Security FAQ - versione 3.1 Y2K - The Day After

Revisore: Massimiliano Baldinelli
Ultima revisione: 15/10/2000
e-mail: M.Baldinelli@agora.stm.it
Distribuzione: http://www.linuxvalley.com/~lserni
(con motore di ricerca)
http://members.xoom.com/gouldukat
(versione .txt)
http://w3.to/citati/
(versione .txt)
http://www.freeweb.org/personali/paolapandolfini/
(versione .txt)
http://www.freeweb.org/risorse/Pericoli/download.htm
(versione .zip)
http://pericoli.freeweb.org
(versione .txt)
http://maxxxxx.cjb.net/informatica/securityIdx.htm
(versione .html)
http://vene.dave.it
(versione .txt, .html e .zip)
http://space.tin.it/io/ptentare/in.html
(versione .html)
ftp://ftp.olisys.it/ComputerVille/faq/securfaq.txt
(versione .testo)
http://utenti.tripod.it/notes/
(versione .testo)
http://utenti.tripod.it/cry/
(versione .zip)
ftp://ftp.computerville.it/pub/faq/
(versione .txt, .zip e .gz)
http://merlino.ghostbbs.cx/
http://genius.allnet.it/merlino/
(versione .txt)
http://www.manuali.net/sicurezza.htm
(versione .txt)
http://members.xoom.it/nietzsche/documenti/securfaq.htm
(versione .html)
http://www.tccity.net/carcar
(versione .txt)
http://italia.esclamativa.isfun.net/
(versione .txt)
http://welcome.to/peppelr
(versione .txt)
http://members.xoom.it/marcgent
(versione .txt)
http://www.aiutamici.com
(versione .txt)
http://www.freeweb.aberont.org
(versione .txt)
http://invest.freeweb.org
(versione .txt)
http://web.tiscalinet.it/sorgi
(versione html)
http://utenti.tripod.it/zut
(versione .txt)
http://www.napoliitaly.it
(versione .txt)
http://members.tripod.it/plf/

Credits: @ExE.ExE
Diego Ravarotto (per alcuni svarioni da lui segnalati)
Enrico Gallesio

fixit
Francesca
Frankj
Giulio
invy
Krmel
Leonardo De Luca (per [B36W])
Leonardo Serni (per la sezione E e un'infinità di altri post)
Marco D'Itri
Marco Zani (per [PORT-Appendice])
Master
Maurizio Cimaschi (per [PORT-Appendice] e [C01a])
Nebbia
Paolo Monti (per [B24])
x-hacker

(e altri che ho certamente dimenticato) per contributi diretti e/o indiretti al materiale qui riportato. Contributi diretti = correzioni, citazioni e materiale diretto a me (tramite e-mail o risposte a miei post su it.comp.sicurezza.varie). Contributi indiretti = tutto il resto che è stato postato su ics.varie e sul quale questa FAQ è basata.

[B08-W][9] E come mi accorgo invece di Netbus?
[B09-W][9] Come si toglie Netbus?
[B10-W][9] Come si toglie TeleCommando?
[B11-W][9] Cos'è Aggressor?
[B12-W] Un bug di mIRC
[B13-W] Che rischi corro usando ICQ?
[B14-W] Cosa sono le scansioni invisibili?
[B15-W] Ma il file windll.dll non è un file di sistema di Windows?
[B16-W] Ho ricevuto un messaggio e-mail con un allegato, ma quando tento di leggerlo il mio Outlook va in crash.
[B17-W] Come vedo se ho il protocollo NetBIOS su TCP/IP installato? Che rischi corro?
[B18-W] Senza programmi come Bo o NetBus è possibile "entrare" nel computer di qualcuno?
[B19-W] Le porte UDP 137 e 138 sono un rischio? E perchè?
[B20-W][95] Ho notato che ogni volta che mi connetto a internet si aprono automaticamente queste due porte 137 e 138. Io ho la versione OSR2 di win95, è un problema di questa versione ?
[B21-W][NT] Da un account NT in pratica senza nessuna autorizzazione, è possibile scovare la password dell'Administrator?
[B22-W][NT] È possibile diventare amministratore sotto Windows NT?
[B23-W][NT] Avendo il diritto di installare ed eseguire programmi, cosa posso fare?
[B24-W][9] Come possono interagire telnet e BO?
[B25-W] In cosa consiste di preciso il "TearDrop Attack"?
[B26-W] Come sono belli i messaggi di posta e news formattati, con tutte quelle belle applet ed effetti speciali!!!
[B27-W][NT] Perchè è meglio chiudere la porta 53 sotto NT?
[B28-W] È possibile camuffare un eseguibile come un file di tipo diverso?
[B29-W] Corro rischi ad usare Netbuster per beccare intrusi?
[B30-W][9x] Ancora sul NetBIOS: può BO usare le sue porte?
[B31-W] Può un attacco sfuggire a Nuke Nabber?
[B32-W] Cos'è Portfuck?
[B33-W] Alcune cosa da sapere su mIRC...
[B34-W] Quando su un sito che visito appare il contenuto del desktop cosa vuol dire? Mi devo preoccupare oppure è normale?
[B35-W] Come ha fatto questo tipo a trovarmi? Basta usare ICQ?
[B36-W] Se Netstat mi dice che non ho porte aperte posso stare davvero sicuro? (le DLL ponte)
[B37-W] Se ho il client di una backdoor, la mia vittima potrebbe a sua volta entrarmi nel computer?
[B38-W] Cos'è il NETBEUI e il NETBIOS? Come li gestisco con Conseal?
[B39-W] Come ci si potrebbe connettere alle porta 137, 138 o 139?

[B01-M] È possibile far piantare il Mac tramite la rete?

[B01-X] Nella mia macchina Linux ho attivo il servizio di finger. È vero che ci sono rischi?
[B02-X] Con X-Window attivo netstat rileva qualcosa sulla porta 6000.
[B03-X] Ho sentito parlare di PHF, ma cos'è? Una backdoor?
[B04-X] Corro rischi ad ascoltare musica in formato MP3 sul mio sistema Linux?
[B05-X] Certi ftp server sono affetti da un problema di buffer overflow. Come posso verificarlo sul mio sistema?

C - Metodi di difesa
[C01-ALL] Proteggere il sistema - Info generali

[C01-W][9] Come si configura correttamente il Nuke Nabber ?
[C02-W][9] Le componenti di rete, ovvero: cosa tengo e cosa tolgo?
[C03-W][9] Ma se tolgo il Client per reti MS non mi memorizza più la password!!!
[C04-W][9] Quali porte controllare con NukeNabber?
[C05-W] Cosa uso per controllare l'attività di rete del mio computer?
[C06-W][9] Password mantenute in cache
[C07-W] Ho il programma WinTOP dei Kernel Toys. Serve a qualcosa?
[C08-W] È vero che si possono far eseguire dei programmi dannosi allegandoli a un messaggio e-mail?
[C09-W][9] Posso proteggere un file o una directory sotto Windows da accessi indesiderati?
[C10-W] Ho messo sotto controllo la porta 31337. Sono al sicuro?
[C11-W] Ho installato NukeNabber per controllare le porte "sensibili". Sono al sicuro?
[C12-W][9] Back Orifice - Server: configurazione ed installazione
[C13-W] Si può vedere se ho un file "Silkroppato"?
[C14-W] Si può creare un file di log per netstat?
[C15-W] Ho saputo che posso proteggere il mio computer con un programma chiamato Conseal. Quando è utile o inutile questo programma?
[C16-W] Si può disabilitare la funzione di autorun per tutte le unità?
[C17-W][NT] Come impedisco ad altri di amministrare il server NT?

==========

0 - Storia

16/10/1998: v. 0.1 pre-alpha
- Prima apparizione

24/10/1998: v. 0.2 alpha
- Aggiunta [B13], Storia, Disclaimer, Distribuzione, Appello, [C05], [C06]
- Aggiornata [A04], [A02], [B01], [B07]

14/11/1998: v. 0.5 beta 1
- Aggiunta [B15], [B16], [B17], [B18], [C07], [C08], [A05], [B19], [B20], [B21], [B22], [B23], [C09], [PORT-Appendice], [C01a], [B24], [B25], [BD-Appendice]
- Aggiornata [C01], [A01], [B04], [C04], [A03], [B01]

22/11/1998 v. 0.51 beta 2
- Aggiornata [A05], [B01]

04/01/1999 v. 1.0 Official Release
- Aggiunta [LINK-Appendice], [B26], [A06], [C10], [C11], [C12], [B27], [B28], [B29], [B30], [C13], [B31], [C14], [D01], [B32], [B33]
- Aggiornata [PORT-Appendice], [B08]

27/01/1999 v. 2.0 Multiplatform
- Riorganizzazione sezioni:

B09 -> B01-ALL	B15 -> B14-W	B30 -> B25-W	
B16 -> B02-ALL	B18 -> B15-W	B33 -> B26-W	
B17 -> B03-ALL	B19 -> B16-W		
B22 -> B04-ALL	B20 -> B17-W	B21 -> B01-M	
B31 -> B05-ALL	B23 -> B18-W		
	B24 -> B19-W	B32 -> B01-X	
B10 -> B09-W	B25 -> B20-W		
B11 -> B10-W	B26 -> B21-W	C01 -> C01-ALL	
B12 -> B11-W	B27 -> B22-W		
B13 -> B12-W	B28 -> B23-W	C01a-> C01-W	
B14 -> B13-W	B29 -> B24-W		

- Aggiunta Legenda, [D02-ALL], [D03-ALL], [D01-X], [C01-X], [C02-X], [C03-X], [C04-X], [C05-X], [C06-X], [B27-W], [D04-ALL], [C07-X], [C08-X], [C09-X], [D02-W], [D03-W], [D04-W], [D05-W], [E01], [E02], [E03], [C15-W], Legal disclaimer, [B02-X], [B03-X] , [C10-X], [B04-X], [D06-W], [D07-W], [C16-W], [B28-W], [B29-W]
- Aggiornata [B25-W], [PORT-Appendice], [B19-W], [D01-W], Disclaimer, Appello, [A04], [B18-W]

11/07/1999 v. 2.1 Enhanced
- Aggiunta [B30-W], [C11-X], [C12-X], [D02-X], [D03-X], [B06-ALL], [D05-ALL], [WG-Appendice], [A07], [B31-W]
- Aggiornata [C03-X], [B08-W], [PORT-Appendice]

20/08/1999 v. 2.2 Service Release
- Aggiunta [B32-W], [D08-W], [C17-W], [B33-W], [D09-W], [B34-W], [C13-X], [B35-W], [B36-W], [B37-W], [B38-W]
- Aggiornata [D02-ALL]

14/11/1999 v. 2.25 Service Release
- Aggiunta [C14-X], [INTERNET-CAFÈ-Appendice], [FIREWALL-Appendice]
- Aggiornata [A03], [B07-W]

07/05/2000 v. 3.0 Y2K - The Day After
- Aggiunta [A08], [C18-W], [C15-X], [A09], [A10], [A11], [B07-ALL], [B39-W], [NETSCAPE-Appendice], [B05-X], [NETBUS-Appendice], [B08-ALL]
- Aggiornata [PORT-Appendice]

15/10/2000 v. 3.1 Y2K - The Day After
- Aggiunta [B09-ALL], [B10-ALL], [B11-ALL], [C17-X], [C18-X], [C19-X], [D10-W], [A12], [B12-ALL], [B13-ALL], [C20-X]
- Aggiornata [C02-X]

Disclaimer
***
Ogni modifica fatta al sistema, riguardante la configurazione hardware e/o software, è ESCLUSIVAMENTE a rischio e pericolo del lettore di questa FAQ, come pure la responsabilità delle conseguenze di tali modifiche (dato che non posso conoscere le infinite varianti dei sistemi in uso e relative necessità di configurazione, in particolare riguardo la rete eventualmente installata). Se il computer da riconfigurare e/o ripristinare non è il proprio, avvertire il proprietario/responsabile per essere autorizzati a metterci le mani.
Questo riguarda soprattutto macchine usate in ambito lavorativo e/o accademico, ma anche più semplicemente il computer non proprio ma del fratello/cugino/amico/fidanzata/...
Precisazione importante: in questo documento sono citati numerosi programmi (free/share/commerciali). Il fatto che un programma venga citato nel testo della risposta a una FAQ non implica necessariamente il suo uso da parte mia: Security FAQ raccoglie gli interventi più interessanti del newsgroup it.comp.sicurezza.varie e del suo fratello più giovane it.comp.sicurezza.windows, tentando di dare al tutto una forma più organica possibile. Pertanto non posso assicurare di essere in grado di rispondere a quesiti specifici riguardanti questo o quel programma (per esempio la configurazione del firewall X o del server della backdoor Y).
***

Legal disclaimer
***
LO SCOPO DI QUESTO DOCUMENTO È DI RACCOGLIERE I CONCETTI DI BASE PER DIFENDERSI DALLE INTRUSIONI TELEMATICHE E NON DI INCORAGGIARE LE INTRUSIONI STESSE. SI RICORDA CHE L'USO DI PROGRAMMI CONCEPITI PER DANNEGGIARE L'OPERATIVITÀ DI ATTREZZATURE INFORMATICHE È UN REATO, E CHE LE AZIONI DENOMINATE "MAILBOMBING", "NUKE", "FLOOD", "DoS", "BOSERVIZZARE" E PROBABILMENTE ALTRE ANCORA SONO ILLEGALI, ANCHE SE COMPIUTE A SCOPO DIFENSIVO.
SI SCORAGGIANO QUINDI CON MASSIMA DECISIONE LE SUDDETTE PRATICHE, MENTRE È SEMPRE POSSIBILE COMPIERE ESPERIMENTI SU AUTORIZZAZIONE DEI GESTORI DEL SISTEMA UTILIZZATO A TALE SCOPO, DOPO AVER IN VIA PREVENTIVA INFORMATO I GESTORI STESSI DELLA FINALITÀ DELLE PROVE ESEGUITE, DEI RELATIVI PERICOLI E AVER PRESO TUTTE LE PRECAUZIONI POSSIBILI PER NON RENDERE IL SISTEMA VULNERABILE DALL'ESTERNO. LO SCOPO ESCLUSIVO DI "ATTACCHI" CONTROLLATI E AUTORIZZATI È QUELLO DI ACQUISIRE INFORMAZIONI SUL LORO FUNZIONAMENTO AL FINE DI POTER PREVENIRE GLI ATTACCHI STESSI CON PIÙ EFFICACIA.
***

Distribuzione
***
Questo documento può essere incluso in siti web e archivi ftp ad accesso pubblico, nonchè inserito in raccolte su floppy o cd-rom il cui prezzo equivalga il costo del supporto e della duplicazione. Nei casi suddetti di distribuzione autorizzata, avvertitemi all'indirizzo e-mail riportato all'inizio, così da includere l'indirizzo web o ftp nella successiva versione.
Nei casi di distribuzione non autorizzata, contattatemi ugualmente inserendo nella mail il vostro indirizzo IP e la configurazione esatta della vostra macchina (sistema operativo e versione di Winsock), ed eseguite il file che sarà incluso nella risposta <evil grin> >:-]
***

Appello
***
Questo documento non vorrebbe avere un approccio troppo Windows- centrico, ma a causa dell'uso prevalente da parte del suo curatore dell'accoppiata Wintel (e, a giudicare dai messaggi in i.c.s.varie, anche da parte di chi si rivolge al gruppo per chiedere aiuto) la situazione non può essere che questa. È quindi gradito l'invio alla mia e-mail di ogni contributo riguardante problemi di sicurezza e (se esistono) relativi rimedi riguardanti anche altri sistemi, come Amiga, OS/2, Mac, Linux, ...
A causa degli impegni lavorativi, non è garantita una risposta immediata alle mail che riceverò, e di questo mi scuso in anticipo, ma comunque è garantito che risponderò a ogni messaggio che mi arriverà in mailbox.
***

Legenda:

ALL: Tutti i sistemi operativi
W: Windows
  9: Windows 95/95a/95b/95c/98
  95: Windows 95 (tutte le versioni)
  NT: Windows NT (tutte le versioni e SP)
X: Unix/Linux
M: MacOS

==========

[A01] Cos'è un nuke

Sappiamo tutti (in particolare gli utenti Windows) che non esiste il sistema operativo perfetto. È possibile mandare in crisi un sistema operativo connesso in rete inviandogli pacchetti di dati costruiti a regola d'arte, che sfruttino per esempio una cattiva implementazione del protocollo TCP/IP, quello usato in Internet. Gli effetti vanno dal Blue Screen of Death al congelamento totale della macchina (= unico comando funzionante: pulsante di reset hardware).
Un esempio di nuke è dato da un pacchetto con indirizzo IP mittente uguale a quello del destinatario, che cortocircuita la connessione (in pratica, il computer nel rispondere comincia a mandare dati a se stesso), oppure un pacchetto sapientemente frammentato in maniera che le parti si sovrappongano parzialmente. Ovviamente il nuke è fatto su misura e sfrutta le debolezze di uno specifico stack TCP abbinato al suo specifico sistema operativo; quindi il nuke che va bene per Windows non va bene (o almeno non è detto che vada bene) per altri computer, e viceversa nuke che buttano giù altri computer, _forse_ potrebbero anche non buttare giù Windows.

[A02] Vari tipi di attacco

- NesTea, Suffer3, Boink, Land, Oob, Smurf

Si tratta di attacchi di tipo DoS (nulla a che vedere con MS-DOS, la sigla significa Denial of Service, Privazione di Servizio). L'effetto varia da noie sullo schermo in presenza di patch a reset della macchina, a schermi blue sotto Win, a stop dei trasferimenti per intasamento delle connessioni;

- Portscan

Serve a trovare le porte aperte di un host remoto.

[A03] Ma cosa sono queste "porte"?

In un ufficio postale esistono vari sportelli, ognuno dei quali svolge un servizio ben determinato: uno per le raccomandate, uno per i pacchi, uno per i telegrammi, uno per vaglia e conti correnti, uno per il pagamento delle pensioni, ecc...
Analogamente, una macchina connessa alla rete (l'"ufficio postale") ha una serie di porte (gli "sportelli"), ognuna delle quali ha un numero ed è associata a un ben determinato servizio. Gli indirizzi di porta vanno da 0 a 65535, e quelli inferiori a 1024 sono i cosiddetti Well Known Services (Servizi Ben Noti). I più usati sono il 21 per l'ftp, il 23 per telnet, il 25 per smtp (invio di posta), 80 (http, pagine web; molti server usano anche la porta 8080), il 110 per pop3 (ricezione di posta), il 119 per nntp (le news). Il file services (in windows è nella directory C:\<dir. di Windows>\System (*)) li elenca in maniera più dettagliata.

VEDERE [PORT-Appendice] per un elenco con maggiori dettagli (tnx Maurizio!)

Perchè ci si possa collegare a una determinata porta, occorre che sulla macchina ci sia un server in ascolto su di essa. Per esempio, quando riusciamo a spedire una mail a qualcuno, è perchè il server di posta del nostro provider ha un "demone" in ascolto permanente sulla porta 25, mentre se l'invio fallisce significa che quel programma non è in esecuzione (macchina spenta perchè guasta, oppure il programma stesso ha dato i numeri). Ancora, poichè Windows 95 non ha un server telnet di serie (ha solo il client), se proviamo a fare telnet standard verso una macchina Windows 95 il tentativo fallirà perchè non c'è niente in ascolto sulla porta 23.

(*) Su sistemi Win98 potrebbe essere anche sotto C:\

[A04] Differenze fra hackers e altri bei tomi

C'è molta confusione sull'uso della parola hacker, per colpa soprattutto della disinformazione a opera dell'informazione (che paradosso!) TV e stampata e di certa cinematografia. L'hacker nell'immaginario comune è colui che cerca di penetrare in un sistema per buttarlo giù, che nel corso delle sue scorribande provoca comunque dei danni, come per esempio il furto di file di password o altre informazioni riservate. Quello non è un hacker, ma un __cracker__.
L'__hacker__ invece è una persona che anzi non lascia tracce, che se viola la sicurezza di un sistema è per dimostrare di esserne capace.

Un hacker cerca di apprendere sempre di più sulla macchina e sistema operativo che usa (e sugli altri ovviamente). Il suo scopo è quello di vincere certe sfide, e in un certo senso anche di rendersi utile alle sue vittime. L'etica hacker infatti vuole che dopo aver violato un sistema si lasci una traccia, da qualche parte nel sistema stesso, che informi il suo amministratore come è stato possibile entrare e quali falle nella sicurezza sono state sfruttate, cosicchè egli possa tapparle.
I __wannabe__ sono invece coloro che "vorrebbero essere" (wannabe = want to be [voler essere], contrazione americana credo) per esempio hacker, ma che non lo sono. Nei newsgroup un wannabe farà spesso sfoggio di termini tecnici, anche a sproposito, salvo volatilizzarsi o buttarla in rissa quando si cerca di approfondire un argomento che non è in grado di sostenere. Un __lamer__ invece è chi si crede un grande esperto, per esempio di sistemi, mentre in realtà sfrutta solo ciò che gli altri hanno già fatto. Un esempio? Tutti i tipi che si danno arie da hacker solo perchè sono capaci di lanciare il client di Bo (che non sarebbero mai capaci di scrivere, per inciso) e mandare un messaggio pop-up sullo schermo del boservizzato.
Questo e molto altro è spiegato in "The Hackers's Dictionary 3rd.", anche in versione WWW, mentre il testo di riferimento per tutte queste definizioni è il Jargon File, disponibile in formato testo e info in parecchi siti, e la cui home page è:

http://www.ccil.org/jargon/

[A05] Ho sentito parlare di "editor esadecimale", ma non ho capito esattamente cos'è...

I programmi tipo edit.com dell'MS-DOS o NotePad (Blocco Note nella versione italiana) di Windows sono degli editor di testo che permettono di leggere e modificare dei file di testo; ne esistono un'infinità commerciali o free. Gli editor esadecimali sono analoghi concettualmente, ma permettono di leggere e modificare ogni tipo di file, quindi vengono usati per aprire e manipolare dei file binari, come eseguibili (.exe e .com), librerie (.dll), eccetera. Si chiamano editor esadecimali perchè con essi viene visualizzato il valore esadecimale dei byte che costituiscono il file, tipicamente in una parte della finestra, mentre nell'altra viene mostrata la sequenza di caratteri corrispondenti (se stampabili a schermo).
Un editor esadecimale è un programma semplice ma potentissimo, perchè permette di fare praticamente tutto su ogni file, e l'unica condizione è di sapere ESATTAMENTE cosa si fa. Questo significa che, se volessimo cambiare la scritta "Avvio di Windows..." che appare al boot o la scritta "Avvio" o "Start" sul pulsante di avvio, dovremmo aprire il file giusto (nel secondo caso explorer.exe) con un editor esadecimale, posizionarci nel punto in cui è memorizzata la stringa e cambiarla. Inutile dire che l'uso di tali programmi è pericolosissimo se fatto per puro cazzeggio, dato che un file binario modificato "alla cieca" diventa con altissima probabilità inutilizzabile.
Per le sue caratteristiche, gli editor esadecimali si prestano anche ad usi non "politicamente corretti" (eufemismo), come sprotezione di programmi, camuffamento rispetto ad antivirus e programmi di monitoraggio in genere, e così via.

[A06] Cos'è un firewall?

È un software. Può girare su macchinette speciali ridotte al minimo, nel qual caso ti vendono un mattoncino hardware con dentro il software su (E)EPROM.
Alternativamente, può girare su un "server" apposito, tipo Linux (v., per esempio, www.debian.org, www.suse.com, www.slackware.org, ecc.).
In tutti i casi è un programma che effettua quattro funzioni:

1) INPUT: determina cosa può ARRIVARE
2) OUTPUT: determina cosa può USCIRE
3) FORWARDING: prende un pacchetto in arrivo dall'interno e lo butta fuori, o viceversa
4) MASQUERADING: prende pacchetti dall'interno e li butta fuori, ma, contemporaneamente, maschera l'indirizzo di partenza, mettendo il proprio. Quando arriva una risposta a lui, cambia l'indirizzo del destinatario, mettendo quello della macchina originaria:

PC protetto: "Da PC1 a WWW.ALTAVISTA.COM, HELLO" --> Firewall
Firewall: "Da FIREWALL a WWW.ALTAVISTA.COM, HELLO" --> Altavista
Altavista: "Da Altavista a Firewall, TI SENTO" --> Firewall
Firewall: "Da Altavista a PC1, TI SENTO" --> PC Protetto

Nel caso di pacchetti DIRETTI

Nemico: "Da NEMICO a PC1, MUORI" --> Firewall
Firewall (opzione 1): (niente)
Firewall (opzione 2): "NESSUN PC1 PRESENTE" --> Nemico

Firewall (opzione 3): "MUORI TE, CAATA!" --> Nemico (crash!)

...le opzioni 2 e soprattutto 3 non sono fornite di serie 8-D

In ogni caso, anche con opzione 1, al server non capita nulla.
Naturalmente, il firewall deve essere in grado di resistere ad un attacco diretto contro di lui.

*** (C) Leonardo Serni

[A07] Che informazioni si possono ricavare dall'e-mail?

Dipende da vari fattori.
Se il msg anonimo è stato mandato attraverso uno dei tanti siti di anomyzer presenti sulla rete allora non si può ottenere nulla. Nel caso invece dei vari mail-bomber, si può risalire all'IP di origine semplicemente cercando negli header del messaggio. La procedura non è la stessa per tutti i programmi di posta.
Per quel che mi riguarda, sul mio fidato Netscape Messenger, View -> Headers -> All; se usate Outlook "sono fatti vostri")TM Raz Degan - o, meglio, chi gliela scrisse)... scherzo!!! Cliccare due volte sul msg e poi nel menu della finestra che appare clicchare Visualizza e poi Opzioni.
In ogni caso, fare attenzione all'ultimo RECEIVED dove viene indicato tra parentesi accanto al nome del server d'appoggio anche l'ip di chi lo manda. Sempre però che non si appoggi ad un server anonimo o ad i siti sopra descritti oppure che abbia inviato direttamente dal server di mail con una sessione telnet.
In quest'ultimo caso, non è detto che al destinatario compaia l'IP del mittente. Infatti in rete si trovano dei sendmail mal configurati. Collegandosi con telnet e usando il comando HELO senza presentarsi, la mail inviata risulterà anonima. Nel caso invece di un remailer anonimo, nell'header si leggeràanell'ultimo received il remailer e da lì in poi è impossibile proseguire.

[A08] Cosa sono i cookies?

Sono molti ormai i siti che fanno uso di questi file. Il cookie è una informazione originata dal server a cui ci si connette, che poi gli viene rispedita pari pari. È come il biglietto dei famosi "salvacoda" nei negozi: serve così che il negoziante possa sapere se è il tuo turno o no, ma non dice nulla su come ti chiami o quanti soldi hai in tasca.
PERÒ, se quel biglietto te lo appunti al bavero, chiunque potràsapere che ti servi in quel negozio.
Per esempio: se ci colleghiamo ad Amazon, la libreria virtuale, questa può mandarci una cosa tipo

> Set-Cookie:ID=298934538; path=/; domain=www.amazon.com

il browser a questo punto ogni volta che si RICOLLEGA a Amazon manda il msg "Cookie:ID=298934538", cosicchè Amazon, avendo un database, saprà cosa abbiamo acquistato la volta precedente e si regolerà di conseguenza.
Dove c'entra la privacy in tutto questo? Bè, se "domain" è per esempio

> Set-Cookie:ID=298934538; path=/; domain=.amazon.com

il cookie non lo mandiamo solo connettendoci a www.amazon.com, ma anche a mail.amazon.com (se esistesse!), così che saprebbero che ti colleghi ad Amazon appunto. Se domain= fosse vuoto, QUALSIASI web server a cui ci si collegasse verrebbe "informato" che siamo clienti di Amazon. Se poi il web server fa qualcosa con questa informazione è cosa aperta alla discussione.
E facciamo un esempio limite: dopo aver fatto login su www.sex.com, quel server manda un cookie

> Set-Cookie:User=Nome&Pass=pass&Email=email; path=/; domain=.com

...questo cookie viene rispedito a _qualsiasi_ server .com, e contiene i nostri dati di email, password e quant'altro. È utile aggiungere che questo è possibile soltanto se l'agent, cioè il browser, non rispetta certe regole di sicurezza. Secondo le specifiche della RFC 2109 i Set-Cookie che hanno un campo domain privo di "embedded dot" devono essere automaticamente rifiutati. Ad esempio, Netscape rispetta questa specifica rifiutando campi domain con meno di 2 dot.
Non è quindi possibile, mediante un cookie, sapere cos'abbiamo sull'HD. Per farlo occorrerebbe che un software GIÀ PRESENTE sul nostro PC aggiungesse, alla lista dei cookies per un certo server, dei dati relativi a quel che abbiamo sull'HD, per esempio

> Software=MSWord60&ID=198345-9283&User=John+Q.+Glen

...ma se così fosse, disattivare i cookies NON SERVIREBBE A NIENTE, dal momento che la "protezione cookie" agisce contro i cookies IN ARRIVO, ma non impedisce l'invio di cookies DAL PC, verso il server.
Con le recenti versioni di Netscape e IE, però, disabilitando completamente i cookie si dovrebbe essere in grado di inibire anche la loro trasmissione, non solo l'accettazione: ai server viene impedita la lettura di eventuali cookie salvati su disco. O almeno così sostengono le guide. Tecnicamente, il campo HTTP_COOKIE non dovrebbe essere popolato di dati.

[A09] Che cos'è la redirezione delle porte?

L'IP redirect significa (per esempio) che il lamer si collega alla TUA porta 7654 ed è COME SE fosse connesso alla porta 6667 di irc.tin.it; e può fare IRC con il tuo IP - perchè sei TU che sei connesso a irc.tin.it, e non lui.
E se qualcuno manda un nuke, sei TU quello che se lo becca. Il lamer si limita a ricollegarsi ad un'altra vittima.
Questo naturalmente nell'ipotesi che la tua macchina invii a irc.tin.it quello che il lamer le manda (e gli invii le risposte), senza metterci, come dire?, del suo ;-) (vedi [C16-X]).

[A10] Cos'è Telnet? Di quali comandi dispone?

Telnet è un protocollo di emulazione terminale che permette di avere accesso a una macchina remota su cui gira un "server telnet", come il telnetd delle macchine Unix. Ovviamente l'accesso è permesso oppure no a seconda che l'utente che prova a collegarsi in questo modo abbia o meno certe autorizzazioni, proprio come se tentasse di accedere localmente. La connessione standard avviene sulla porta 23/TCP, ma indicando altre porte (sempre TCP) è possibile usare pressochè ogni servizio basato su TCP, come FTP, posta e news.
In pratica telnet è un protocollo "di livello più basso", che rende disponibile un mezzo (più precisamente, una "shell") per poter usare protocolli più complessi come appunto quelli citati sopra. I comandi che è possibile usare variano quindi a seconda del servizio che si utilizza tramite telnet. In ogni caso telnet stesso è un servizio (usato per accedere a macchine remote) e dispone quindi di un insieme di propri comandi:

clos	chiudi la connessione in corso
logout	termina la sessione utente remoto e chiudi la connessione
display	mostra i parametri operativi
mode	tenta dientrare il modo linea o carattere ('mode ?' per altre informazioni)
open	connetti a un sito
quit	esci da telnet
send	trasmetti caratteri speciali ('send ?' per altre informazioni)
set	imposta parametri operativi ('set ?' per altre informazioni)
unset	azzera parametri operativi ('unset ?' per altre informazioni)
status	stampa informazioni di stato
toggle	inverti il valore dei parametri operativi ('toggle ?' per altre informazioni)
slc	cambia stato dei caratteri speciali ('slc ?' per altre informazioni)
z	sospendi telnet
!	invoca una subshell
environ	cambia variabili di ambiente ('environ ?' per altre informazioni)
?	stampa informazioni di aiuto

Esistono tantissimi client telnet, più o meno completi. Windows dispone di un programma telnet di serie, molto scarno a dire la verità, è in finestra grafica ma bisogna lanciarlo dal prompt DOS (o da Avvio/Start -> esegui) scrivendo "telnet <nome_server>" o "telnet indirizzo_IP>", oppure solo "telnet". In quest'ultimo caso, dal menù della finestra che si apre si può scegliere il server remoto e anche la porta da usare (il default è la 23), oltre ad alcune (poche) opzioni. Su Linux il comando è lo stesso con la differenza che il funzionamento è in modalità carattere ("man telnet" farà accedere in questo caso a tutte le informazioni possibili).
Per quel che riguarda l'ambiente Windows, potrebbe essere necessario un maggior controllo sui parametri di funzionamento di telnet. In tal caso ottime alternative sono NetTerm (shareware), TeraTerm (freeware) e QVT Term (http://tucows.thebrain.net/adnload/dlqvtterm.html).

[A11] È possibile limitare l'accesso a file/directory contenenti informazioni private?

Bisogna distinguere diversi casi.
Sistemi Windows 9x: Qualunque cosa vi possa essere detta, la risposta in questo caso è ASSOLUTAMENTE NO. Windows 95 e 98 si basano ancora sul file system FAT tipico del sistema MS-DOS su cui questi Windows (come del resto il precedente Windows 3.xx) sono costruiti. Il file system è in pratica il modo in cui le informazioni sono

organizzate sul disco (rigido, floppy, ZIP, ecc.) e ogni sistema operativo ha il proprio. MS-DOS e i Windows fino al 98 compreso sono sistemi operativi monoutente (non confondete il multitasking con la multiutenza), cioè sono pensati per l'uso da parte di un solo utente. La conseguenza è che nè il sistema operativo nè il file system possiedono meccanismi di protezione dei dati a livello di utente o di file. Chi ha accesso alla tastiera può fare qualunque cosa. Esistono in realtà programmi per impostare un accesso con password a file o cartelle in vari modi, ma tutti sono aggirabili facendo reboot da floppy (se non è stato disabilitato da BIOS). In altri termini, un sistema Windows 9x è sostanzialmente indifendibile da questo punto di vista, e l'unico appiglio è la crittografia: appositi programmi criptano un file o una partizione, decrittandola "al volo" in caso di accesso (previa immissione di password). Il rischio è quello di perdere i dati così protetti in caso di errori di vario tipo, come un cluster rovinato sull'hard disk. Un programma che fa questo è PGP Disk.
Sistemi Windows NT/2000: La famiglia NT è stata concepita anche per supportare la multiutenza, e perciò fornisce un sistema di account e di gestione di permessi adatto allo scopo. La condizione è che i dati da proteggere devono trovarsi in una partizione NTFS, in quanto le partizioni FAT, come detto sopra, non forniscono il supporto ai meccanismi di protezione. Senza voler entrare in guerre di religione fra sostenitori dei vari sistemi operativi (confrontare il gruppo it.comp.os.discussioni :-)), diciamo che il principale svantaggio di Windows NT, oltre al costo, è dato dalle risorse hardware molto generose di cui ha bisogno, di solito sproporzionate per utenti non aziendali.
Sistemi Unix: Storicamente i primi sistemi operativi pensati per la multiutenza (il progenitore risale ai primi anni '70). I file sono dotati di attributi che consentono di regolamentarne l'accesso, mentre gli utenti sono suddivisi in gruppi a cui si può associare il diritto di eseguire determinate azioni (un utente può far parte di più gruppi). Impostando in modo opportuno i permessi dei file e l'appartenenza di ogni account a uno o più gruppi è possibile concedere o negare gli accessi a livello di file e di utente (in maniera, per così dire, "bidimensionale"). Dal momento che esistono diversi Unix, non necessariamente uguali in tutto, non è il caso di andare più in dettaglio a questo punto. Tra i vari Unix apparsi nel tempo un posto speciale ha naturalmente Linux, sia a causa della sua gratuità che dei requisiti di sistema richiesti, generalmente non elevati se non si usa intensamente X. Ovviamente, per quello che riguarda questa discussione, Linux è assolutamente analogo ai suoi parenti.

[A12] Che cosa sono gli indirizzi 0.0.0.0 e *:*?

Con queste notazioni particolari si intende "tutti gli indirizzi IP".
Un programma in attesa di connessioni che provengano da un indirizzo IP qualunque genererà nell'output di netstat una riga del tipo

TCP 127.0.0.1:<porta> 0.0.0.0 LISTENING

Come esempio ecco l'output del comando "netstat -na" sul mio sistema in un qualsiasi momento senza connessione Internet:

C:\WINDOWS>netstat -na

Connessioni attive

Proto	Indirizzo locale	Indirizzo remoto	Stato
TCP	0.0.0.0:119	0.0.0.0:0	LISTENING
TCP	192.168.100.1:137	0.0.0.0:0	LISTENING
TCP	192.168.100.1:138	0.0.0.0:0	LISTENING
TCP	192.168.100.1:139	0.0.0.0:0	LISTENING
UDP	192.168.100.1:137	*:*	
UDP	192.168.100.1:138	*:*	

C:\WINDOWS>

La prima riga si riferisce al newsserver locale Hamster, in ascolto sulla porta 119, le altre al Netbios. Da notare i diversi indirizzi locali: Hamster è in ascolto su qualsiasi indirizzo, mentre NetBIOS ascolta solo sull'indirizzo IP associato alla scheda di rete (avere NetBIOS aperto anche sull'interfaccia di Accesso Remoto è Male, come spiegato in [B17-W] e seguenti). La notazione *:* è usata per il protocollo UDP, che non ha il concetto di connessione.

==========

[B01-ALL] Scoprire trojan in generale.

Un metodo applicabile a questo tipo di trojan client-server è quello di installare il client e di provare a contattare il server, dando l'indirizzo IP 127.0.0.1, che corrisponde appunto alla macchina locale (localhost). Se il client ottiene una risposta, avete trovato il server che andràrimosso prontamente.

[B02-ALL] Ma cosa può passare da 'ste benedette porte?

Le porte comunemente utilizzate sono elencate alla faq [A03], mentre altre sulle quali si verificano spesso degli attacchi sono riportate alla faq [C04-W]. È importante però sapere che il tipo di attacco che si può condurre (e quindi i pericoli che si corrono) su una porta aperta dipende da cosa risiede su quella porta, cioè dal server in ascolto su di essa.
Non bisogna però farsi prendere dalla frenesia di chiudere tutte le porte. Infatti, se una porta è aperta è (normalmente) perchè ci deve passare qualche dato "legittimo", come la porta 80 su macchine che ospitano un server web. In generale, prima di chiudere una porta bisogna sapere perchè sia aperta; per esempio, il famigerato ICQ apre una porta per ogni comunicazione che ha in corso, e queste non cadono nell'intervallo WKP, formato dalle porte <1024. È possibile rendersene conto aprendo una shell MS-DOS con ICQ attivo e scrivendo il comando "netstat -na" (senza virgolette) che mostreràtutte le porte attive e l'indirizzo remoto a cui sono connesse, oltre allo stato della connessione ("netstat /?" per avere tutte le opzioni).

[B03-ALL] Può un intruso conoscere quello che scrivo sulla tastiera?

Sì . Per far questo però è necessario che l'intruso riesca a far eseguire sul computer da spiare un "server" che intercetti la tastiera e memorizzi i tasti a mano a mano che vengono premuti, e a intervalli più o meno regolari (o a ogni connessione) li invii al "pirata", per esempio alla sua e-mail. La regola è quindi sempre un controllo assiduo di quello che gira sul proprio computer, con il programma AVP System Watcher (http://www.avp.it) o anche il WinTop dei Kernel Toys (se si usa Windows 9x). Se sul computer è stato installato il server di Back Orifice, tale funzione è svolta dal file windll.dll (fra le altre).

[B04-ALL] È possibile che qualcuno riesca a navigare "sembrando me"?

È in effetti possibile. Questi simpaticoni cercano di connettersi alla porta 1080, dove potrebbe esserci in ascolto un proxy socket. Se riesce nell'intento il tuo computer può essere usato dall'attaccante come proxy im modo che il suo computer venga "nascosto" all'esterno e tutte le operazioni che compirà risulteranno effettuate dal computer attaccato.

[B05-ALL] Con tecniche di IP spoofing si riesce facilmente a falsificare l'indirizzo IP di una macchina?

In altre parole:
Se faccio il traceroute dell'indirizzo finto, dovrei comunque riuscire a risalire la catena dei router attraversati fino al finto, oppure risalgo la catena fino all'IP vero?
Fai il traceroute VERO dell'indirizzo FINTO. In teoria, se i vari routers avessero un pò di ingegno, non potresti fare neanche spoofing (o quasi).

In pratica può succedere questo:

```
A(F) ---> B ---> C ---> D
                 /
F ---> E --->--+
```

A ti manda un pacchetto fingendosi F. B, che controlla la sottorete A, ed in teoria non dovrebbe veder passare pacchetti DA F verso "NON A", invece passa questo strano pacchetto "F verso D". Lo stesso fa C, che "dovrebbe" vedere arrivare i pacchetti di F solo da E (ma C non può sapere se F sia anche collegato o no a B).

D si vede arrivare un pacchetto da un certo "F" che arriva da "C", di cui si fida e che in passato gli ha mandato pacchetti veri di F.

Un traceroute D-->F rivela: D, C, E, F ... B e A sono rimasti fuori.

È possibile naturalmente sapere se F stia originando una connessione con D. A non può impedirlo (a meno di cagar bulloni e avere la sfera di vero cristallo del mago Zurlì ; o a meno che D o F siano Windows :-)).

Però, sapere che quel pacchetto "F->D" è spoofato non ti fa trovare A.

Se hai dei sospetti, puoi verificarli in maniera induttiva :-), ma se non hai dei sospetti in particolare, o se A dispone di software adatto (credo vada bene Aggressor per Windows, o qualsiasi cosa per Linux :-)), fine.

*** (C) Leonardo

[B06-ALL] È vulnerabile una macchina su cui gira un X-server?

X-Window, l'ambiente grafico degli Unix, si basa sul paradigma client/ server. Se su un server Unix gira un programma grafico, questo è il CLIENT di X, e X stesso può produrre l'output su una qualunque altra macchina collegata al server. Tali macchine sono di solito i client, e perchè quest'architettura funzioni esse devono avere in esecuzione un X SERVER (quindi si ha in questo caso un'inversione dei ruoli, con il client che offre un servizio al server - spiegazione terra terra, ma spero che me la passiate). Le comunicazioni fra l'X client (il programma in esecuzione sul server) e l'X server (programma che riceve le richieste dal programma client e le traduce in operazioni grafiche sulla propria macchina, che può essere Unix, Windows o qualunque altra), si svolgono attraverso la posta 6000 TCP.
La lunga introduzione serviva a spiegare perchè X-Window può essere un punto delicato per la sicurezza di un sistema, quando invece si occupa di primitive grafiche che (apparentemente, almeno in questo caso) con le reti non c'entrano niente. Il punto è che se la porta 6000 del client (su cui ricordiamo che gira l'X SERVER) è aperta verso la rete per i traffici client/server di X, e non è protetta, da qualunque macchina della rete si può trasmettere e operare sulla macchina che ha l'X SERVER stesso. Se quindi sul proprio computer è installato un X server, anche la porta 6000 TCP va controllata.
Attenzione: non è detto che le finestre generate da un X server si possano distinguere visivamente da quelle di Windows (tipo "Ma sul mio computer io non vedo le tipiche finestre 'tipo X', ma solo normali finestre Windows, quindi non dovrei avere un X server"). Infatti esistono implementazioni X per Windows che utilizzano le comuni API Windows per la manipolazione dell'interfaccia. Quindi questo non vuol dire necessariamente che non sia X.
Inoltre non è neanche necessario che l'attacco che parte da un altro client passi attraverso il server Unix. Infatti queste connessioni possono passare direttamente da una macchina all'altra. Se la porta 6000 accetta connessioni da ogni dove basta, da qualunque macchina, dare un comando seguito da (sotto Unix) "-display ip_macchina" per farlo apparire lì . Inoltre il server Unix non ha alcun "potere di veto". Questo dipende invece dall'X server che gira sulla macchina (magari Windows) attaccata. Bisogna cercare i settaggi di quest'ultimo relativi alla porta o se è disponibile qualcosa simile a xhost, un comando che sotto Unix regola gli accessi alla 6000 con autenticazione basata su IP.
Per controllare la vulnerabilità del proprio X server bisogna tentare di aprire delle connessioni sulla porta 6000: questo si ottiene lanciando da qualche altra macchina un processo che abbia display sul computer da testare. Se l'esperimento riesce, vuol dire che la porta 6000 della macchina controllata è accessibile da fuori.

[B07-ALL] È possibile che un trojan/virus effettui telefonate a mia insaputa?

[Questa non c'entra molto con la sicurezza. L'ho inserita perchè ultimamente nei gruppi di sicurezza è stata postata molte volte in varie salse].

Sì e no. Nel senso che è ovviamente possibile utilizzare le funzioni API di Accesso Remoto per creare nuove connessioni e/o comporre numeri di telefono via software, ma nella maggior parte dei casi responsabili di questo comportamento sono dei programmi scaricabili da alcuni tipi di siti (erotici, ma non solo - vedi archivi .mp3 ecc.) che promettono una maggiore velocità di accesso e di download dai rispettivi siti se utilizzati per la connessione al posto dell'Accesso Remoto standard, nonchè una presunta "gratuità' dei servizi così utilizzati.
Questi programmi non sono altro che dei "dialer", cioè software "di chiamata": in pratica compongono un numero telefonico, di solito intercontinentale, sostituendosi ad Accesso Remoto o cambiano le impostazioni di Accesso Remoto in modo che non venga più chiamato il provider locale ma il suddetto numero intercontinentale. La gratuità del programma e dei servizi relativi, nonchè le virgolette che ho usato nel paragrafo precedente, si spiegano con il fatto che questi siti si pagano indirettamente tramite una percentuale sul traffico generato sulla linea utilizzata, che la locale compagnia telefonica accredita appunto ai gestori del sito (in pratica, il meccanismo dei 144 e 166 italiani).
È sbagliato utilizzare il termine "virus" per questi programmi così come è sbagliato pretendere che gli antivirus vengano istruiti per riconoscerli, perchè non si tratta di virus, ma di applicazioni utente perfettamente "legittime" (anche se al limite della truffa) e di solito scaricate e installate volontariamente dalle vittime. L'unico modo

ragionevole per non trovarsi nelle condizioni di pagare bollette di milioni è quello anzitutto di non scaricarli/installarli (pare logico, no?), poi quello di controllare la cartella di Accesso Remoto e le proprietà delle connessioni esistenti AL PRIMO DUBBIO. Utili accorgimenti sono quelli di non azzerare del tutto il volume del modem in modo da accorgersi subito se il numero composto è più lungo o comunque diverso dal solito (fidatevi, dopo poche connessioni la sequenza di impulsi prima e di toni poi mi era già familiare, e quando cambiai provider, impiegai ugualmente non più di pochi giorni per abituarmi al nuovo numero), e di NON SALVARE LA PASSWORD della connessione, in modo che la sequenza di connessione non si completi automaticamente; in tal caso, una connessione che vada su senza richiesta di password dovrebbe ugualmente destare allarme.

[B08-ALL] Nel settaggio di un programma di monitoraggio della rete, quali porte remote conviene ignorare?

- la porta 25 del server dove mandate la posta
- la porta 110 del server da dove la ricevete
- le porte 3128 e 8080 dei proxies che usate
- le connessioni alle porte 80 e 443 di un sito remoto
  da porte fra 1025 e 5000 (locali) dell'indirizzo 0.0.0.0/0.0.0.0

Queste porte remote appartengono infatti a servizi standard. Il lato negativo di tutto ciò è che è sempre possibile, naturalmente, che un attaccante remoto usi una di tali porte per i propri tentativi, proprio perchè il loro uso "standard" è ben conosciuto. Occorre quindi valutare caso per caso se è più conveniente monitorare o ignorare pacchetti/connessioni provenienti dalle porte suddette, anche tenendo conto dell'uso della macchina che vogliamo tenere sotto controllo.

[B09-ALL] Cos'è "smurf"?

Smurf ("puffo") è un attacco indipendente dalla piattaforma che consiste nell'esaurire la banda a disposizione della vittima (quindi un DoS). In pratica viene attuato facendo sì che un gran numero di macchine in rete invii dei pacchetti alla macchina bersaglio in risposta a richieste mai fatte, o meglio fatte dall'attaccante a nome della vittima. Il modo in cui ciò avviene: mandare dei PING con l'indirizzo IP della vittima a degli indirizzi IP "multicast" di reti non bene amministrate, che vengono ricevuti dai gateway delle suddette reti. Questi, che di solito smistano il traffico in arrivo agli host che ne sono effettivi destinatari, ricevendo un pacchetto broadcast lo inoltrano a tutte le macchine facenti parte della sottorete, che vedendosi arrivare un PING rispondono con il relativo pacchetto PONG. Il traffico così generato subisce un'amplificazione che può anche essere molto grande, in quanto la vittima riceve le risposte da tutte le macchine della rete pingata. Se l'attaccante inoltra una serie di PING di questo tipo non ad una sola rete ma a molte (e gli elenchi di reti che si prestano a questi attacchi sono disponibili in rete, se si cercano bene - NON ME LI CHIEDETE, NON LI CONOSCO!!!), ecco che con una banda a disposizione anche non grandissima si può generare verso la vittima un volume di traffico sufficiente per travolgerlo e in pratica isolarlo da Internet. La vittima non può fare nulla per difendersi, perchè non può controllare il traffico che arriva dalla sua connessione, e il filtraggio dei pacchetti (fondamentale in caso di attacchi di altro tipo) è del tutto inutile in questo caso, in quanto il problema non è nel tipo dei pacchetti ricevuti ma nel loro numero, ed essi devono comunque essere ricevuti per essere gestiti, cioè inoltrati o scartati. La soluzione, come dicono i politici, "è a monte", nel senso che il filtro dev'essere a livello dell'upstream, cioè del provider (nel caso di utenza domestica), o in generale del fornitore di connettività Questo tipo di collaborazione, manco a dirlo, è estremamente rara e inesistente nel caso di connessioni via modem di utenti "privati".
Come si può realizzare tutto questo? Per Linux esistono programmi appositi, mentre in ambiente Windows esiste per esempio "Aggressor Exploit Generator" (www.aggressor.net x info).

[B10-ALL] Cos'è l'IP spoofing?

È una tecnica che consiste nel creare pacchetti IP contenenti nel campo indirizzo un valore diverso da quello del proprio indirizzo IP vero. Ciò può esser fatto riconfigurando l'interfaccia di rete o programmando un router in modo che riscriva l'IP del server sui pacchetti in uscita (esistono anche dei programmi che consentono di comporre pacchetti IP in maniera completamente libera, ma solo sotto Linux in quanto lo stack TCP/IP nativo di Windows non consente questa libertà, anche se è possibile aggirare la limitazione).
In questo modo tutti i pacchetti risulteranno provenire da un altro IP, arbitrario. Una conseguenza di questa operazione è che dopo non funzionerà più alcuna applicazione di rete, proprio nessuna nessuna, neanche per sbaglio, neanche una volta ogni tanto. Si possono sempre *inviare* pacchetti, però non arriverà mai alcuna risposta. Per certi scopi la cosa può anche essere accettabile, se non interessa che le risposte arrivino, nel caso per esempio di attacchi smurf (vedi B09-ALL).

(adattato da un post di Leo)

[B11-ALL] Come fa il sito che ho visitato a farmi vedere il contenuto del mio desktop/C:?

> E soprattutto, sono solo io che riesco a guardare l'interno del disco o anche chi gestisce il sito?

Risposta:
Sei solo tu a vedere l'interno del disco... Nella pagina HTML c'e un link del tipo clicca qui per vedere il contenuto del MIO disco. Questa non è prerogativa del solo Windows:

<a href="file:///"> o <a href="file:///dev/mouse"> sono validi esempi. Il concetto importante comunque è che ognuno che si connette vede il PROPRIO desktop, o radice, o quel che è, dato che il link non fa altro che puntare a un URL locale la cui esistenza deve essere ragionevolmente probabile sulla macchina del navigatore, come per esempio c:\windows\desktop o la cartella Internet Temporary Files (ma provate a far seguire a me un link alla seconda...). Nonostante possa far impressione vedere il contenuto del proprio desktop in seguito al clic su un link contenuto in un sito Web, bisogna ricordarsi sempre che il sito stesso non ha letto il contenuto del proprio hard disk nè ha la possibilitàdi farlo: se un altro navigatore cliccasse sullo stesso link, vedrebbe delle informazioni diverse, e se questo non avesse Windows otterrebbe solo un messaggio di errore dal browser.

[B12-ALL] È possibile sconnettere il modem "da fuori"?

Sì , inviando o facendo in modo che la vittima invii un pacchetto contenente la stringa +++ATH0 (la cifra ZERO), per esempio in IRC:

//raw PRIVMSG Nick/#chan : $+ $chr(1) $+ PING +++ATH0 $+ $chr(1)

Questo è dovuto a un bug di alcuni modem. Per proteggersi da questo DoS bisogna impostare ATS2=255 nei settaggi del modem:

Avvio -> Impostazioni -> Pannello di controllo -> Modem -> Proprietàmodem -> Connessione -> Avanzate -> Altre impostazioni : inserire S2=255.

Per quanto riguarda IRC bisogna che il client risponda con un Ping reply +++ATH0, comunque le ultime versioni del mIRC dovrebbero essere patchate a dovere.

Il bug non è di IRC o qualche altro protocollo particolare, ma è dovuto proprio a questa determinata STRINGA che attraversa il modem, che sia un PING reply di IRC, una username per FTP, o una risposta echo ICMP.

*** (C) Frankj ***

[B13-ALL] Perchè ricevo dei ping sulla porta 113 quando scarico la posta?

Semplicemente, il gestore dell'account di posta si informa su chi sei TU, cosa che si può fare semplicemente connettendosi alla porta 113, servizio ident. Ma siccome tu non hai il servizio ident, hai la porta 113 chiusa per default. Per evitare i warning emessi dai firewall, si deve aprirla ponendo su di essa un demone ident di controllo, come per esempio quello incluso in mIRC (molti server IRC, fra l'altro, permettono di connettersi ad essi solo se la loro richiesta sulla 113 viene soddisfatta).

[B01-W][9] Cos'è Bo?

È un programma cosiddetto trojan, che permette intrusioni indesiderate nel proprio computer. BO è l'acronimo di Back Orifice, nome che irride il prodotto Back Office di Microsoft, oltre ad essere molto esplicito sulla parte del corpo che duole dopo esserselo installato :-))). Esso si compone di un client e di un server, quest'ultimo dev'essere installato sul computer della vittima, dopodichè il client permette al "buon samaritano" che lo possiede, e a chiunque abbia il client installato, di compiere varie operazioni sul computer "boservizzato" (viene indicato in questo modo un computer che abbia installato il server). Le operazioni possono essere le più svariate, dal trasferimento di file all'esecuzione di programmi, alla lettura di informazioni contenute nei dischi (fissi, cd-rom, zip, ...).
Bo fa parte della categoria delle backdoor. In effetti, nel sito Web dei creatori di Back Orifice (il gruppo Cult of the Dead Cow, http://www.cultdeadcow.com), esso è definito come un programma di controllo a distanza. Da notare che esso funziona perfettamente sia sotto Windows 95 che sotto Windows 98, mentre non se ne conosce ancora

una versione per Windows NT.

[B02-W] Ma cos'è un trojan?

Un trojan, da non confondere con i virus che sono un'altra cosa, è un programma che si nasconde sotto le mentite spoglie di un altro programma. Per esempio l'autoinstallante che si spaccia come un fantastico screen saver con il filmato di Pamela. Oltre al Bo rientrano in questa categoria anche programmi come NetBus e TeleCommando. Il nome ovviamente deriva dal mitico Cavallo di Troia, che dentro l'apparenza di un dono di pace celava gli uomini che avrebbero distrutto la cittàstessa.

[B03-W][9] Infettare con il Bo

Il veicolo di trasmissione di Bo è un programma chiamato SilkRope. Esso incapsula il server di Bo in un altro programma in maniera apparentemente invisibile, a meno di non aprirlo con un editor, e lo installa quando il programma viene eseguito (ecco il parallelo col Cavallo di Troia). È questa caratteristica che giustifica il fatto di considerare Back Orifice un trojan, oltre che una backdoor.

[B04-W][9] SilkRope? E che d'è?

Dati due programmi a 32 bit li fonde in un unico programma che quando viene eseguito lancia i due originari. Il programma in sè non è pericoloso, dato che esso può fondere due eseguibili a 32 bit qualunque. In tutti i casi in cui sull'hard disk è presente un eseguibile formato da due programmi uniti con SilkRope, un controllo antivirus potrebbe dare comunque l'allarme, anche se i due programmi sono perfettamente innocui.

[B05-W][9] Cosa si fa con BO

È possibile eseguire operazioni remote sul computer boservizzato come se si stesse operando direttamente su di esso. Bo mette in grado il suo utilizzatore anche di conoscere eventuali password digitate, intercettando la tastiera (funzione svolta dal file windll.dll). Si può anche aprire la porta 23, quella del telnet, sul PC boservizzato. In tal caso è possibile avere una shell sul computer della vittima, esattamente come se si telnettasse su sistemi Unix, utilizzando però il command.com del DOS invece delle shell Unix come bash.

[B06-W][9] Come faccio a sapere se ho il Bo?

Di certo non leggendo la finestra che appare premendo CTRL-ALT-DEL. Bo usa una funzione dell'API di Windows che serve a nascondere il processo che la chiama. "Nascondere" vuol dire appunto che non si vede nella taskbar nè nella finestra che appare premendo CTRL-ALT-DEL. Mentre si è in linea, aprite una finestra DOS e lanciate il comando netstat -na. Questo mostrerà tutte le connessioni attive in quel momento (aggiungere un numero per specificare un controllo periodico ogni <X> secondi): se fra esse ce n'è una sulla porta 31337, è lui! Questo non esaurisce l'argomento, dato che la porta è configurabile e quindi può essere cambiata da chi tenta di introdursi nelle macchine altrui. Naturalmente l'infame può decidere di manifestarsi apertamente, con messaggi pop-up, e in tal caso non c'è dubbio. Un programma utile al controllo è AVP System Watcher (http://www.avp.it, freeware), che controlla il sistema alla ricerca di BO.
Antigen è un altro programma per eliminare il Boserve nella forma di default. In ogni caso, anche se il Boserve che vi siete ritrovati sull'HD ha nome e porta di comunicazione differenti, Antigen non riesce a rimuoverlo ma vi rivela comunque la sua presenza e lo disattiva sino al seguente reboot (non riesce a cancellare l'exe del bo in versione non default e la seguente chiamata dal registro di Win).

[B07-W][9] Ho scoperto di avere Bo, come lo tolgo?

Si può fare anche a mano. Cercare e cancellare il file " .exe" (sì , il nome del file è uno spazio) e windll.dll. Il primo è il server vero e proprio. Cercare comunque la stringa "bofilemap" nell'hard disk è più sicuro, dato che il nome del server può essere variato. Andare nel Registro di Windows alle chiavi

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

dove sono i programmi lanciati all'avvio. Cancellare da tale chiave qualunque cosa non sia di "sicura" provenienza (esempi di applicazioni "sicure" sono la Barra di Office, antivirus, demone ICQ, ...). Controllare anche

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce

[B08-W][9] E come mi accorgo invece di Netbus?

Il file sysedit.exe nella directory C:\<dir di Windows>\System è di 20k. Se invece è grande ~400k è il server di Netbus. Attenzione anche a file di nome patch.exe, splat1.exe o contascatti.exe e persino explore.exe, diverse versioni del trojan possono essere in uno di questi! Riconoscimento: il client ha di solito un'icona che raffigura un ingranaggio grigio. Il server invece ha un'icona fatta a torcia su sfondo blu, ma dipende dalla versione che si ha: a seconda del compilatore che hanno usato, infatti, l'icona cambia. Per esempio il patch ha la spada, il sysedit l'ingranaggio, ma la versione precedente è quella più utilizzata come server essendo apparsa prima (non tutti hanno aggiornato!). Un file accessorio, che invece NON fa assolutamente parte di Windows, è keyhook.dll, il cui scopo è di intercettare i caratteri digitati sulla tastiera.

NB: Il programma sysedit.exe di 20k è un'utility di windows (grafica Win 3.1)che fa partire gli editor dei vari autoexec.bat, system.ini ecc.

[B09-W][9] Come si toglie Netbus?

========== citazione by Giulio ==========
La versione 1.53 presenta gravi bug, come ad esempio l'impossibilità di rimuoverlo attraverso il pulsante di server admin (server admin --->remove server). In questo caso convinene eliminarlo manualmente. In tutti gli altri casi basta avere Netbus versione client e cliccare appunto su server admin e selezionare remove server. Questo dopo essersi collegati all'indirizzo di localhost (127.0.0.1). Nel caso esista una password la ricerca di tale pass è semplice. Si cerca nel registro di Win il nome del server (Patch oppure Explore) e si leggerà la pass scritta in chiaro alla voce settings.
========== end citazione ==========

[B10-W][9] Come si toglie TeleCommando?

Procurarsi il client ed eseguire il comando "Uninstall Server". Se la risposta è "You have NO Rights", tentare un password vuota. Altrimenti il metodo manuale:

1) Aprire il registro con Regedit e andare alla chiave

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

togliere il riferimento al file odbc.exe, che si trova in C:\<dir. di Windows>\System

2) Riavviare il computer

3) Cancellare il file

[B11-W][9] Cos'è Aggressor?

È un exploit generator. Esso genera pacchetti anomali, che sfruttano delle pecche specifiche di ogni sistema operativo. Per esempio, un pacchetto con una sesta word tale che, in AND con 0x0FE0, ti dà un valore diverso da zero, non gestito da Windows. L'utilizzatore gli dà un IP a cui inviare i pacchetti strani, e il PC della vittima subisce malfunzionamenti vari (si blocca, si resetta, ecc..). Per ovviare al fatto che, sotto Windows, non si possono inviare pacchetti "raw", Aggressor implementa un proprio sistema di controllo del flusso di dati. In Aggressor, fra l'altro, si può specificare il Source IP: vuol dire che l'attacco sembra arrivare dall'IP specificato e non dal proprio, ossia ogni pacchetto IP che venisse loggato o ispezionato dal remoto, avrebbe quell'indirizzo invece di quello effettivo di provenienza.

[B12-W] Un bug di mIRC

Sembra che la versione 5.4 di IRC 5.4 abbia un bug che causa il blocco del computer attraverso il DCC. Il problema si può risolvere con il seguente script che funziona *solo* con mirc 5.4; il bug dovrebbe essere risolto nella versione 5.41.

```
phixme {
   %ip = $rand( ?phixer-cut? )
   raw -q privmsg $1 : $+ $chr(1) $+ DCC SEND $r(1,99) $+ .txt %ip
$r(113,9000) $+ $chr(1) $+ $lf $+ privmsg $1 : $+ $chr(1) $+ DCC
RESUME $r(1,99) $+ .txt $+ $chr(1)
}
```

[B13-W] Che rischi corro usando ICQ?

La prima cosa da sapere è che ICQ, come tutti i programmi basati su TCP/IP, utilizza delle porte, attraverso le quali passano i dati che inviate e ricevete. In particolare, ICQ apre una porta per ogni utente con cui state comunicando, quindi le conclusioni restano all'intuito del lettore di questa FAQ...
Può essere in teoria possibile che un programma si camuffi da ICQ e quindi faccia uso delle porte che l'utente di ICQ apre per dialogare con un utente remoto (c'è qualcuno in grado di confermare o smentire?). Esistono anche dei programmi che permettono di usare ICQ come backdoor (avviso ai lamer: non li conosco, quindi non scrivetemi per chiedermi dove sono ^__^).
È quindi buona norma anche per l'utente di ICQ (come il sottoscritto... sigh!) controllare sempre il PC alla ricerca di presenze sospette.

[B14-W] Cosa sono le scansioni invisibili?

È possibile sapere se sono state effettuate delle "stealth scan" standard anche sotto Windows 95. Bisogna aprire un prompt MS-DOS e dare il comando:

```
C:\WINDOWS\Desktop>netstat -snap tcp

TCP Statistics

  Active Opens                    = 245
  Passive Opens                   = 8
  Failed Connection Attempts      = 9
  ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

Il valore della riga sottolineata corrisponde al numero di porte aperte scansionate dall'esterno (solo per le porte aperte è possibile sapere se sono state scansionate). In particolare, il valore indicato è il numero di scansioni "invisibili" avvenute in successione su porte che ha trovato (NON, come in Linux, il totale delle scansioni che ha tentato).
Per esempio, se abbiamo una sola porta aperta e quello scansiona sei volte tutto l'intervallo da 1 a 1024, il valore di "Failed Connection Attempts" è 6. Se invece scansiona tutto l'intervallo TRANNE quell'unica porta aperta, il valore sarebbe 0.

[B15-W] Ma il file windll.dll non è un file di sistema di Windows?

No. Il file windll.dll viene creato dal boserve.exe quando viene eseguito la prima volta. Attenzione che il fatto di non averlo può non essere significativo: il nome di questo file può essere facilmente modificato all'interno del file boserve.exe usando un editor esadecimale. AVP System Watcher, quando deve rimuovere la dll creata dal BO, prevede questa possibilitàed è in grado di eliminarla anche se ha un altro nome.

[B16-W] Ho ricevuto un messaggio e-mail con un allegato, ma quando tento di leggerlo il mio Outlook va in crash.

"..questo bug affligge sia Outlook 98 sia Outlook Express compreso l'ultimissimo Outlook 4.01 SP1 fornito con Microsoft Internet Explorer. In pratica, quando il client e-mail riceve un messaggio con un attachment dal nome lunghissimo può bloccarsi.

.....un hacker preparato può preparare ad hoc un attachment il cui nome contiene codice eseguibile con risultati imprevedibili"

Fonte: "Internet news", novembre 98

*** Nota del curatore: (C) Leonardo Serni per le seguenti spiegazioni
*** (e seconda lamerata ai suoi danni da parte mia :-P)

L'exploit è possibile perchè la ricezione del nome dell'attachment non controlla se la lunghezza vada oltre il buffer designato ad ospitare il nome stesso. Oltretutto, la parte di codice che verrebbe eseguita dopo lo scarico sembra essere pericolosamente vicina a questo buffer. Di conseguenza la parte finale del nome viene messa in esecuzione poco dopo lo scarico.
Ci sono due casi: se si ha a disposizione i sorgenti del programma che si vuole attaccare in questo modo, con uno strumento di debug si guarda dove va a cadere l'esecuzione dopo lo scarico dell'allegato; a questo punto, in quella posizione basta scrivere una istruzione di salto all'indirizzo del buffer dove si trova il programmino (che costituisce la parte finale del nome dell'allegato) e il gioco è fatto.
Se i sorgenti non ci sono, il gioco si fa più difficile, si va per tentativi /intuizioni, debug non simbolico ma la sostanza non cambia.

[B17-W] Come vedo se ho il protocollo NetBIOS su TCP/IP installato? Che rischi corro?

Basta andare in Pannello di Controllo / Rete / Protocolli e controllare la lista. I rischi che si corrono sono che è possibile entrare nel computer inserendo il suo IP in Avvio/Trova/Computer, se si ha Accesso Remoto aggiornato. Naturalmente bisogna avere attivato delle condivisioni di risorse su alcune unità/directory del computer. Se questo è necessario, almeno proteggerle con password.

[B18-W] Senza programmi come Bo o NetBus è possibile "entrare" nel computer di qualcuno?

Alcune versioni di Windows 95, di serie (o quasi), consentono l'accesso da Internet al disco. Win95 OSR2 se ne accorge all'installazione di Internet Explorer 4.0, e propone di chiudere l'accesso. Si ricorda che se nel computer è attivata la condivisione di file e stampanti, magari senza password, è possibile, conoscendo il suo indirizzo IP, vederlo come unità di rete da Gestione Risorse. Quando si installa Windows o quando si compra il computer con Windows preinstallato, controllare ed eventalmente disattivare ogni condivisione. Ricordo che Windows 95/98 offre servizi di rete senza avere quelle caratteristiche di sicurezza (permessi associati ai file, password) che hanno invece i sistemi multiutente come gli Unix, concepiti anche pensando a tali problematiche.
Un esempio di attacco a un computer con condivisioni attive e non protette: basta mettere il comando opportuno nell'AUTOEXEC.BAT, ed alla successiva accensione (che può essere anche dopo 30 secondi - perchè basta mandare un nuke, il PC si pianta, e il riavvio è necessario) esso verrà eseguito, con quali risultati dipende dal comando. Se per esempio il comando è un bel format /autotest...

[B19-W] Le porte UDP 137 e 138 sono un rischio? E perchè?

Sono porte dedicate al NetBios, che consiste nei File/Print/Disk Services di Windows via protocollo SMB/NetBEUI; in pratica, serve per condividere file/stampanti/dischi (vedi [B17-W], [B18-W]).
La porta 137 è dedicata al NetBios Name Service, la 138 al NetBios Datagram Service. Fanno parte delle cosiddette "well known ports" i cui indirizzi sono stati assegnati dallo IANA (Internet Assigned Numbers Authority), che attualmente gestisce le assegnazioni delle porte nel range 0-1023. Possono essere soggette ad attacchi DoS (Denial of Service). Anche il semplice WinNuke, con il suo invio di dati OOB, può risultare efficace sulle porte 137 e 138, sebbene in prima istanza l'attacco OOB venne concepito sulla porta 139 (NetBios Session Service). Riguardo al WinNuke, Microsoft ha rilasciato delle patch sul suo sito Web.

*** (C) Paolo Monti
[con adattamenti]

[B20-W][95] Ho notato che ogni volta che mi connetto a internet si aprono automaticamente queste due porte 137 e 138. Io ho la versione OSR2 di win95, è un problema di questa versione ?

Potrebbe esserlo se ti attaccassero su quelle porte sfruttando bug dello stack TCP/IP di MS o semplicemente i limiti insiti in tutti i protocolli basati sul TCP/IP (vedi alla voce "SYN flooding"). Per impedire l'apertura delle due

porte suddette, basta eliminare il supporto per il NetBios nelle risorse di rete. Il supporto del NetBios su TCP/IP (NBT) diventa particolarmente pericoloso se hai anche le "shares" (condivisioni di file e/o stampanti) impostate senza password, fatto che si verifica comunemente in almeno il 5% degli utenti Windows. In quel caso, chi localizza il tuo IP sulla rete può entrare nel tuo computer come un falco, usando semplicemente il comando NET o l'Esplora Risorse.

*** (C) Paolo Monti

[B21-W][NT] Da un account NT in pratica senza nessuna autorizzazione, è possibile scovare la password dell'Administrator?

Forse sì , sfruttando un bug nella gestione delle librerie... in pratica, anche un utente normale ha una serie di processi che girano con maggiori privilegi, e in teoria non sarebbero influenzabili.
Il guaio è che alcuni di quei processi usano codice non privilegiato, e quel codice è accessibile a tutti, anche in modifica. Quindi, teoricamente, È possibile. Come farlo in pratica, non so (è vero, non lo dico per evitare richieste). Questo vuole solo essere un incentivo per che gestisce un sistema NT a porre la massima cautela a dove vengono riposti i dati "strategici" per la vita del sistema.

[B22-W][NT] È possibile diventare amministratore sotto Windows NT?

Purtroppo sì . A causa di un baco nel sistema operativo, certe funzioni a livello supervisore non controllano bene i puntatori passati. Come conseguenza, è possibile modificare una serie di variabili nel kernel, senza essere amministratore.
E, siccome il livello di sicurezza (utente, amministratore, Dio, figlio di nessuno) sta in una variabile, ti puoi immaginare il resto...
Naturalmente, bisogna avere a disposizione un login, ed il diritto di eseguire un eseguibile che avremo installato (quindi, diritto di scrittura). Non è poco.

*** (C) Leonardo
[con adattamenti]

[B23-W][NT] Avendo il diritto di installare ed eseguire programmi, cosa posso fare?

Per esempio, scrivere un programma che acceda alle funzioni che non controllano i puntatori (vedere [B27]) e passargli un indirizzo illegale corrispondente ai dati da modificare.

[B24-W][9] Come possono interagire telnet e BO?

Per quanto riguarda una sessione telnet, la si può aprire, ma dal client Bo. Il comando è App Add, si deve scrivere nella finestra exe.location Command.com e scegliere una porta a piacere come listen port. Poi si fa telnet all'indirizzo ip target sulla porta appena scelta... È una vera e propria shell.
Per quanto riguarda invece il comunicare col server del BO tramite telnet, cioè collegarsi alla sua 31337 (o qualunque altra porta abbia configurato) con telnet, non si può fare. Il motivo è che BO usa UDP, mentre telnet usa TCP.

[B25-W] In cosa consiste di preciso il "TearDrop Attack"?

Nell'inviare un pacchetto IP scorretto, cioè frammentato in un modo non valido. Tentando di riassemblarlo, quasi tutti gli stacks TCP-IP ottengono indici negativi ed indirizzi di memoria scorretti, dal che si ottengono magni inchiodamenti. Il protocollo usato è ICMP. [a voler essere più precisi, è la semplice accoppiata IP+UDP, (per evitare le noie dei numeri di sequenza nel caso di spoof) TNX invy].
Naturalmente, la patch (consistente nell'aggiungere "...è un indice negativo? Se sì , butta via il pacchetto e incazzati fortemente") è disponibile per Linux da un pezzo.
Windows 95 è ancora vulnerabile (esistono vari modi di creare rogne con il metodo teardrop), Windows NT parzialmente (solo ai nuovi TD e non al teardrop originale).
I sockets di Windows però non consentono il raw socketing, e quindi non esiste teardrop per Windows. Il teardrop è un attacco che parte solo da sistemi Unix, dove l'acher ;-) deve essere root.
Volendo si puo` modificare il datagram a mano prima che esso venga inviato.

[B26-W] Come sono belli i messaggi di posta e news formattati, con tutte quelle belle applet ed effetti speciali!!!

Disabilitare i messaggi in formato HTML! Immediatamente!!! La ricchezza espressiva consentita dall'HTML e dalla possibilità di incorporare in esso delle funzioni JavaScript e/o delle applet Java non vale la sicurezza del proprio computer. Un esempio "innocuo" è dato dal seguente codice:

```
<script language=VBscript>
do
msgbox ("MANGIATE STRONZI !!!")
loop
</Script>
```

[nota: un messaggio che includeva questo è stato veramente postato in alcuni gruppi della gerarchia it.*]

Innocuo significa che non causa danni alla macchina, ma comunque è fastidioso e per terminarlo occorre ammazzare il programma di posta. "Regalini" come questi sono particolarmente subdoli se si usa il programma Outlook Express di Microsoft, che riesce a eseguire il formato HTML senza bisogno di "aiuti" esterni, con il risultato che non chiede nulla prima di visualizzare un tale messaggio, applet e script compresi. Se questi contengono del codice "malizioso", che per esempio sfrutti dei bug della JVM del browser, i danni causati dipendono solo dall'altruismo del loro mittente...
In OEx si può disabilitare l'esecuzione degli script intervenendo in Strumenti/Opzioni/Protezione/Impostazioni personalizzate; in ogni caso basta cliccare su Strumenti/Opzioni/Area Internet/Personalizzato/ e qui scegliere che cosa si deve eseguire automaticamente e che cosa no.

[B27-W][NT] Perchè è meglio chiudere la porta 53 sotto NT?

La porta 53 è destinata al servizio DNS. I sistemi Windows NT sono vulnerabili a un programma chiamato NTCrash, che è uno script che mette fuori combattimento il server DNS di NT, se presente. È quindi saggio, se non necessario, disabilitare tale servizio sul proprio sistema NT.

[B28-W] È possibile camuffare un eseguibile come un file di tipo diverso?

In linea di principio sì , e anche in pratica. Per esempio, se in Gestione Risorse (Esplora Risorse) è disabilitata la visualizzazione delle estensioni per i tipi di file registrati, un file di nome PIPPO.BMP.EXE viene mostrato in G.R. come PIPPO.BMP; se l'infame che l'ha mandato gli ha dato l'icona di una bitmap e il file sta da solo nella sua cartella, si può restare ingannati e non accorgersi subito che è un file eseguibile. In tal caso, si può essere indotti a tentare di "visualizzarlo" con un doppio click, e quest'azione in realtà lancia il programma che può compiere le sue buone azioni...
Ulteriore pericolo è dato dal fatto che quando si cambiano le associazioni delle estensioni nel file win.ini, Windows non deve ripartire per rileggerle, ma lo fa sul momento.

[B29-W] Corro rischi ad usare Netbuster per beccare intrusi?

Con il Netbuster basta un PortFuck (SYN flood) sulla porta 12345 per avere il sistema bloccato. Per la precisione, Portfuck è un programma DoS usato per floodare porte TCP aperte. È simile ad un flood SYN. Il suo uso principale è bloccare servizi come Telnet o FTP. In pratica Portfuck stabilisce molte connessioni ad un'unica porta TCP di un host remoto. Stabilita una connessione, essa viene chiusa immediatamente e ne viene aperta un'altra.
Esistono addirittura dei programmi che sono fatti apposta per causare errori critici a Netbuster. Dopo tale attacco il netbuster si blocca, con un effettivo rischio per la stabilità del sistema. Anche BoSpY può essere bloccato inviandogli pacchetti UDP molto grandi.

[B30-W][9x] Ancora sul NetBIOS: può BO usare le sue porte?

Bisogna distinguere alcuni casi: se rileviamo connessioni UDP sulle porte 137 *E* 138, allora il responsabile è sicuramente NetBIOS (oppure DUE Orifices), e in quel caso BO *deve* dare errore di bind(), dato che non è possibile tenere aperti due socket sulla stessa porta. Però è possibile avere una connessione *TCP* su 137 e una UDP sempre su 137: gli spazi TCP e UDP sono separati.
Praticamente, se su un computer è installato il NetBIOS, sarebbe molto insolito che BO si potesse mettere in ascolto sulla porta 137 o 138. Attenzione anche alla presenza della porta 139: NetBIOS usa 137 e 138 UDP e 139

TCP, mentre Back Orifice può usare qualsiasi porta UDP *chiusa*, aprendola lui. Se uno ha NetBIOS ha 137 e 138, ma, se avesse SOLO 137, allora quel 137 non è NetBIOS.

[B31-W] Può un attacco sfuggire a Nuke Nabber?

Cerrrrrrrtoo! Per esempio, vari portscanners lo lasciano del tutto indifferente. Anche perchè Nuke Nabber non riesce a monitorare le porte a livello di sistema operativo, perciò un portscanning tipo "stealth" (fatto bene), o il neonato "Spread Spectrum", sono in grado di passargli sotto il naso senza problemi. Nel secondo caso, senza neanche lasciare tracce su quale IP ha l'attaccante.

[B32-W] Cos'è Portfuck?

Portfuck è un programma DoS usato per floodare porte TCP aperte. È simile ad un flood SYN. Il suo uso principale è bloccare servizi come Telnet o FTP. In pratica Portfuck stabilisce molte connessioni ad un'unica porta TCP di un host remoto. Stabilita una connessione, essa viene chiusa immediatamente e ne viene aperta un'altra. Esistono addirittura dei programmi che sono fatti apposta per causare errori critici a NetBuster. Dopo tale attacco il netbuster si blocca, con un effettivo rischio per la stabilità del sistema. Anche BoSpy può essere bloccato inviandogli pacchetti UDP molto grandi.
Per questi motivi è sconsigliabile aprire porte normalmente chiuse sul sistema, quindi anche l'uso del netbuster.

[B33-W] Alcune cosa da sapere su mIRC...

Un uso/settaggio imprudente di mIRC può portare a buchi di sicurezza sul proprio computer. Gli errori più classici in tal senso riguardano la ricezione di file da altri utenti IRC:

* il fileserver attivato che usi C:\ come root;
* l'opzione di accettazione di file via DCC regolata sull'accettazione automatica;
* come sopra, con la finestra pure minimizzata;
* sovrascrittura automatica senza conferma di un file esistente dallo stesso nome di quello che si sta per ricevere.

Di default mIRC non è impostato così , ma basta installare uno script da guerra che abbia il "regalino" che di nascosto gli setti queste opzioni.

[B34-W] Quando su un sito che visito appare il contenuto del desktop cosa vuol dire? Mi devo preoccupare oppure è normale?

Significa solo che sulla pagina web che stai visitando, nel codice HTML, che puoi vedere anche da Explorer visualizzando il sorgente della pagina, c'è un richiamo ad un istruzione tipo questa:

<A HREF="file://C:/windows/desktop">Il tuo desktop</A>

che apre un link al tuo desktop. Quando lo clicchi Explorer ti si trasforma in Gestione Risorse e ti mostra il contenuto del tuo desktop che appunto dovrebbe stare sotto C:\windows\desktop .. se Windows è installato in un'altra directory ti dàerrore ovviamente.
Se invece parte automaticamente e appare un form interno alla pagina col tuo desktop vuol dire che c'è sempre nel codice html un TABLE, ovverosia un luogo dove mettere certi dati ricavati dal tuo sistema. Ma non è che il webmaster 'li conoscè, te li fa solo vedere e solo tu li vedi; se un'altra persona chiamasse quella pagina vedrebbe il proprio desktop!
Esempio pratico. Creare col Notepad un file di testo PROVA.HTM contenente queste righe:

```
<html>
<table cellspacing="0" border="0" width="400">
  <tr>
    <td valign="MIDDLE"><p align="CENTER">
    <object id="browserIcons"
classid="clsid:EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B"
    height="129" width="400">
      <param name="Location" value="c:\windows\desktop\*.*">
```

```
    <param name="AlignLeft" value="1">
    <param name="AutoSize" value="0">
    <param name="AutoSizePercentage" value="100">
    <param name="AutoArrange" value="1">
    <param name="NoClientEdge" value="false">
    <param name="ViewMode" value="3">
   </object>
   </td>
  </tr>
</table></html>
```

Salvarlo ed eseguirlo. Si aprirà una pagina su Explorer con dentro un form table contenente appunto il tuo desktop.

*** (C) Master ***

[B35-W] Come ha fatto questo tipo a trovarmi? Basta usare ICQ?

Perchè qualcuno possa provare a connettersi al tuo PC, la prima condizione è che conosca l'indirizzo IP con cui navighi, che sia statico o dinamico non importa. Per conoscere il proprio indirizzo IP bisogna eseguire il programma WINIPCFG dopo aver lanciato la connessione. Una volta che l'estraneo conosce anche lui questa informazione, può tentare connessioni con o senza backdoor.
Ma la domanda era: come fa lui a conoscerlo? ICQ non è indispensabile, ma certo aiuta chi cerca una persona ben precisa. Basta che inserisca l'UIN della vittima nella sua lista di contatti, ed ecco che viene comodamente informato quando questa è online. Però non è necessario avere un nemico telematico che ci venga a cercare, basta che un rompipalle caciarone decida di spazzare (sweeping in gergo) la sottorete che ci ospita, e ci troverà In questo caso il tipo non cercava proprio noi, ma chiuque fosse nella sottorete.
Esempio. Io ho questo bellissimo programma per nukkare ecc., e voglio provarlo sul primo tapino che mi capita a tiro. Allora prendo una sottorete su cui sono sicuro di trovare qualcuno e provo tutti i suoi indirizzi (con un programma apposito, o anche con lo stesso programma di cui sopra, se prevede questa... hihihi... feature). Diciamo che provo da 212.216.1.1 a 212.216.254.254 (che mi causerà anche una lettera di ringraziamento da Telecom per l'aumento del fatturato e l'intestazione di una quota azionaria). Se tu sei, per esempio, 212.216.13.147, prima o poi ti arriva il ping, anche se io sedicente "acher" non so neanche che sei tu.

[B36-W] Se Netstat mi dice che non ho porte aperte posso stare davvero sicuro? (le DLL ponte)

Ancora una volta la risposta è no.
Netstat, così come i programmi più diffusi per il monitoraggio delle porte aperte, si serve di alcune funzioni esportate dalla libreria INETMIB1.DLL che si trova nella dir di windows. Il codice vero e proprio per interrogare lo stato delle porte è quindi posto interamente in questa DLL. Supponiamo adesso di aver installato una backdoor nel pc di un amico e di volergli nascondere in qualche modo l'apertura di una porta. Non sappiamo quale utility userà per fare questa operazione ma sappiamo che molto probabilmente i risultati (rappresentati in una forma più o meno user-friendly) verrano ricavati effettuando delle chiamate sempre alla stessa libreria. A questo punto possiamo percorrere diverse strade ma la più ovvia, semplice ed immediata è quella di sostituirsi alla inetmib1.dll e falsare i dati di ritorno. Non abbiamo certamente i sorgenti di questa libreria e non possiamo compilarne una nuova da zero, quindi con ogni probabilità la nostra dll funzionerà da ponte tra l'applicazione che effettua la chiamata e la vera inetmib1.dll (che avremo rinominato ad esempio inetmib1.dev).

Nota: i nomi e gli esempi usati non sono casuali ma ricalcano il comportamento di una dll ponte esistente scritta ed utilizzata proprio per nascondere l'apertura di alcune porte.

Approssimativamente la situazione sarà la seguente:

	Programma	DLL Ponte	DLL Originale
Richiesta:	NETSTAT o simili ------>	INETMIB1.DLL ------>	INETMIB1.DEV
Risposta:	NETSTAT o simili <------	INETMIB1.DLL <------	INETMIB1.DEV

La DLL ponte in pratica non fa altro che passare le richieste alla DLL originale e restituire al programma che effettua la chiamata il risultato di tali richieste. Apparentemente quindi il funzionamento sarebbe identico a quello precedente (c'è in realtà un leggero rallentamento ma è a dir poco impercettibile) se non fosse per il fatto che quando la libreria originale ci restituisce dei valori questi passano attraverso un filtro che eventualmente ne blocca

il ritorno al programma richiedente (più precisamente dopo la chiamata alla funzione SnmpExtensionQuery).
Inutile dire che il filtro che abbiamo inserito nella DLL ponte non fa altro che controllare che il numero della porta aperta restituito non sia quello che abbiamo deciso di rendere invisibile e quindi ignorare la chiamata.
Nell'esempio è stato descritto molto grossolanamente il funzionamento di una libreria che inganna netstat e programmi simili ma quello che bisogna tenere a mente è il concetto semplice ed efficace secondo cui anche l'applicazione di cui ci fidiamo di più potrebbe fallire....
Per tirarvi un pò su di morale voglio solo ricordarvi che qualsiasi chiamata, anche quelle fatte alla carissima DLL Winsock, può essere ingannata efficacemente attraverso un uso avanzato di questa antica ma attualissima tecnica.
Adesso avete qualcosa in più di cui preoccuparvi ;)

.....Leonardo De Luca.....

[Post Scriptum by Firebeam]
Questa situazione dovrebbe spingerci a tenere a portata di mano delle copie sicuramente pulite e affidabili di programmi e DLL di sistema, come winsock.dll, wsock32.dll, la succitata inetmib1.dll, nonchè netstat.exe, explorer.exe e così via. Il modo? Floppy protetti da scrittura, o meglio ancora un CD-RW da leggere all'occorrenza esclusivamente dal lettore (non dal masterizzatore, se si hanno tutti e due).

[B37-W] Se ho il client di una backdoor, la mia vittima potrebbe a sua volta entrarmi nel computer?

No. Il BOGUI non "interpreta" e non "esegue" quello che gli arriva dalla porta che tiene aperta. Però vuole un pacchetto UDP onesto, questo sì .
Se su quella porta arriva un nuke - BOGUI è lì a pigliarselo. Non puoi neanche usare NukeNabber... perchè altrimenti non funzionerebbe più il BOGUI! 8-)

Leonardo

[B38-W] Cos'è il NETBEUI e il NETBIOS? Come li gestisco con Conseal?

Il NetBIOS (Network Basic Input/Output System) è sostanzialmente un'interfaccia di programmazione, una API (Application Programming Interface). Anzi, per dirlo in termini più rigorosi possibili, è "un'interfaccia a livello di sessione", usata dalle applicazioni per comunicare con protocolli basati su tale interfaccia, come NetBEUI (NetBIOS Extended User Interface - introdotto da IBM nel 1985) o il network redirector di Windows. Originariamente, il NetBIOS venne sviluppato nel 1983 dalla Sytek Inc. per conto di IBM ed era incluso come firmware nei chip ROM delle schede di rete. In seguito, Microsoft sviluppò un'interfaccia NetBIOS per Windows allo scopo di supportare nei propri prodotti questo standard emergente. Se ConSeal Firewall ti ha segnalato "outgoing data" (dati in uscita) via NetBIOS, significa che hai il Client per le Reti installato con relativo supporto per NetBT (NetBIOS su TCP/IP). Quest'ultimo apre le porte UDP/TCP 137 e 138 (anche la 139, se si stabilisce una comunicazione), che fanno parte delle "well known ports": la 137 è dedicata al NetBIOS Name Service, la 138 al NetBIOS Datagram Service e la 139 al NetBIOS Session Service. In una delle "rules" di ConSeal viene specificato che certi protocolli notificano la presenza del client connesso sulla rete inviando dei pacchetti (UDP e ICMP) su indirizzi broadcast (*.*.*.0 o *.*.*.255), questo comportamento è utile in una rete locale, ma può risultare pericoloso su Internet, oltre che inutile.
Grazie al filtro di un Virtual Device Driver dinamico (FW13.VXD) che interagisce con VxD del NDIS (Network Driver Interface Specification), ConSeal è in grado di intercettare questa operazione, filtrata da una "rule" impostata per default, e quindi la blocca impedendo al tuo PC (o, meglio, al NetBT) di notificare la sua presenza sulla rete.

*** (C) Paolo Monti ***

[B39-W] Come ci si potrebbe connettere alle porta 137, 138 o 139?

Per le prime due, con NBTSTAT.EXE, mentre per la terza con NET.EXE. La domanda successiva è: servirebbe un applicativo che introdotto l'ip di una macchina si collegasse all'host remoto attraverso questa porta, riuscendo a vedere le risorse condivise di quel computer. È possibile una cosa del genere?
Sì , _SE_ quel computer ha il NetBIOS-over-TCP, _SE_ ha risorse di tipo condiviso, _SE_ la linea non è ingorgata 8-) Si deve mettere la mappatura nome/IP nel file LMHOSTS. Windows di serie ha un file campione ("LMHOSTS.SAM").

*** (C) Leonardo Serni ***

[B01-M] È possibile far piantare il Mac tramite la rete?

L'unica cosa che manda in bomba il System 8.1 con l'ultimo OpenTpt è se sta collegandosi (attivamente) a un server DDP e il server crasha. Resta per un pò confuso, poi si pianta il Finder e tocca riavviare. Anzi, una volta su cinque tocca pure resettare la P-RAM. Il problema sembra essere più grave utilizzando una scheda di rete Dayna 10/100, evidentemente non molto affidabile. Un dispositivo comunque non Apple.

[B01-X] Nella mia macchina Linux ho attivo il servizio di finger. È vero che ci sono rischi?

Forse. In realtàera un bug di vecchie versioni, che potevano essere "indotte" a concedere una shell verso un client remoto se questo gli inviava una particolare stringa, contenente quelli che finivano per essere interpretati come comandi. Se il demone girava con diritti di root, l'operatore all'altro capo della connessione aveva a disposizione una shell con i diritti di root... In maniera più pedestre, il server poteva essere fatto crashare mandando una stringa molto lunga.
In ogni caso, le versioni attuali non dovrebbero più essere affette da questo problema. Il consiglio, però, è quello di disabilitare i servizi che non sono necessari, come può essere il finger in una Linux box per uso "domestico".

[B02-X] Con X-Window attivo netstat rileva qualcosa sulla porta 6000.

Facciamo un esperimento: da console (non come terminale di X-Window, ma proprio in "modo testo") diamo il comando

```
netstat -a | grep LISTEN\\b | cut -f2 -d':'
```

un possibile risultato è:

```
auth *
printer *
```

Sulla stessa macchina, dando lo stesso comando da KDE, si ottiene:

```
auth *
printer *
6000 *
```

L'entità misteriosa in ascolto sulla porta 6000 è proprio il server X-Window, che di default e` gia` chiuso agli estranei (vedere la pagina di manuale relativa, comando "man xhost"). Si ricorda che a differenza di Windows, il sistema grafico X-Window funziona secondo il paradigma client-server, anche se abbiamo un semplice PC stand-alone.

[B03-X] Ho sentito parlare di PHF, ma cos'è? Una backdoor?

No, è un CGI installato con Apache. A causa di un bug, se gli si domandava con garbo, per esempio

```
http://www.victim.com/cgi-bin/phf?...
```

ti restituiva il contenuto di QUASI qualsiasi file del sistema, compreso il file delle passwords di Unix.
Il "bug" consisteva nel FIDARSI che la richiesta inviata al PHF fosse buona e lecita, e nel non elaborarla con la dovuta cautela.

<ESEMPIO NON FUNZIONANTE>

```
Diciamo che io prendo un parametro dall'esterno
QUERY=...(parametro)...

e poi costruisco una query formattata come

echo "<PRE>" $QUERY "</PRE>"
```

...se qualche furbacchione mi manda come query

QUERYLEGITTIMA; cat /etc/passwd; echo

il comando diventa, all'interno del CGI,

echo "<PRE>" QUERYLEGITTIMA; cat /etc/passwd; echo "</PRE>"

...che significa: "Invia la query normalmente. Invia anche
tutte le passwords di sistema. Grazie" ;-)
</ESEMPIO NON FUNZIONANTE>

Attualmente, il PHF standard controlla se la richiesta è lecita... e se lo è risponde normalmente, altrimenti fa qualcos'altro (non saprei cosa; come minimo logga l'accaduto).
Esistono stringhe di test che si possono usare con i vari CGI per vedere se sono "sicuri" da questo punto di vista.

*** (C) Leonardo

[B04-X] Corro rischi ad ascoltare musica in formato MP3 sul mio sistema Linux?

I files .MP3 possono contenere, con _alcuni_ lettori MP3, un exploit per sistemi Linux su piattaforma x86. È stato presentato un mini virus realizzato con script bash, che si propaga via MP3, a patto di eseguire il lettore del file con diritti di "root".
L'attacco avviene con un giro un pò complicato. Si basa su un exploit di Erikson, un programma in C che crea un file MP3 bacato. Il baco fuziona solo su Linux, solo su Intel x86. Secondo la descrizione del programma, contenuta nel suo header, esso crea un file MP3 che esegue un programma se suonato con il programma mpg123 versione 0.59k (mentre la versione 0.59o sembra non affetta da questo problema). Il suo autore dice che sarebbe anche possibile inserire del codice che crei un nuovo account e far saltare l'esecuzione all'inizio di quel codice.
Qualcuno è riuscito ad eseguire una system(), che esegue uno script ESTERNO, che di per sè sarebbe privo di diritti. Lo script contiene dei commenti su come sarebbe possibile, a questo punto, compromettere la sicurezza del sistema e propagare script ed MP3 impestato. Naturalmente, un sistema dove root esegue file MP3 ha già problemi di sicurezza, quindi in un caso del genere sarebbe da rivedere la politica con cui viene gestito... Per inciso, lo script di cui sopra non prevede l'infezione di altri files MP3, ma forse ciò non sarebbe affatto difficile, vista la natura dell'exploit.

<PROGRAMMATORI C>
L'exploit si basa sul seguente bug contenuto nel file "common.c":

```
if(newhead == ('R'<<24)+('Ì <<16)+('F'<<8)+'F') {
        char buf[40];
        fprintf(stderr,"Skipped RIFF header\n");
        fread(buf,1,68,filept);
        goto read_again;
}
```

In sostanza, il vettore buf è lungo 40 bytes, ma la fread() legge 68 bytes. La soluzione? Il buffer dovrebbe essere lungo 68, non 40. I programmatori di mpg123 se ne sono già accorti, e l'ultima versione è quindi pulita.
</PROGRAMMATORI C>

[Adattato da un messaggio di L. Serni]

[B05-X] Certi ftp server sono affetti da un problema di buffer overflow. Come posso verificarlo sul mio sistema?

Provare a fare telnet alla porta ftp e a loggarsi. Il test consiste nel creare una directory molto lunga. Se il demone muore il server ftp è vulnerabile. In un sistema ben amministrato, gli accessi anonimi non dovrebbero poter creare directory, per questo e altri motivi.

==========

[C01-ALL] Proteggere il sistema - Info generali

La prima regola fondamentale è di non eseguire __MAI__ alcun file che non sia di provenienza più che accertata. Questo ancor di più se si è soliti, per esempio, chattare con mIRC o ICQ e qualche interlocutore vi spedisca dei file. Non eseguiteli, neanche se promettono di farvi materializzare dal modem una Pamela Anderson nuda e disponibile :-)) Il pericolo può essere maggiore di quello costituito da un virus "tradizionale". In ogni caso, poichè prevenire è meglio che curare, due programmi di utilità sono:

- Nuke Nabber (http://tucows.iol.it, http:/volftp.tin.it)
- AVP System Monitor (http://www.avp.it/utility)

Il primo è un antinuke che però ha il difetto di aprire le porte per controllarle; dovrebbe esistere però una patch che serve a chiuderle. Il secondo è un anti-BO/monitor di sistema, freeware, scritto da Paolo Monti (l'autore è reperibile su it.comp.irc). Per utilizzare NukeNabber bisogna avere Winsock 2 o superiori (attualmente siamo alla 2.2), se si hanno versioni precedenti l'aggiornamento è scaricabile come al solito dal sito Microsoft o da vari archivi ftp (con VOLftp si va tranquilli); la versione 2 o superiore del Winsock è necessaria per la scansione ICMP.
Questo introduce un'altra regola di base, che è quella di tenere costantemente aggiornato il sistema nelle sue componenti vitali come lo stack TCP/IP, per evitare di esser vittime di vecchi bug corretti da versioni successive del software.

[C01-W][9] Come si configura correttamente il Nuke Nabber ?

Come già indicato sono necessarie le winsock 2.x per utilizzare tutte le funzioni dello stesso (per incisio, se lo si utilizza su di un sistema winNT, oppure in rete locale con macchine UNIX è possibilie configurare le attività di logging rispettivamente nell' event monitor oppure verso il demone syslogd).
Vi sono due filosofie d'utilizzo di questo sw:(a) Permettergli di controllare tutto il controllabile, (b) Sintonizzarlo solo ed esclusivamente dove è utile; la seconda serve ad evitare che il sistema sia vittima di attachi che richiedono "porte aperte" e che il Nabber non è in grado di gestire. Quando il Nabber controlla una porta, questa viene lasciata aperta (vedi sez. TCP/IP), dovrebbe esistere una patch per effettuare una chiusura preventiva [[dove ?????]], solo dopo uno scan e/o attacco questa viene chiusa. Configurare il Nabber, in File -> Options -> General almeno due opzioni devono essere selezionate: "Block port scan" (chiude le porte dopo uno scan) e "Disable port for....." (evita di riaprirle per X secondi). Poi, in File -> Options -> Advanced si possono controllare le attività di monitoring sulle porte. Se si decide per (a) (vedi sopra) indicare le porte segnate con (a) alla voce monitoring nell'elenco presente in [PORT-Appendice] e riportate anche qui per brevità
NukeNabber di default controlla le seguenti porte: 5001 (tcp), 5000 (tcp), 1080 (tcp), 1032 (tcp), 1029 (tcp), 1027 (tcp),
- 139 (tcp), 138 (tcp), 137 (tcp),
  Queste devono restare, ma disinstallando NetBIOS o installando
  WinNuke95 e selezionando "Patch against Nuke", le si può togliere.
- 129 (tcp), ma non è un servizio standard.
- 53 (tcp),
  si può togliere, a meno di non avere un DNS sul PC, accessibile
  dall'esterno.
- 19 (udp).
  su Windows 95 non c'è il servizio chargen corrispondente alla porta.
  Su WinNT, va elimitato, dal pannello di controllo "Small TCP Services",
  perchè si può indurre NT a cortocircuitare le proprie porte 19 e 53,
  con risultati non proprio esaltanti. Con Windows 95/98 no (non c'è il
  servizio).

Vanno aggiunte invece le seguenti:
- 31337 (udp), Porta di default del Bo.
- 61466 (tcp), 50505 (tcp)
- 12345 (tcp), 12346 (tcp), porte utilizzate da NetBus.

Se si segue la filosofia (b) ci si limiterà a:
ICMP / 139 (TCP) / 19 (UDP)

Si tenga comunque presente che
- gli scan alla ricerca di backdoor/server vari non sono pericolosi in quanto tali
- il Nabber è veramente essenziale solo se si utilizza IRC, dal momento che ci sono persone che attaccano sistematicamente tutti quelli che si affacciano su di un canale

[C02-W][9] Le componenti di rete, ovvero: cosa tengo e cosa tolgo?

Anzitutto, se possibile. togliere assolutamente i protocolli NetBEUI e IPX/SPX, o almeno il binding con Accesso Remoto (se si ha Windows). Questi servono per reti locali e non per Internet; nel caso di un computer a casa collegato a Internet con modem e accesso tramite provider su linea telefonica, nelle proprietà della Rete dovrebbe esserci solo Scheda di Accesso Remoto e TCP/IP in binding con essa. Eliminare se possibile anche il client per reti Microsoft.
Condivisioni: eliminare o, se necessarie, proteggere con password le directory condivise. I protocolli NetBEUI e IPX/SPX non devono comunque essere associati ad Accesso Remoto ma solo al driver della scheda di rete.

[C03-W][9] Ma se tolgo il Client per reti MS non mi memorizza più la password!!!

Meglio!!! ^__^ Ogni informazione memorizzata nell'hard disk è a disposizione dell'hacker oppure lamer di turno. Almeno gli si renda la vita più difficile non facendogli trovare bello e pronto quel che cercano. I file .pwl di Windows, poi, dove vengono memorizzate le password, non sono certo difficili da decifrare (vedi patch per la sicurezza che Microsoft ogni tanto emette). Ricordo che se qualcuno vi frega la pass di accesso a Internet poi si può connettere e per il provider (E PER L'AUTORITÀ GIUDIZIARIA) sarete voi a esservi connessi e ad aver commesso eventuali atti illeciti. A meno che riusciate a dimostrare di essere stati craccati (della serie, campa cavallo...).

[C04-W][9] Quali porte controllare con NukeNabber?

NukeNabber di default controlla le seguenti porte:

5001 (tcp), 5000 (tcp), 1080 (tcp), 1032 (tcp), 1029 (tcp), 1027 (tcp),	Queste possono essere cancellate: le >1024 sono aperte in outbound
139 (tcp), 138 (tcp), 137 (tcp)	Queste devono restare, ma disinstallando NetBIOS o installando WinNuke95 e selezionando "Patch against Nuke", le si può togliere
129 (tcp)	129 non è un servizio standard
53 (tcp)	si può togliere, a meno di non avere un name server sul PC, accessibile dall'esterno
19 (udp)	su Windows 95 non c'è il servizio chargen corrispondente alla porta. Su WinNT, va elimitato, dal pannello di controllo "Small TCP Services", perchè si può indurre NT a cortocircuitare le proprie porte 19 e 53, con risultati non proprio esaltanti. Con Windows 95/98 no (non c'è il servizio)

Vanno aggiunte invece le seguenti:

- 31337 (udp),
  Questa è la porta di default del Bo.

- 61466 (tcp),
  Master Paradise

- 50505 (tcp),
  icqtrogen

- 12345 (tcp), 12346 (tcp).
  Su queste porte può arrivare una connessione a NetBus.

Attenzione che NukeNabber è un programma di monitoraggio e non una protezione vera e propria. Esso consente di sapere se le porte sotto controllo sono sotto attacco, ma non è efficace contro attacchi tipo Land, Boink, Teadrop I e II, Ssping ecc...

[C05-W] Cosa uso per controllare l'attività di rete del mio computer?

DOS	Win95	Linux
tracert	tracert	traceroute
ping	ping	ping

DOS	Win95	Linux
netstat	netstat	netstat
nbtstat	nbtstat	nbtstat
-	NukeNabber	tcplogd
-	-	tcpd
-	NukeNabber(?)	icmpd
-	-	strobed
-	-	-
route	route	(1) route
-	aggressor	aggressor
fdisk	fdisk	fdisk
-	win	Startx
-	office	staroffice
pov	pov32	povray

...

(1) Non funziona bene
(2) Children, DO NOT DO THIS AT HOME

(C) Leonardo Serni, da un post del quale ho brutalmente copy&pastato la tabella di cui sopra (siiiì , anch'io lamer!)

[C06-W][9] Password mantenute in cache

Un piccolo suggerimento per tutti: è possibile evitare l'uso delle cached password modificando una chiave nel Registry. Basta impostare al valore 1 la seguente chiave:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
Network\DisablePwdCaching

[C07-W] Ho il programma WinTOP dei Kernel Toys. Serve a qualcosa?

Sì . WinTOP (che si può lanciare da Avvio[Start]/Esegui, scrivere wintop.exe<RETURN>) mostra un elenco di tutti i processi attivi nel computer, con la possibilità per ognuno di essi di avere l'elenco dei thread generati. A differenza della finestra che appare premendo CTRL- ALT-DEL, in WinTOP viene mostrato tutto quello che è in esecuzione, e quindi si possono individuare cose "non regolari".
Idle, kernel32, msgsrv32, mprexe, mmtask, explorer, rundll32 sono task di sistema. Per vedere i dettagli di un processo, cliccate con il tasto destro e scegliete Properties: qui in due schede sono mostrate, appunto, le proprietà del processo. Quello che interessa è la seconda, dove può essere presente un bottone "Terminate process now", che permette appunto di uccidere il processo. Il bottone è disponibile sui processi contrassegnati dalla finestra, mentre quelli contrassegnati dalla ruota dentata non possono essere terminati in questo modo.
Attenzione: WinTop non permette di effettuare la chiusura dei processi con caratteristiche di servizi di sistema, mentre con AVP System Watch è possibile fare anche questa operazione.

[C08-W] È vero che si possono far eseguire dei programmi dannosi allegandoli a un messaggio e-mail?

Dipende da cosa si intende dire. In generale, una mail è costituita da una sequenza di caratteri ASCII, che vengono mostrati in una finestra del programma di posta elettronica, ma non sono eseguiti. La mail può però contenere un allegato di tipo qualunque, e ai fini della sicurezza del sistema interessano due classi di file: eseguibili (.exe, .com) e binari creati da applicazioni che hanno un certo livello di programmabilità per mezzo di macrolinguaggi (documenti Word o Excel, per esempio). Il testo della mail non è pericoloso, al contrario di quel che dicono dei messaggi terroristici che periodicamente spammano i newsgroup.
Il discorso cambia per gli allegati suddetti. Un file di Winword può contenere una macro che in realtà è un macrovirus, e la sua apertura CON WINWORD può infettare il computer col virus stesso. Un file eseguibile può anch'esso essere infetto. Non si proseguirà qui sul discorso dei virus, esistendo un newsgroup dedicato ad essi, cioè it.comp.sicurezza.virus, e le relative FAQ.
I pericoli che possono nascondersi negli eseguibili non sono però finiti. Un eseguibile può nascondere un trojan o una backdoor, ed eseguendolo vengono installati questi ultimi. Qui il trucco non sta solo nell'avere programmi antivirus e di monitoraggio aggiornati e sofisticati, ma soprattutto in un settaggio furbo del programma di posta. Questo deve essere impostato in modo che gli allegati "sensibili" non vengano aperti direttamente cliccandoci

sopra, ma salvati su disco per poterli passare con comodo all'antivirus e agli altri controlli. In poche parole, un .jpeg può essere automaticamente aperto, un documento Word NO, NO, NO, NO, NO (ripetere n volte, con n->oo) e neppure un eseguibile.

[C09-W][9] Posso proteggere un file o una directory sotto Windows da accessi indesiderati?

Certo. Naturalmente, a causa della natura intrinsecamente insicura di Windows (TUTTE le versioni dal 98 in giù) dovuta al fatto che si tratta di un sistema sostanzialmente monoutente, questo è impossibile in maniera nativa, e i programmi che si possono trovare sono tutti più o meno aggirabili (basta un boot da dischetto per accedere al sistema, anche se da DOS puro, a meno di disabilitarlo dal BIOS).
Se la partizione in cui si trova il file/directory da proteggere è formattata FAT-16 (cosa facilmente verificabile con un click destro sulla unità, scegliendo Proprietà/Generale e controllando la presenza o meno della dicitura FAT-32 accanto alla riga Tipo: Disco locale), c'è però un trucco semplice, che necessita di un programma come il buon vecchio PC-tools.
Per facilitare le cose, si mettano i file in un'unica directory, chiamata ad esempio "VARIEK". Riavviare in Modalità MS-DOS (NON il prompt!!!), lanciare PC-tools, localizzare la directory VARIEK e sostituire la K con ALT+255; questo è un carattere che sembra lo spazio, e l'effetto è di rendere la directory inaccessibile sia da DOS che da Windows. Per entrarvi, occorre utilizzare di nuovo PC-tools e rimpiazzare ALT+255 con un carattere alfanumerico. La cosa può sembrare macchinosa, ma è possibile scrivere un programma che faccia il cambio in automatico, cosicchè per entrare nella directory e accedere ai file contenuti basta lanciare il programmino e una volta finito rieseguirlo per compiere l'operazione opposta. Stessa cosa per i nomi dei singoli file, per esempio per creare in dos dei file con spazi inframezzati, o in Windows (3.1 o anche 95) scrivere file che windows non può rileggere se non dopo accurata modifica del nome.

[C10-W] Ho messo sotto controllo la porta 31337. Sono al sicuro?

Non direi. Per default, il BO apre in listening una sola porta TCP/UDP: la 31337 (in realtà sono due, dal momento che le porte TCP sono diverse da quelle UDP, anche se hanno lo stesso indirizzo). Volendo è possibile impedire/monitorare il flusso di dati da certe porte, i firewall servono proprio a questo (ad es., Conseal o Green Dog). Il problema è che il BO può essere configurato per "ascoltare" anche da porte diverse da quella di default.

(P.Monti)

[C11-W] Ho installato NukeNabber per controllare le porte "sensibili". Sono al sicuro?

Con Nuke Nabber installato, ti possono straziare la macchina usando, per esempio, Teardrop, Newdrop, Fraggle e Nestea (*). Per quanto ne so. E non so se funziona anche Jolt (*), un altro attacco simile. C'è un paio di note in FAQ, http://www.linuxvalley.com/~lserni/glossary.cgi?ITEM=attacks, però sono "in fieri" e lontanissime dall'essere complete. Mi raccomando, dite se ci sono errori o inesattezze.

(*) Cercarli!!! Anche Land, Boink, Ssping

[C12-W][9] Back Orifice - Server: configurazione ed installazione

*** Nota: questo paragrafo non vuole essere un incitamento alla boserverizzazione dei computer altrui. Dato che è comunque bene conoscere i propri nemici per poterli meglio sconfiggere, l'ho ugualmente inserito nella FAQ. Potrete fare così degli esperimenti sul vostro PC (utilizzando l'indirizzo 127.0.0.1 sul BoClient) o su quello di un vostro amico CONSENZIENTE ed INFORMATO DI TUTTI I PERICOLI, che verrà IMMEDIATAMENTE RIPULITO DAL SERVER al termine degli esperimenti. ***
Il server Back Orifice si può installare semplicemente lanciando il file boserve.exe; una volta avviato, questo file copia il server (vero e proprio) nella directory SYSTEM di Windows 95, aggiunge una chiave nel registro di configurazione ed infine si cancella dalla directory da cui è stato lanciato.
Il BO server può essere configurato (prima di essere installato) per impostare il nome dell'eseguibile del server, la porta su cui deve ascoltare, la password, etc. ma funziona anche senza una particolare configurazione utilizzando le seguenti impostazioni di default:

Nome eseguibile del server: " .exe" <spazio>.exe
Porta: "31337"
Password: (nessuna)

Per configurarlo, invece, va usata l'utility boconfig.exe nel seguente modo:

Dopo aver estratto il pacchetto BO in una directory, dal prompt di MS-DOS, posizionarsi in questa directory e digitare:

```
boconfig boserve.exe     [Invio]
```

Ora viene chiesto di specificare le varie opzioni di configurazione:

```
Prompt di MS-DOS
C:\bo>boconfig boserve.exe
BOConfig 1.0 - Configures execution options for a Back
Orifice server

Runtime executable name: (does not necessarily have to end in
.exe)
server.exe
Exe description in registry:
ServerBO
Server port:
12345
Encryption password:
my_passwd
Default plugin to run on startup:
my_plugin.dll:_start
Arguments for plugin:
parametro1,parametro2
File to attach:
freeze.exe
Write file as:
my_plugin.dll

C:\bo>
```

Runtime executable filename: è il nome con cui verrà chiamato il file eseguibile del server; non è necessario specificare l'estensione .exe, ma se non lo si fa, BO non la aggiunge automaticamente;
Exe description in registry: è il nome che si vuole dare alla chiave che verrà creata nel registro di Windows 95 per far sì che il server venga lanciato automaticamente ad ogni avvio del sistema. Questa chiave si trova in:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices.

Se non si specifica un nome, il riferimento al server verrà creato nella chiave "(Predefinito)";

Server port: è la porta su cui sarà attivo il server;
Encryption password: è la password usata per la criptazione. Si può anche scegliere di non usarla, digitando semplicemente Invio;
Default plugin to run on startup: qui va specificato un plugin da lanciare all'avvio. La sintassi è la seguente:

```
nome_plugin.dll:_funzione
```

Per ulteriori informazioni riguardo i plugin di BO, leggi il file plugin.txt incluso nel pacchetto e visita il sito cDc. Se non si vuole usare nessun plugin digitare Invio.

Argument for plugin: qui vanno specificati gli argomenti da passare al plugin. Se hai scaricato dei plugin da Internet, questi parametri li trovi nella loro documentazione;
File to attach: qui va inserito il percorso di un file che si vuole attaccare al server. Questo potrebbe essere un plugin per BO, che può essere attivato automaticamente. Se non si vuole attaccare nessun file, digitare Invio;
Write file as: se si è specificato di attaccare un file al server, bisogna ora specificare il nome che si vuole dare al file attaccato.
A questo punto il file boserve.exe è stato modificato per queste impostazioni.

Nota: se vuoi fare un'altra configurazione, non usare il file boserve.exe già configurato: cancellalo ed estrailo di nuovo dall'archivio compresso.

×-h4ck3r - SPP member
Liberamente tratto dal sito di x-hacher
(by M.D'Itri)

[C13-W] Si può vedere se ho un file "Silkroppato"?

Dipende da come è stato fatto il lavoro: se uno usa silkrope e basta, gli antivirus attuali ti dicono che il file è infetto da BO. Se, invece, dopo aver fatto silkrope passi il tutto ad un compressore di eseguibili, l'antivirus non vede niente.

[C14-W] Si può creare un file di log per netstat?

Dipende da cosa si intende per log. Si può fare in modo che l'output di netstat venga scritto su un file piuttosto che sul video, basta usare il pipe ">" o ">>". Per esempio potresti scrivere

```
netstat -na 30 > c:\dir\log.txt
```

oppure

```
netstat -pa TCP 30 > c:\dir\log.txt
```

scegliendo i parametri che vuoi passare al netstat e poi, invece di mandare i risultati a video, ci si crea un bel file di log.

Bisogna fare attenzione a 2 cose:

1. il singolo ">" fa in modo che il log venga sovrascritto ogni volta che si esegue il comando, mentre il doppio ">>" fa sì che i risultati vengano di volta in volta aggiunti nel file in coda ai precedenti (occhio alle dimensioni del file log!).
2. se si imposta un intervallo di tempo molto breve, è sicuro che non sfugge nulla ... o quasi ;-), ma si rischia di ritrovarsi con un log immenso!

Poi si può scrivere un piccolo file batch in modo da non doverlo digitare ogni volta: aprite il notepad, scrivete il comando in una riga, sceglere Salva con nome (nella lista dei tipi dei file scegliere "tutti i file") chiamandolo "nome_che_vuoi.BAT".
Poi per cercare qualcosa si va di grep... <hem!!!> si apre con Wordpad e con <CTRL>+F si cerca, per esempio, "31337" (che originale!!!), usando F3 per trovare tutte le connessioni loggate con la sottostringa cercata.

*** (C) x-hacker
[con adattamenti]

[C15-W] Ho saputo che posso proteggere il mio computer con un programma chiamato Conseal. Quando è utile o inutile questo programma?

Conseal viene fornito con un semplice insieme di regole, o ruleset, che impedisce gli attacchi più comuni. Le restrizioni devono essere adattate caso per caso per avere un'efficacia più sicura, e l'help del programma è come al solito una lettura d'obbligo per avere maggiori informazioni. Esiste anche il sito Internet

```
http://www.betatesters.com/firewall
```

dove si possono trovare utili indicazioni e consigli, fra cui varie configurazioni del ruleset tutte documentate.
Un timore che si può avere è che qualcuno dall'esterno possa in qualche modo manomettere le regole impostate nel firewall. Ebbene, questo non è possibile farlo da remoto, a meno che ovviamente non si possa entrare nel sistema con i soliti mezzi: backdoor, porte aperte in eccesso (cioè servizi attivi non necessari), condivisioni magari non protette da password, IE4 bacato, ...
È quindi importante assicurarsi di non avere un sistema aperto, controllando prima tutto il controllabile di ciò che è stato citato nel paragrafo precedente, poi si installerà il Conseal configurando il tutto secondo le specifiche necessità, dopodiché si può stare relativamente tranquilli in relazione alla configurazione adottata. In altre parole, per tutte le porte che per necessità devono restare aperte bisogna accertarsi che non possano venire attacchi da quella direzione, per esempio aggiornando sempre il software e lasciando il meno possibile del sistema visibile al mondo.

[C16-W] Si può disabilitare la funzione di autorun per tutte le unità?

La chiave del registry che ci interessa si trova nella gerarchia HKEY_CURRENT_USER che ha le impostazioni dell'utente di default (se no si cerchi la gerarchia dell'utente interessato). In particolare, il percorso è il seguente:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\"NoDriveTypeAutoRun"

(si cerchi con Regedit, Avvio -> Esegui -> regedit.exe).

Il valore per disabilitare l'autorun su tutti i tipi di unità è "FF, 0, 0, 0". Ogni bit del primo byte rappresenta un certo tipo di unità, se il bit è impostato a 1, allora l'autorun è disabilitato per quel tipo di unità cui il bit fa riferimento.

[C17-W][NT] Come impedisco ad altri di amministrare il server NT?

Per definizione, l'amministratore di un computer NT è che ha i diritti di amministratore. Se la macchina NT fa parte di una rete, è possibile che più utenti abbiano un account su quella macchina. Per accedere alle funzioni di amministrazione, però, quegli account ne devono avere i diritti, perchè a un utente normale l'accesso viene negato. Per evidenti ragioni, è sconsigliato dare i privilegi di amministratore a tutti gli utenti della stazione NT. Invece, usando la sicurezza di NT, se si vuole essere gli unici a mettere le mani sulle funzioni delicate, bisogna fare in modo di essere gli unici amministratori. D'altra parte un amministratore ha diritto ad avere accesso al server in ogni condizione (per definizione), e se non si è gli unici con tali prerogative non si ha il diritto di bloccare il sistema in modo totalmente esclusivo e NT non lo permette. Se quindi non è possibile essere gli unici amministratori, non è possibile nemmeno bloccare l'accesso a certe funzioni.

[C18-W] Come posso impostare il firewall per utilizzare ICQ?

Il problema è che icq cambia porta ogni volta... lasciando il learning mode del firewall, quando arriva un msg da icq vuole aprire una porta dall'ip remoto (il mittente) verso il tuo (destinatario). Tu gli dici sì e lui crea il rule per *quegli* indirizzi e *quelle* porte. Al secondo messaggio, magari, la porta cambia, e di nuovo non incontra più alcun rule (quello di prima era per una porta diversa!!!), e così si ferma ancora... e alla fine ci si crea un rule per ogni messaggio!!
Tutto quello che ti serve è un rule (anzi due) così composto:

Service ICQ
Protocol: UDP
Direction: inbound/outbound (entrambe "checked")
Remote address: 205.188.252.0 (che è il server di icq)
Remote mask: 255.255.255.0
Remote port: 4000
Local address: my address (imposta automaticamente anche la mask)
Local port: temp range (*)

Il secondo rule è identico, solo che il remote address deve essere 205.188.254.0 (altro server di icq). Si deve ovviamente aprire un rule per i tcp/ip (se non è già aperto):

Service: ICQ
Protocol: TCP/IP
inbound/outbound allow
Remote address: all address
Remote ports: 1024-65535
Local address: my address
Local port: temp range (*)

Questo per permettere di scambiare eventi come msg, file o altro. I TCP/IP sono infatti i pacchettini di dati.

(*) = attenzione, con icq99 diventa tutto più complicato, perchè icq99 continua a usare per certi segnali delle porte "alte" (in particolare il segnale di online/offline per la gente in contact list). Le prime build erano un totale disastro, perchè instradavano pure tutti i dati sulle porte alte, quindi era una tragedia. Questo significa che con ICQ 98, la local port può essere temp range (1024-5000) normalmente, con il 99 invece bisogna aprire 1024-65535, perdendo ovviamente ogni sicurezza perchè è proprio sulle porte alte che arrivano il 99% delle eventuali aggressioni... in questo caso meglio fare a meno del firewall.
Viceversa, per tenere in conto di chi può avere icq99, bisogna impostare il remote address del tcp come 1024-

65535 anziché temp range (1024-5000), perchè chiaramente se uno ha icq99 potrebbe mandarti dei dati DALLA sua porta (es.) 26535 sulla nostra (sempre es.) 1046. La nostra 1046 è nel temp range (perchè abbiamo icq98), ma la sua è fuori dal temp range...

[C01-X] Come posso rendere Linux più sicuro da intrusioni?

Regola generale è di disabilitare tutti i servizi che non verranno forniti ad altre macchine (vale anche per macchine effettivamente usate come server). Esempi di tali servizi sono: httpd (server web), telnet, ftp, pop3 e sendmail; ci sono inoltre time stream, time dgram, shell, login, ntalk, systat, netstat, auth. Ancora, togliere portmapper, nfsd e mountd.
In particolare, se la macchina Linux di cui si parla è una stazione di lavoro domestica o comunque non integrata in una rete (LAN oppure Intranet/Internet), vanno tranquillamente disabilitati anche quelli. Ricordate che più servizi sono attivi più grande è il numero di porte aperte, e maggiori sono quindi le possibilità di attacco.

[C02-X] Come faccio a sapere che servizi ho attivi?

Si dia il comando:

grep -v "^#" /etc/inetd.conf

per vedere quali servizi ti serve di OFFRIRE. Di solito, nessuno. Forse non sarebbe malvagio dare via un identd, ed a quel punto l'UNICA riga non #-ata di /etc/inetd.conf sarebbe

ident stream tcp wait nobody /usr/sbin/in.identd in.identd -w -t120

dove l'utente nobody dovrebbe avere diritti molto ristretti, per usare un eufemismo. Poi si dia:

killall -HUP inetd

per resettare inetd, e per sapere che servizi il proprio computer espone all'esterno:

netstat -a | grep LISTEN\\b | cut -f2 -d':'

Bisogna anche tenere conto che smbd, netbios ed altri servizi non partono sempre da inetd ma da un file in /etc/rc.d/...

Se invece in inetd.conf è presente anche la seguente riga non commentata:

auth stream tcp wait root /usr/sbin/in.identd in.identd -w -t120 -l

se la macchina è destinata all'uso personale e non devono essere offerti servizi all'esterno, è meglio togliere il flag -l. Questo perchè identd serve al remoto solo finchè il sistema locale non è stato compromesso; ma in caso di macchina per uso personale, la distinzione è inutile; secondo perchè si potrebbe floodare il sistema con una serie di richieste alla porta 113 facendo sì che il file di log o la consolle diventino incomprensibili. Spesso l'opzione serve ai root di un sistema multiutente per beccare i fake-mailer alle prime armi o i cretinotti su IRC che si fan regalare la K.

Inoltre:

```
shell   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd -L
login   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind
ntalk   dgram   udp     wait    root    /usr/sbin/tcpd  in.talkd
comsat  dgram   udp     wait    root    /usr/sbin/tcpd  in.comsat
```

Togliere, altrimenti si permette a qualcuno di fuori di avere una shell o un login remoto sulla propria macchina.

```
systat  stream  tcp     nowait  nobody  /usr/sbin/tcpd  /bin/ps -auwwx
netstat stream  tcp     nowait  root    /usr/sbin/tcpd  /bin/netstat
```

Idem...

```
time    stream  tcp     nowait  root    internal
time    dgram   udp     wait    root    internal
```

Di questo si può fare a meno

```
ntalk   dgram   udp     wait    root    /usr/sbin/tcpd  in.talkd
```

Solo se si pensa di usarlo per chattare con altri (con ip dinamici un incubo)

```
systat  stream  tcp     nowait  nobody  /usr/sbin/tcpd  /bin/ps -auwwx
netstat stream  tcp     nowait  root    /usr/sbin/tcpd  /bin/netstat -a
```

Con questi due si fa sapere a tutti cosa gira sulla propria macchina e quali porte aperte ci siano, meglio che con un portscan.

Altri processi/porte:

6000

Questo non parte da inetd.conf, ma è X-Window. Usare xhost - e magari bloccare la porta mediante un packet filter (ipfwadm o ipchains).

```
syslogd
klogd
```

Se si vuol continuare ad avere i log, bisogna lasciarli.

[C03-X] Non posso disabilitare tutti i servizi di sistema. C'è modo di difendersi comunque?

Basta sfruttare la gestione dei permessi di Linux. Se lasci qualcosa di attivo in inetd.conf, metti in /etc/hosts.deny:

ALL: ALL

e in etc/hosts.allow:

ALL: 127.0.0.1

[Ovviamente se non intendi fornire servizi ad altre macchine]. Il significato (espresso in modo un pò pedestre) di tali istruzioni è il seguente: a tutte le macchine è vietato tutto (ALL: ALL in hosts.deny), alla macchina locale è però permesso tutto (ALL: 127.0.0.1 in hosts.allow). In tal modo il sistema caccerà a pedate qualunque intruso che tentasse di connettersi.

*** Attenzione***
Questi file vengono letti da tcp, quindi la riga in inetd.conf DEVE essere del tipo

[ecc. ecc] /usr/bin/tcpd [path][demone][parametri]

[C04-X] È necessario che sendmail venga lanciato al boot della macchina?

Anzitutto ci sono demoni di posta più leggeri, come qmail. Se però si usa sendmail allora non conviene farlo partire al boot, se sei l'unico utente della macchina non ce n'è bisogno ed è un pò più difficile controllarlo. Lo si faccia invece partire da inetd mettendo in inetd.conf:

```
smtp    stream  tcp     nowait  mail    /usr/sbin/tcpd  /usr/sbin/sendmail -bs
```

[C05-X] Come posso sapere se e chi mi sta attaccando?

Tcpd permette di monitorare la connessione TCP. Si può affiancare a tcpd i pacchetti iplogger (per controllare anche il traffico ICMP e quello TCP non loggato da tcpd) e udplog di Leonardo Serni, reperibili a: http://www.linuxvalley.com/~lserni.

Se poi al momento della connessione si lancia il comando:

xterm -e tail -f logfile

dove logfile e` il file di log usato dai programmi sopra citati, es. /var/log/secure per tcpd (nella RH), /var/log/messages (nella Slack), in caso vedi in syslog.conf dove vanno i messaggi con facility authpriv, /var/log/messages per udplog ecc., si può disporre di un vero e proprio monitor in tempo reale dei tentativi di attacco.

Nei primi due file citati ci sono sia i log del kernel (generati da
klogd) che i log per la rete (syslogd).

[C06-X] Pericolosità dei commenti in host.equiv

Dal suddetto file è necessario togliere tutte le righe commentate, cioè quelle che iniziano con il carattere "#". Esiste infatti un modo di exploitare una macchina con un file host.equiv contenente dei commenti. Infatti, pare che una riga del tipo

#
Questa riga
#

affermi che lo host "#" può loggarsi senza password. Se così è, e se qualcuno riesce ad assumere abbastanza controllo DNS da rifarsi un nome come "#", ha tutti i numeri per giocare un brutto tiro alla macchina con tale buco.

[C07-X] Voglio stampare in locale, togliendo la disponibilità del server di stampa al "resto del mondo".

Si può fare lanciando lpd in /etc/inetd.conf, sotto tcpd, come qui indicato:

printer stream tcp nowait root /usr/sbin/tcpd /usr/bin/lpd -i

A questo punto inserisci nel file /etc/hosts.deny la linea

ALL:ALL:spawn safe_finger -l @%h 2>& 1| mail -s "%d-%h %u" root

(se hai safe_finger, se no "ALL:ALL")

e inserisci in /etc/hosts.allow la linea

ALL:127.0.0.1
in.identd:ALL

[C08-X] Come posso sapere chi sta usando i miei servizi?

Il demone che serve si chiama auth. Esso in pratica fa un finger a chi cerca di fare qualcosa, e comunica al sistemista (cioè a te) il risultato via mail. Naturalmente l'host che riceve il finger deve avere questo servizio attivo, altrimenti non daràla risposta che si cerca.

Ecco come si può lanciare auth:

ident stream tcp wait nobody /usr/sbin/in.identd in.identd -w -t120 -o -e

questo fa sì che non venga usato syslog e che inetd non debba fare troppa fatica per gestire le connessioni, dal momento che si limita ad avviare identd. Questo impedisce di fare flooding troppo facilmente, e in casi estremi è

possibile identificare chi fa flood con uno script e tagliarlo fuori con route o ipfwadm.

[C09-X] Non mi va / non posso disabilitare tutti i servizi della mia Linux box.

Soluzione alternativa: ricompilare il kernel con il supporto per il firewall, lasciare tutti i servizi che occorrono ma bloccarli con ipfwadm.

[C10-X] Se non voglio/posso fare a meno di usare X, posso almeno renderlo sicuro?

Se si è su una rete, bisogna controllare che il server X sia ben protetto. Da un'altra macchina della rete si dia un comando di questo tipo:

```
xterm -display tuo_IP:0
```

Se la macchina da controllare non fa parte di una rete, si può usare un bounce o chi per lui, che permetta di connettersi alla porta 6000 di localhost. In ogni caso, se la connessione alla porta 6000 riesce ed appare l'xterm sullo schermo, il server X è aperto al mondo come il back orifice di un BOservizzato. Il comando da dare è

```
xhost -
```

mentre un rimedio duraturo consiste nel filtrare con ipfwadm ogni connessione alla porta 6000 da proteggere, che non provenga dalla interfaccia lo (ifconfig).

[C11-X] Quali servizi possono essere chiusi sulla mia Linux Box?

In un computer per uso domestico di solito non c'è bisogno di alcun servizio di rete attivo, a meno che esso non sia il server di una minirete (per esempio, con il vecchio 486 ancora usato come client e/o per esperimenti sulle reti). Spesso, può essere utile lasciare il demone identd, cosicchè nel file /etc/inetd.conf l'unica riga non commentata sarà

```
ident   stream  tcp  wait   nobody /usr/sbin/in.identd in.identd -w -t120
```

dove l'utente nobody dovrebbe avere diritti molto ristretti, anzi quasi nulli. Se la nostra Linux Box è anche server di posta, dovràessere lasciato attivo anche il relativo demone. Nel caso di sendmail, la riga di idetd.conf saràdel tipo:

```
smtp    stream  tcp     nowait  mail    /usr/sbin/tcpd  /usr/sbin/sendmail -bs
```

I apparenza, dendmail dovrebbe girare come root, altrimenti avrebbe problemi, per esempio, a scrivere direttamente nelle directory degli utenti oppure a lanciare procmail in maniera che scriva direttamente nei folder di posta con umask 300. In realtàsi può dare accesso ai maildrop al gruppo smtp, che non ha diritti su nient'altro; i maildrops ovviamente avranno diritti 660, e saranno di tipo username.smtp.

[C12-X] Che meccanismo usa inetd per lanciare i processi "di rete"?

Inetd esegue un binding sulla porta richiesta dal servizio, ma non attiva il processo. Quando lo fa, gli passa il socket ma il processo gira con l'effective userid specificato, e non può neanche aprire un nuovo socket nel range dei servizi "Well Known" (<1024).

[C13-X] Come posso proteggere la mia Linux box senza pasticciare troppo con pacchetti, protocolli e troiai vari?

Inserisci nel file /etc/hosts.deny la seguente regola:

ALL EXCEPT identd: ALL EXCEPT localhost 10.0.0.0/255.0.0.0

[E dopo un'eternitàfinalmente ho inserito nelle FAQ il giusto consiglio di MdI]

[C14-X] Si può intercettare tutto cio` che transita attraverso la porta seriale?

Nei sistemi Unix i dispositivi sono visti come file, contenuti nella directory /dev/. È possibile creare un device /dev/a che si incarichi di rimappare tutto (tenendo traccia di cio` che interessa) verso il dispositivo dev/xxxx da controllare. Bastera` a questo punto che le applicazioni usino /dev/a invece di /dev/xxxx. Questo compito è svolto da ttysnoops, disponibile su Sunsite alla URL /utils/terminal/ttysnoop-*.taz

[C15-X] Si può intercettare tutto cio` che transita attraverso la porta seriale?

Nei sistemi Unix i dispositivi sono visti come file, contenuti nella directory /dev/. È possibile creare un device /dev/a che si incarichi di rimappare tutto (tenendo traccia di cio` che interessa) verso il dispositivo dev/xxxx da controllare. Bastera` a questo punto che le applicazioni usino /dev/a invece di /dev/xxxx. Questo compito è svolto da ttysnoops, disponibile su Sunsite alla URL /utils/terminal/ttysnoop-*.taz

[C16-X] Come posso monitorare una redirezione in corso?

Il lamer chiede: "Ridirigimi la tua QUERYPORT su TARGETHOST:TARGETPORT" e un micro-diavolo aggiunge temporaneamente

$QUERYPORT stream tcp nowait nobody /usr/bin/netcat /usr/bin/netcat
-o /tmp/netcat-$LAMERIP.log $TARGETHOST $TARGETPORT

a /etc/inetd.conf, quindi invia un SIGHUP a `pidof inetd`

Tu fai

tail -f /tmp/netcat-$LAMERIP.log e ti leggi quello che scrive il pollo, con tanto di suo *vero* IP 8-D

...in Windows, tutto ciò non so neanche se si possa fare.

Leonardo che forse sì . Dieci mega fra eseguibile e bestemmie

*** (C) Leonardo Serni ***

[C17-X] Come posso limitare il login come root solo alla console (e impedirlo da remoto)?

Esiste il file securetty che elenca i terminali da cui permettere l'accesso a root. Se non esiste, è VIVAMENTE consigliabile crearlo, per esempio con questo contenuto:

tty1
tty2
tty3
tty4
tty5
tty6

se vuoi connetterti come root solo dalle console virtuali (parliamo di linux) 1-6, altrimenti aggiungere i terminali richiesti... nel file stesso, se giàpresente, non devono inoltre comparire righe che si riferiscono ad accessi via linee seriali, modem, e anche rete (tutti quelli che dopo la stringa tty hanno lettere maiuscole o minuscole prima o dopo il numero).

[C17-X] Che permessi è opportuno impostare per i file usati per il collegamento?

/sbin/pppd

-rwsr-s---	1 root	pppusers	109572	Aug 10 1998	/usr/sbin/pppd/sbin/chat
-rwxr-xr-x	1 root	root	15924	Aug 10 1998	/usr/sbin/chat/etc/ppp/options
-rw-------	1 root	root	94	Apr 2 13:04	options.flashnet/etc/ppp/pap-secrets
-rw-------	1 root	root	108	Apr 20 13:04	pap-secrets.<conn>/dev/modem
lrwxrwxrwx	1 uucp	root	10	Feb 7 11:44	/dev/modem -> /dev/ttyS2
crw-------	1 uucp	root	4, 66	Apr 21 14:51	/dev/ttyS2

[C18-X] Dove trovo/come loggo gli eventuali vari tentativi di accesso (soprattutto quelli riusciti)?

Di solito /var/log/messages e se lo usi /var/log/iplogd.log

[C19-X] Perchè non vedo loggate le connessioni entranti sull'Xterm?

Un buon metodo per vederle è spararle su una consolle tipo tty7+. In ogni caso, dipende da quale stato del syslog usino. Provare al limite con qualche bel grep sui log. Ad ogni modo può anche darsi che le rule di log di tali binari vadano specificate meglio.

[C20-X] Non riesco a lanciare la connessione ppp senza essere root!

Questo è il messaggio, o comunque simile?

/usr/sbin/pppd: must be root to run /usr/sbin/pppd, since it is not setuid-root

Si potrebbe lanciare lo script come root e poi navigando come utente normale, ma se si vuole abilitare degli utenti ordinari a lanciare una connessione di questo tipo, la soluzione esatta la dà Linux stesso nel messaggio di errore, che dice che pppd deve essere suid root (login: root e chmod u+s /usr/sbin/pppd); a quel punto, se anche lo lancia un utente normale, pppd ha diritti root. TENERSI INFORMATI SU BUG E RELATIVE PATCH/AGGIORNAMENTI DISPONIBILI, come sempre.

==========

[D01-ALL] Un attacco sembra venire dall'indirizzo x.y.w.z. Posso essere sicuro che provenga da veramente da lì ?

Non è detto. È possibile fare in modo che i pacchetti trasmessi da un certo indirizzo IP sembrino arrivare da un altro; la tecnica si chiama __spoofing__. Quando si riceve un tentativo di attacco e il programma usato per monitorare la rete riporta un certo indirizzo di provenienza, è bene non passare direttamente al contrattacco, perchè si potrebbe colpire qualcuno che non c'entra niente, rendendolo la seconda vittima dell'attacco (il suo indirizzo IP potrebbe essere usato come indirizzo di provenienza dell'attacco per vari motivi, non ultimo una forma di "ritorsione" contro il proprietario di tale indirizzo).

*** (C) Leonardo Serni ***
Se uno proprio vuole assicurarsi (nei limiti del possibile) di chi effettivamente ha fatto ping:
1) Risponde
2) Risponde a tono ai comandi più ovvi
3) Se, come nel 75% dei casi (esperienza mia) arriva il comando di attivazione web server, dice di sì
4) Quando arriva una connessione TCP da quell'indirizzo alla porta 80, _ALLORA_ l'identità del tizio è non dico SICURA, però insomma abbastanza PROBABILE.

*** fine (C) ***

[D02-ALL] Riesco a beccare un attaccante che usa ICQ?

Pare che ICQ dia la possibilità di nascondere l'IP. In realtà si può usare il programma ICQ Sniffer, 85 Kb, per scoprire l'IP in "quasi" ogni caso. Questo programma, però, non sembra del tutto affidabile: infatti può fornire numeri IP diversi se usato a distanza di qualche minuto, e sembra più attendibile nel caso di IP statici.
Un metodo alternativo prevede l'uso di un programma come AtGuard. In tal caso basta mandare un messaggio ad uno degli utenti della propria lista online, e, anche se questo non risponde, andando a vedere nella lista delle connessioni si trovano IP e porta di comunicazione del destinatario [funziona anche con netstat?].
In conclusione un consiglio sempre valido è: fare attenzione a chi si dà l'autorizzazione per la contact list.

*** Integrazione a cura di Enrico Gallesio ***

[D03-ALL] Ma è proprio sicuro che l'IP che scopro è quello dell'attaccante?

Basta che l'attaccante utilizzi un proxy dedicato, per rendere inefficaci i tentativi di scoprire il proprio IP. In questo caso, il programma utilizzato, come ICQ sniffer, riporterebbe l'indirizzo IP del proxy invece di quello effettivo. Perciò vale anche qui la regola di pensarci bene prima di rispondere al fuoco...

[D04-ALL] Ci sono programmi con cui mi posso difendere in maniera più "attiva" e magari rispondere per le rime? >:-]

La prima cosa che bisogna dire è che se è illegale che qualcuno violi le nostre macchine, altrettanto lo è rispondere al fuoco, o meglio, lo è se il nostro scopo è quello di danneggiare a sua volta l'attaccante. Ciò non vuol dire che non si possa "rispondere al fuoco" in maniera innocua e lecita, ma tale da divertirci un pò alle spalle dell'attaccante, cercando magari di fargli capire che forse è meglio che si cerchi altri svaghi.
Come primo tentativo, ci si procuri il client delle solite backdoor (Bo, NetBus, TeleKommando, 'r tegame di su mà). Più frequentemente di quel che si pensa, infatti, i lamerini che vanno a caccia di backdoor hanno a loro volta anche il server installato, o perchè fanno esperimenti su se stessi senza proteggersi, o perchè hanno scaricato versioni "non proprio affidabili" delle backdoor da siti non ufficiali, e queste installano il server a loro insaputa. Senza procurare loro danni, si può fargli apparire sul desktop un messaggio di "avvertimento", da rendere via via più "deciso" se i tentativi non cessano.
Esistono poi dei programmi che simulano i server delle backdoor, in particolare NetBuster per NetBus e BoFake, BoSpy e NoBo per Back Orifice. Tali server (perchè server sono a tutti gli effetti) si mettono in ascolto sulle porte opportune, e all'arrivo di una richiesta di connessione rispondono, permettendo fra l'altro di loggare le azioni che l'attaccante richiede al server. È possibile (nel caso di BoSpy) far anche apparire al client un sistema virtuale definito in appositi file di configurazione.

ATTENZIONE: L'USO DI TALI PROGRAMMI VA FATTO SOLO SE PERFETTAMENTE CONSAPEVOLI DEL LORO FUNZIONAMENTO. Inoltre il loro utilizzo potrebbe non essere lecito ai sensi delle leggi in vigore.

[D05-ALL] Come faccio a sapere chi mi attacca su IRC?

Sono disponibili i comandi /who e /whois. Al primo si deve passare l'IP di un utente, ma può capitare che la risposta sia

xxx.xxx.xxx.xxx End of /who list?

Il problema è che se l'utente si è marcato "invisibile" non è possibile rintracciarlo con /who, tranne FORSE nel caso in cui si sia collegati nello stesso canale dove è collegato lui.
Con /whois, invece, si raggiungono anche gli "invisibili", a patto di digitare correttamente il nome del nick.

[D06-ALL] Come rintraccio un attaccante in IRC?

/who *<ip>*
/dns ip
*** Resolved 12.34.56.78 to <host>
/who *<host>*

e ottieni il nick se sta su uno dei tuoi canali

/msg <nick> Ciaoo :)

Più di questo non puoi fare

*** (C) Frankj ***

[D01-W] Ho installato un firewall fra il computer e la rete e Nuke Nabber non vede più gli attacchi.

Significa che il firewall sta facendo il suo dovere. Se i nuke e i tentativi di connessione non arrivano più al NN, vuol dire che sono stati giustamente neutralizzati. Sappi che con questa configurazione Nuke Nabber è "ridondante", in quanto i suoi compiti (monitorare la connessione su certe porte) sono svolti dal firewall, che fa anche dell'altro; in

particolare, il log di NN sarà sempre praticamente vuoto. Per conoscere ugualmente eventuali attacchi, puoi far sì che sia il firewall stesso a loggare i pacchetti che vengono intercettati, l'effetto collaterale di questa configurazione sarà costituito da eventuali DoS che ti faranno finire lo spazio su disco quando i tentativi diventeranno troppo numerosi, e questi potrebbero essere fatti proprio a questo scopo.
Con un firewall installato, Nuke Nabber può comunque essere utile, infatti possiamo fargli monitorare la connessione con il firewall. Perchè? Perche se NN dovesse vedere qualcosa nonostante il firewall vuol dire che l'attaccante ha trovato il modo di crashare o bypassare il firewall stesso arrivando fino alle tue porte, e a questo punto si può già parlare di "intrusione" (anche ai sensi del codice penale).

[D02-W] Si può, a chi usa NetBus, far vedere solo quel che voglio io?

Sì , con un programma chiamato NetBuster, che simula il server netbus dando l'illusione di essere dentro un sistema. In realtà quello che vedi e che fai è solo un illusione, l'attaccante sta solo vedendo e facendo ciò che vuole NetBuster, che in quel momento sta monitorando tutto quel che avviene scrivendo le azioni compiute in un file log insieme all'ip e ad altri dati. L'indirizzo è:

http://fly.to/netbuster

È possibile configurare il programma in modo tale che i lamers pensino che sia un vero NetBus.

[D03-W] Esistono dei programmi che simulano Bo?

Sì , ne esistono diversi. Uno di essi è NoBo che si può trovare qui:

http://web.cip.com.br/nobo/

però non ha le stesse funzioni del netbuster, infatti NOBO si limita a registrare ciò che fai dentro un sistema e ti consente di inviare dei messaggi all'intruso, ma non impedisce l'accesso al sistema come NetBuster (creando un sistema virtuale dove non è possibile fare danni), nè individua od elimina il server di BO. È possibile avere informazioni sull'intruso (ottenibili anche con NukeNabber settato sulla 31337) ma non fornisce protezione contro attacchi vari. Secondo gli autori di NOBO è possibile che il BO possa essere usato su una porta diversa dalla 31337 inficiando così il controllo di NOBO. In ogni caso, versioni >1.2 permettono di scegliersi la porta.
Un altro programma è BoSpy, che sta a Bo come NetBuster sta a Netbus. Con BoSpy si può loggare chiunque tenti di entrare dalla 31337; il programma crea un fake server in tutto e per tutto, simulando le varie risposte alle azioni del "visitatore", ed è comodissimo per vedere che intenzioni ha l'intruso e agire di conseguenza. Molto carino e funzionale, supporta anche la funzione di invio messaggi, facendoti vedere ip e porta da cui arriva il ping.

[TNX ChRoMe]

[D04-W] Ho un programma antiBo o anti-NetBus, e NukeNabber mi segnala la backdoor!

Tranquilli, non è successo niente. Quei programmi sono a tutti gli effetti dei server delle relative backdoor, che per funzionare devono stare in ascolto sulle opportune porte. Se NukeNabber controlla quelle porte anche lui, si accorgerà che c'è "qualcosa" in ascolto e, come deve fare, lo segnalerà diligentemente. La soluzione è di togliere il monitoraggio della porta segnalata da parte di NN; se c'è già un programma che l'ascolta è inutile che ce ne sia un altro.

[D05-W] È possibile bypassare la pasword di NetBus???

Fai un copia-incolla con queste stringhe:

Password;1,Password

poi premi return, ti appare scritto

Access;1.60 ServerPwd;Password

in questo modo setti la pass del netbus su "Password"; poi dal client del netbus, quando ti appare la richiesta inserimento password, metti quella pass lì . Naturalmente la parola Password dopo ServerPwd è indicativa e la puoi cambiare a piacimento.

Da questo momento puoi usare il client nel modo che vuoi. Si rinnova qui il consiglio, di non fare la carogna, e di limitarsi a mandare avvertimenti.

[D06-W] È possibile sfruttare nella direzione opposta la "connessione" da parte di un BoClient?

In effetti, il BO funziona nelle due direzioni e con poca fatica si può risalire la connessione al contrario. Bisogna utilizzare delle versioni "sicure" di netstat e tracert, per esempio prendendo gli eseguibili dal CD-ROM di installazione di Windows e comprimendole con appositi programmi (NON NEL SENSO DEL WINZIP!!!). Questo, per evitare che il boserverizzatore possa toglierci due strumenti molto utili. Un consiglio ulteriore, se si ha un masterizzatore o un amico che ce l'ha, è quello di preparare un CD-ROM contenente programmi di utilitàvari come i due succitati, in modo da poterli ripristinare in caso di intrusioni distruttive.
Se il PC che attacca ha determinate caratteristiche, si può dedurre che o è un pirlone galattico, o è un boserverizzato che fa da relay. Possibili indizi: shares aperte, Back Orifice installato, e simili... Con poca fatica si può (a) capire se c'è Netbus o BO su quel PC, e (b) entrare nonostante password varie (Netbus: istantaneo; BO: pochi minuti).
Si lancia poi il NETSTAT sicuro sul PC boserverizzato, e si può scoprire (in poco tempo o subito, a seconda, se il boserverizzatore ha attivato servizi TCP) da quale IP viene controllato. Prima di tutto si fa saltare il BOSERVER in modo da bonificare quel PC; si prosegue nella catena nel caso si tratti di un BO multiplo, arrivando così al boserverizzatore. E qui, come dice l'autore del messaggio originale, lo caa l'orso.

[D07-W] Perchè bisogna avere da parte delle versioni particolari di netstat e tracert?

Perchè, se si è in caccia di intrusi telematici, è necessario e utile poter vedere che cosa dicono netstat e tracert. Niente di più facile per questi figuri che impedire ciò, rimpiazzando netstat e tracert con due programmi che, per esempio facciano sì che la connessione si interrompa appena vengono attivati (appena inizia la caccia, in altre parole). Perciò, anzichè usare netstat e tracert del boserverizzato (per esempio), si usino i propri, che FORSE sono sicuri.

[D08-W] Come faccio a divertirmi un pò con i pingatori senza troppa fatica?

[Info tratte con adattamenti da un messaggio di Master e correzione di L.Serni]

Se si ha un minimo di esperienza di programmazione, ci si può cimentare nella creazione di un programma adatto all'uopo :-))
La libreria Windows che fa al caso nostro è la winsock.ocx. Tutto quel che si deve fare è aprire un form con una connessione UDP, mettere il programma in ascolto sulla porta 31337 UDP (nel caso si voglia intercettare i BO-seekers) con UDPserver.localport 31337 e ricevere i dati. Ma come? Siamo sotto UDP, quindi non disponiamo di qualcosa tipo UDPserver.listen. La soluzione consiste nel settare sempre remotehost come se stessi (127.0.0.1, localhost) e localport 31337, e per la lettura dei dati si usa udpserver.getdata <p>, con p che punta a un dato di tipo stringa associato all'evento DataArrival.
Alla ricezione di un ping su quella porta, basta che con UPDserver.senddata si mandino sulla 31336 (la porta su cui riceve il client... quella giusta si può comunque verificarle) la stessa stringa che invia il Boclient col ping, presa per esempio con un copia/incolla dalla finestra di Nuke Nabber, seguita da un testo a piacere. Ricordiamo che i caratteri strani che su vedono sul N.N. sono l'header del protocollo di Back Orifice.
Quello sopra descritto è il cuore del programma, che può essere dotato anche di un'interfaccia più o meno ricca di opzioni (se gradite trastullarvi con il Visual Basic). Un'alternativa è costituita dall'uso di netcat, in modo simile a quanto appena descritto: con un primo netcat si ricevono i dati su udp e si registra l'ip del mittente, con un secondo si inviano i messaggi. Per realizzare il tutto basta un file .bat, al massimo due righe di un qualunque linguaggio per estrarre l'ip dalle videate info di netcat che purtroppo stravolge il pipe 'normalè per suoi specifici bisogni.
Per implementare il protocollo di Back Orifice si può usare un trucco. Per prima cosa, si metta in ascolto Nuke Nabber sulla porta 31337 UDP, oppure si fa la stessa cosa con netcat (netcat -l -u -v -v -p 31337), oppure ancora si fa il il solito programmino in VB o in C con l'evento DataArrival che, quando arrivano i dati del boclient, spedisce su una casella di testo il contenuto della stringa che si grabba con UDP.GetData. Ecco il trucco:
Far partire il boclient e settare ad esempio Process Spawn. Nei parametri si metta una frase a piacere (suggeriva "OH ROTTO N'CULO! FINISCILA!"), dopodichè si dàSEND su nukenabber o sul programmino o su netcat (quello usato, insomma) e viene fuori la frase giàcodificata. Nel caso in cui si sia usato il winsock, su UDP.RemoteHostIp si avrà l'IP del tizio che ha mandato roba col boclient (casualmente in questo caso sei tu, 127.0.0.1) mentre su UDP.RemotePort è settata la porta che ha usato il Boclient per mandare il tutto.
Se tu adesso su UDP alla stessa porta, e settando

```
UDP.remoteHost = UDP.RemoteHostIp,
```

mandi con UDP.SendData quella stessa stringa, sul BoClient esce una scritta come se si fosse fatto il ping ad un boserverizzato e quello avesse risposto con

```
 Pong .. ip found.. ecc..ecc..
-----------------------------------------------
 OH ROTTO N'CULO! FINISCILA!
-----------------------------------------------
```

TRUCCHI BASTARDI:

Se al posto di <UDP.SendData stringa> si manda un bel

```
DO { UDP.SendData stringa } UNTIL (FALSE)
```

il nostro avràdi che meditare... :-DD

Ancora, dato che quello che scassa veramente l'anima è lo scrolling della finestra, il divertimento massimo consiste anche nel mandare una sequenza di CR + LF fino alla saturazione del buffer. Tra l'altro si può comprimere molto, e si trasmette non malaccio.

[D09-W] A chi volesse contrattaccare usando BO.

Connessione a 192.168.0.119: "PONG!1.20!CHAPLIN" - SUCCESSO!
Connessione a 192.168.0.168: "PONG!1.20!TOWER" - SUCCESSO!

Se, connettendovi con BO a un computer remoto, ottenete una delle precedenti risposte, desistete immediatamente dal tentativo.

[D10-W] A chi volesse contrattaccare a una connessione Netbus.

1) mandare la stringa con winsock1.sendata("Netbus Server 1.70" & vbCrLf) al"evento winsock1_request connection().=>Il client penseràdi essere connesso
2) mandare al client con winsock1.sendata("Info;messaggio" & vbCrLf) n volte (mettendolo in un ciclo for).=> nel momento della connessione il client riceverebbe n msgbox con scritto "messaggio".
3) a voi tutte le modifiche necessarie (flood,colloqui diretti,frasi per sfottere con tanto di valore di ritorno del bottone del msgbox premuto...etc)!

Il mio è un consiglio..non offenderti :-P

*** (C) ??? - se mi leggi e vuoi essere citato qui, scrivimi ***

[D01-X] È possibile capire le intenzioni di chi pinga con BoClient?

I comandi in arrivo da un Bo client si possono in effetti riconoscere, cosa che fa il programma udplog v. 1.7 disponibile per Linux. Esso distingue fra ping BO "classici" e "buoni samaritani". Risponde come un PC boservizzato e sta a vedere se invii un codice 0x09 (gruppo zero), 0x31/0x3F/0x26/0x2A/etc (gruppo uno) oppure 0x02,0x03,0x04 (gruppo due).
Il gruppo zero sono i codici da buoni samaritani (appare la dialog box), il gruppo uno sono codici da curiosi e FORSE buoni samaritani. Il primo codice "gruppo due" che passa ti identifica per figlio di puttana e autorizza pure l'intervento della magistratura 8-D, cosa che il ping non fa.

*** (C) Leonardo Serni

[D02-X] Non riesco a far lanciare programmi al BoClone!

In udplog.conf, nella sezione [Misc] dev'essere inserita una riga del tipo:

```
boclone=/usr/local/sbin/my-queSO
```

Poi bisogna creare e rendere eseguibile lo script my-queSO:

```
--------------------
   #! /bin/sh
   queSO $1 | mail root
--------------------
```

In questo modo l'output di my-que-SO arriva per e-mail. Ovviamente è possibile ridirigere l'output su file, ecc. Se neanche così funziona c'è un intoppo, come per esempio se le prove avvengono in loopback. Infatti in udplog.conf l'indirizzo 127.0.0.1, di default, è risolto come localhost, quindi allo script viene passato "localhost", ma se in /etc/hosts c'è localhost.localdomain per fare andare sendmail, queSO non trova l'host.
Un difetto è che così ad ogni comando inviato dal pingatore verrebbe lanciato lo script (cmq, $2 è l'IP risolto, mentre $1 è quello non risolto): non ha senso rifare ogni volta un queSO o uno stealth scan, per cui un'alternativa è la seguente.

```
##### (C) LEONARDO Serni #####
   # Crea una log entry ordinabile per data ed IP

   LOGENTRY="$( date +%Y-%m-%d-%H-%M ):$1"
   LOGFILE=/var/log/boscript.log
   LOGTEMP=/tmp/tmp-boscript.$RANDOM.$$

   if [ ! -r $LOGFILE ]; then
         touch $LOGFILE
   fi

   if ( grep "$LOGENTRY" $LOGFILE >/dev/null ); then
   # L'amico è conosciuto, si esce
         exit 0;
   fi

   # Qui andrebbe altra roba per essere sicuri di non
   # essersi ciucciati un UDP spoofato a bestia... sai
   # che ganzo se uno manda un UDP da "127.0.0.1" ?

   grep -v "$LOGENTRY" $LOGFILE > $LOGTEMP
   OS=$( queso "$1:139" )
   SHARES=$( nbtstat -W "$1" | grep "<" | tr -d "\t " | tr "\n" ":" )
   echo "$LOGENTRY:$OS:$SHARES" >> $LOGTEMP
   cat $LOGTEMP > $LOGFILE

   #Eventualmente facciamo saltare la connessione per omnia saecula
   #saeculorum. Un file contiene gli indirizzi "sani" che NON devono
   #essere fatti saltare (ulteriore protezione antispoof).

   if ( ! grep "^$1=\|^$2=" /etc/udplog-dontkill.conf >/dev/null); then
         #ipfwadm ...
   fi

   rm -f $LOGTEMP
```

Altra soluzione:

Sezione [Misc] (versione 1.7d/1.7e):

```
   script=/usr/local/bin/che/mi/frega/script-file
```

Sezione [Rules]
...una regola che invochi "script x", x=modificatore a caso, se
indifferente usare 'pianò ("script piano").

```
   chmod +x /usr/local/bin/che/mi/frega/script-file
```

(altrimenti non viene eseguito), e script-file nella forma:

```
##### (C) Leonardo Serni #####
   #!/bin/sh

   # Let's play a sound
   cat /usr/share/sounds/au/computer.au >/dev/audio

   # Let's leave trace into system logs
   logger "UDPScript[$5]: got UDP from $1 [$2], port $4, to local $3"
   # (Vedi nota (1)

   cat<<-MAIL | mail root

         Someone is trying to access the machine.
         Address: $1 [$2]
         OS: $( queso $2:137 )
         nbtstat:
         $( nbtstat -W $2 )
         host -a $2:
         $( host -a $1 )
         $( host -a $2 )
         traceroute $2 2>/dev/null
         $( traceroute $2 )

   # DANGEROUS
   # It is possible to SPOOF an UDP packet and force your PC
   # to block ANY source subnet.
   # Use ipfwadm only if confirmed in some other way (TCP if
   # at all possible, with at least one GET from bo-http and
   # a non-portable one at that _AND_ no misgets, see README
   # for bo-http for details).
   #
   # /sbin/ipfwadm -I -i deny -S $2/24 -o

   MAIL

   exit 0;
```

Se il problema continua, verificare l'invocazione dei programmi nello script.
Infatti, anche se essi si trovano nella path della shell, nello script non vengonono chiamati se non era indicata la path completa. Fatto questo, funziona tutto.

(1) $4, in script, restituisce 'port 10xx' e non solo '10xx'... lo so che è una cosa di poco conto... ma... :))

*** (C) Leonardo Serni ***

[D03-X] E archiviare i tentativi di accesso con BO a fini statistici?

Occorre un server attivo 24h, un programma che logga i ping ed un altro che li infila in una pagina web. [Sol. per udplog 1.7.] Mettere "boclone" come risposta standard ad invii UDP su porta 31337 in /etc/udplog.conf, e nel file "boclone" ci va, su una sola riga:

```
##### (C) Leonardo Serni #####
   WEBLOG="lynx -dump
   http://www.loggersite.com/cgi-bin/bologger.cgi?HOST=$1&PACKET=$3
   >/dev/null"
```

...metodo semplice e brutale. Poi nel caso 1) (ping):

```
   case "$TYPE" in
         1)    # Hès pinging. We be good and reply in kind.
               echo -n "!PONG!1.20!$HOSTNAME"
```

```
            $WEBLOG &
        ;;
```

Naturalmente occorrerebbe prendere precauzioni contro possibili DOS ottenuti mandando tempeste di PING spoofati... o con DNS contenenti shell metacharacters.
Eventualmente, nelle prime righe, si mette

```
HOST=$( echo "$1" | tr -cd "A-Za-z0-9-." )
```

anzichè

```
HOST="$1"
```

...stesso discorso o quasi per ARG1 ed ARG2 (anche passando parametri "carogna" a a boclone, non ci sono effetti collaterali, ma non è mai detto). Infine, per ottenere le reti di origine (non gli IP! la 675 incombe!), una volta che si ha lo host, il comando è cut -f1-3 -d'.'. Notare che non è possibile sapere a chi corrisponde un IP, in generale, o chi sia. Di conseguenza, se violazione di privacy c'è, la opera chi "mappa" l'IP sull'utente, e dunque il provider.

==========

[E01] Il ping di BO si configura come sabotaggio informatico, violazione della privacy o roba del genere?

Paradossalmente, no. La legge 23 dicembre 1993 n. 547 definisce i "reati informatici", ma il semplice PING del Back Orifice non è, in sè, reato (non configura nè la fattispecie di "alterazione di funzionamento", né quella di "violenza sulle cose" in senso lato).
L'unica apparenza di punibilità perciò (nel caso di un PING) deriva da come tale PING è stato inviato, i.e. usando un client Back Orifice? Nel caso, il pingatore è in possesso di uno strumento "atto a...", e quindi (in teoria!) si configura la fattispecie di possesso di strumento idoneo a introdursi in un sistema telematico od informatico (art. 615 quater). Ma si tratta di una interpretazione piuttosto ambigua, perchè tale art. è nato con in mente il *traffico* delle *password*, non la *detenzione* di *tools*. Appare tuttavia possibile una estensione per analogia. Cioè tutto dipende da quanto è cazzuto il PM :-)
Inoltre ci si deve basare su una interpretazione relativa ad un reato di pericolo; il ping viene cioè visto come "attività ordinata ad ottenere l'accesso ad un sistema informatico o telematico". Sarà, in caso, onere dello hacker dimostrare che questa attività (pur svolgendosi) non fosse però ordinata ad un fine criminoso.
Per esempio il seguente script

```
...
for i in $ICMP_FOUND_HOSTS; do
    if ( bo_ping $i 31337 "" ); then
        cat <<-HERE | bo_send $i 31337 "" 9
                Non dovrei essere qui. Lei ha
                installato BACK ORIFICE sul suo
                PC. Per rimuoverlo, consulti
                SUBITO http://www.kazzimazzi.com
                ---
                Finchè non lo farà, sarà possibile
                a me o ad altri ENTRARE NEL SUO PC!
        HERE
    fi
done
...
```

genera una *tempesta* di PING su una sottorete, ma, qualora acquisito da un inquirente, vale a dimostrare se non altro la buona fede - e il fatto che l'attività non fosse ordinata all'accesso abusivo.
Completamente diverso è invece il discorso, per chi si spinge al di là del semplice "ping":

```
Nov  2 20:28:48 jag BOCLONE: a-rm29-14.tin.it: <Send system passwords>
Nov 20 09:51:22 jag BOCLONE: [194.243.173.132]: <Send system passwords>
```

...in questo caso si procede a querela di parte. Io 'sti due non ho mica intenzione di querelarli, anche perchè il

secondo sta a 700 metri da me e se proprio volessi potrei pingarlo con una spranga ;-). E l'unica pass che hanno ricevuto è, credo, "gioppino".
Ma se li querelassi, il pretore acquisisce i dati di Telecom o di FOL, e qui c'è proprio una violazione del 615 quater: <Send System Passwords>, infatti, configura la fattispecie di "... procurarsi abusivamente codici di accesso a sistemi informatici o telematici". Reclusione fino a 1 anno e multa fino a 10 milioni (il che vuol dire che può anche essere zero e zero).
In più c'è l'ingresso abusivo in un sistema informatico (e anche qui a dire il vero c'è da discuterci: "ingresso", significa shell?), art. 615 ter C.P., reclusione fino a tre anni. Se danneggia i dati od installa un rootkit, reclusione da uno a cinque anni. Appare palese che per chi vada ad installare il BOServer via NetBEUI si configuri appunto tale ipotesi.
Inoltre l'A.G. può acquisire ugualmente i dati, anche in assenza di una denuncia: "...nella stragrande maggioranza dei casi l'interessato è del tutto ignaro della effettuazione di un illecito ai suoi danni [...] vero è che in tal caso trova applicazione l'art. 346 CPP per cui in mancanza di una condizione di procedibilità [la querela di parte, NdR], che può ancora sopravvenire, possono essere compiuti gli atti di indagine preliminare necessari ad assicurare le fonti di prova..."

[E02] Ma il ping di BO comunque è configurabile come tentativo?

Sì , più che altro perchè il Back Orifice serve unicamente come backdoor o come "amministrazione remota" -- ma ENTRAMBE queste attività, se svolte su PC di terzi senza il preventivo consenso, sono reati.
Però il tentativo in sè non è un reato: e il fatto che POSSA essere una attività ordinata a commettere un reato, non significa che lo SIA. Però, naturalmente, a quel punto tocca al pingatore dimostrare di essere onesto.
Per esempio, uno che giri intorno ad una casa osservando finestre, porte e serrature *PUÒ* essere un curioso... come un ladro che studia il colpo; e infatti l'articolo 55 del CPP prevede fra i DOVERI della P.G.:

- prendere notizia di reati: attività informativa, diretta ad assumere la conoscenza della perpetrazione di reati, già commessi od in fieri; può essere svolta sia in forma tipica che in forma atipica. "Forma atipica", in linguaggio tecnico, significa "post civetta, tcpdump e sniffers sulla porta 31337 a tutti i providers; monitoraggio newsgroups; ecc.". (Non si incazzi, Brigadiere: io mi limito a riportare l'ovvio).

Va da sè che le notizie così acquisite non possono dare l'avvio ad una indagine in mancanza di una precisa nozione di reato. In pratica, se uno risulta originare o ricevere uno svagello di attività UDP:31337, questo non autorizza a piombargli in casa fisicamente o telematicamente. (Allo stesso modo, le pattuglie sul territorio _possono_ vedere per caso il ragionier Brambilla con l'amante; e a questa violazione della privacy il ragioniere deve sottostare. Purtroppo, per poter vedere un reato, uno deve tenere gli occhi aperti, e se li tiene aperti vede _TUTTO_; ci sono regole che stabiliscono che cosa uno deve far finta di non aver visto).
A dire il vero questo mi pare confligga con l'art. 13 della Costituzione - ma in effetti, quello parla della sfera _personale_, mentre un tcpdump sul provider è quanto di più _impersonale_ ci possa essere :-) ... sul merito c'è una sentenza (n. 30, 27/03/1962) della Corte Costituzionale, che in effetti ha compendiato l'art. 4 del testo unico sulle leggi di P. S. e che con qualche fatica si potrebbe estendere all'ambito telematico.

- impedire che i reati giungano a conseguenze ulteriori
- ricerca degli autori dei reati: a reato commesso e stabilito, la P.G. si dedica a individuare il reo, sia con atti atipici che con atti tipici (e cioè perquisizioni, fermi, arresti in flagranza, ecc. ecc.).
- individuazione ed assicurazione delle fonti di prova (qui ci si deve poi rifare alla definizione di 'fonti di provà telematica, data dalla legge 547/93; e le attività in ordine a questa sono poi governate dagli artt. 350,351 ("cat /var/log/messages"), 352 ("find / -[...]"), 353 ("tar czvf /zip/mailboxes.tgz /var/spool/mail/*"), 354 ("toc toc! - chi è? - apra, Polizia").

In presenza di "comportamento sospetto" nel mondo fisico, la P.G. può, di iniziativa, sottoporre a misure limitative della libertà personale.
Nello specifico (legge 22 maggio 1975 n. 152), coloro il cui atteggiamento o la cui presenza, in relazione a specifiche circostanze di tempo e luogo, non appaiono giustificabili, possono essere sottoposte a perquisizione, al fine di individuare oggetti o strumenti atti a nuocere.
Poichè la legge 23 dicembre 1996 n.547 ha esteso il concetto di domicilio alla sfera telematica, si potrebbe altresì estendere il concetto di "pura presenza"; per esempio se io telnetto su www.nasa.org, "in un certo senso" sono "telematicamente presente", alle porte di www.nasa.org. Nè del resto si potrebbe configurare una violazione di domicilio esteso in senso fisico (altrimenti la legge mi punirebbe solo se io mi introducessi *FISICAMENTE* nel computer di un altro, passando per es. dal buco del floppy!).
Ma questa è una elucubrazione mia, che sostengo solo fino al rogo escluso - la verità è che la legislazione in materia è un gran casino, e basata su "estensioni analogiche" - e mi viene in mente il diverbio fra i rabbini chassidici (?) se l'elettricità sia o meno "fuoco". Perchè se lo è, nel giorno di sabato non si può accendere la luce; e se non lo è, si può, a patto che s'installi un condensatore in parallelo che elimina la scintilla di apertura circuito, la quale sicuramente è compartecipe della natura di fuoco.
Fra un pò sentiremo discutere se un SYN scan sia "comportamento sospetto" essendo "assimilabile analogicamente" ad un "agire furtivo" 8-D

La mia impressione generale è che, se uno fa casino, lo prende nel ciocco come sonare a predica; altrimenti, tutto dipende da chi è e da chi ha nel ruolo di avvocato. In pratica uno già cuccato a telnettare in casa altrui è bene che smetta di usare anche il normale "ping" di Windows :-)

[E03] Se installo Back Orifice via NetBIOS su Internet ad un tizio che non sa niente, mi possono beccare? E cosa mi possono fare?

La risposta si articola nei seguenti punti:

1) L'installazione sopradetta configura la violazione dell'art 615 ter, comma due (violenza sulle cose, come da definizione ex art 392 comma due CP) del CP, e in aggiunta art 615 quinquies.
2) Sì , ti possono beccare in un modo semplicissimo, che io (fossi nel nucleo di Polizia delle Telecomunicazioni) avrei installato da parecchio tempo (del resto, è previsto dalla legge). Basta, evidentemente, che tu ti colleghi dal telefono di casa tua, poi avere l'indirizzo è questione di due (2) ore.
3) Reclusione da un minimo di un anno a un massimo di cinque, più multa sino a lire venti milioni.

Contrariamente a quanto io stesso credevo, NON è necessaria la denuncia del boserverizzato: si procede d'ufficio (50 CPP) e la competenza è pretorile (7 CPP). Non è consentito il fermo di indiziato del delitto, nè l'arresto, o tantomeno l'adozione di misure cautelari personali.

==========

*** APPENDICI ***

[PORT-Appendice] - Elenco ragionato delle porte più utilizzate
by Maurizio Cimaschi
integrato da Marco Zani

Ecco un' elenco delle porte più utilizzate, alcune indicazioni fanno riferimento a risposte date nella FAQ, e si rimanda ad esse.

Legenda:
Porta (Prot): Indica la porta ed il protocollo utilizzato
C/S: Se si tratta di un servzio lato server oppure lato client, se non vi è alcuna indicazione significa che non è rilevante
WKS: Indica il tipo di Well Known service (se presente).
Monitorig: Se deve essere monitorato dal programma Nuke Nabber (o simili), il valore può essere (a) o (b), sul significato si rimanda alla domanda [C01a]
Poss. att.: Indica le possibilitàdi attacco alla porta.
Note: Varie ed eventuali, come ad esempio possibilitàdi attacco ai servizi presenti su quella porta, presenza di back door, ecc.

Sono elencati in ordine crescente rispetto al numero di porta e non per importanza.

Porta (Prot) : **ICMP** detta anche porta zero.
C/S :
WKS :
Monitorig : (a) e (b)
Poss. att. : Possono essere ricevuti pacchetti formattati in maniera anomala che mandano in crash lo stack TCP/IP.
Note : È la sezione relativa alla manutenzione del protocollo IP
**
Porta (Prot): **13** (TCP)
C/S: S
WKS: daytime
Monitorig:
Poss. att.:
Note
**
Porta (Prot): **13** (UDP)
C/S: S
WKS: daytime
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **19** (TCP)
C/S: S
WKS: ttytst source
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **19** (UDP)
C/S: S
WKS: ttytst source
Monitorig: (a)

Poss. att.: In winNT è possibile indurre la macchina a cortocircuitare le porte 21 e 53, mandando in crash lo stack TCP/IP
Note:
**
Porta (Prot): **20** (TCP)
C/S: S
WKS: ftp-data
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **21** (TCP)
C/S: S
WKS: FTP
Monitorig: no
Poss. att.:
Note: Il monitoring, se presente, non deve essere del tipo "chiudi porta", altrimenti quella macchina non può essere usata come server dal momento che rifiuterebbe a priori tutte le connessioni.
**
Porta (Prot): **23** (TCP)
C/S: S
WKS: Telnet
Monitorig: No
Poss. att.:
Note: vedi porta 21.
**
Porta (Prot): **25** (TCP/UDP)
C/S: S
WKS: SMTP - invio della posta
Monitorig: No
Poss. att.: Bug di Sendmail (Unix)
Note: Scaricare sempre l'ultima versione di sendmail (ftp://ftp.sendmail.org/pub/sendmail) Vedi porta 21.
**
Porta (Prot): **31**
C/S: S
WKS: Message Authentication
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **37** (TCP)
C/S: S
WKS: timeserver
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **37** (UDP)
C/S: S
WKS: timeserver
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **39** (UDP)
C/S: S
WKS: resurce location
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **53** (TCP)
C/S: S
WKS: DNS / Domain
Monitorig: No

Poss. att.:
Note: vedi nota porta 21. per winNT vedi anche nota porta 19
**
Porta (Prot): **53** (UDP)
C/S: S
WKS: Domain
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **69** (TCP)
C/S: S
WKS: tftp
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **70** (TCP)
C/S: S
WKS: gopher
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **79** (TCP/UDP)
C/S: S
WKS: Finger
Monitorig: No
Poss. att.: Puo essere usato per un "denial of service" attack
Note: Disabilitare il finger o montare una versione aggiornata
**
Porta (Prot): **80** (TCP/UDP)
C/S: S
WKS: Server WEB
Monitorig: No
Poss. att.: CGI/BIN attacks (PHF ecc.)
Note: Utilizzare sempre l'ultima versione del server Web Vedi porta 21.
**
Porta (Prot): **88** (TCP)
C/S: S
WKS: Kerberos
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **88** (UDP)
C/S: S
WKS: Kerberos
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **101** (TCP)
C/S: S
WKS: Hostname
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **103** (TCP)
C/S: S
WKS: X-400
Monitorig:
Poss. att.:
Note:

**
Porta (Prot): **104** (TCP)
C/S: S
WKS: X-400-send
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **109** (TCP)
C/S: S
WKS: POP2
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **110** (TCP/UDP)
C/S: S
WKS: POP3 - ricezione posta elettronica
Monitorig: No
Poss. att.: Possibile lettura file in posta
Note: vedi porta 21.
**
Porta (Prot): **111** (TCP)
C/S: S
WKS: RPC
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **111** (UDP)
C/S: S
WKS: RPC
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **119** (TCP)
C/S: S
WKS: NNTP - Server News
Monitorig: No
Poss. att.:
Note: vedi nota porta 21.
**
Porta (Prot): **129** (TCP)
C/S:
WKS:
Monitorig:
Poss. att.: (a)
Note:
**
Porta (Prot): **137** (TCP)
C/S: S
WKS: netbios
Monitorig: (a) e (b)
Poss. att.:
Note: È necessario disattivare NetBIOS (sempre che non se ne abbia bisogno). Oppure installare WinNuke95 e selezionare "patch aganist Nuke". Cancellare dal registro di configurazione le chiamate al driver di periferica virtuale vnetbios.vxd se la porta resta aperta dopo aver disinstallato NetBIOS.
**
Porta (Prot): **137** (UDP)
C/S: S
WKS: Netbios (nbname)
Monitorig:
Poss. att.:

Note: vedi porta TCP
**
Porta (Prot): **138** (TCP)
C/S:
WKS: Netbios (nbdatagram)
Monitorig: (a) e (b)
Poss. att.:
Note: vedi nota porta 137.
**
Porta (Prot): **139** (TCP)
C/S:
WKS: Netbios (nbsession)
Monitorig: (a) e (b)
Poss. att.: si con WinNt
Note: C'è un baco (??) nello stack TCP/IP di winNT, che risulterebbe vulnerabile a dati fuori banda. Vedi inoltre nota porta 137.
**
Porta (Prot): **143** (TCP)
C/S: S
WKS: imap2 - Interim Mail Access Protocol v2
Monitorig: No
Poss. att.: Possibile lettura file in posta
Note: vedi porta 21.
**
Porta (Prot): **555** (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note:
**
Porta (Prot): **666**
C/S:
WKS: MDQS
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **1027** (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note:
**
Porta (Prot): **1029** (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note:
**
Porta (Prot): **1032** (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note:
**
Porta (Prot): **1080** (TCP)
C/S: C-S
WKS: proxy
Monitorig: server No (e comunque vedi nota porta 21) client (a)
Poss. att.:

Note: Chi cerca una connessione sulla 1080 vuole mandare in giro per la rete pacchetti a nome vostro, alcuni ISP mettono a disposizione un server proxy per velocizzare le comunicazioni, ma un effetto collaterale è che tutti i pacchetti di uscita hanno l'indirizzo IP del PROXY.
**
Porta (Prot): **5000** (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note:
**
Porta (Prot): **5001** (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note: Porta destinazione degli attacchi di Socket de Trois.
**
Porta (Prot): **6667** (TCP)
C/S: S
WKS: IRC
Monitorig:
Poss. att.:
Note:
**
Porta (Prot): **8080** (TCP)
C/S: S
WKS: Server WEB
Monitorig: No
Poss. att.:
Note: vedi nota 21, alcuni server web utilizzano questa porta invece della standard (80).
**
Porta (Prot): **12345** (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note: È una delle due porte del server NetBus, si possono ricevere scan alla ricerca di quel programma.
**
Porta (Prot): **12346** (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note: È la seconda porta del server di NetBus, vedi nota porta prec.
**
Porta (Prot): **31337** (UDP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note: È la porta standard del server di Back Orifice, si possono ricevere scan alla ricerca di Boserverizzati.
**
Porta (Prot): **50505** (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:
Note:
**
Porta (Prot): 61466 (TCP)
C/S:
WKS:
Monitorig: (a)
Poss. att.:

Note: Porta destinazione degli attacchi di TeleCommando.

[BD-Appendice] Appendice BD

Name: **Back Orifice** 1.20 S.O. : Win95,Win98,Win3.XX
Ports: 31337(TCP&UDP)
Reg Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\(Predefinito)
Value: ".exe"
File: C:\WINDOWS\SYSTEM\EXE~1 (124.928)
C:\WINDOWS\WINDLL.DLL (8.192)
Note:

Name: **Netbus** 1.60 S.O. :Win95,Win98,WinNT
Ports: 12345&12346(TCP)
Reg Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PATCH
Value: C:\WINDOWS\PATCH.EXE /nomsg
File: C:\WINDOWS\PATCH.EXE (472.576)
Note: non è detto che il server si chiami patch.exe!!!! Quindi file e chiave di registro variano a seconda... altri esempi: splat1, explore, pamela, webaccel, icqupdate,... e molti altri!

Name : **Phase** S.O. :
Ports:
Reg Key:
Value:
File:
Note:

Name : **Telecommando** S.O. : Win95, Win98
Ports: 61466
Reg Key:
Value:
File: c:\windows\system\ODBC.EXE (~207 Kb)
Note:

Name : **Sokets de Trois** v1 S.O. : Win95, Win98
Ports: 5001
Reg Key:
Value:
File:
Note:

[WG-Appendice] WinGate, proxy casalingo

*** Da messaggi di Carlo e L.Serni ***

Wingate è un programma che permette di accedere a Internet da tutte le postazioni di una rete, pur essendo l'accesso fisico (a.k.a. modem) su un solo ocmputer. Ne esiste una versione per win95 e una per NT; la versione demo consente l'accesso ad un solo client per volta, ma la registrazione è veramente economica. Il programma funziona; va installato prima sul server con opportuni settaggi e poi sul client, dove offre una utilità che va a configurare in automatico i vari applicativi (browser, email, ftp ecc). La cosa fondamentale è avere il supporto del protocollo TCP/IP sia sul server che sui client. L'help del programma è molto ben fatto ed assiste passo passo.
Per configurarlo è semplicissimo:

1) Installare sul server e sui client i protocolli TCP/IP;
2) Configurare su tutte le maccihne il file hosts nella directory di sistema (per esempio C:\windows, C:\win32, C:\winnt, ...);
3) Controllare che il TCP/IP funzioni (es.: ping server, ping client1 etc.);
4) Controllare che il server abbia una connessione ad internet funzionante;
5) Installare il wingate sul server rispondendo a tutte le domande del caso (nome mailserver, nome newsserver etc. etc.);

6) In ogni client assicurati che il browser e qualsiasi altro prg. per internet abbiano come riferimneto sotto la voce "proxy server" il nome dato al server nel file hosts (se nel file hosts sul client c'è scritto

192.168.0.1 server

allora nella voce "proxy server" va messa tale voce;

7) Configura wingate con le varie opzioni (es. che ad ogni richiesta faccia il numero di telefono in automatico etc.);
8) Lanciare la connessione ad internet dal server e vedere se anche i client funzionano.

ATTENZIONE:
Wingate non permette il gioco via TCP/IP e alcune applicazioni simili, per il resto è ottimo.....
Per reti di più di 5 computers, è meglio un mini-server Linux. Basta una macchina obsoleta (486 o anche 386), senza monitor, ed ha svariati altri vantaggi - transparent proxying, firewalling, eccetera. OK, c'è da configurarla, e non è poco, ma...

[LINK-Appendice] - Siti che trattano di sicurezza dei sistemi informatici

Siti contenenti informazioni di vario tipo inerenti la sicurezza

http://www.nttoolbox.com
http://www.ntsecurity.net
Nella home page, notevole sulla sinistra i link diretti a diversi articoli in materia di sicurezza sotto NT

http://www.securityfocus.com
La casa madre delle mailing list Bugtraq e collegate, in inglese.

Programmi di utilità

http://www.hcvorg.com/ihu/welcome.html
Informazioni utili per ICQ

http://www.hack.cc/icq.html
Qualche utility per difendersi

http://surf.to/netbusprotector
A questo indirizzo si può scaricare il protector per netbus, che serve a mandare un messaggio di errore al client. Il messaggio può essere impostato, e in più il programma fornisce l'indirizzo IP da cui si tenta di controllare la macchina.

http://www.angelfire.com/id/chaplincorp/
BOSpy: un programma che finge di essere il server di Bo, e permette di vedere cosa sta tentando di fare il lamer di turno, e all'occorrenza "prendere provvedimenti" (Avvertenza: non diventare lamer a tua volta, limitati a rispondergli ^__^).

Protocolli
http://www.openssl.org
http://www.apache-ssl.org
http://www.apache.org
Secure Socket Layer, per connessioni http crittografate (quelle che iniziano con https:)

[INTERNET-CAFÈ-Appendice]

Questa appendice non ha la pretesa di esaurire l'argomento enunciato dal titolo.
Dato che però questo genere di locali e affini si sta diffondendo sempre più, almeno può dare qualche idea. La domanda, posta su it.comp.sicurezza.varie un bel giorno, è:

> Salve a tutti,
>
> a un mio amico, proprietario di un bar, è stata proposta l'installazione

> di un internet point.
> Legalmente non penso possa essere ritenuto responsabile di
> eventuali malefatte perpetrate da un cliente, però vorrei
> il consiglio di un esperto.
> (il mio amico non prevede di "monitorare" l'utilizzo della macchina
> come avviene invece in alcuni locali dove c'è sempre qualcuno che
> dàun'occhiata al monitor per vedere cosa succede)
>
> grazie

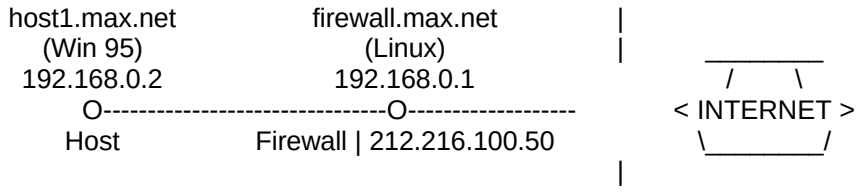
Anzitutto, una pratica diffusa è far lasciare un documento d'identità, dato il potere deterrente che ha anche a livello psicologico questa prassi. La cosa è comunque un pò delicata, dal momento che possono esserci dei casi di violazione della legge sulla privacy. Forse siamo al limite, forse un pò dentro, forse un pò fuori, ma data l'ignoranza delle istituzioni in materia Internet la strada da seguire può essere un altra, quella di rendere, se non impossibile, almeno parecchio arduo compiere reati e casini vari in rete. Ecco una soluzione.
Anzitutto, mettere sul gateway con Internet un filtro di pacchetti che permetta solo connessioni WWW, IRC, FTP, poi un proxy che salvaguardi la LAN dell'Internet Point ed i clienti dai simpaticoni su IRC stesso. Per telnet ci si può affidare ad un applet JAVA che permetta alcune connessioni solo dalla macchina PROXY mediante LOG del sistema chiamato. Questo permette di avere un controllo NON invasivo di quello che succede, nel caso un cui dall'host remoto si lamentassero.
NON permettere email, ma lasciar usare i vari sistemi via web tipo HotMail e co., in modo da non essere direttamente responsabile di minacce e spacci di droga, o simili. I sequestri a causa di email in Italia si contano sulla punta delle scaglie di GODZILLA, vedi alcuni noti casi recenti tipo Isole nella Rete (sempre considerando l'ignoranza di cui sopra).
Assicurarsi, soprattutto, di avere in mano la sicurezza delle macchine che saranno nel bar. Troppo spesso si vedono ragazzini in grado di manipolare il povero Win come fosse una trottola. Occhio al floppy, ai tasti di accensione (meglio sarebbe un controllo centrale dell'alimentazione), agli eseguibili che possano far bypassare l'uso del PROXY, e così via [Tenere conto che i ragazzini noiosi sono la minoranza rispetto agli allupati da xxx.com, ai capelloni da testi delle canzoni, ai caciaroni su #hottube ed alle ragazzine su dicaprio.net].
Nel caso però in cui la macchina o le macchine usate come client non siano di proprietà del locale, ma per esempio prese in affitto o comodato, modificare la configurazione hardware/software del sistema e/o installare e disinstallare applicativi potrebbe essere impedito dal relativo contratto. La soluzione, in questi casi, consiste nel mettere fra i client e Internet, o meglio fra il server e Internet, una macchina dedicata alla protezione da/verso l'esterno.
Se non è possibile togliere/disabilitare la spedizione di email direttamente dai client, magari per i suddetti problemi contrattuali, tale macchina dedicata farà da filtro e l'invio della mail dal client fallirà, analogamente per ogni altro servizio di cui si volesse inibire l'uso. Il computer da usare come firewall e/o proxy non è detto che debba essere di grande potenza, dal 486 in su vanno tutti bene e anzi già un 486 sarebbe eccessivo (però così se ci si vuole mettere qualcosina di più evoluto lo può fare senza strangolare la macchina): infatti i compiti richiesti non implicano una mole di calcoli elevatissima, nè la presenza di un'interfaccia grafica pesante come Windows o X-Window. Al limite, sarebbe persino superfluo il monitor se non per compiti di amministrazione che comunque non si fanno certo tutti i giorni.

[FIREWALL-Appendice]

Nell'appendice relativa agli Internet Point si è parlato di un computer da dedicare al compito di isolare la LAN di uno di questi locali da Internet; lo scopo è, in quel contesto, impedire ai clienti di compiere atti scorretti o addirittura illegali dalle macchine del locale stesso. Vediamo come si potrebbe ottenere lo scopo senza impiegare ingenti capitali :-)
La prima considerazione da fare è relativa al ricambio tecnologico che nel mondo dell'informatica è sempre più veloce. Questo ha portato a considerare obsolete macchine che fino a pochissimi anni fa erano all'avanguardia. Prendiamo ad esempio un 486 dx2 66 hd: di un aggeggio del genere era addirittura vietata l'esportazione nei paesi dell'Est, per la sua elevata potenza di calcolo!
Un'altra cosa da tenere presente è che l'attuale inadeguatezza di macchine come i 486 è dovuta principalmente alla pesantezza delle interfacce grafiche degli ambienti operativi contemporanei, da Windows 95 in poi. Stesso discorso per i sistemi Unix per quanto riguarda l'ambiente X-Window. Queste interfacce sono più facili (quasi sempre) da usare rispetto alla linea di comando, ma vogliono grandi quantità di memoria e di cicli macchina.

Perchè questa lunga introduzione? Perchè la necessità di un firewall per proteggere una piccola rete può essere soddisfatta recuperando proprio una di queste macchine, che altrimenti verrebbe buttata come un oggetto ormai inutile. È da tenere presente che un firewall deve essenzialmente monitorare il traffico da e per la rete che

sorveglia, per cui non deve far girare pesanti interfacce grafiche o applicazioni che ne saturerebbero le capacità di calcolo, ma le sue esigenze possono essere benissimo soddisfatte da un computer pre-pentium. Anzi, persino monitor e tastiera non sono strettamente necessari, potendosi compiere le operazioni di amministrazione via telnet o attraverso un terminale (magari recuperato anch'esso).
Sul 486 va ovviamente installato Linux, una qualunque distribuzione va bene. Il kernel va compilato includendo le capacità di rete, e vanno installati solo quei pacchetti strettamente necessari, quindi niente compilatori se non forse C e Perl nel caso occorrano, ASSOLUTAMENTE NO X-Window (vedi paragrafo precedente) e in generale niente che non abbia a che fare con il compito di firewall. Una volta installato il sistema e compilato il kernel, va configurato disattivando tutti i servizi inutili che occuperebbero memoria senza motivo e aumenterebbero le possibilità di attacco. Riguardo la versione del kernel, nel momento in cui scrivo c'è il 2.2.12, se necessario http://www.kernel.org è il posto da cui scaricare il kernel più recente disponibile. Aggiornare il kernel è sempre raccomandato, ogni nuova versione corregge bug della precedente e/o introduce novità od ottimizzazioni.
Per quel che riguarda l'hardware, il neonato firewall dovrà avere una scheda di rete connessa al computer o alla rete protetta (nel secondo caso ci sono diverse possibilità, per esempio potremmo avere un hub oppure un collegamento a cascata dei computer). Per quanto riguarda gli indirizzi IP da usare per le macchine in rete, firewall compreso, devono essere del tipo 192.168.x.y, che il protocollo IP riserva alle reti locali. Usando questi, non dovrebbe essere possibile avere accesso agli host della rete dall'esterno; nel momento in cui si connette a Internet, il firewall avrà anche un indirizzo diverso, e solo quello sarà accessibile da Internet:



Da qui in poi ci si può sbizzarrire. Se dietro il firewall c'è una piccola rete aziendale o anche un Internet Cafè si può configurare il firewall anche come server di posta, oppure si può installare un news server e creare uno o più newsgroup locali da usare come messaggerie, e magari se la connessione è perenne anche ricevere da server esterni una o più gerarchie ufficiali. Per quando riguarda la navigazione sul web, si può installare squid, dopodichè sui client si potrà usare qualunque browser, impostando una cache minima. Il client avrà l'impressione di scambiare i dati solo col firewall/proxy, e la velocità non potrà che beneficiarne.
Dal punto di vista della sicurezza, che è quello di maggiore interesse qui, bisogna ricordare che con questa configurazione la macchina che esce sulla rete è il PC (486) con Linux, e solo quella. Per Internet, i client posti dietro il firewall, che hanno magari Windows 9x con Internet Explorer e relativi bug, semplicemente non esistono. La conseguenza? Non è possibile buttar giù i client visto che non sono raggiungibili dall'esterno, e gli attacchi diretti contro il firewall generalmente non funzionano, dato che sfruttano debolezze specifiche di Windows. Per lo stesso motivo la ricerca di backdoor (sport che pare essere molto di moda da un pò di tempo) è destinata a fallire, sempre che il nostro bestiolino non sia programmato per rispondere in modo, diciamo, "creativo" :-))) (OCCHIO! Sconsiglio quest'ultima cosa, è anche reato).

[NETSCAPE-Appendice]

[1] Quali dati possono uscire usando Communicator?

Netscape, 4.5 per windows 95 e 4.08 per NT, consente di

- Leggere contenuto interpretato di file HTML locali ("interpretato" vuol dire il testo mostrato, non il sorgente HTML)
- Leggere il contenuto interpretato di file HTML su un server web bloccato da un firewall (il browser e il web server devono essere dallo stesso lato del firewall)
- Leggere la cache dell'utente
- Sfogliare le directory
- Probabilmente altro cose
  (Evviva la privacy!!! - N.d.F. (Nota di Firebeam)

Dimostrazione all'indirizzo:
http://www.nat.bg/~joro/nsfind.html

[NETBUS-Appendice]

[1] Come funziona il tasto "port redirect" di Netbus 1.70?

In pratica, collegandoti su victimhost:port, è come se ti collegassi ad un otherhost:otherport... l'altro host vede la vittima, non te.

Esempio:

PC1 ----------> Netbus ----------> mail.tin.it

Tu ti colleghi al NetBus, gli dici di ridirigere la porta 25 sulla porta 25 di mail.tin.it, e metti l'indirizzo della vittima di NetBus come SMTP server in Eudora.

Parte Eudora e ti scarica la tua posta da mail.tin.it, però se qualcuno domandasse mai a TIN: "Chi ha scaricato la posta?", TIN darebbe l'IP del malcapitato.

(A parte il fatto che mi sono intrecciato, SMTP e 25 si riferiscono alla TRASMISSIONE di posta, non alla sua RICEZIONE... in pratica non scarichi la posta di nessuno col 25, però puoi fare mailbombing anonimo).

*** (C) Leonardo Serni ***

INDICE