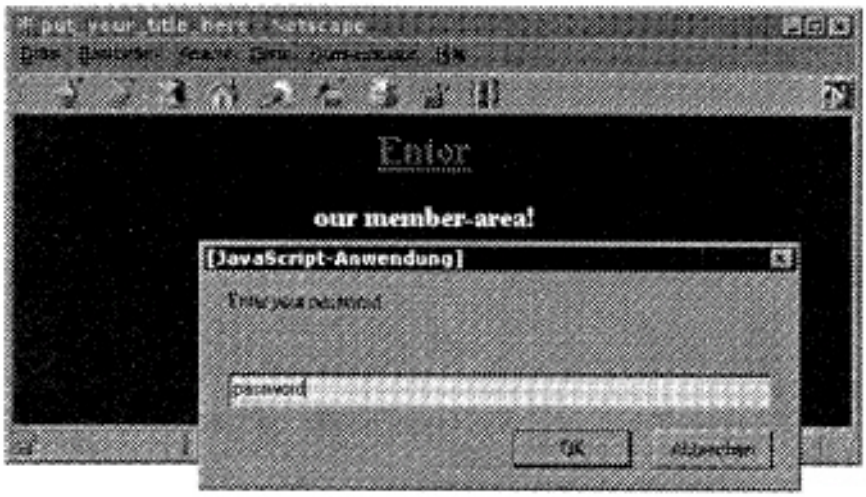
Dieses Werk wurde mit größter Sorgfalt ausgearbeitet und dient nur zu Informationszwecken. Fehler können jedoch nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autoren können für die Benutzung der angegebenen Information und deren Folgen weder Verantwortung noch Haftung übernehmen.

Webmaster, die die in diesem Report beschriebenen Techniken kennen, haben wesentlich bessere Aussichten, Ihre Website sicher gegen Eindringlinge zu schützen.

Unter der URL: http://spezialreporte.de/blackbook/ befindet sich links im Menu unter “Bereich für Leser” ein Link zum Mitgliedsbereich dieses Reports. Dort finden Sie Utilities und Tools, um die in diesem Report beschriebenen Techniken nachzuarbeiten.

JavaScript-Passwortschutzsysteme

Die einfachste Art von Passwortschutzsystemen ist der sogenannte JavaScript-Schutz. Dabei wird der Benutzer beim Betreten einer Seite oder beim Anklicken eines bestimmten Links dazu aufgefordert, ein Passwort einzugeben. Diese Art von Schutz ist sehr einfach und bietet nur ein Minimum an Schutz.



Beim Betrachten des HTML-Quellcodes der Seite findet sich dann oftmals ein JavaScript-Code ähnlich dem folgenden:

```
<head><title> Website-Titel </title>
<script>
function jprot() {
pass=prompt(“Enter your password”,”password”);
if (pass == “nasenbaer”) {
document.location.href=”http://protectedserver.com/index.html”;
{
else (
alert( “Password incorrect!” );
{
{
</script>
</head>
```

Wie man sieht, wird das eingegebene Passwort verglichen und bei Korrektheit an eine angegebene URL gesprungen. Nun sieht man, wie das Passwort zu heißen hat und kann es einfach eingeben oder direkt die Ziel-URL wählen.

Oft wird auch das Passwort benutzt, um eine Ziel-URL zu generieren. Beispielsweise könnte die geheime Ziel-URL http://members.protectedserver.com/members/hu8621s.html heißen, das Passwort “hu8621s” würde als Teil der URL kodiert. Die entsprechende Schutz-Funktion im HTML-Code der Seite sähe dann folgendermaßen aus:

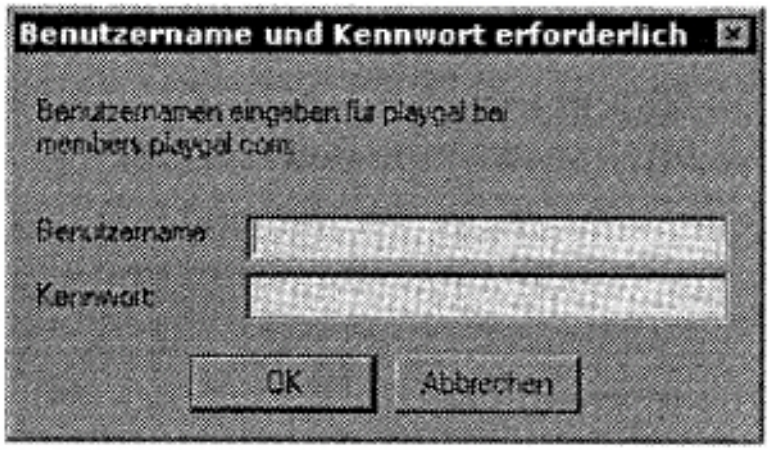
```
function jprot() {
pass=prompt("Enter your password","password");
document.location.href=”http://members.protectedserver.com/members/”+pass+”.html”
;
{
```

Hier besteht mehr Schutz als in der ersten Variante, allerdings sind die Verzeichnisse mittels des HTTP-Servers oft nicht gegen unerlaubtes Listen des Verzeichnisses geschützt. Wählt man mittels des Browsers die URL **http://members.protectedserver.com/members/** direkt in den Browser, so erhält man oftmals eine Auflistung aller HTML-Seiten in diesem Verzeichnis, also auch die Seite, die über den JavaScriptPasswortschutz angesprungen wird.

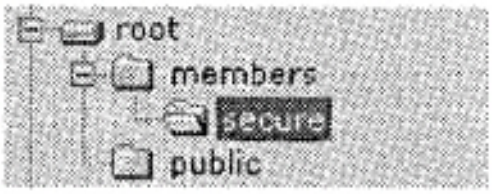
HTACCESS-Passwortschutzsysteme

Fast alle heute eingesetzten Webserver beherrschen den sogenannten HTACCESS-Passwortschutz. Zuerst wurde er vom Apache-Webserver eingesetzt, mittlerweile sind jedoch viele andere Webserver zum HTACCESS-Standard kompatibel. Daher wird er auch sehr häufig von sogenannten Paysites eingesetzt. z.B. die Websites www.playgal.com oder www.hotsex.com setzen diesen Schutzmechanismus ein.

Eine Website, die HTACCESS einsetzt, ist daran zu erkennen, dass bei Betreten des Mitgliedsbereichs ein Popup-Dialog erscheint (NICHT JavaScript-generiert), der folgendermaßen aussieht:



Um die Arbeitsweise dieses Schutzes zu verstehen, sollte man einige Grundlagen des Unix-Betriebssystems kennen. Unter Unix (bzw. Linux, BSD etc.) und auch unter Windows-Webservern wie dem Microsoft IIS sind die HTML-Dokumente wie auch bei einem normalen PC hierarchisch in Verzeichnisstrukturen angeordnet und abgelegt. Man spricht hier insbesondere von einer "Baumstruktur". Die Wurzel des Baumes (engl. "Root") ist die Domain selber ohne weitere Informationen. Zum Beispiel www.ibm.com ist die Domain und dies ist das Root der Verzeichnisstruktur.



Wenn in dem Verzeichnis "secure" nun die zu schützenden HTML-Dokumente und Grafiken liegen würden, so müsste in diesem Verzeichnis nun ein HTACCESS-File abgelegt werden. Das File muss den Namen ".htaccess" (mit Punkt davor) tragen. Das HTACCESS-File legt fest, in welcher Datei die Passwörter liegen und auf welche Art das Verzeichnis zu schützen ist. Das HTACCESS-File sieht folgendermaßen aus:

```
AuthUserFile /usr/home/myhomedir/passes
AuthName MyProtectedSite
AuthType Basic
<Limit GET POST PUT>
require valid-user
</Limit>
```

Diese HTACCESS-Datei legt fest, dass das Passwortfile die Datei **/usr/home/myhomedir/passes** auf dem Server ist. Sinnvoller Weise sollte die Passwort-Datei nicht im Bereich der HTML-Dokumente liegen, also nicht via WWW zugebar sein. Die Option "AuthName" gibt an, welche Bezeichnung im PopUp-Dialog erscheinen soll (im Dialog oben beispielsweise "playgal").

Das interessante am HTACCESS-Schutz ist, dass durch das HTACCESS-File auch alle Unterverzeichnisse unterhalb des Verzeichnisses, in dem sich die HTACCESS-Datei befindet, mitgeschützt sind. Und dies bis zu einer beliebigen Tiefe. In unserem Beispiel könnte man also unterhalb des Verzeichnisses "secure" beliebig viele weitere Verzeichnisse anlegen. Diese wären alle geschützt.

Wie sieht nun die Passwort-Datei selber aus? Im Folgenden eine beispielhafte Passwort-Datei:

```
robert:$1$4A$JRL0VdCRzYtbpekrLBYzl/
manfred:$1$30$ddEyRldHykHUo654KE01i/
thomas:$1$sa$09grZEC5VRIWw.QkLA/Ge/
```

Für jedes Mitglied enthält die Passwortdatei eine Zeile, die aus zwei Teilen besteht, die durch einen Doppelpunkt getrennt sind. Der erste Teil ist der Login-Name, der zweite Teil enthält das Passwort in verschlüsselter Form. Diese Verschlüsselung ist sehr sicher. Sie ist maschinenspezifisch. Das heißt, dass selbst wenn man diese Passwortdatei in die Finger bekommen würde, könnte man aus den verschlüsselten Passwörtern nicht die wirklichen Passwörter zurückberechnen. Bei der Passworteingabe wird das Passwort durch die Unix-Systemfunktion "cryptQ" kodiert und mit dem in der Passwortdatei abgelegten verschlüsselten Passwort verglichen. Ist es gleich, so ist der Login OK.

Wie man also erkennen kann, ist es sehr schwierig, in Websites, die mittels HTACCESS geschützt sind, zu gelangen. Allerdings sind manche Webmaster einfach zu dumm, den HTACCESS Schutz richtig einzusetzen, und bieten so dem Angreifer einige Möglichkeiten.

Schwache Passwörter

Ein schwaches Passwort ist ein Passwort, dass leicht erraten werden kann. Hier einige der am häufigsten eingesetzten Username/Password Kombinationen:

```
asdf/asdf
123456/123456
fuck/me
qwertz/qwertz
qwerty/qwerty
qlw2e3
abc123
```

Besonders bei großen Pay-Websites, die einige tausend Mitglieder haben, ist es sehr wahrscheinlich, dass solche "schwachen" Passwörter dabei sind. Außerdem muss man sich vorstellen, dass einige Mitglieder in vielen verschiedenen Websites Mitglied sind und sich nicht alle möglichen Passwörter merken wollen.

Daher wird auch oft der Name der jeweiligen Website von den Mitgliedern als Passwort gewählt.

Beispiel:
```
www.hotsex.com: username: hot, password: sex
www.hotbabes.com: username: hot, password: babes
```

Oder die Mitglieder benutzen einfach nur ihren Namen. Dabei sind natürlich die am häufigsten vorkommenden Namen besonders interessant:

Im Amerikanischen zum Beispiel
```
john/smith
john/john
miller/miller
rick/rick
frank/frank
```

und weitere mehr. Im Deutschen sind natürlich andere Namen interessanter.

Der einfach zu merkende Login bestehend aus "username/password", so wie er auch im Passwort-Dialog gefragt wird, kommt auch häufig vor.

Das schwächste von allen Passwörtern ist allerdings das sogenannte "ENTER" -Passwort. Dabei muss beim Erscheinen des Passwort-Dialogs einfach bestätigt werden, ohne überhaupt etwas einzugeben. Hat nämlich der Webmaster beim Erzeugen neuer Mitglieds-Daten einfach ohne Eingabe irgendwelcher Daten aus Versehen einmal unbemerkt sein Tool gestartet, so befindet sich im Passwort-File ein eben solcher "leerer" Eintrag.

An den engagierten Webmaster richten sich folgende Sicherheitstipps:
- Das Erzeugen "leerer" Passwörter verhindern und kontrollieren
- Die Mitglieder nicht die Passwörter selber wählen lassen, sondern eines per Zufall generieren (z.B. "kd823joq")
- Falls die Kunden ihre Username/Password-Kombination selber wählen dürfen, nicht zulassen, dass der Username gleich dem Passwort ist.

Direktes Hacken der Passwort-Datei

Normalerweise sollte es nicht möglich sein, an das Passwort-File zu gelangen. In einigen Fällen ist es jedoch möglich, daran zu kommen, und zwar in folgenden Fällen:

- Die Passwort-Datei liegt im public html-Bereich des Webservers, also in den Verzeichnissen, in denen auch die via WWW zugänglichen HTML-Dokumente liegen
- Auf dem Webserver haben viele User einen eigenen virtuellen Webserver

Der zweite Fall tritt dann auf, wenn der Website-Betreiber seinen Webserver bei einem großen Webspaceprovider mietet, der auf einem Rechner viele weitere Webserver betreibt (z.B. www.webspaceservice.de, www.webspace-discount.de, www.simplenet.com, etc.)
Dann ist es möglich, an die Passwortdatei zu kommen, falls man auf dem gleichen Rechner einen Account hat und die Passwortdatei öffentlich lesbar ist. Dann kann man mittels FTP oder TELNET in das Verzeichnis wechseln, in dem derjenige seine Passwortdatei aufbewahrt und diese lesen. Mittels eines Brute-Force-Passwort-Crackers wie "Crack V5.0" lassen sich dann die Passwörter zurückberechnen. Das Programm braucht allerdings oft viele Stunden dazu und es führt nicht immer zum Erfolg.
Für einen absolut sicheren Schutz sollte also der Webmaster seine Paysite nicht auf einem Webserver betreiben, den er sich mit anderen Websites teilen muss.

Die Admin-Tools

Viele Webmaster der Paysites haben einen sogenannten "Admin-Bereich", der nur für sie selber gedacht ist. Dort erzeugen Sie neue Passwörter oder löschen alte Passwörter etc.
Oft liegen diese Admin-Bereiche jedoch nicht in einem passwortgeschützten Bereich. Die Webmaster denken nämlich, es würde ja keiner die URL ihres Admin-Tools kennen. Aber die URL ist manchmal einfach zu erraten. Oft heißt die URL

```
www.thepaysite.com/admin.htm
www.thepaysite.com/admin.html oder
www.thepaysite.com/admin/
```

Man sollte auch weitere Namensmöglichkeiten austesten. Denn gelingt es, an die Admin-Seite zu kommen, so ist man natürlich am allerbesten bedient: Man kann selber so viele neue Passwörter hinzufügen, wie man möchte!

Phreaken

Unter "Phreaken" versteht man den Einsatz von falschen Informationen, um sich bei einer Paysite als neues Mitglied zu registrieren. Das ist natürlich verboten und diese Hinweise hier sollen in erster Linie den Webmastern dienen, damit sie sich vor solchem Missbrauch schützen können.

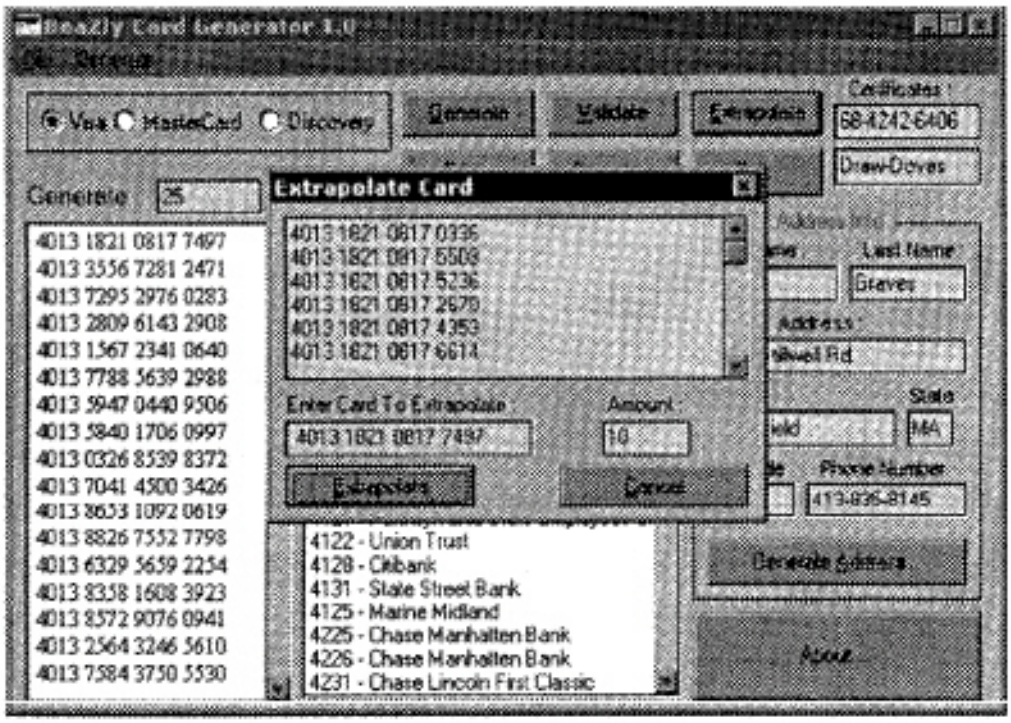
Wir wollen hier den am weitesten verbreiteten Fall beschreiben, bei dem die Mitgliedschaft online via Kreditkarte bezahlt wird und danach sofortiger Zugang erteilt wird.

Phreaker benutzen dazu einen anonymen Internetzugang. Dazu wird oft der Test-Zugang von AOL missbraucht. Test-Mitgliedschaften finden sich nahezu in jeder Computerzeitung. Aber auch okay.net bietet sofortigen Zugang nach Angabe aller Daten. Dabei meldet man sich mit Phantasienamen und irgendeiner Kontoverbindung an, die man aus irgendeiner Rechnung oder sonst wo her kennt. Schon ist man einen Monat lang anonym via AOL oder okay.net im Internet unterwegs.

Des weiteren benötigt man eine "gültige" Kreditkarten-Nummer (vorzugsweise VISA oder Mastercard - in Deutschland Eurocard). An diese zu kommen, ist schon etwas schwieriger. Eine gängige Methode ist es, einen sogenannten "Credit-Card-Generator" wie z.B. "Credit Wizard", "Cardpro" oder "Creditmaster" einzusetzen. Ein Suchen mittels "metacrawler.com" und den Begriffen "Credit Card Generator" o.ä. bringt oft schon die gewünschten Programme.

Dazu sollte man wissen, dass die Online-Transaktionszentren nicht genau überprüfen können, ob eine Kreditkartennummer wirklich existiert und wem sie gehört. Es gibt lediglich bestimmte Algorithmen, um die Nummer und die Gültigkeitsdaten einer Kreditkarte auf eine gültige Struktur hin zu überprüfen. Daher kann man bei der Anmeldung beliebige Namen und Adressen angeben und eine der generierten Nummern. Allerdings liefern die Generatoren nicht das dazugehörige Gültigkeitsdatum.

Jedoch gibt es einen einfachen aber recht wirksamen Trick, um Kartennummern mit richtigem Gültigkeitsdatum zu erhalten: Die meisten der obengenannten Programme bieten die Möglichkeit, aus einer real existierenden Kreditkarten-Nummer neue Nummern zu generieren. Dieses Verfahren wird „Extrapolation" genannt. Die generierten Nummern unterscheiden sich meist nur in den letzten Stellen, und da die Kartennummern bei den Kreditkarten-Herausgebern in der Regel in aufsteigender Reihenfolge vergeben werden, haben die so generierten Kartennummern meistens das Gültigkeitsdatum der Karte, von der aus extrapoliert wurde. Folgender Bildschirmauszug zeigt den Extrapolationsvorgang:



Dabei kann man seine eigene, real existierende Kreditkarte nehmen und aus ihrer Nummer neue Kartennummern berechnen. Das Gültigkeitsdatum ist dann mit größter Wahrscheinlichkeit bei den extrapolierten Nummern identisch mit dem Gültigkeitsdatum der eigenen, realen Kreditkarte.

Dabei braucht der Benutzer dieser Techniken keine Angst zu haben, dass man ihn zurückverfolgen kann. Der Zugang mittels anonymer AOL-Testzugänge bietet maximalen Schutz. Steht kein solcher Zugang zur Verfügung, sollte ein "Anonymizer" benutzt werden. Einen solchen findet man beispielsweise unter www.anonymizer.com. Surft man über den Anonymizer, ist die IP-Adresse nicht zurückverfolgbar. Eine etwas schwächere Variante, seine IP-Adresse zu verstecken ist die, einen Proxy-Server zu benutzen. Die meisten Internet-Zugangsprovider bieten die Möglichkeit an, über einen Proxy zu surfen.

Aber Achtung: Benutzt man seinen eigenen Internet-Zugang, also keinen anonymen AOL-Zugang oder Anonymizer oder Proxy, so kann der Betreiber der Website, bei dem man sich mittels der falschen Kreditkartendaten anmeldet, mittels der IP-Adresse, die der Server protokolliert, herausfinden, wer ihn betrogen hat bzw. es versucht hat. Dazu braucht er lediglich Ihren Zugangsprovider zu kontaktieren und ihm die IP-Adresse mitzuteilen. Die Provider führen i.d.R. über die letzten 80 Tage ein Protokoll, wann wer mit welcher IP-Adresse online war.

Login-Name Checker

Manche Pay-Sites geben möglichen neuen Mitgliedern während der Anmeldungsprozedur bereits vor der eigentlichen Zahlung die Möglichkeit, einen Mitgliedsnamen zu wählen. Ist der gewünschte Name bereits vergeben, wird dies mitgeteilt und man soll einen anderen Namen wählen. Gibt man beispielsweise "John" als Mitgliedsnamen ein, so sagt der Server meistens, dass der Name bereits vergeben ist. Das ist natürlich eine prima Voraussetzung für die oben genannten Tricks zum Erraten von Passwörtern. Denn nun weiß man, dass es zumindest den Namen "John" schon gibt, somit muss nur noch das entsprechende Passwort erraten werden. Das ist eine wesentliche bessere Ausgangslage, als wenn man Passwörter zu Usernamen erraten muss, von denen man gar nicht weiß, ob sie überhaupt existieren!

Als Webmaster einer Paysite sollte man also darauf achten, dass das Neumitglied erst nach verifizierter Zahlung seinen Usernamen wählen kann!

Login-Generator nicht sicher

Oftmals ist es so, dass das Neumitglied zur Zahlung von der Paysite zu einem Kreditkarten-Service geschickt wird (z.B. www.ibill.com). Nach Verifizierung der Zahlung kommt der Neukunde dann wieder zu den Seiten der Paysite und wird dort entsprechend weiterbehandelt. In der Regel wird er nach erfolgreicher Zahlung zu einem Formular geschickt, mit dem die Login-Daten erzeugt werden. Das Neumitglied kann einen Usernamen und ein Passwort wählen und erhält nach Wahl derer sofortigen Zugang. Das Formular fügt die Daten automatisch in die Passwort-Datei ein. Hier liegt jedoch ein oft gemachter Fehler: Geht man nach Erzeugung eines Username/Passwort-Paares einfach mittels des „Back"-Buttons des Browsers zurück zum Formular, so kann man auf einfache und legale Weise ein weiteres Username/Passwort-Paar erzeugen und das immer wieder.

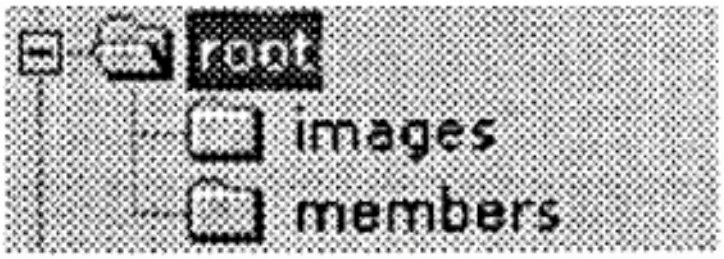
Als Webmaster sollte man folgende zwei Schutzmechanismen einsetzen:

- Das Kreditkarten-Unternehmen sollte nach erfolgreicher Prüfung einen einmalig PIN-Code übermitteln, den man dann aus der Liste der noch gültigen PIN-Codes streicht und so das Formular zur Username/Passwort-Erzeugung bei jeder Zahlung nur genau EINMAL eingesetzt werden kann. Dieses Verfahren wird von den meisten Kreditkarten-Unternehmen auch als "One-Time PIN-Hardcoding" bezeichnet.
- Das Script, dass die Usernamen/Passwörter erzeugt, sollte auch mittels der HTTP REFERRER-Servervariablen überprüfen, ob der User auch vom Kreditkartenunternehmen kommt. Sonst kann ein gewiefter Hacker ein Script schreiben, das von seinem Rechner aus einfach solange verschiedene PIN-Nummern ausprobiert, bis es eine noch gültige findet. Sind die PINs z.B. siebenstellig, so dauert es im statistischen Mittel nur 5000 Sekunden, bis man eine gültige PIN findet, wenn das Script jede Sekunde eine PIN testet. Bei einer schnellen Internetverbindung sind jedoch auch mehrere Tests pro Sekunde möglich!

Bilder nicht in geschützten Verzeichnissen

Dieser Fehler ist einer der häufigsten, da er leicht übersehen wird: Wie bereits erwähnt, sind mittels des HTACCESS-Schutzes immer das jeweilige Verzeichnis und alle Unterverzeichnisse geschützt. Befinden sich die Bilder der Mitgliederseiten jedoch in einem Verzeichnis, das nicht in dieser geschützten "Baumstruktur" enthalten ist, so kann dieses Verzeichnis und die Bilder darin ohne Eingabe von Username/Passwort angesehen werden. Besonders einfach ist es dann, wenn das Bilder-Verzeichnis auch nicht gegen Auflisten geschützt ist. Dann genügt das Eingeben des Pfades, um alle Bilder aufzulisten.
Diese Bilderverzeichnisse haben oft den Namen "images", "gfx", "pics", "pix", "pictures", "pic" oder "graphics". Ein einfaches Durchprobieren mit etwas Phantasie führt hier bereits oft zum Erfolg.

Beispiel:



Das .htaccess-File liegt im geschützten Verzeichnis "members". Dort liegen auch die HTML-Dokumente für die Mitglieder. Die dazugehörigen Bilder liegen jedoch in diesem Beispiel im Verzeichnis "images", welches nicht in der members-Hierarchie ist und somit nicht passwortgeschützt ist. Handelt es sich beispielsweise um www.pornsite.com als root dieser Paysite, so kann im Browser einfach die URL www.pornsite.com/images eingegeben werden, und man erhält eine Liste der gesammelten Bilder (vorausgesetzt, das Directory-Browsing ist nicht serverseitig ausgeschaltet).

Packet Sniffing

Diese Möglichkeit ist etwas komplizierter als die anderen beschriebenen, denn es müssen einige Voraussetzungen getroffen werden: Sie müssen in einem LAN (Ethernet-Netwerk) an einem Rechner sitzen und Root-Access haben. Dann kann man einen sogenannten "Packet-Sniffer" wie beispielsweise "SNOOP" einsetzen. Packet-Sniffer findet man meist als C-Sourcecode im Internet. Diese kurzen Sourcecodes muss man dann nur noch mittels gcc auf der UNIX-Shell compilieren und schon ist es möglich, die Pakete, die zu und von anderen Rechner im LAN gesendet werden, abzuhören. Denn Ethernet-Netzwerke setzen die sogenannte "Broadcast"-Technologie ein. Ein Paket, dass für einen Rechner in einem LAN bestimmt ist, wird im Prinzip an alle Rechner im LAN ausgesandt. Packet-Sniffing ist also wiederum besonders in den Fällen gefährlich, bei denen man bei einem Webspace-Provider seinen Webserver mietet und sich dort naturgemäß mit vielen anderen Kunden in einem LAN befindet. Ein Beispiel ist www.pair.com, einer der größten kommerziellen Webspace-Provider in den USA. Dort befinden sich über 70 Webserver in einem LAN, auf dem z. Zt. über 30.000 Kunden einen virtuellen Webserver betreiben!

Als Schutz gegen Packet-Sniffing bietet sich der Einsatz eines "Segmented Networks" an. Bei einem solchen Netzwerk wird nicht die Broadcast-Technologie benutzt, sondern die Pakete werden direkt mittels Routing-Tabellen zu dem Ziel-Rechner geroutet. Eine besonders für Web-Server geeignete Lösung ist der Einsatz von SSL (Secure Sockets Layer). Dies Protokoll verschlüsselt alle Pakete, die somit zwar noch abgefangen werden können, aber nicht mehr gelesen werden können. SSL wird von den meisten Webhosting-Unternehmen gegen geringen Aufpreis angeboten. SSL-Verschlüsselte Webinhalte sind am Protokoll-Prefix "https://" zu erkennen. Zum Betrieb einer SSL-geschützten Website muss man eine SSL-ID haben, die es beispielsweise bei www.verisign.com gibt. Ein kleiner Nachteil ist jedoch, dass HTTPS-Verbindungen etwas langsamer sind als gewöhnliche HTTP-Verbindungen, da ein relativ hoher Verschlüsselungs-Overhead existiert.

Trojanische Pferde

Back Orifice und NetBus

Back Orifice
Die amerikanische Hackergruppe Cult Of The Dead Cow (http://www.cultdead-cow.com) veröffentlichte ein Programm mit dem Namen "Back Orifice", das sie als "Fernwartungswerkzeug für Netzwerke" bezeichnet. Dass die Intention eine andere ist, ergibt sich schon aus dem Namen: Back Orifice (hintere Öffnung) übersetzt man hier am besten mit "Hintertür", denn das Programm macht es fast zum Kinderspiel, Schindluder mit Windows-PCs zu treiben. Witzig die Anspielung auf Micro$oft's "Back Office"-System.

Das nur 124 KByte große "Server-Modul" lässt sich nämlich an ein beliebiges Windows-EXE-Programm koppeln, um es nichtsahnenden Anwendern unterzuschieben. Wird die Datei unter Windows 95 oder 98 ausgeführt, klinkt sich der Server quasi unsichtbar im System ein. Von diesem Moment an wartet das trojanische Pferd nur noch darauf, über das UDP-Protokoll geweckt zu werden.

Mit dem Client lässt sich bequem auf den befallen Rechner zugreifen. Unter anderemkann man das Dateisystem manipulieren (Dateien runterladen, hochspielen etc.),Tasks beenden, uvm. Die Funktionsweise des Back Orifice ist schon aus anderen Hacker-Tools bekannt; neu ist in erster Linie der Bedienungskomfort der grafischen "Wartungskomponente" - wenige Eingaben und Mausklicks genügen, um Prozesse zu beenden, Tastatureingaben zu protokollieren, die Windows-Registry zu manipulieren oder IP-Adressen umzuleiten.

Einen interessanten Praxisbericht findet man unter der deutschen Adresse
http://www.puk.de/BackOrifice/default.html oder
http://www.bubis.com/glaser/backorifice.htm

Um Ihr System auf ein vorhandenes Back-Orifice zu untersuchen, gibt es Programme wie BoDetect (http://www.spiritone.com/~cbenson/current_projects/backorifice/backorifice.htm) oder das Programm BORED (http://www.st-andrews.ac.uk/~sjs/bored/bored.html).

Es ist aber auch manuell sehr einfach, Back Orifice zu entfernen: Öffnen Sie die Registry (regedit.exe ausführen) und schauen unter dem Schlüssel "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices"

nach einem Eintrag mit dem Namen "<blank>.exe" (DefaultFilename) bzw. mit einem Eintrag der Länge 124,928 (+/- 30 Bytes). Löschen Sie diesen Eintrag; er bewirkt, dass der "Back Orifice"-Server bei jedem Windows-Start automatisch aktiviert wird.

Das Programm selbst liegt im allgemeinen im Verzeichnis "\Windows\System" und ist daran erkennbar, dass es kein Programm Icon hat und eine Größe von 122 Kbyte (oder geringfügig mehr) besitzt. Sollten Sie die Datei aus irgendwelchen Gründen nicht finden, kann es Ihnen helfen, dass verschiedene Informationen als ASCII-String im Programm-Code zu finden sind; so ist mit großer Wahrscheinlichkeit die Zeichenkette "bofilemappingcon" enthalten, die Sie über Suche im Explorer finden werden.

Zusätzlich zur "Back Orifice-Programm-Datei" wird im selben Verzeichnis noch die "WINDLL.DLL" zum Mitloggen von Tastatureingaben installiert, die Sie auch sinnvoller Weise löschen, die aber alleine keinen Schaden anrichten kann.

Das Problem bei Back-Orifice ist, dass es schwierig ist, die IP-Adresse des Hosts zu erkunden, da diese sich ja bei jedem Einwählen des befallenen Rechners ändert. Dieses Problem gelöst und eine noch mächtigere Lösung geschaffen hat Carl-Fredrik Neikter mit seinem Programm "NetBus", welches recht ähnlich ist. Es bietet noch weitgehendere Funktionen und ist einfacher zu installieren.

NetBus
Nachdem Sie sich die entsprechende Datei heruntergeladen haben, sollten Sie diese entpacken. Nun erhalten Sie drei Dateien: NETBUS.EXE, NETBUS.RTF und PATCH.EXE

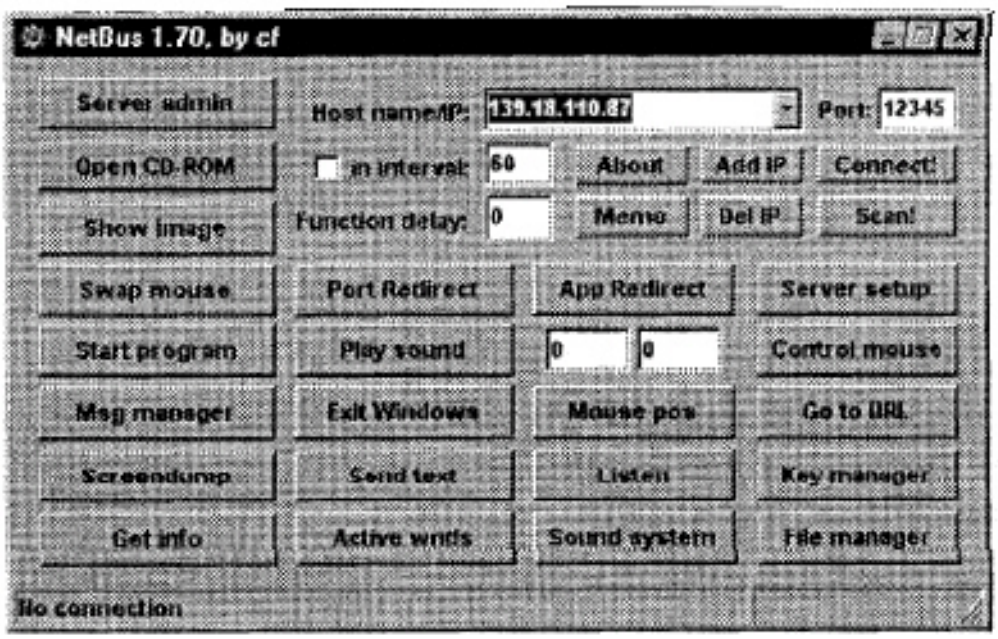
Bei PATCH.EXE handelt es sich um das gefährliche Infizierungsprogramm, das eigentliche Trojanische Pferd. Starten Sie diese Datei also nicht! Die Datei NET-BUS. RTF enthält eine kurze englische Anleitung des

Authors. Die Datei NET-BUS. EXE ist der "Client" mit dem Sie auf infizierte Server zugreifen können. Diese können Sie ohne Sorgen starten. Starten Sie zum Testen den Server auf Ihrem eigenen Rechner, indem Sie eine DOS-Eingabeaufforderung öffnen und im Verzeichnis von NetBus den Server mit dem Parameter "/noadd" starten, also

PATCH.EXE /noadd [RETURN]

Nun läuft der Server. Jetzt können Sie den Client starten (NETBUS.EXE doppelklicken) und auf Ihren eigenen Rechner zugreifen. Wählen Sie dazu als Adresse "localhost" oder "127.0.0.1". Wenn Sie den Server beenden wollen, wählen Sie im Client "Server Admin" und dann "Close Server".

Die Oberfläche des NetBus-Clients, mit dem Sie den NetBus-Server steuern.



Außerdem kann das Infizierungsprogramm so geändert werden, dass es die IP-Adresse automatisch an eine von Ihnen gewählte Email Adresse schickt, sobald jemand mit einem von NetBus infizierten Rechner in das Internet geht. Dies ist der gewaltige Vorteil gegenüber Back Orifice. Dazu wählt man im NetBus-Client den Button "Server Setup" und gibt die entsprechenden Informationen ein. Schwierig ist es lediglich, einen freien Mail-Server zu finden, der Mails von jeder IP-Adresse akzeptiert. Dann wählt man "Patch Srvr" und wählt die zu patchende Infizierungsdatei (standardmäßig "patch.exe").

Wer versucht, einen anderen Rechner zu infizieren, kann die Datei PATCH.EXE nun einfach per Email an einen anderen Internetnutzer schicken und die Datei als "Windows-Update" oder als irgendeine tolle lustige Animation bezeichnen. Die Datei kann dazu beliebig umbenannt werden (z.B. Win98update.exe oder siedler2_patch.exe etc.). Wird die Datei nun gestartet, passiert optisch gar nichts. Jedoch hat sich der NetBus-Server bereits auf dem Rechner versteckt installiert und wird von nun an jedes mal automatisch gestartet, wenn der Rechner gebootet wird.

Hat man obige Veränderungen am Infizierungsprogramm vorgenommen, bekommt man nun immer automatisch eine Email mit der IP-Adresse des infizierten Rechners, sobald dieser online ins Internet geht. Diese IP-Adresse können Sie nun im NetBus-Client eingeben und den Rechner manipulieren.

Hacker benutzen sicherheitshalber anonyme Email-Adressen, die es beispielsweise bei hotmail.com oder mail.com gibt.

Um Ihr System zu schützen, empfiehlt sich Norton Antivirus http://www.syman-tec.de/region/de/avcenter/ welches neben NetBus auch Back Orifice erkennt. Sie können auch wiederum manuell arbeiten. Der automatische NetBus-Start ist in der Registry unter

"\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"

eingetragen und sollte entfernt werden. Allerdings kann der Dateiname variieren (patch.exe, sysedit.exe oder explore.exe sind einige bekannte Namen)

Weiterführende Info finden Sie unter
http://www.bubis.com/glaser/netbus.htm

Tipp des Autors

Sollten Sie beabsichtigen, einen passwortgeschützten Internetservice zu betreiben, so kommen Sie nie auf die Idee, einen Microsoft NT-Webserver einzusetzen! Windows NT hat ein Sicherheitssystem, das mehr Löcher hat, als ein Schweizer Käse. Statt dessen sollten Sie ein Unix-System wählen. Leider bieten deutsche Webspace-Provider größtenteils NT-Lösungen an. Hier heißt es also, Ausschau halten und ggf. konkret bei einem Webspace-Provider nach einem Unix-Server fragen! Ein wesentlicher Vorteil eines Unix-Servers ist neben der Sicherheit der Vorteil, dass man sich dort auch per TELNET einloggen kann und so wesentlich mehr Kontrolle über den Server hat. Bei NTServern ist dies nicht möglich! Empfehlenswert und preiswert sind besonders unter BSDI oder Linux laufende Webserver. Wie jeder weiß, ist Linux sogar kostenlos und Apache, einer der besten Webserver, ist ebenfalls kostenlos erhältlich. Außerdem sollte man auch die Performance-Vorteile eines Unix-Systems nicht unterschätzen. Besonders im Bereich Trafficstarker Webangebote wird fast ausschließlich Unix eingesetzt. Sollten Sie also beispielsweise ein Erwachsenen-Angebot mit vielen tausend Bildern etc. planen, so lege ich Ihnen den Einsatz eines Unix-Servers wärmstens ans Herz. Eine interessante Website zum Thema „Unix vs. NT" findet sich unter http://www.lot-germany.com/magazin/unixnt.htm !

Rechtliche Aspekte

Was sagt das Gesetz zum "Hacken"

§ 202a Ausspähen von Daten:
1. Wer unbefugt Daten, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
2. Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 263 Computerbetrug:
1. Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines Anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch Verwendung unrichtiger Einwirkungen auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 303a Datenveränderung:
1. Wer sich rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
2. Der Versuch ist strafbar.

§ 303b Computersabotage:
1. Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er... a) eine Tat nach §303a Abs. 1 begeht oder b) eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit einer Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
2. Der Versuch ist strafbar.

Das Berufsbild des Hackers

1. Eine Person, die gerne die Details von programmierbaren Systemen erforscht und versucht, deren Möglichkeiten auszudehnen.
2. Jemand, der enthusiastisch (sogar obzessiv) programmiert oder lieber programmiert, als nur über Programme zu theoretisieren.
3. Eine Person, die hack values zu schätzen weiß.
4. Eine Person, die gut darin ist, schnell zu programmieren...
5. (missbilligend) Jemand, der sich hemmungslos überall einmischt und versucht Informationen aufzudecken, indem er herumschnüffelt. Daher Password Hacker, Networt Hacker.

Der korrekte Begriff ist Cracker (Aufbrecher).

Der Begriff Hacker beinhaltet oft auch die Mitgliedschaft in der weltweiten Netz-Gemeinschaft (z.B. Internet). Er impliziert, dass die beschriebene Person sich an die Hackerethik hält (hacker ethik). Es ist besser, von anderen als Hacker bezeichnet zu werden, als sich selbst so zu bezeichnen. Hacker betrachten sich selbst als eine Art Elite (eine Leistungsgesellschaft, die sich durch ihre Fähigkeiten definiert), allerdings eine, in der neue Mitglieder sehr willkommen sind. Daher verleiht es einem Menschen eine gewisse Befriedigung, sich als Hacker bezeichnen zu können (wenn man sich allerdings als Hacker ausgibt und keiner ist, wird man schnell als Schwindler - bogus - abgestempelt).

The New Hacker's Dictionary

Der Begriff hacken kann die freie intellektuelle Erforschung des höchsten und tiefsten Potentials von Computersystemen bezeichnen . Hacken kann die Entschlossenheit beschreiben, den Zugang zu Computern und damit Information so frei und offen wie möglich zu halten. Hacken kann die von ganzem Herzen empfundene Überzeugung einschließen, dass in Computern Schönheit existiert, dass sie Ästhetik eines perfekten Programms die Gedanken und den Geist befreien kann ...

...davon ausgehend, dass Elektronik und Telekommunikation noch immer zu großen Teil unerforschte Gebiete sind, kann überhaupt nicht vorhergesagt werden, was Hacker alles aufdecken können.

Für einige ist diese Freiheit wie das Atmen von Sauerstoff, die erfindungsreiche Spontanität, die das Leben lebenswert macht und die Türen zu wunderbaren Möglichkeiten und individueller Macht öffnet. Aber für viele - und es werden immer mehr - ist der Hacker eine ominöse Figur, ein besserwisserischer Soziopaht, der bereit ist, aus seiner individuellen Wildnis auszubrechen und in anderer Menschen Leben einzudringen, nur um seines eigenen, anarchischen Wohlergehens willen.

Jede Form der Macht ohne Verantwortung, ohne direkte und förmliche Überprüfungen und ohne Ausgleich macht den Menschen Angst - und das mit Recht.

The Hacker Crackdown

Hacker-Ethik
Der Chaos-Computer-Club definierte die Hackerethik 1997 in den folgenden Maßregelungen. Leider werden diese Grundregeln der Hacker-Ethik oftmals benützt, um Straftaten zu legitimieren. Einige der Regeln sollten natürlich nicht nur für Hacker gelten und sind recht allgemeingültig.

- Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Misstraue Autoritäten - fördere Dezentralisierung.
- Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können Dein Leben zum Besseren verändern.
- Mülle nicht in den Daten anderer Leute.
- Öffentliche Daten nützen, private Daten schützen.

Anonymes Arbeiten

Professionelle Hacker wenden folgende Tricks an, um möglichst lange unentdeckt zu bleiben. Viele dieser Ratschläge sind für jedermann sinnvoll, damit es Firmen im WWW nicht gelingt, Benutzerprofile anzuwenden. Einige dieser Maßnahmen sind also nicht nur für Kriminelle sinnvoll!

- Emails verschlüsseln (mit PGP, gibt es kostenlos). Benutze anonyme im Ausland liegende Email-Server (benutze keinen gehackten Account, besser www.hot-mail.com, www.yahoo.com, ...). Du solltest deinen Spitznamen (Nick) unregelmäßig ändern und natürlich auch regelmäßig ein neues PGP secretkey-publickey Paar erstellen (auch die Passphrase ändern!).
- Wenn Du viel IRCen möchtest, dann ändere immer Deinen Nick und wechselt 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)
- Versuche, Deinen Hackerstolz zu unterdrücken und hänge Deine Aktivitäten nicht an die große Glocke. Auch dann nicht, wenn Dir ein großer Coup gelungen ist und Du Dir davon durch Bekanntmachung große Reputation erhoffst. Merke Dir, dass es Dich nicht weiterbringt, wenn Dich Anfänger bewundern. Du brauchst nur Reputation bei den wirklichen Insidern und die Erfahren durch die Buschtrommeln des Internets schon schnell genug davon, wenn Du mal ein größeres Projekt gemacht hast. Schwätz nicht im IRC herum, da hängen oft Ermittler und private Dissidenten herum, bleibe im IRC immer so abstrakt wie möglich.
- Benutze zum IRCen einen unabhängigen ISP-Zugang, den Du für keine anderen Aktivitäten benutzt, so können IP-Adressen nicht zugeordnet werden und kein er weiß, dass der, der da gerade chattet, derjenige ist, der eben den Großrechner gehackt hat!
- Verwende nur Schlüssel mit mindestens 1024 Bit. Benutze nur PGP-Software aus authentischer Quelle, nicht von unbekannten Homepages runterladen!
- Benutze Rerouter, die eine TCP Verbindung weiterleiten, damit wirst Du anonym und der Rerouter schützt Dich ebenso vor Angriffen anderer Hacker/ Ermittler (siehe "Meine Arbeitsumgebung" weiter unten)

Meine Arbeitsumgebung

Ich benutze große Provider oder eine große Uni als Internetzugang. Über den Internetzugang via PPP ist es möglich, mehrere Clients gleichzeitig zu benutzen (FTP, Telnet, WWW etc.). So kann ich im Hintergrund einen Brute-Force Hacker via Telnet auf einen zu hackenden Account loslassen oder einen umfangreichen Portscan durchführen und währenddessen im WWW rumsurfen.

Ein kleinerer Linux-Rechner dient mir als Firewall und Router, ich baue die PPP-Verbindung zu meinem Einwahlpunkt auf und überwache alle eingehenden Pakete an der Firewall.
Per SSH wähle ich mich im Einwahlrechner des ISP (sofern es sich um einen Unix-Rechner handelt) ein und checke kontinuierlich alle eingeloggten Nutzer und Connections (Verbindungen).

Wenn plötzlich ein User "Admin" im Einwahlrechner aktiv ist, sollte man so langsam anfangen, seine Sachen zu packen. In der Nacht ist das natürlich nicht sehr wahrscheinlich und zum Schluss der Session kann ich mit Logfile-Overflooding alle meine Spuren leicht verwischen! Wenn Du mitten in einem wichtigen Projekt bist, wenn der Admin kommt, musst Du (wenn Du es dringen zuende bringen möchtest) den Admin oder Einwahlrechner mit DoS (Denial-Of-Service)-Attacken außer Gefecht setzen und Dir somit etwas Zeit verschaffen.

Der zweite, größere Rechner ist meine Workstation, von hier aus baue ich eine SSH-Verbindung zum ersten Anti-Trace Rechner auf.

Dieser Anti-Trace Rechner wechselt regelmäßig, liegt im Ausland (Übersee). Hinter diesen Anti-Trace-Rechner schalte ich nach belieben weitere Anti-Trace Rechner als Zwischenstation ein, je nachdem wie gefährlich mir das Projekt erscheint.

Der zweite PC ist nur ein einfacher TCP-Relay, der meine TCPPakete verschleiert und die Herkunft somit schwieriger herauszufinden macht. Meinen eigentlichen Hacking-Rechner benutze ich dann schließlich für meine Projekte, um beispielsweise in sehr sichere Domains zu gelangen oder ich hacke von hier aus andere Netzwerke. Wenn Du fleißig bist, gelingt es Dir vielleicht, einen kleinen Vorrat an Hacking-Rechnern zu hacken, die Du dann im Wechsel benutzen solltest. So minimiertst Du das Risiko ein weiteres mal.

Ich habe auch immer ein paar Port-Scanner in Übersee laufen, die Tag und Nacht alle möglichen IP-Adressen und Ports abtasten und die Daten sammeln, die ich dann für meine Hack-Angriffe benutze. Die Scanner sind zusätzlich mit 3DES oder Blowfish verschlüsselt, genau wie die Daten, die sie für mich erzeugen. Wenn mal jemand meinen Scanner entdeckt, kann er doch nichts mit den Daten anfangen.

Unter Linux ist es praktisch, den Kernel zu patchen. Es gibt Patches, die Dir wesentlich mehr Info über laufende Connections und Pakete geben als es die Normalen Netzwerk-Layer tun. Damit ist es einfacher DoS Attacken, Source-Routing Angriffe, Traceroutes etc. und Deine Angreiffer zu erkennen!

Anonym Surfen

Viele Hacker surfen anonym im Internet um zum Beispiel mit gefakten Kreditkarten-Informationen Dienstleistungen oder Waren zu bestellen. Dabei ist es wichtig, dass die IP-Adresse nicht zugeordnet werden kann. Sie erreichen dies, indem Sie einen anonymen Proxy dazwischen schalten. Dieser wird benutzt wie ein normaler Proxy, den ein ISP i.d.R. anbietet. Nur liegt der benutzte Proxy des Hackers meist in fernen Ländern, und die Hacker wissen von diesen Proxies, dass die Besitzer keine Logfiles über Ihre Benutzer anlegen.

Eine sehr gute Informationsquelle bietet die Seite "Proxys-4-all" unter http://proxys4all.Cgi.net

Suchen Sie sich einen dieser öffentlichen Proxies aus und stellen Sie ihn in Ihrem Browser als Proxy ein (beispielsweise unter "Bearbeiten->Einstellung->Erweitert->Proxies" bei Netscape 4++) und schon surfen Sie genau wie ein Hacker anonym im Netz.

Aber leider sind die Proxies oftmals sehr langsam oder fallen ganz aus, weshalb man immer eine Ausweichmöglichkeit haben sollte!

Achtung beim Download!

Niemals Software oder Updates aus einer nicht vertrauenswürdigen Quelle herunterladen. Problematisch wird diese Aussage, wenn man sich bewusst macht, dass alle großen und kleinen Anbieter aus Kostengründen mit (transparenten) sogenannten PROXY-CACHES arbeiten, deren Anwesenheit gar nicht mehr zu bemerken ist (CISCO SILENT PROXY, SQUID im "silent mode"). Selbst FTP-Server, die häufig benutzt werden, um Share- oder Freeware zum Download anzubieten, arbeiten oft mit zwischengeschalteten Proxies.

Da solch ein PROXY nur frei zugängliche Daten aus dem Internet zwischenspeichert, legen die Systemoperatoren auch keinen großen Wert auf die Absicherung dieses Servers gegen Angreifer. Abgesehen davon ist ein solcher PROXY-Server auch nicht durch eine Firewall zu sichern, da einfach zu viele Verbindungen zu kontrollieren wären. Die Performance würde arg leiden. Angreifer machen sich diese Tatsache dadurch zunutze, indem sie die PROXY-CACHES mit manipuliertenTreibern /Updates/Software füttern und somit indirekt für eine vorzügliche Verbreitung Ihrer Netbus/BackOrifice o.ö. trojanischer Pferde sorgen!

Denial of Service - Attacken
Oder: Wie legen Hacker ganze Server lahm

Angriffe auf den TCP/IP-Stack sind gegenwärtig die Ursache von immensen Ausfällen bei ISPs und innerhalb des Netzwerkes von Unternehmen. Verantwortlich sind hierbei häufig mangelhafte TCP/IPStacks in Servern und Routern, die empfindlich auf defekte Netzwerkkarten und speziell konstruierte TCP/IP-Pakete reagieren. Diese Pakete werden von Programmen erzeugt, die im Internet im Quellcode und als Windows-Programm veröffentlicht werden. Diese werden exploits genannt und sind im BUGTRAQ Archiv zu finden (http://www.geek-girl.com)

Viele dieser hübschen Windows-Applikationen legen Internet-Server lahm und greifen arglose Surfer an. Insbesondere Microsoft hat sich hierbei nicht mit Ruhm bekleckert, die Folgen waren allerorts zu spüren: Computerwoche, SWF3, Microsoft, Netscape... - InternetServer und viele andere waren wochenlang »offline«, hunderttausende von Surfern werden mit DoS-Angriffen belegt, die ein Einfrieren vor allem von Windows 95/98/NT Workstations bewirken.

Microsoft z.B. sperrte seinerzeit alle direkten Zugriffe auf deren Internet-Server und ließ über mehrere Wochen nur Pakete zu, die über bekannte PROXY's bei ISP's geroutet wurden.

PROXY's oder CACHING PROXY's nutzen zwangsläufig ihren eigenen TCP/IP-Stack für ein- und ausgehende Pakete. Pakete von Angreifern über PROXY's mussten somit scheitern. Eine vollständige Liste der unter den Namen "teardrop", "land"... bekannt gewordenen Angriffe findet sich leicht durch eine entsprechende Recherche mit einer guten Suchmaschine.

Um einen solchen Angriff selber zu entwickeln bzw. zu programmieren, müssen Sie zunächst ROOT Zugriff auf einen UNIX Server haben. Programmbeispiele finden sich unter http://www.rootshell.com. Sie sollten außerdem etwas Ahnung von der sogenannten RAW Sockets Programmierung haben. Unter C ist das eher kompliziert und frustrierend, aber PERL bietet dazu ein prima Modul, welches sich Net::RawIP nennt. Leider haben die meisten Webspace-provider, bei denen man einen Unix-Telnet Zugang bekommen kann, dieses Modul aus verständlichen gründen NICHT installiert. Sie finden es beispielsweise unter http://quake.skif.net/RawIP/, oder auf Sergey Kolchev's Homepage in der Ukraine, http://www.ic.al.lg.ua/~ksv/. Dort befinden sich auch viele Source-Code Beispiele (Perl).

Falls Sie hierzu irgendwelche Fragen haben, es gibt auch eine ausführliche FAQ dazu, wo alle Anfängerfragen erläutert werden, darunter auch diejenige, wie ich mit diesem Toolkit gespoofte IPPakete erzeuge, bei denen die Absendeadresse gefälscht ist. Aber Vorsicht, viele Provider können Spoofing bestimmter IP-Nummernbereiche erkennen, andere leider nicht ....

Einige Suchmaschinen, wie z.B. Yahoo und HOTBOT haben net::rawip mittlerweile zensiert und liefern keine brauchbaren Ergebnisse. Die Suchmaschine http://www.northernlight.com/ liefert jedoch zu diesem Thema einige hundert Informationen.

Bekannte Attacken heißen beispielsweise "Ping of Death", "LandAttack". Eine Suchmaschinen-Recherche zu diesen Themen wird Ihnen schnell entsprechende Source-Codes oder sogar komplette, kinderleicht zu Bedienende Windows-Applikationen liefern!

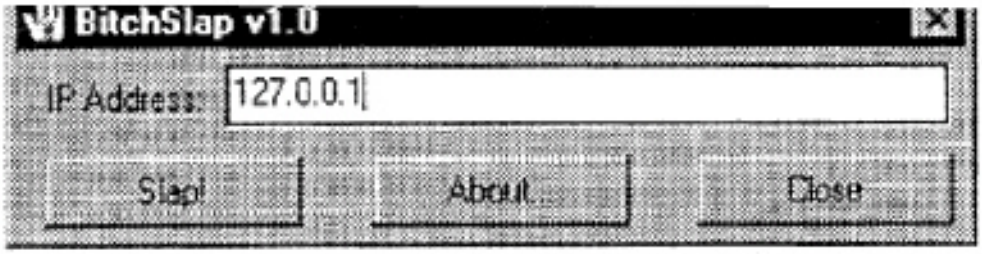
Wie durchschlagend diese Angriffe sind, wird daran deutlich, dass Microsoft in den Beschreibungen der Service Packs diese Problematik erst gar nicht dokumentiert, sondern Patches immer heimlich mitliefert. Wer Microsoft NT Server in Unternehmen einsetzt, der hat leider auf das falsche Pferd gesetzt. Microsoft kann bis heut noch keinen vernünftigen TCP/IP Stack liefern, was auch die riesigen Ausfälle bei Internet-Providern mit NT-Servern zeigen. Mittels der Visualbasic-Macros in Office-Anwendungen wie Winword kann die alte anfällige Winsock2.1 sogar direkt von einem Word-Makro angesprochen werden und so DoS-Attacken aus einem Winword Dokument heraus an das firmeneigene Intranet senden!

Die Gartner GROUP hat signifikante Unterschiede bei den Ausfallzeiten der großen Betriebssystem-Plattformen festgestellt, siehe INFORMATIONWEEK 17/18 vom 19. August 1999, Seite 40:

AS/400 5.3 Stunden/Jahr
S/390 8.9 Stunden/Jahr
UNIX 23.6 Stunden/Jahr
Windows NT 224.5 Stunden/Jahr

Denial Of Service-Attacken im Detail

OOB-Angriff (auch "Nuke" genannt)
Ansatzpunkt für den OOB-Angriff war eine fehlerhafte Implementierung des NetBIOS-Treibers von Micro$oft. Sobald über Port 139 ein Datenpaket eintraf, welches nicht NetBIOS-konform war, stürzte der Rechner ab. Das Tool WinNuke, welches man als C-Source-Code für UnixBetriebssysteme noch häufig im Netz vorfindet, war das erste NukingTool, um Windows95/NT-User abzuschießen. Schließlich fanden sich auch Programmierer, die ein praktisches Windows-Prograämmchen daraus machten - wie beispielsweise BitchSlap.



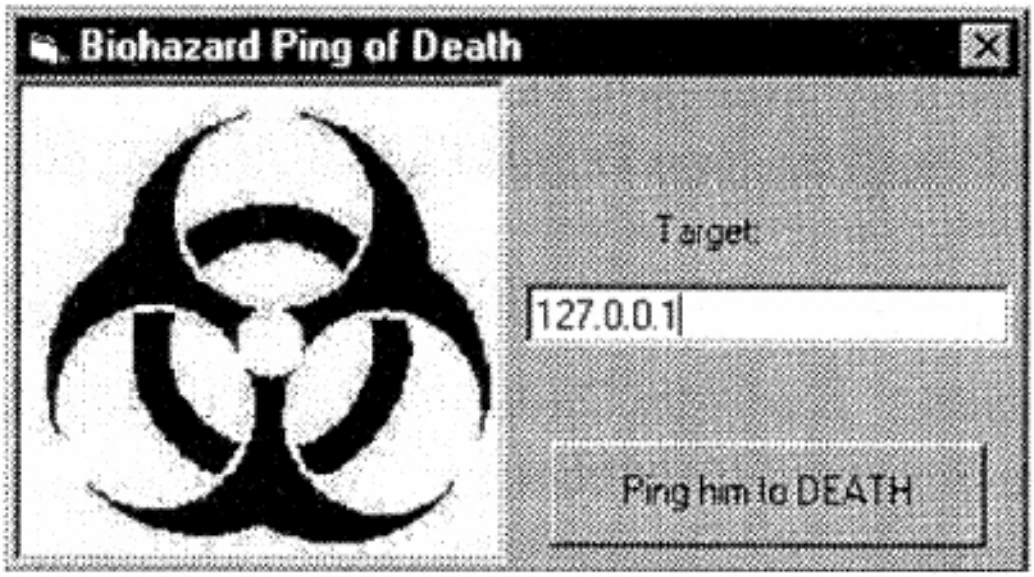
Windows95 und NT sind erst nach Installation der letzten ServicePacks gegen OOB-Attacken Resistent geworden. Ob Ihr System sicher ist, können Sie ausprobieren, indem Sie einfach Ihre Localhost-Adresse 127.0.0.1 benutzen. Stürzt Ihre Internet-Verbindung oder gar Ihr ganzer Rechner ab, haben Sie ein Problem...

Land-Angriff
Land ist ein schwerer Angriff der 1997 entdeckt wurde. Bei einem Land-Angriff wird ein TCP/IP-SYN-Paket mit identischer Absender und Empfängeradresse an den lahmzulegenden Host gesendet.

Es die neueste der hier beschriebenen DoS-Attacken. Einzelne an das Netz angeschlossene Rechner waren hiervon jedoch nicht so sehr betroffen wie die sogenannten Router, welche an den Knotenpunkten der Internet-Backbones (Hauptschlagadern des Internets) stehen. Hier kommen meist Router der Firma CISCO zum Einsatz, die 1997 leider nicht nicht gegen eine SYN-Attacke wie LAND abgesichert waren. Folge war, dass 1997 durch Land-Angriffe ganze Netzwerke nicht mehr erreichbar waren und Router zum Totalabsturz gebracht wurden.

Um einen einzelnen befeindeten Rechner lahm zulegen ist Land also nicht die DoS-Attacke der Wahl, da man sich hier im wahrsten Sinne des Wortes eine eigene Grube graben kann. Denn wenn man die LandAttacke lossendet und dadurch gerade der Router des eigenen Providers seinen Dienst quittiert, hat man sich prima unfreiwillig vom Internet verabschiedet ...

Ping Of Death
Pakete des TCP/IP-Protokolls dürfen maximal 216 Bytes (also 64 KB) groß sein. Größere Datenpakete werden also entsprechend segmentiert und beim Empfänger wieder zusammengesetzt. Die Zusammensetzung benutzt dabei einen Offset, der mit jedem Päckchen mitgeschickt wird und bestimmt, wo es hingehört. Beim Ping of Death wird dem letzten Paket ein Offset gegeben, der dieses größer als 64 KB macht. Dadurch wird auf Empfängerseite beim Zusammensetzen der Pakete ein Buffer-Overflow erzeugt, der die Internetverbindung oder den ganzen Rechner abstürzen lässt. Die Windows-Implementierung des TCP/IP-Protokolls (im unsäglichen WINSOCK.DLL bzw. WSOCK32.DLL) war natürlich nicht auf so etwas vorbereitet, weshalb es auch immer noch bei Windows95-Rechner funktioniert ... Ein einfach zu bedienendes Tool für Windows-Benutzer gibt es auch für den Ping of Death: Biohazard POD



Auch hier können Sie wieder mit Ihrer Localhost-Adresse 127.0.0.1 probieren, ob Ihr System gegen den POD geschützt ist.

Kostenlos Surfen

Wirklich verboten und illegal ist im Moment die sogenannte "Faker" Technik, bei der man sich mit "gefakten" (falschen) Personen-Angaben bei einem Internet-by-Call-Anbieter registriert und das Passwort dann auch noch öffentlich auf sogenannten "Fake-Sites" preisgibt! Eine Seite zu diesem Thema findet sich leicht, indem man einmal das Keyword "fake" sowie ein oder zwei bekannte Internet-by-Call-Anbieter als weitere Stichworte in eine Suchmaschine eingibt (viag, etc.). Es gibt sogar Registrierungs-Generatoren (beispielsweise für Viag-Interkom) die beliebig viele gültige Registrierungen generieren. Da die meisten Internet-by-Call-Anbieter dann eine eigene Rechnung schicken und nicht über das Telekom-Inkasso abrechnen, landen die Gebühren als Rechnung im Briefkasten desjenigen, auf den der Account angemeldet wurde - und den gibt es oftmals nicht. Und solange diese Rechnung noch nicht zurückkommt, ist der Zugang offen und es wird kostenlos gesurft.

Aber zum Glück sind die Provider ja nicht so dämlich wie manche Hacker, die glauben, nun kostenlos surfen zu können. Oft ist es so, dass der Zugang, sobald mehr als eine Person ihn gleichzeitig benutzt, zu einem teureren Minutenpreis über das Telekom-Inkasso abgerechnet wird! Und dann landen doch die Gebühren auf der Rechnung! Denn man sollte immer bedenken, dass die Provider die Telefonnummern der eingewählten Benutzer loggen und somit (solange man nicht von einem öffentlichen Telefon aus surft) immer Bescheid wissen, wer da auf die Kosten eines anderen oder auf die Kosten eines nicht existierenden gefakten Benutzers surft! Denn die Nummer wird ja heute immer übertragen - auch bei analogen Anschlüssen! Das deutsche Telefonnetz ist bereits komplett digitalisiert. Und selbst wer sich sicher glaubt, weil er die CLIP bei der Telekom hat ausschalten lassen (wird dann nicht mehr angezeigt), den muss ich leider enttäuschen. Jeder, der schon einmal von einem anonymen Anrufer belästigt wurde und eine Fangschaltung beantragt hat, weiß wie einfach das ist! Für ca. 20 DM pro Woche liefert Ihnen die Telekom die Telefonnummern ALLER Anrufenden!

Hier surfen Sie LEGAL (!) kostenlos, es fallen lediglich Telefongebühren an!

Conradkom (www.conradkom.de)
Hier ist die erste Stunde im Monat sogar kostenlos, es fallen noch nicht einmal Telefongebühren an - also eine Stunde im Monat absolut kostenlos und gebührenfrei surfen bei Conradkom!

Incl. Telefongebühren, Grundgebühr: 0,00 DM, Freie Stunden: 1,00, Einwahlknoten: Einheitsnummer, Probezugang: keiner, Anmeldegebühr: 0,00 DM, Eigene Homepage: 2 MB, Email-Adressen: 1, Abrechnung erfolgt mit VIAG Interkom über Telekom. 60 Sekunden-Takt.

Mobilcom (www.01019freenet.de)
Bezeichnet sich selber als „kostenlosen Internetzugang" Incl. Telefongebühren, Grundgebühr: 0,00 DM, Freie Stunden: 0,00, Einwahlknoten: Einheitsnummer, Probezugang: keiner, Anmeldegebühr: 0,00 DM, Eigene Homepage: 0 MB, Email-Adressen: 1, Abrechnung erfolgt über Telekom, Minutentakt (bei Preselection sekundengenau).

Germanynet (www.germanynet.de)
Bei germany.net haben Sie die geniale Möglichkeit, kostenlos (zzgl. Telekom Ortstarif) ins Internet zu gelangen. Mittlerweile ist das Angebot nicht mehr nur auf Deutsche Websites beschränkt, sondern erlaubt den uneingeschränkten Zugriff auf das gesamte World Wide Web. Die kostenlosen Surf-Trips finanzieren sich durch Werbung, die während des Surfens eingeblendet wird.

Grundgebühr: 0,00 DM, Freie Stunden: 0, Einwahlknoten: 34, Probezugang: unbegrenzt (kostenlos), Anmeldegebühr: 0,00 DM, Eigene Homepage: 2 MB, Email-Adressen: 1, Finanzierung erfolgt über Werbeeinblendungen. (Internetzugang nur über Proxy-Server).

AOL und Compuserve (www.aol.com und www.compuserve.com)
Viele Provider bieten einen zeitlich begrenzten Testzugang für Interessierte. Nutzen Sie das kostenlose Angebot, und machen Sie sich ein eigenes Bild von den Leistungen. AOL bietet die Zugangssoftware auf CD-ROM oder Diskette inklusive Passwort zum kostenlosen Zugang für 50 Stunden. Man erhält diese CD fast in jedem Computermagazin als Zugabe. Compuserve ermöglicht Ihnen einen vollen gebührenfreien Monat und stellt Ihnen zudem die Software auf CD-ROM oder Diskette kostenlos zur Verfügung.

Stand: 1.5.99 - Angaben jedoch ohne Gewähr!

Wie Hacker kostenlos PayTV sehen

Sender wie Premiere verschlüsseln bereits seit einiger Zeit Ihr Angebot, so dass es für den normalen Fernsehbesitzer zwar empfangbar ist, jedoch das Bild verzerrt ist. Zur Entschlüsselung benötigt man einen Decoder, den die Sender für eine monatliche Gebühr zur Verfügung stellen. Das gute an diesen Sendern ist, dass Sie werbefrei senden und aktuelle Spielfilme bereits kurze Zeit nach Erscheinen auf Video zeigen. Die Verschlüsselung macht es den Anbietern möglich, die Zielgruppe auf den einzelnen Zuschauer genau zu bestimmen und so die Filmlizenzen und Serienabos zu günstigen Preisen einkaufen zu können, da keine landesweite oder sogar europaweite Ausstrahlungslizenz erworben werden muss.

Antisky war ein erster Softwaredecoder und wurde von Marcus Kuhn für das Decodieren des englischen Senders SKY entwickelt. Er hatte erkannt, dass bei der Codierung lediglich Zeilen untereinander vertauscht wurden. Dadurch, dass sich benachbarte Zeilen immer sehr ähnlich sind, konnte sein Programm benachbarte Zeilen wieder korrekt zuordnen.

Natürlich wird zum Empfang neben der Decodersoftware auch eine TV-Karte benötigt. Dabei ist darauf zu achten, dass diese einen weit verbreiteten Chip wie den BT848 oder BT878 besitzt, da diese Chips von den meisten Decoder-Programmen unterstützt werden.

Zum Decoderprogramm selber gehört auch die eigentliche Entschlüsselungsdatei, die oft "key.txt" benannt ist. Diese enthält das Schema, nach dem die Zeilen getauscht werden müssen.

Diese Datei kann man im Internet erhalten, denn sie wird oft aus Wettbewerbsgründen nicht mitgeliefert. Manche Decoder besitzen auch eine Funktion, um diesen Schlüssel selber zu berechnen.

Deutsche Sender wie Premiere (nicht das neue digitale Premiere World) benutzen das Verfahren „Nagravision". Dieses Verfahren permutiert den Schlüssel ständig. Die benötigten Informationen enthält der Decoder alle 255 Halbbilder digital und verschlüsselt in der Austastlücke (nicht sichtbarer Bereich des Bildes - oben über dem sichtbaren Bild). Pro Halbbild gibt es schließlich 2hoc h15 = 32768 verschiedene Möglichkeiten der Zeilen-Permutation.

Wenn man nun aber alle Zeilen miteinander vergleicht, kann man ähnliche Zeilen finden und unter der Annahme, dass ähnliche Zeilen zueinander gehören, diese wieder in die richtige Reihenfolge bringen. Alle Zeilen komplett zu vergleichen würde selbst einem Athlon 700 starkes Kopfzerbrechen bescheren, weshalb man nur stichprobenartig einzelne Punkte aus verschiedenen Zeilen vergleicht. Wie viele Stichproben gemacht werden, ist einstellbar und resultiert in der Qualität der Decodierung. Schließlich wird aus den 32768 verschiedenen Permutationen die gewählt, die am ehesten zu dem Ergebnis der Stichproben passt. Diese Permuation wendet man dann auf das gesamte Bild an und erhält so ein komplett decodiertes Bild.

Es gibt auch Decoder (besonders für die VideoCrypt-Sender, die jedoch in Deutschland nicht angeboten werden), die durch Auswertung des Decoders oder Hacken des Alogirthmus entwickelt wurden. Diese sind jedoch absolut verboten und eine Anwendung ist strafbar. Das hat die folgenden Gründe:

- Strafbares Ausspähen von Daten
- Verletzung des Urheberrechts
- Gesetz gegen den Unlauterern Wettbewerb, das Betriebsgeheimnisse schützt

Noch gibt es in Deutschland einige Seiten, die sich öffentlich mit den Decodern des Zeilentauschverfahrens beschäftigen, jedoch kann niemand sagen, wie lange diese Websites noch existieren werden.

Abhören und Modifizieren einer Mobilfunk-Mailbox

Dieser Hack-Trick ist so einfach, dass man schon fast nicht glauben mag, dass er tatsächlich funktioniert. Auch ich war zunächst der Meinung, dass dies doch so nicht wahr sein kann. Aber wenn Sie es mal bei einigen Mailboxen ausprobiert haben und dann schließlich eine Mailbox vorfinden, wo der Hack funktioniert, werden Sie Ihre Meinung über diesen Hack schnell ändern.

Im Folgenden beschreibe ich, wie man bei einer D2-Mailbox vorgeht. Für andere Netzbetreiber ist der Trick jedoch genauso anwendbar.

Wählen Sie 0172-55-XXXXXX von einem normalen Telefonanschluß mit Tonwahl-Unterstützung. Dabei ersetzen Sie XXXXXXX durch die Nummer des Anschlusses, den Sie hacken möchten. Bei neueren D2-Anschlüssen müssen Sie natürlich statt der 0172 eine 0173 vorwegwählen.

Sie werden von der Mailbox begrüßt und nun aufgefordert, das Mailbox-Kennwort einzugeben. Geben Sie nun 1,1,1,1 ein.

Aus Erfahrungswerten schätze ich die Erfolgsquote auf mindestens 25 Prozent. Die 1111 ist die vom Netzbetreiber voreingestellte PIN für die Mailbox. Solange der Besitzer diese nicht geändert hat, können Sie mit der 1111 seine Mailbox abhören, Nachrichten löschen und sogar die PIN ändern, was dem Besitzer unmöglich macht, seine Mailbox abzuhören (er muss dann Kontakt mit dem Netzbetreiber aufnehmen). Wenn Sie eine bestimmte Mailbox abhören möchten und die 1111 partout nicht funktionieren möchte, versuchen Sie andere einfach konstruierte Nummern, die man sich leicht merken kann: 2222, 3333, 1234, 9876, 4711, 0815... Oder wenn Sie die Person kennen probieren Sie das Geburtsdatum oder das Geburtsdatum der Freundin oder des Freundes. Sie haben je Anwahl 3 Versuche. Sind diese erfolglos, wegen Sie einfach auf und wählen Sie die Mailbox erneut an - Sie haben sofort wieder 3 weitere Versuche.

Anonyme Emails versenden *oder*
Wie Mann Emails ohne Email-Programm verschickt

Um eine Mail anonym oder ohne Mailprogramm verschicken zu können, benutzt man das SMTP Protokoll, welches in der RFC 821 definiert ist.

Wir wählen nun einen frei zugänglichen Mailserver (damit will ich sagen, dass beispielsweise die T-Online Mailserver (mailto.btx.dtag.de etc.) nur von einem T-Online-Zugnag aus nutzbar sind. Es gibt aber viele sogenannte öffentliche Relay-Server, die man für das folgende Experiment benutzen kann.

Viele Firmen-Mailserver sind nicht hinreichend geschützt und akzeptieren daher Verbindungen von jedem beliebigen Internet Zugang, also von jeder beliebigen IP-Adresse aus. Einfach mal mail.XXX.de ausprobieren, wobei XXX durch bekanntere Firmennamen zu ersetzen ist. Sie werden schnell einen nicht geschützten Mail-Server finden!

Wenn Sie so einen gefunden haben, hat das außerdem den Vorteil, dass Sie diesen Server in Netscape oder Outlook als Postausgangsserver einstellen können und diesen dann von jedem beliebigen Internet-by-Call-Provider benutzen können und somit nicht jedes mal einen anderen Server konfigurieren müssen bzw. mehrere Profile anlegen müssen.

Hier das Beispiel:
START -> Ausführen -> Eingeben: Telnet mail.XXX.de 25

Hierbei ist mail.XXX.de durch den von Ihnen gefundenen öffentlichen Mail-Server zu ersetzen! Das SMTP-Protokoll läuft also auf PORT 25. Durch die Angabe einer Nummer hinter dem Host-Namen signalisieren Sie TELNET, dass Sie auf einem anderen als dem Standard-Telnet-Port konnektieren möchten. Um zu sehen, was eingegeben wird, unter "Einstellungen" von Telnet das lokale Echo einschalten.

Hier eine Beispiel-Session:

```
220 squid.dvs.org ESMTP server (Post.Office v3.5.3 release 223
ID# 127-60479U800
0L8000S0V35) ready Wed, 24 Nov 1999 15:34:42 +0100
help
214-This SMTP server is a part of the post.office
214-E-mail system. For information about
~
214-post.office, please See http://www.software.com
~
214
~
214- Supported commands:
214- EHLO HELO MAIL RCPT DATA
214- VRFY RSET NOOP QUIT
214-
214- SMTP Extensions supported through EHLO:
214-
214- ETRN EXPN HELP SIZE
214-For more information about a listed topic, use "HELP
<topic>"
214 Please report mail-related problems to Postmaster at this
site.
MAIL FROM:<wv@alphaflight.com>
250 Sender <wv@alphaflight.com> Ok
RCPT TO:<wv@alphaflight.com>
250 Recipient <wv@alphaflight.com> Ok
DATA
354 Ok Send data ending with <CRLF>.<CRLF>
Hallo, das ist meine kleine anonyme (?) Nachricht an mich selber.
Auch sehr praktisch, um eine Email zu verschicken, wenn kein
Mail-Programm zur Hand ist...
Viel Spass!
```

```
250 Message received:
19991124143526.AAA17545@squid.dvs.org@(62.157.61.235]
quit
221 squid.dvs.org ESMTP Server closing connection
```

Der Mailserver antwortet auf jede Eingabe (außer wenn die Zeilen der Nachricht eingegeben werden) mit einer Status-Antwort (dreistellige Zahl plus Fehlermeldung/Bestätigung).

Wichtig sind also die Kommandos "MAIL FROM:" wobei hiernach die Absender-Email in <> eingeschlossen folgen muss. Das tolle: Hier kann man irgendetwas angeben (z.B. someone@somewhere.org).

"RCPT TO:" gibt entsprechend die Email-Adresse des Empfängers dieser Nachricht an.

Auf das Kommando "DATA" schließlich folgt die Eingabe der eigentlichen Nachricht. Wenn sie fertig ist, einfach eine Zeile eingeben, die nur einen Punk enthält.

Exkurs: Wie erfahre ich einen zu einer Domain gehörenden Mail-Server?

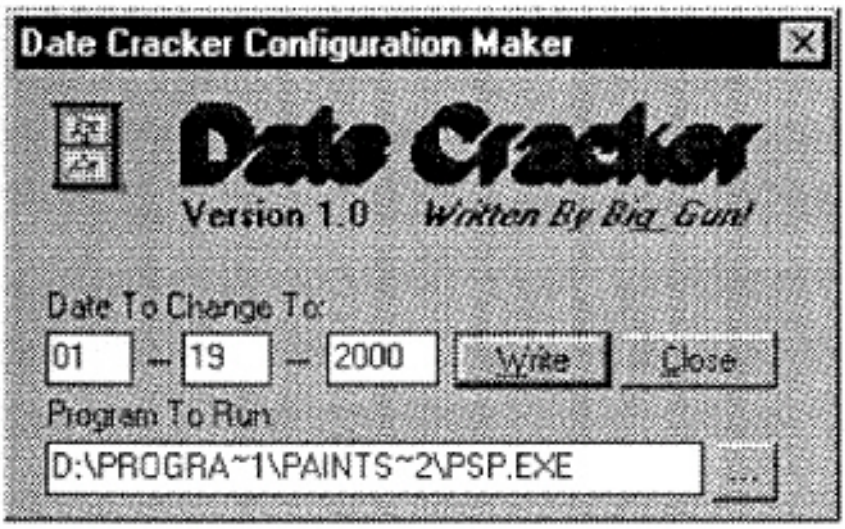
Benutzen Sie dazu das Programm "Net.Demon" (http://netdemon.simplenet.com) und wählen Sie die Option "DNS-Lookup". Stellen Sie beispielsweise den Nameserver der Deutschen Domainverwaltung DENIC ein (Server: DNS.DENIC.DE). Zusätzlich die Optionen „Get authoritative Answer" und "Recursion" aktivieren. Sodann kann unter "Domain" eine zu prüfende www-Domain angegeben werden (beispielsweise "colossus.net"). Die Nameserver-Anfrage liefert nun neben den Nameservern dieser Domain auch die eingetragenen Mailserver, in diesem Fall mail.colossus.net.

Was ist ein Blackbook?

Ein Blackbook ist weniger als “Schwarzes Buch” sondern vielmehr als “Schwarzbuch” zu übersetzen. Darunter versteht man einen Enthüllungsreport, der Gefahren oder Skandale aufdeckt. So gibt beispielsweise der Bund der Steuerzahler jährlich das “Schwarzbuch der Steuerverschwendung” heraus, worin skandalöse Fälle von Steuerverschwendung aufgedeckt werden. So ist auch dieser Report zu verstehen. Ein Einblick in aktuelle Möglichkeiten, Aktivitäten und Hintergründe der Hackerszene.

Aufhebung der zeitlichen Limits von Demo-Software

Heute ist es üblich, dass Softwarefirmen neue Produkte als Demoversion zum Download im Internet anbieten. Diese Demoversionen besitzen oft bis auf eine zeitliche Limitierung vollen Funktionsumfang. Im Folgenden beschreibe ich, wie diese zeitliche Limitierung entfernt werden kann. Das Programm "Date Cracker" kann einer Demo-Version ein falsches Datum vortäuschen.



Beispiel:

Ihr zu "crackendes" Programm ist leider bereits am 31.12.1999 abgelaufen.

- Stellen Sie die Systemzeit auf ein Datum vor dem Testzeitraum z.B. 1.10.1999 (Doppelklicken auf die Systemzeit unten in der Taskbar von Windows) und deinstallieren Sie die Demo-Software
- Installieren Sie die Demo-Software erneut. Sie sollte nun korrekt laufen.
- Suchen Sie im Programmverzeichnis (in welches Sie die Software installiert haben) nach der eigentlichen Programm-Datei (z.B. PSP.EXE) und starten Sie dann den Date-Cracker.
- Wählen Sie als "Program To Run" die eben gesuchte EXE-Datei Ihrer Demo-Anwendung und stellen Sie das Datum ein, mit der die Anwendung funktioniert (1.10.1999).
- Wählen Sie nun "Write".

Sie können nun Date-Cracker schließen und das Datum wieder richtig stellen. Sobald Sie nun die gecrackte Anwendung starten, wird vorher das Datum immer automatisch auf das alte Datum gestellt (1.10.1999) und bei Beenden der Anwendung wieder zurückgestellt.

Rechtliche Betrachtung der Hacker-Aktivitäten

Hier möchte ich anhand der eingangs bereits zitierten Paragraphen einige Beispiele für Straftaten von Hackern nennen:

Computerbetrug
Der Paragraph 236 des StgB (Strafgesetzbuch) regelt den Bereich des Computerbetrugs. Auf Computerbetrug steht laut Gesetz in schweren Fällen bis zu 10 Jahre Haft oder hohe Geldstrafen. Hierzu zählt z.B. unbefugte Verwendung von Daten, unrichtige Gestaltung eines Programms, etc. Als Beispiel könnte hier die Manipulation eines Geldautomaten oder Glückspielgeräts genannt werden.

Computersabotage
Paragraph 303b StgB nennt bis zu 5 Jahre Haft für Computersabotage. Dazu zählen das Zerstören, Beschädigen und die Veränderung einer Datenverarbeitungsanlage. Ein wichtiges Beispiel sind hier die Viren. In USA wurden bereits Virenprogrammierer zu langen Haftstrafen verurteilt, wie erst kürzlich der Programmierer des Melissa-Virus.

Computerspionage
Bis zu 3 Jahre Haft setzt es auf Computerspionage. Dieser Paragraph dürfte insbesondere die klassichen Hacks betreffen, bei denen sich mittels verschiedener Techniken Passwörter zu geschützten Informationen erhackt werden.

Blueboxing

Blueboxing zählt zu den Phreaker-Techniken, die es ermöglichen, kostenlos zu telefonieren. Leider sind fast alle der im Internet zu findenden Boxing-Technoligien (benannt mit verschiedenen Farben) einschließlich des hier exemplarisch beschriebenen Blueboxing heute nicht mehr anwendbar, da wir in Deutschland ein mittlerweile zu 100% digitalisiertes Telefonnetz besitzen. Die Boxing-Techniken wurden indes für das analoge Telefonnetz entwickelt.

Kernpunkt des Blueboxing ist die Tatsache, dass man mit den Frequenzen 2400 Hz sowie 2600 Hz in einem Telefonnetz mit sogenannten C5-Vermittlungsstellen (Abkürzung für den Standard CCITT5) Gespräche unterbrechen kann.

Bei der häufigsten Blueboxing-Anwendung wurde versucht, eine kostenlose Verbindung zu den mit neuesten Raubkopien ausgestatten US-Mailboxen wie Cesars Palace etc. einzurichten.

Der Trick war einfach:
Der Blueboxer in Deutschland wählte eine US-Amerikanische Telefonnummer an, die sofort wieder auflegte. Aufgrund der Relais-Trägheit in den alten transkontinentalen Telefonnetzen dauerte es oft mehrere Sekunden, bis die deutsche Vermittlungsstelle das Auflegen auf amerikanischer Seite registrierte und das Besetztzeichen zu hören war. In diesem kurzen Zeitfenster musste der Phreaker nun einen C52400 hz Ton senden (sogenannter Size-Ton), welcher dem amerikanischen Vermittlungscomputer das korrekte Trennen der Verbindung von deutscher Seite mitteilte. Der Ton kam aber vom Phreaker und nicht von der deutschen Vermittlung und daher war die Leitung auf deutscher Seite noch offen. Nun konnte der Phreaker munter eine neue Nummer (diesmal die der Warez-Mailbox) wählen und kostenlos stundenlange Downloads und Uploads durchführen.

Mail-Order Betrug

Dieser einfache Titel benennt ein Verfahren, mit dem Hacker in den 80er und auch 90er Jahren noch international agierende3n Versand Unternehmen immense Schäden zufügten. Auch heute funktioniert der Mail-Order Betrug teilweise noch problemlos.

Dazu benötigen die Hacker die Kreditkartennummer einer gültigen Kreditkarte sowie das Gültigkeitsdatum. Das könnte man ja auch einfach mit einem Creditcard-Generator erledigen - jedoch benötigt der Täter beim Mail-Order Betrug auch den korrekten Namen des Karteninhabers, da die Versandunternehmen im Gegensatz zu SexSites im Internet die Kartendaten prüfen und beim Kartenunternehmen den Karteninhaber abfragen. Denn die Versandunternehmen müssen nicht in wenigen Sekunden entscheiden (wie bei einer Onlineprüfung eines Internet-Sex-Anbieters) sondern haben vor dem Versand in der Regel etwa einen ganzen Tag zeit, die Daten zu prüfen.

Den Namen und die zugehörige Kartennummer zu finden ist jedoch teilweise erschreckend einfach und der Autor selber ertappte sich bereits schon einmal dabei, beinahe seine Karteninformation preis gegeben zu haben: Zum Beispiel beim Tanken erhält man nach der Zahlung einen Beleg über die Kartenzahlung (Durchschrift des unterschriebenen Kreditkarten-Belastungsbelegs). Darauf befindet sich stets die 16-stellige VISA/MASTERCARD/AMEX-Nummer und das Gültigkeitsdatum. Auch der Name wird oft mit auf den Beleg gedruckt - wenn nicht, so findet man auf dem Beleg immer noch die Unterschrift des Karteninhabers.
Diese Belege werden leider oft gedankenlos weggeschmissen, denn man denkt sich, man kann die Benzinkosten sowieso nicht steuerlich absetzen - was soll ich also mit dem Beleg ...
Ein Mail-Order-Betrüger braucht sich nun also nur die Mülleimer einer Tankstelle genauer anzusehen und wird sicher nicht nur einen solchen Beleg finden! Oftmals haben solche Betrüger auch einen Komplizen, der bei der Tankstelle arbeitet und den ganzen Tag fleißig Belege abschreibt oder gar unter der Theke die Karte ein zweites Mal durch einen Magnetstreifen-Leser zieht.

Nachdem genügend Kartenmaterial gesammelt wurde, bestellt der Betrüger nun bei ausländischen Versandfirmen entsprechend der Belastungsgrenze der Karte (Kartenlimit). Das Kartenlimit ermittelt der Betrüger durch einen kurzen Anruf bei der Clearing-Zentrale des jeweiligen Kartenunternehmens. Hierbei gibt er sich als Mitarbeiter einer größeren Firma aus (z.B. Automvermietung) und teilt dem Mitarbeiter der Kartenfirma mit, er habe einen Kunden, der ein Auto mieten möchte und er möchte nun wissen, wie hoch das Limit der Karte ist, damit er feststellen kann, ob das Limit reicht, um die Kaution per Karte zu zahlen.

Hat er nun das Limit erfragt, so kann die Karte bis auf die letzte Mark benutzt werden, um Waren zu bestellen. Vorzugsweise bestellen die Mail-Order-Betrüger Speicher-Module, CPUs oder ähnliche Ware. Wichtig ist nur, dass die Ware klein aber dennoch teuer ist, sich gut hehlen lässt und keine Seriennummern besitzt. So hat er größte Chancen, die Waren weiterzuverkaufen.

Der kritische Punkt des Mail-Order-Betruges ist jedoch die Lieferadresse. Denn diese Betrugsform ist den Ermittlungsbeamten längst bekannt und daher wäre es vom Betrüger äußerst dämlich, sich die Ware an die eigene Adresse liefern zu lassen. Dadurch wäre selbst im Nachhinein wenn der Kreditkartenmissbrauch dann eines Tages durch die unerlaubte Abbuchung entdeckt wir, die Identität des Täters erkennbar.
Stattdessen werden hier verschiedene Methoden mit unterschiedlicher Effektivität eingesetzt, um eine Inflagranti-Verhaftung zu verhindern.

Unbewohntes Haus
Der Täter sucht ein unbewohntes Haus und lässt die Ware dorthin liefern. Wird schwierig, wenn die Tat bereits vor Lieferung aufgedeckt wird und die Lieferung von einem Polizeibeamten begleitet wird.

Lieferung postlagernd
Der Täter lässt die Ware postlagernd zu UPS, DHL oder gar zur guten alten Deutschen Post AG liefern. Dort hat er einen Mittelsmann, der Mitarbeiter der jeweiligen Firma ist und den Betrüger informiert, wenn die Ware da ist und scheinbar kein Polizeibeamter die Lieferung begleitet.

Prüfung vor Abholung
Wirkliche Profis des Mail-Order-Betrugs checken, bevor sie Ware abholen, ob sie sich nicht daran die Finger verbrennen können. Dazu rufen Sie wiederum das Clearing-Zentrale der Kreditkarten-Firma an und fragen

wiederum nach einer Deckung für irgendeine Bestellung. Wenn der Betrug bereits aufgedeckt wurde, ist die Karte längst gesperrt und so erfährt der Betrüger, wie heiß seine Ware ist und lässt sie bei einer positiven Antwort einfach am Postlagerungsort liegen, ohne sie abzuholen.

Kostenlos telefonieren mit der T-Card

Bereits 1994 brachte die Telekom eine eigene Calling Card, genannt "T-Card" heraus. Sie war in mehreren Variationen, z.B. mit 25 DM Guthaben, erhältlich. Noch im letzten Jahr wurde in Diskussionsforen und IRC-Kanälen offen darüber gesprochen, dass es mit der 25 DM-Variante der T-Card möglich wäre, kostenlos zu telefonieren (ohne die Karte zu manipulieren).
Dieser Trick beruht darauf, dass die Telekom hier einen besonderen Service eingerichtet hat, welcher der Telekom eigentlich höhere Gewinne bringen sollte. Statt dessen wurde hierdurch aber eine Sicherheitslücke geschaffen ...

Wenn das Guthaben der Karte nämlich während eines Gesprächs auf unter 48 Pf. fällt, wird der Angerufene darauf hingewiesen, dass sein Gesprächspartner bald kein Guthaben mehr auf seiner Karte haben wird und er die Möglichkeit hat, das Gespräch vom Anrufer dann auf seine Kosten (als sogenanntes R-Gespräch) weiterzuführen.

Insoweit wird nun sicherlich noch nicht ganz klar, wie hier kostenlos telefoniert werden soll. Wenn man jedoch daran denkt, dass es auch Telefonzellen gibt, an denen man angerufen werden kann, wird schnell klar, wo die Lücke entstanden ist: Der T-Card-Inhaber ruft einen Partner an einer Telefonzelle an und telefoniert mit ihm solange, bis nur noch 48 Pf. Guthaben auf der T-Card sind. Dann nimmt der angerufene Gesprächspartner an der anderen Telefonzelle die Möglichkeit wahr, das Gespräch bei Ablauf des Guthabens als R-Gespräch weiterzuführen. Dumm nur, dass die Telekom Ihrer eigenen Telefonzelle dann später keine Rechnung zuschicken kann. Obwohl dies wahrscheinlich bei der Telekom schon einmal passiert ist, dass einer Telefonzelle eine Rechnung geschickt wurde oder sogar der Gerichtsvollzieher ...

Wichtige Links

Weiterführende Informationen finden sich unter anderem hier:

http://www.false.com/security
http://www.insecurity.org/nmap
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.lOpht.com
http://www.infonexus.com/-deamon9
http://www.cert.org
http://www.cert.dfn.de
ftp://ftp.blib.pp.se/pub/cracking

Hacker-Glossar

0-day-warez
Als 0-day-warez wird Software bezeichnet, die an diesem Tag auf den Server zum Downloaden gespielt wurde. (Meist auch am selben Tag gehackt!)

Appz
Dies ist der Ausduck, der auf Warez-Seiten für Standardapplikationen gebraucht wird.

Courier
Couriere sind Mitglieder von Hackerclubs oder Warez-Seiten, die dafür zuständig sind, dass sie die gehackte Software möglichst schnell in Umlauf bringen. Dies geschieht meist über einen schnellen Internetzugang (Standleitung) oder die Software wird über gebrannte CDs verschickt.

Cracker
Ein Cracker ist ein Hacker, der in fremden Systemen die Sicherheitsmechanismen überwindet. Der Begriff Cracker wurde Mitte der 80 Jahre eingeführt. Cracker erstellen meist kleine Programme, die von verschiedenen Programmen den Passwortschutz oder das Testzeitlimit außer Kraft setzen. So gibt es beispielsweise für verschiedene Softwarepakete, die normalerweise 30 Tag lang zu testen sind, einen Crack, mit dem die Zählfunktion für die benutzten Tage ausgeschaltet wird und somit das Programm für immer nutzbar gemacht wird.

Cracking
Cracking nennt man das Überwinden von Sicherheitsvorkehrungen in einer Software oder das einbrechen in Computersysterne. Auf entsprechenden Hackerseiten findet man oft ganze Anleitungen zum "Hacken" von Programmen.

Elite
Anwender, der aktuelle Software vertreibt, keine alte. Gegenteil von Lamer.

Hacker
Hacker haben Spaß am Umschreiben von Programmen. Ihr Ziel ist es, sich ständig zu verbessern und Zusammenhänge zu begreifen, die sich nicht auf Anhieb erschließen. Hacker reagieren empfindlich, wenn sie ausschließlich mit illegalen Aktionen in Verbindung gebracht werden. Hacker sehen sich gerne als Elite.

Lamer
In der Warez-Szene ist unter einem Lamer ein Anwender zu verstehen, der alte Warez weiterleitet. Alt bedeutet in diesem Zusammenhang meist älter als drei bis fünf Tage. Lamer laden auf Warez-FTPs oft Shareware rauf um die Rate umgehen zu können.

Larval Stage
Als Larval Stage bezeichnen Hacker eine Phase, in der sie sich auf nichts anderes als auf das Umschreiben von Programmen beschränken. Dieser Begriff wird besonders gerne in Filmen benutzt.

Leecher
Als Leecher werden die Anwender bezeichnet, die sich der Warez bedienen, ohne eine Gegenleistung dafür zu erbringen. Wer auf einen umfangreichen Download nur wenige Uploads folgen lässt, wird als Leecher bezeichnet. Leecher sind in der Szene nicht sehr beliebt, da durch sie die Verbreitung der Warez gebremst wird.

Phreaking
Unter Phreaking versteht man das Knacken von Telefonsystemen. Durch Phreaking wird es möglich, umsonst oder auf Kosten anderer zu telefonieren.

Rate (Ratio)
Auf FTP-Servern wird oft eine bestimmte Rate beim Download der Daten gefordert. Dass heißt, wenn man beispielsweise ein Programm mit 5MB herunterlädt, muss man dafür auf den Server ein Programm mit z.B. 3MB hinaufladen. Dies entspräche einem Verhältnis von 5:3. Damit wird garantiert, dass ständig neue Programme in Umlauf gebracht werden.

Request

Einige Cracker bieten auf ihren FTP-Servern ein Request-Verzeichnis an, in dem jeder die gesuchte Software eintragen kann. Wenig später wird diese meist von irgendjemandem, der diese Software hat, hinaufgeladen.

Warez
Unter Warez versteht man geknackte Vollversionen von kommerziellen Programmen oder Sharewareprogrammen. Wenn auf einer Software ein Kopierschutz ist, wird dieser entfernt und dann die Software auf sogenannten WarezSeiten vertrieben. Derzeit gibt es in Westeuropa über 85.000 Warez-Seiten.

Warez DOOdz
Hier stehen verschiedene Gruppen in Konktirrenz. Solche Gruppen stellen Software ins Internet, bei der sie vorher den Kopierschutz entfernen. Die Gruppe, die am meisten Programme am schnellsten herausbringt hat gewonnen.

Anonymizer
Wenn man eine Webseite im Internet besucht, können jede Menge Daten über den Besucher festgestellt werden. Darunter sind zum Beispiel Browser, Betriebssystem, Provider unter anderem ist auch die IP-Nummer dabei, anhand dieser man zurück-verfolgt werden kann. Sogenannte Anonymizer filtern solche Informationen heraus und setzen dafür andere ein. Somit kann man sich im Internet anonym bewegen.

Backdoor
Backdoors sind sogenannte Hintertüren, die Programmierer meist zum Austesten eines Programmes eingebaut haben, um zum Beispiel nicht jedes mal sämtliche Passwörter eingeben zu müssen.

Firewall
Ein Firewall stellt sich vor einen Server und überwacht jeglichen Datenverkehr, der zu bzw. von dem Server geschickt wird. So ist es möglich, bestimmte Internetadressen zu sperren, bzw. den Zugriff auf den Server nur bestimmten Leuten zu ermöglichen.

Sniffer
Sniffer hören den gesamten Datenverkehr ab, der über die angeschlossene Netzwerkkarte geht. So können beispielsweise bestimmte Passwörter herausgefiltert werden.

Port-Scanner
Im Internet hat jeder Dienst seinen eigenen Port, so steht zum Beispiel für HTTP der Port 80 und für FTP der Port 21. Diese Ports können fast immer frei belegt werden. Oft dienen solche Ports auch für spezielle Admin-Programme, mit denen man den Server betreuen kann.

SSL
Im Internet wird eine sichere Verbindung meist mit Hilfe des SSL-Protokolls aufgebaut. In einer solchen Verbindung werden alle Daten verschlüsselt übertragen, somit haben es Hakker sehr schwer solche Daten abzuhören. SLL (Secure Sokkets Layer) wurde von Netscape entwickelt.

Authentifizierung
Während der Authentifizierung wird die Identität des Benutzers oder des Servers sichergestellt.

Attachment
Unter Attachment versteht man einen Anhang, der mit einer Email verschickt wird.

Denial-of-Service Attacke
Ein solcher Angriff ist nur darauf aus, einen bestimmten Dienst oder Rechner zu blockieren bzw. zum Absturz zu bringen.

Plugin
Ein Plugin ist ein kleines Zusatzprogramm zu einem Anwendungsprogramm, mit dem dieses um zusätzliche Funktionen erweitert wird.

Spoofing
Darunter versteht man das Vortäuschen eines falschen Absenders von IP-Paketen (IP-Spoofing). Es lassen sich auch Internetnamen spoofen, was dann DNS-Spoofing genannt wird. Wenn ein kompletter Internet-Bereich über einen Zwischenrechner umgeleitet wird, nennt man dies Web-Spoofing.

Remailer

Mit Hilfe eines Remailers kann man anonyme Emails verschicken, die auch keine Provider-Kennung mehr enthalten.

Incoming - Verzeichnis
So wird ein Verzeichnis auf einem FTP-Server genannt, in dem jeder Lese- und Schreibzugriffe hat. Solche Verzeichnisse sind häufig auf Servern von Universitäten vorhanden. Dies wird sehr häufig von Hackern ausgenutzt, um illegale Raubkopien zu verteilen.