GUIDA ITALIANA ALL'HACKING.

INDICE:

Responsabilità

Usa queste informazioni a TUO rischio e pericolo. Io, InfectedMachine e qualsiasi altra persona mi abbia aiutato a scrivere questa guida non si assumerà NESSUNA responsabilità per l'uso, l'utilizzo o l'abuso di questo testo.
Le seguenti informazioni sono state scritte SOLAMENTE per scopo educativo e informativo e NON possono essere usate per scopi illegali.
Leggendo questo file tu accetti i seguenti termini:
Comprendo che usare le seguenti informazioni è un atto illegale. Capisco e accetto di essere il SOLO responsabile delle mie azioni. Se vengo messo nei guai da queste informazioni NON incolperò o tirerò nei guai colui (InfectedMachine) che ha scritto questo testo, ogni altro suo collaboratore come qualsiasi persona mi abbia dato questo file.
Io capisco che le infomazioni qua contenute sono SOLO per scopo di educazione.
Questo file può essere usato per controllare la sicurezza del TUO sistema.

Considerazioni personali:

Mi sono arrivate parecchie mail in cui mi si diceva che quello che ho scritto e' stato scopiazzato da riviste e da faq sparsi in tutta la rete. Questo
e' completamente vero!
Non ho voluto fare questa guida basandomi sulle mie conoscenze, ho voluto solamente tradurre i documenti principali che chiunque riuscirebbe a trovare facendo alcune semplici ricerche.
Quindi in questa guida non troverete (forse) nulla di nuovo se avete gia letto documenti come la guida all'hacking di Sir Hackalot o la guida dei novizi della LOD (o altri ancora).
Io ed alcuni miei amici stiamo scrivendo una rivista chiamata "SystemDown" nella quale trattaremo gli argomenti dal nostro punto di vista e con le nostre conoscenze; quindi se volete leggere qualcosa che non e' tratto dalle varie guide sparse per la rete vi consiglio di tenere d'occhio il
sito dal quale avete scaricato il testo che state leggendo.
Questa guida inoltre e' stata scritta APPOSITAMENTE per i principianti e cioe' per quelli che ancora ne sanno poco o nulla; i piu' esperti (ma credo
che esperti sia anche troppo...diciamo i piu' informati) tra di voi corrono il
rischio di trovare questa guida di scarsa utilita'...
Io vi ho avvisato; vi prego non mandatemi mail dicendomi: "ma quella tua

guida in italiano la credevo piu' professionale" o cose del genere ok?
Un'ultima cosa:
Vorrei ringraziare una persona che sta permettendo a questa guida di rimanere online:
JADER ti ringrazio tantissimo; senza il tuo aiuto molto probabilmente questa guida l'avrei letta solo io!

Hacking?!?!?!

L'hacking è l'atto di penetrare nei sistemi per guadagnare conoscenze sul sistema e su come questo lavora.
Quest'azione è illegale perchè noi guadagnamo l'accesso a tutti i dati e li possiamo anche prendere.
Noi veniamo puniti per cercare di capire. I vari governi del mondo spendono un'esagerazione di soldi per cercare di arrestarci quando invece potrebbero investirli per cercare di catturare persone di gran lunga più pericolose degli hackers.
In giro ci sono assassini, stupratori, maniaci e terroristi e sono queste le
persone che i governi dovrebbero catturare, non gli hackers.
Al contrario di quello che dicono i governi i veri hackers non sono pericolosi; tutto quello che vogliamo è capire, imparare e forse un giorno le persone del mondo riusciranno a capirlo.
Vorrei anche fare notare una piccola differenza tra gli hackers e i crackers.
Per hacker si intende quella persona che, come abbiamo detto sopra, penetra nei sistemi informatici solamente per capire come essi funzionino realmente; i crackers sono coloro che penetrano nei sistemi informatici e non solo, per causare danni o rubare informazioni. La gente "normale" non conosce questa differenza e tende ad associare all'hacker il classico giovane ragazzo con i capelli lunghi, anarchico che seduto davanti allo schermo del suo computer aspetta che il programma pirata che lui sta usando gli consenta l'accesso al sistema bancario della città per poter rubare soldi in grandi quantità. Fino a che la gente non capirà che gli hackers non sono cattivi come si intende, la polizia li continuerà a perseguitare come assassini o terroristi o come criminali della peggior specie.

Perchè quindi hackerare un sistema?

Come ho detto sopra noi penetriamo nei sistemi per ottenere conoscenze sul sistema stesso e su come questo funziona e lavora. Noi NON vogliamo danneggiare in alcun modo i sistemi in cui penetriamo. Se tu danneggi un sistema, tu puoi essere individuato ed arrestato. Se invece tu non danneggi nulla è molto difficile (ma non impossibile!) che ti riescano a prendere senza spendere molti soldi (e non tutti, governi e grandi industrie a parte,
li possiedono ;-)).
I novizi è meglio che leggano qualsiasi cosa sull'hacking prima di compiere l'atto vero e proprio poichè più conoscenze si hanno, meglio si può operare.
E' molto utile anche una buona conoscenza dei linguaggi: c, c++ e assembler oltre ad una totale conoscenza del sistema Unix.

LE 10 REGOLE DELL'HACKING:

1) Non dannegiare mai un sistema. Se lo fai potresti fregarti con le tue stesse mani;
2) Non alterare nessuno dei file di sistema eccetto quelli che devi modificare per non essere individuato (i log file) e quelli che ti permetteranno di avere accesso a quel computer in futuro;
3) Non distribuire i tuoi progetti sull'hacking a nessuno a cui non affideresti la tua vita;
4) Quando posti sulle news, su un bbs (Bulletin Board System) o quando chatti su IRC sii più vago possibile quando parli dei tuoi
futuri progetti riguardo all'hacking. Ogni cosa può essere monitorata dalle forze dell'ordine;
5) Non usare mai il tuo vero nome o il tuo vero numero telefonico quando posti su un bbs, sulle news oppure su IRC;
6) Non lasciare i tuoi manipolamenti (tranne quelli necessari) su qualsiasi sistema in cui penetri;

7) NON hackerare i computer dei governi in particolar modo del TUO governo;
8) Non parlare dei tuoi progetti riguardo all'hacking quando parli sulla tua
linea telefonica di casa;
9) SII PARANOICO. Metti tutto il materiale riguardo all'hacking in posti sicuri;
10) Per diventare un vero hacker, tu devi hackare. Tu non puoi sederti a leggere un file di testo come questo e pensare di essere un vero hacker.

Strumenti basici di partenza:

Prima di tutto trova una copia dei vari scompattatori esistenti:
ARJ; ZIP; sono i due più importanti; su internet li si può trovare facilmente con un pò di ricerca.
A questo punto, su qualsiasi guida all'hacking reperibile sulla rete, ti consigliano di trovarti un "prefix scanner" cioè uno scanner di prefissi telefonici (detto anche war dialer) che ti permette di trovare i numeri telefonici che possono agganciare la chiamata di un modem; purtroppo visto che l'Italia non è l'America noi non abbiamo dei programmi adeguati alle nostre linee (sebbene sia possibile crearne uno usando - come mi hanno detto alcuni - il visual basic).
Poco male.
Sinceramente non ho verificato se gli scanner di prefissi americani funzionano anche sulle nostre linee; penso di provarci un giorno e comunque non è fondamentale: ci sono altri metodi oltre a quello.
Se proprio vuoi prenderne uno rimedia "Autoscan" (chiamato anche A-Dial) oppure "ToneLoc".

Regole basiche per hackerare uno UNIX:

Il sistema operativo UNIX è il più diffuso in assoluto su Internet poichè è stato progettato esclusivamente per le reti.
L'emulazione dello UNIX sotto il dos si chiama LINUX ed è disponibile la vesione "slackware" su internet; provate su ftp.cdrom.com.
Ci sono tre metodi principali per hackerare un sistema:
1) Default Login
2) Password List
3) Backdoors

Solitamente il login è di 1-8 lettere mentre la password di 6-8.
Lo UNIX e' il piu' diffuso sistema operativo su internet per la sua ottima gestione delle reti; sebbene questo registra le chiamate (non sempre!) e le
memorizza nei file utmp, wtmp e btmp raggiungibili in /etc oppure /var/adm (che sono usati dai comandi login, rlogin, su, remsh, rexec) e' ottimo per provare un primo inserimento.
Piccola parentesi:
Vi sono dei comandi per visualizzare gli ultimi login e cioe':
last (restituisce l'ultimo login)
lastb e blast (restituiscono gli ultimi login falliti).
Occhio al file syslog che registra connessioni andate a buon fine e non.
Un consiglio:
Se proprio non riuscite a rimediare lo Unix per poterlo montare su una vostra macchina o su di una partizione di quest'ultima, installate il sistema
operativo "LINUX" poichè alcuni comandi non esistono sotto windows (95 o 3.1) o sotto dos. Sebbene il Linux sia un sistema un pò "rognoso" nell'installazione (per i principianti), permetterà alcune manovre (chiamiamole così) impossibili con il dos.
Appena dentro un sistema in genere si vede un simbolo di questo tipo:
$ (oppure qualsiasi altro speciale simbolo di quel sistema).
Se tu inserisci il comando "man" ti apparirà una lista di tutti i comandi possibili nel sistema.

1) DEFAULT LOGIN:

Questo è il primo dei tre metodi di intrusione in un sistema e consiste nell'inserire una lista di account seguiti da password comuni, ovvero di quelle password che i sysop (system operator: operatori di sistema cioè coloro che controllano tutto il sistema) più ingenui mettono per

controllare i propri accessi.
Prima di incominciare ad inserire le password e gli account, dovete scoprire tutte le informazioni possibili sul bersaglio tramite comandi come whois, finger, showmount.
Questi sono tutti comandi dello Unix che danno informazioni su di un utente o su un sistema.
Usate questi comandi anche sull'account root.

ACCOUNT	PASSWORD
root	root, system, sysop, nomesistema, nomepersona quando il root è fingerato (il finger è uno strumento per prendere informazioni su qualcosa collegato ad internet), none, provare anche le password della lista sotto. Molto importante!
sys	sys, system, manager, nomedelsistema, vedi root
daemon	daemon, background, none
uucp	uucp, vedi guest
tty	tty
test	test
unix	unix, test
bin	bin, system, vedi root
adm	adm, admin, sys, vedi root
admin	adm, admin
sysman	sysman, sys, system
sysadmin	sysadmin, sys, system, admin, adm
who	who, none
learn	learn
uuhost	uuhost
guest	guest, user, anonymous, visitor, bbs, nome del sistema o dell'organizzazione.
host	host
nuucp	nuucp, vedi uucp
rje	rje, none, vedi root
games	games, player
sysop	sysop
demo	demo, nomedelsistema, none
visitor	vedi guest
anonymous	vedi guest
anon	vedi guest
user	vedi guest
nomedelsistema	vedi guest
student	student, vedi guest
ftp	ftp, ftpuser, vedi guest
ftpuser	vedi ftp
xxcp	xenix
system	manager
nobody	nobody, none
field	service
archie	archie, none
qarchie	qarchie, none
whois	whois, none
bbs	nomedelsistema, bbs, waffle, none
services	nomedelsistema, services, none
info	nomedelsistema, info, none
new	nomedelsistema, new, none
newuser	nomedelsistema, newuser, none
ingres	none, ingres, nomedelsistema
date	date, none
lpq	lpq, none
time	time, none
weather	weather, forecast, none
forcast	vedi weather
help	help, none
test	nomedelsistema, test, none
waffle	vedi bbs
trouble	trouble, vedi root
lp	lp, printer, print, vedi root
unmountsys	unmountsys, unmount, vedi root
setup	setup, vedi root
makefsys	makefsys, vedi root

sysadm	sysadm, sys, system, vedi sys-adm-root
powerdown	powerdown, vedi root
mountfsys	mountfsys, vedi root
checkfsys	checkfsys, vedi root

In poche parole tenta di trovare un account che abbia il nome di un servizio ed aggiungergli una password con un altro nome di servizio oppure con qualcosa che abbia a che fare con il sistema (nome del proprietario quando si fà il whois, nome del sistema, ecc.).

2) PASSWORD LIST detto anche PASSWORD GUESSING

Un altro metodo per inserirsi in un sistema è quello di "rubare" la password di un altro utente.
Per prendere un valido account a cui dare una password bisogna "fingerare" (usare i vari comandi detti sopra per ottenere le informazioni su di un utente o un sistema) l'utente e leggere (anche se criptato) il passwd file; è meglio se il finger viene fatto durante il giorno.
Una volta trovato l'account (tramite il finger oppure nel passwd file), bisogna inserire una alla volta le password della lista sotto riportata per cercare di individuarne una giusta e per poter così accedere al sistema.

Lista delle più comuni password (in America):

100	foresight	persona
666	format	pete
6969	forsythe	peter
AAA	fourier	phiber
aaa	fred	phiberoptick
academia	friend	philip
acdc	frighten	phoenix
ada	frocio	phreak
adrian	fuck	pierre
aerobics	fufi	pinkfloyd
aids	fun	pirata
air	fungible	pizza
airplane	gabriel	plover
albany	gardner	plugh
albatross	gardener	plymouth
albert	garfield	polynomial
alex	gauss	pondering
alexander	gay	pork
algebra	george	poster
alias	gertrude	praetorian
aliases	giants	praise
alpha	gibson	precious
alphabet	giga	prelude
ama	ginger	prince
amato	glacier	princeton
america	gnu	protect
amerigo	golf	protocol
amore	golfer	protocollo
amorphous	gorgeous	protozoa
amy	gorges	pumpkin
analog	gosling	puneet
anarchy	gouge	puppet
anchor	graham	Purdue
andromanche	green	purdue
andy	gryphon	rabbit
andrea	guerra	rachmaninoff
angerine	guest	rainbow
anna	guitar	raindrop
annabella	gumption	raleigh
annalisa	gunsnroses	random
anne	guntis	rascal
anumal	hack	read
animals	hacker	reading
answer	hackers	reagan
anthropogenic	hamlet	really
anvils	handily	rebecca

anything
areato
aria
ariadne
arrow
arthur
asshole
athena
atmosphere
attacker
attackers
aztecs
azure
bacchus
badass
bailey
banana
bananas
bandit
banks
barber
baritone
bass
bassoon
bastard
batman
beater
beatles
beauty
beaver
beethoven
bella
bellissima
beloved
benz
beowulf
berkley
Berkeley
berlin
berliner
beryl
beta
beverly
bicameral
bisessuali
bisex
black
blacklotus
blu
blue
bob
boston
brenda
brian
bridget
broadway
brown
bumbling
burgess
caffe
caffè
camel
campanile
cantor
cardinal
cardinale
carmen
carolina
caroline
cascades
castle
cat
happening
hard
hardrock
harmony
harold
harvey
hashish
heavy
heavymetal
hebrides
heinlein
hello
help
herbert
hiawatha
hibernia
hiv
hollywood
holmes
honey
horse
horus
hutchins
imbroglio
imperial
include
ingres
inna
innocuous
inside
id
ip
irishman
ironmaiden
isis
italia
jack
jackdaniels
japan
jessica
jester
jets
jfk
jixian
yngwie
johnny
joker
joseph
joshua
judith
juggle
julia
juventus
kathleen
kbyte
kbites
kennedy
kermit
kernel
kernel32
kevin
king
kirk
kirkland
knight
krypto
kryptonite
kult
kurt
ladie
ladle
lambda
red
redder
remote
repubblica
republic
rick
ripple
robot
robotics
rochester
rolex
rollingstone
roma
romano
ronald
rosebud
rosemary
roses
router
rsa
ruben
rules
ruth
sal
satan
satana
saxon
scamper
scheme
scott
scotty
secret
send
sender
sending
sensor
serenity
sex
sexpistols
shark
sharks
sharon
sheffield
sheldon
sherlock
shit
shiva
shivers
shuttle
sid
sidvicious
signature
simon
simona
simple
singer
single
sirio
smile
smiles
smooch
smother
snatch
snoopy
soap
socrates
sorriso
sossina
sparrows
spit
spring
springer

cayuga
cazzo
cazzone
cd
celtics
cert
cerulean
change
charles
charlie
charming
charon
chester
cigar
classic
clusters
cocaina
cocaine
coffee
coke
collins
comrade
comrades
computer
comrade
condo
condom
cookie
cooper
cornelius
couscious
cracker
crackers
create
creation
creator
creosote
cretin
cyan
daemon
dancer
daniel
daniels
danny
dark
dave
deb
debbie
deborah
december
defoe
deluge
desperate
develop
diet
dieter
digital
digitale
discovery
disney
dog
dragon
dragone
drought
duncan
dylan
eager
easier
easy
eatme
ecco
eccomi
lamination
larkin
larry
lawrence
lazarus
lebesgue
led
lee
leland
leroy
lewis
light
linux
lisa
list
lista
lists
listato
lorenzo
louis
love
low
lower
lowered
lynne
mac
macintosh
mack
mage
maggot
magic
magica
magiche
mago
magù
maiden
malcolm
malmsteen
marco
marlboro
mark
markus
marty
marvel
marvin
master
maurice
mega
megabyte
megabytes
mel
mela
mellon
merlin
metal
metallica
mets
michael
michelle
mike
milan
milano
minimum
minsky
mit
modena
mogul
moose
morley
mozart
nancy
napoleon
squires
sri
star
starwar
starwars
stilskin
strangle
strangolare
stratford
stregone
strozzapreti
stuttgart
subway
success
summer
super
superman
superstage
support
supported
surfer
suzanne
swearer
symmetry
tangerine
tape
target
tarragon
taylor
tcp
tcp-ip
tcp/ip
tcpip
telephone
temptation
thailand
TheNic
thenic
tiger
toggle
tohack
tomato
topography
tortoise
toyota
trails
train
trains
transfer
transfering
trasferimento
trash
trivial
trofei
trofeo
trombone
tron
trophy
trophies
trustno1
TrustNo1
trustnoone
TrustNoOne
tubas
tuttle
u2
umesh
unhappy
unicorn
unix
unknow
urchin

edges
edinburgh
edwin
edwina
egghead
eiderdown
eileen
einstein
elephant
elizabeth
ellen
elsewhere
emerald
engine
engineer
enterprise
enzyme
eretiny
ersatz
establish
estate
etere
etereo
etero
euclid
evelyn
exadecimal
extension
fairway
felicia
fender
fermat
fibre
fidelity
figa
finite
firenze
fishers
flakes
float
flower
flowers
foolproof
football
nasa
ncsc
nepenthe
ness
network
newton
next
none
noxious
nutrition
nygiants
nyjets
nyquist
ocean
oceano
oceanography
ocelot
olivetti
olivia
omosessuale
open
oracle
orca
orwell
osiris
outlaw
oxford
pacific
painless
pakistan
pam
paper
papers
parma
pascoli
passwd
password
passwords
pat
patricia
penguin
peoria
percolate
persimmon
utility
Uunet
vasant
veleno
venezia
venom
vertigo
vicious
vicky
village
virginia
vittoria
war
warcraft
warcraft2
warren
water
weenie
whatnot
whiting
whitney
will
william
williamsburg
willie
winston
wisconsin
wizard
wombat
woodwind
wormwood
xyzzy
yaco
yacov
yang
year
years
yellowstone
yosemite
zap
zimmerman
zorro
zupperman
z

E non possono mancare i classici zz e zzz

Ci sono nel mezzo anche parole italiane che mi ha passato un mio conoscente e che dice siano maggiormente usate...mi voglio fidare... :-))

3) BACKDOORS

Le backdoors sono quelle password che il programmatore del sistema mette per avere accesso in futuro a quel dato computer e che solamente lui conosce.
Per cercare di individuare la password bisogna fare lunghe ricerca sulla persona che ha impostato tutto il sistema: che squadra tifa, quali sono i suoi hobby, i suoi idoli, il nome dei vari componenti della famiglia, le date
di nascita, queste ultime al contrario o mischiate tra loro, ecc.
Tanto per capirci se avete visto il film "wargames", il protagonista passa intere giornate a studiare vita morte e miracoli del programmatore del sistema oppure anche nel più recente film "hackers" i due protagonisti cercano addirittura gli appunti gettati via nella spazzatura pur di trovare una password o qualcosa che li possa aiutare.
Sicuramente questo è il sistema più difficile ma credo che dopo una lunga ricerca sia anche il più sicuro poichè poche persone (cioe' quelle furbe) inseriscono come password qualcosa che non gli è famigliare.
In genere tutti gli user che si connettono ad internet usano nomi che riescono a ricordarsi facilmente tipo una data di nascita, il nome della ragazza o del giocatore preferito o anche qualcosa di meno evidente ma

sempre e comunque legato a loro e che difficilmente potrebbero scordarsi. Del resto romperebbe abbastanza le palle dovere cambiare la propria password perchè ce la siamo scordata no?

Ci sono altri sistemi per penetrare in un computer ma sono molto più complessi di questo anche se magari più efficaci.
Due tra i tanti sono l'IP SPOOFING e successivamente a questo l'Hijacking.
Ne parlerò più avanti.

Ora, se volete essere veramente paranoici (meglio esserlo che fregarsene) e avete paura ad hackerare dalla vostra linea di casa (comprensibile per chi non l'ha mai fatto), potreste, se avete le opportunità e i mezzi, collegarvi ad una cabina telefonica tramite un computer portatile oppure collegare il vostro computer alla linea telefonica del vicino di casa.
Nel primo caso purtroppo esistono pochissimi documenti (per non dire nessuno) sul phreaking (cioè l'atto di telefonare gratis beffando le compagnie telefoniche) in Italia e poichè il sistema telefonico italiano funziona diversamente da quello americano (anche se devo dire che non ho mai approfondito veramente l'arte del phreaking) poche possono essere le conclusioni.
Se non sapete come trafficare con le cabine telefoniche vi consiglio di provare a fare un collegamento tra i modem di tipo vecchio, cioe' quelli in cui si doveva appoggiare la cornetta sull'apparecchio, e uno di tipo nuovo; questa e' solo una mia teoria e sto raccogliendo informazioni in questi giorni.
Nel secondo caso, si farebbe certo prima che studiare il mezzo di connettersi ad una cabina telefonica però c'è da dire che il vicino di casa potrebbe scoprire dalla bolletta telefonica che qualcosa non và...state SEMPRE attenti a quel che fate.
Comunque anche in questo secondo caso vi serve un portatile:
Prendete i cavi che escono dal modem e tagliate via la parte di plastica alle
estremità, trovate vicino alla casa della vittima la scatolina dove vanno a finire i cavi telefonici uscendo dalla casa ed apritela.
Dopo che vi siete procurati un paio di alligator clips (i cavi che hanno il
beccuccio in fondo a forma di bocca di coccodrillo) collegate il cavo rosso del vostro modem a quello rosso del clip e quello verde a quello verde.
Poi connettete i cavi in questione con quelli rossi e verdi che escono dalla
cassetta e il gioco dovrebbe essere fatto...controllate che vi dia la linea e
siete ok!

PROGRAMMI UTILI

Ci sono dei programmi che si rendono indispensabili in questo campo:
Il primo è il ToneLoc oppure l'A-Dial o qualsiasi altro war dialer. Poi oltre
agli scompattatori sono utili anche i seguenti programmi:
Il SATAN (o SANTA) è un programma che gira sotto macchine Unix e sue emulazioni e richiede perl5.0, un browser (netscape và bene), 32 MB di ram; questo programma consente l'analisi di reti e sottoreti di un sistema per trovare falle e aperture. E' stato progettato per poter trovare ingressi non controllati nei sistemi ed eventualmente chiuderli. E' stato usato (oltre a questo nobile scopo) da un certo signore chiamato Kevin Mitnick il quale ha fregato programmi segreti del governo, una cosa tipo 20.000 numero di carte di credito e chi più ne ha più ne metta.
Un altro programma simile al SATAN è l'ISS che lo precede come data di uscita su internet. L'Internet Security Scanner funziona in modo simile al SATAN ma non sò dire che requisiti voglia per girare.
Se vi siete accorti che qualcosa nel vostro sistema non và potete usare due programmi per vedere se il SATAN o altri netscanners (esaminatori di reti) vi hanno fatto una "visitina".
Uno è il GABRIEL, l'altro il COURTNEY che sono due strumenti che riescono a capire se si è stati sottoposti all'attacco del SATAN.
Un altro programma indispensabile è il crack jack (o crackerjack) oppure il Brute.
Questi due programmi comparano le password di una lista, che voi avrete compilato prima in un file di testo, con quelle del passwd file cercando di

trovarne una uguale per poter così usufruirne al momento del login.
Attenzione perchè possono solo decifrare le password criptate col metodo DES, NON quelle shadowed.
Una cosa: chi ha detto in giro che ha decriptato il passwd file racconta solo un mucchio di balle perchè non è possibile decriptarlo. Al massimo si può, utilizzando i programmi sopra citati comparare una lista di password e trovarne una (o più se si è MOLTO fortunati) giusta.
Altri programmi utili possono essere il pgp (Pretty Good Privacy) e il pgpcrack.
Il primo serve per criptare dei messaggi in modo che nessuno (tranne il ricevente con la giusta chiave) possa capire. Questo programma ha, diciamo, fatto un pò di confusione su internet poichè riusciva a criptare i messaggi con una sicurezza quasi totale e i militari (soprattutto americani
) non erano un gran che contenti di questa cosa.
Il secondo programma, pgpcrack, serve per l'opposto: crakkare i messaggi criptati col il pgp (vedi sotto). Anche qua bisogna comparare una lista di
password con il file pgp a meno che non si conosca un pò di assembler il che ti potrebbe permettere ad esempio di scrivere al posto della lista di password la parola Random e ciò (dopo aver appositamente modificato il programma) ti permetterebbe di fare una scansione di tutti i caratteri ascii.
Ho sentito dire che il pgpcrak non servirebbe a nulla...io non ho sperimentato di persona i risultati e non posso confermare o smentire tale voce. Lascio a chi si intende di più di chiavi criptate il compito di dare una
risposta a tutti quelli che la cercano.

Apro una piccola parentesi su tre parole che forse avrete sentito dire in giro su internet:
Virus, Trojan Horse, Worm che tradotti sarebbero virus, cavallo di troia e verme.

VIRUS

Questo è un programma indipendente che riesce a riprodursi. Può attaccare gli altri programmi e può creare copie di se stesso. Può danneggiare o corrompere i dati su di un computer o calare le performance del vostro computer utilizzando risorse come la memoria oppure lo spazio libero sul disco fisso.
Alcuni virus scanner (anti-virus) individuano alcuni virus. NESSUN anti-virus individua tutti i virus conosciuti e non ti può proteggere quindi da essi.
Avevo letto da qualche parte una frase che era abbastanza significatica sia in questo caso che nel caso dell'hacking:
"...ricorda, le forze dell'ordine fanno passi avanti nella sicurezza dei sistemi, scoprono nuovi mezzi per bloccare i nostri attacchi e scoprono nuovi trucchi per scovarci ed arrestarci.
Il loro unico problema è che la tecnologia non si espande solo per loro..."

TROJAN HORSE ovvero IL CAVALLO DI TROIA

Chi non sa cos'è il cavallo di Troia?
Spero che pochi non sappiano cos'è.
Comunque era quell'inganno che dei gran cattivi ragazzi avevano usato per portare morte all'inteno di una città nella quale sembrava impossibile entrare.
Un TROJAN (abbrevio il nome) da computer è molto simile.
E' un programma che, con funzioni non autorizzate, si nasconde dentro un programma autorizzato. Un trojan ha diverse funzioni...ad esempio può mandarti tutte le password che vengono digitate in un giorno al tuo indirizzo di posta elettronica e contemporaneamente può cancellarsi da solo.
Se non è intenzionale (ovvero non viene immesso nel sistema da un hacker) questo viene chiamato bug (cito una storia che mi ha detto un mio amico, RaggedRobin..."per chi non sapesse perchè viene usato il termine bug per indicare un errore in un sistema, deve sapere che quando avevano inventato il primo computer, che era grande come una stanza, tra i suoi circuiti un giorno si infilò una cimice che lo mandò fuori uso e da allora i difetti di un sistema vengono chiamati bug cioè insetto...").
Alcuni anti-virus individuano alcuni trojan ma come nel caso dei virus,

nessuno può sentirsi al sicuro poichè per ogni nuova scoperta in campo di protezione ne viene fatta una nel campo dell'attacco.
Per maggiori dettagli sui cavalli di troia vi rimando al primo numero di "SystemDown" nel quale ne parla RaggedRobin nel suo articolo.

WORM cioè VERME

I worms (i vermi) sono programmi simili ai virus che si riproducono e si copiano di file in file e di sistema in sistema usando le risorse di quest'ultimo e talvolta rallentandolo. La differenza dai virus è che mentre loro usano i file per duplicarsi, i vermi usano i networks.
Nota: sono stati creati, credo e non vorrei dire una balla, da un certo Robert Morris Jr.

ERRORI:

Quando inserisci un account non valido oppure una password non valida (oppure entrambi) tu dovresti vedere un messaggio di errore.
In genere è qualcosa di simile a: Login Incorrect.
Quando il computer ti dice questo, significa che hai sbagliato una delle due cose ma (per ovvie ragioni) non ti dice qual'è.
Quando tu sbagli il login, la chiamata viene registrata in appositi file (error log) che registrano chi è l'utente e da dove sta chiamando per puro scopo di sicurezza.
Altri tipici errori sono: "Cannot change to home directory" oppure "Cannot change directory". Questo significa che la home directory (la directory dell'account in cui ti sei inserito) è la root directory per quell'account.
Tanto per capirci è come ritrovarsi sul dos in c:\ e sai che indietro non puoi andare perchè non c'è nulla, l'unica differenza è che sullo unix non ci
sono c:\ oppure a:\ quando parti con il sistema ma /homedirectory.
Piccola nota: nello unix è usato questo simbolo per delimitare le directory / e non \.
Molti sistemi dopo che ti hanno dato questo messaggio ti sconnettono automaticamente ma altri ti dicono semplicemente che ti hanno messo nella root directory (/).
Un altro errore è "No Shell". Significa che nessuna shell (programma di interfaccia con il kernel del sistema che esegue tutti i comandi) è stata impostata per quell'account. Per maggiori dettagli vedi oltre.
Come sopra, alcuni sistemi ti sconnettono dopo questo messaggio, mentre altri ti dicono di usare una shell regolare dicendo "Using the bourne shell"
oppure "Using Sh".

ACCOUNT IN GENERALE

Il sistema unix ha due livelli di sicurezza: potere assoluto e user regolare.
Quelli che hanno potere assoluto sono i root, i system operator, gli amministratori di sistema in altre parole.
Lo unix è impostato (per i livelli di sicurezza) su numeri: associa un numero con un account; alcuni account possono avere lo stesso numero.
Il numero che definisce i poteri di un root (amministratore di sistema) è 0. Qualsiasi altro account abbia un UID (User ID) di 0, ha i privilegi di un root.
Tenete in considerazione che il livello normale di uno user è 100.

SHELL

La shell è un programma eseguibile che si "associa" ad un utente quando si inserisce (normalmente o irregolarmente) in un sistema.
Questa shell può essere qualsiasi programma eseguibile definito nel passwd file. Ogni login ha una shell unica. Le shell sono interpreti dei nostri comandi e cioè provvedono a fare da tramite tra noi e il sistema vero
e proprio. Tanto per capirci le shell sono qualcosa di simile al "command.com" del dos.
Alcuni esempi di shell sono:
-sh: Questa e la "bourne shell" e si potrebbe definire il "command.com" dello unix.
-csh: Questa è la "C" shell e ti permette di inserire comandi simili al

"C".
-ksh: Korn Shell. Un altro interprete di comandi.
-tcsh: Permette l'editing dei comandi. E' usata al MIT.
-vsh: Visual Shell. Questa è come il windows per il dos cioè un interprete grafico dei comandi.
-rsh: Restricted Shell o Remote Shell. Spiegato dopo.
Quando ti inserisci in un sistema la shell ti dà un simbolo e da questo puoi
capire a che livello ti sei infiltrato (spero l'abbiate capito prima di questo
simbolo!).
$: In genere il dollaro è il simbolo che si associa all'user regolare senza alcun potere.
#: Questo invece si associa in genere ai root.

CARATTERI SPECIALI:

Control-D: Fine di un file. Quando usi la mail oppure un editori di testi, questo comando capisce quando sei arrivato alla fine. Se sei nella shell (nel prompt dei comandi normale) e premi control-d tu ti disinserisci dal sistema.

Control-J: Su alcuni sistemi questo è come premere "invio".
@: Questo qualche volta è "null" che tradotto significa "nullo, qualcosa di nullo".
?: Può rappresentare una lettera (come * nel dos). Ad esempio se tu inserisci qualcosa tipo b?b, lo unix capisce che può essere bob, bib, bub ed ogni altra lettera e numero da 0-9 e a-z.
: Questo rappresenta ogni numero di caratteri ed è simile a quello sopra descritto. Se inseriamo infatti quacosa tipo Hi può voler dire Hit, Him e qualsiasi cosa parta per Hi. Se invece si inserisce H*l rappresenta qualsiasi cosa parte per H e finisce per l.
[ ]: Specificano un campo. Se diciamo b[o,u,i]b lo unix capisce bob, bub, bib. Se gli dico b[a-d] lo unix pensa a qualsiasi lettera compresa nel campo (cioè in questo caso da a fino a d).
In qualsiasi caso lo unix è molto "SENSIBILE" e quindi inserire D al post che d non significherà la stessa cosa.
Occhio quindi ad inserire le password giuste. ;-)

COMANDI DA USARE SOTTO LO UNIX:

ls: Questo elenca il contenuto delle directory (è uguale a dir nel dos).

cat: Questo comando stampa a video il contenuto di un file. Può essere usato sui file di testo.

cd: Cambia la directory come nel dos tranne per il fatto che per tornare indietro di una directory non bisogna fare cd.. ma cd .. (cioè separare di uno spazio il cd dai puntini). Per il resto è uguale al dos.

cp: Copia un file. Sintassi "cp dalfile alfile"

mv: Questo rinomina un file. Sintassi "mv vecchionome nuovonome".

pwd: Dà il nome della directory in cui ti trovi.

rm: Cancella un file. Sintassi "rm nomefile" oppure "rm -r nomedirectory".

write: Manda una chat ad un altro user. Sintassi "write nomeuser"; per uscire dal programma write digitare control-d.

who [w, who, whodo]: Dicono chi è online cioè chi è collegato alla macchina sulla quale fai who. Se al fianco del nome dello user c'è un + significa che puoi usare il comando write su di lui.

man: Ti stampa a video l'aiuto sui comandi che vuoi. Sintassi "man nomedelcomando"; ad esempio "man who". Questo comando deve essere seguito dal comando che si vuole consultare. Ad esempio man -k ricerca i comandi che hanno a che fare con la keyword.

stty: Setta le caratteristiche del tuo terminale.

sz, rz: Manda e Riceve (send o receive) con lo zmodem

rx, sx: Manda e Riceve con lo xmodem.

rb, sb: Manda e Riceve via batch ymodem. Questi 6 programmi possono e non possono esserci su di uno unix.

umodem: Manda e riceve con lo umodem. Esempio di trasmissione:
$ sz nomefile
ready to send...
$ rz nomefile
please send your file....
..etc..

ed: Editor di testi. Sintassi: "ed nomefile". Alcune versioni ti possono dare
un prompt tipo "*" altre non lo fanno. Il piu' comune, comunque, e' il "vi".

mesg: Cambia il permesso o no di ricevere chat da altri utenti (il + spiegato sopra nel comando write).

cc: Il compilatore C.

chmod: Cambia i diritti di un file. Sintassi:"chmod mode nomefile". Ad esempio chmod a+r newtext: Tutti possono leggere newtext perchè a=all r=read. Questo è comunque spiegato oltre.

chown: Cambia il possessore e il gruppo di un file. Sintassi "chown possessore (owner) nomefile".

chgrp: Cambia il gruppo (spiegato dopo) di un file. Sintassi "chgrp group file"

finger: Stampa a video le informazioni basiche su un account. Sintassi: "finger nomeuser".

grep: Cerca un qualcosa dentro un file. Sintassi "grep pattern file".

mail: Questa è una utility molto interessante e utile. Al contrario del nome
esistono molte versioni della Mail come ad esempio ELM, MUSH e MSH.
Il programma basico della mail è comunque chiamato "mail".
La sintassi e:
"mail nomeuser@indirizzo" oppure
"mail nomeuser" oppure
"mail" oppure
"mail addr1!addr2!addr3!user"
comando "mail nomeuser@indirizzo" è usato per mandare una mail a qulcun'altro su di un altro sistema che solitamente è un altro unix ma anche dos e vax possono ricevere posta dallo unix.
Quando usi "mail nomeuser@indirizzo" il sistema dove sei DEVE avere uno "smart mailer" (conosciuto come smail) e deve avere quello che noi chiamiamo sistem maps. Lo smart mailer così può trovare l'indirizzo e mandare così la mail.
Per le macchine locali basta che digiti "mail nomeuser" dove nomeuser è il login a cui vuoi mandare la mail.
Scrivi il tuo messaggio poi premi control-d.
Per leggere le TUE mail digita "mail".
Ad esempio:

$ mail

From McKrak ....
To Inf ....
Subject: bene ora.......................

Arghhh!

?

Il ? è un prompt che aspetta un comando:

d - delete (cancella)
f nomeuser - manda allo user
w fname - salva il messaggio con intestazione nel file
q - quit / update mail
x - quit ma non cambia nulla
m nomeuser - mail allo user
r - reply
[invio] - leggi il prossimo messaggio
+ - vai avanti di un messaggio
- : torna indietro di un messaggio
h - stampa a video le intestazioni dei messaggi che sono nella tua mailbox.
Ci sono altri comandi e per vederlo basta digitare ?.
Se mandate fakemail (false mail) date un'occhiata anche al file
/var/adm/maillog

ps: Process. Questo comando permette di vedere tutti i processi che occupano la memoria (come ad esempio i programmi aperti). Ogni volta che lanci un programma tu assegni un Process ID number (PID) per scopi di registrazione e tramite ps puoi andare a vedere cosa e' stato lanciato. Solitamente la prima voce del comando ps è la shell con il tuo nome. pf -f dà una lunga lista di processi.

kill: "Uccide" un processo. Questo è usato per terminare un programma nella memoria del computer. Si possono solo uccidere i processi che si possiedono a meno che tu non sia un root o il EUID è lo stesso di quello che vuoi terminare (spiegato dopo). Se "uccidi" la tua shell, tu sei espulso fuori dal sistema.

shwomount (/usr/bin di solito): serve per mostrare quali parti del file-system una macchina esporta sulla rete, e se seguito dall'opzione -e visualizza inoltre chi ha la possibilita' di montare tramite nfs la partizione
esportata (Se compare la scritta "everyone" siamo a posto).

rusers: consente di sapere quali utenti sono collegati su macchine remote connesse alla tua.

HACKING

Il primo passo consiste nell'infiltrarsi in un sistema operativo trovando un
valido account/password. L'obiettivo dell'hacking è solitamente quello di guadagnare i pieni privilegi (root) sul sistema hackerato.
Piccola nota:
Quando in un sistema si vedono scritte tipo: drwxr-xr-- Infected (ad esempio) significa questo:
la prima lettera "d" significa che quella riga è una directory e ne contiene
forse delle altre; poi seguono una serie di simboli (rwx) che stanno per r=read=leggere w=write=scrivere x=execute=eseguire.
Sono ripetuti tre volte perchè i primi tre si riferiscono al possessore del file; nell'esempio sopra di Infected, potevo sia leggerlo che modificarlo che eseguirlo. La seconda serie di lettere si riferisce al gruppo a cui Infected appartiene e cioè se quelli appartenenti allo stesso gruppo possono o no leggere, modificare o eseguire il dato file. L'ultima serie di lettere si riferisce ad ogni altro user che non sia Infected e non faccia parte
di quel dato gruppo.
Quelle lettere possono essere cambiate con il comando chown (spiegato sopra) ma lo può fare solo l'operatore di sistema e solo colui che ha creato
il file a meno che questo file non sia modificabile dalla terza categoria.
Se per caso ti dovesse capitare di trovare nel passwd file (localizzato in /etc/passwd) un account privo di password (cioè c'è dello spazio bianco dove ci dovrebbe essere la password) significa che puoi inserire il nome dell'account e se ti chiede la password battere invio e così dovresti essere
automaticamente dentro.

UNA VOLTA DENTRO??? SPECIALI FILE...

/etc/passwd: Questo è il più importante file su di uno unix poichè contiene

le password e gli account validi per poter entrare nel sistema. Il formato per il passwd file è questo:
nomeuser:password:UserID:GroupID:descrizione(o vero nome):homedir:shell
Ci sono due esempi da fare:
infectedm:89fGc%^&a,Ty:100:100:InfectedMachine:/usr/infectedm:/bin/sh
demo::101:100:Test Account:/usr/demo:/usr/sh
Prendiamo in considerazione il primo esempio:
Il primo campo dove c'è scritto infectedm si riferisce al fatto che infectedm
è uno user valido. Il secondo campo dovrebbe contenere la password ma è criptata con il metodo di criptazione DES.
Potresti anche trovare qualche carattere tipo * al posto della password e se
lo trovi (cosa praticamente ormai certa nei sistemi odierni) significa che
la password è shadowed (ombrata) cioè è nascosta e solamente il root può andare a vedere l'originale.
Per combattare quest'ultima "minaccia" si può usare un programma chiamato ypcat (vedi sotto)che gira sui sistemi operativi SunOS.
Parentesi:
Le password shadowed sono presenti in due casi:
Il sistema e' stato reso sicuro (trusted)
Sono installate le YellowPage e in questo caso si puo' utilizzare il comando ypcat.
Prendiamo ora come esempio il secondo che avevamo fatto sopra: qua possiamo notare che l'account è privo di password e quindi inserendo (come detto sopra) il nome dell'account (in quel caso era demo) e premendo invio si potrà accedere al sistema senza bisogno di inserire la password.

/etc/group: Questo file contiene i gruppi validi. La sintassi solitamente è:
nomegruppo:password:groupid:users nel gruppo. Se vedi uno spazio bianco dove dovrebbe stare la password, puoi diventare parte del gruppo usando l'utility "newgrp". Comunque ci sono alcuni casi in cui a solo certi users è permesso usare il comando "newgrp" per poter accedere al gruppo.
A questo proposito voglio specificare che se l'ultima riga cioè "users nel gruppo" è bianca significa che tutti possono inserirsi; al contrario se c'è scritto qualcosa significa che solo quello user o quegli users possono usare il comando e inserirsi.
Apro una piccola parentesi sul comando "newgrp": questo è un comando che può cambiare la tua attuale group id in una che tu specifichi. La sintassi è "newgrp nomegruppo".

/etc/hosts: Questo file contiene la lista degli host che sono connessi attraverso un hardware network (tipo un x.25 link) o, qualche volta anche quelli connessi attraverso UUCP. Questo è un ottimo file quando vuoi hackerare un grande network e infatti ti dice in che sistemi puoi usare la rshell (remote shell) oppure rlogin e il telnet o qualsiasi altro ethernet/x.25 program.

/usr/adm/sulog (oppure su_log): Il file sulog può essere trovato in molte directory ma solitamente è in questa. Questo file è ciò che dice la parola stessa, un log file per il programma SU. Infatti questo registra ogni user (e
ogni suo dato compreso da dove chiama) che usufruisce del programma SU.
Se devi usare questo programma per entrare nel sistema cerca questo file e prova ad editarlo cancellando così le tue tracce.

/usr/adm/loginlog
/usr/adm/acct/loginlog: Questo è un log file (per non dire IL log file) e registra le tracce di ogni persona che si inserisce all'interno del sistema. E'
un file di sicurezza per verificare le persone che hanno usufruito del sistema.
A volte non esiste neppure sul sistema.

/usr/adm/errlog: Questo è un error log. Può essere ovunque sul sistema. Questo registra le tracce di ogni chiamata errata grave e non. Di solito

contiene un codice che classifica le entrate sbagliate.
Và da 1 a 10.
Quando si hackera un computer in genere questo file lo classifica con il numero 6; il numero 10 è il system crash.
Dopo che sei penetrato in un sistema cancella le tue tracce anche su questo file.

/usr/adm/culog: Questo file contiene le informazioni su chi ha usato il programma CU, da dove ha chiamato, chi era, ecc.
Un altro file per la sicurezza del sistema.

/usr/mail/<userLogin>: Questo è dove il programma mail registra le lettere di un utente. Per leggere una particolare mailbox devi essere quello user, uno user nel gruppo "mail" o un root. Ogni mailbox ha un nome. Se si trova questo file leggere bene i nomi scritti qua perchè possono benissimo essere gli account degli users.

/etc/shadow: Il file di cui parlavo prima cioè il file shadowed dove ci sono
le password ombrate.

/var/adm/maillog: registra la partenza e la destinazione (credo) delle mail.

IL BIN ACCOUNT

In genere il bin account è solo a livello user ma benchè sia solamente a questo livello, è molto forte.
Questo è potrebbe essere il possessore di molti dei più importanti file del sistema compreso /etc/passwd.
Se hai letto la sezione precedente sulla possessione o no dei file (quelle tre lettere rwx) puoi capire che se questo account possiede il file /etc/passwd essendo un account a livello user ti permette di editare il mitico file e di crearti una root entry per te stesso.
Puoi farlo tramite il comando ed.
Ad esempio:

```
$ ed passwd
10999 [ la grandezza del passwd varia ]
* a
infectedm::0:0: Infected Machine:/:/bin/sh
( control-d )
* w
* q
$
```

Ora tu puoi usare il comando Login per reinserirti nel sistema, usare il nome infectedm ed essere un root. Facile no?

Addizionare Account

Ci sono alcuni programmi, diversi dal comando "ed" che permettono di addizionare lo user al sistema ma molti non permettono di inserirsi come root o con UID meno di 100. Uno di questi programmi è chiamato "adduser".
Quello che segue è quello che devi fare se vuoi un indirizzo di posta elettronica su di un computer:
Se lo Unix in questione (quello in cui devi mettere la tua email) ha l'uucp
oppure è una università, ci sono possibilità di fare il traserimento di posta
elettronica.
Tu ora puoi testare lo Unix mandando una mail ad un tuo amico oppure a te stesso e se quando ti arriva, il mittente è indicato come "smail" probabilmente significa che il sistema può mandare le mail UUCP.
Questo è un buon metodo per prendere contatto con le persone in maniera tranquilla e sicura.

Hackerare un sito ftp tramite l'FTP di windows95:

TYPE
ftp vittima.com (vittima.com e' il sito da hackerare)
Il server ora puo' richiedere uno username...premere INVIO.
Ora il server richiedera' la password...premere anche qui INVIO.

Poi digitare:
quote user ftp
e poi:
quote cwd ~root
in seguito:
quote pass ftp

Sii sicuro di cancellare i log file per fare in modo di renderti "invisibile" al
system operator.
Per fare questo metodo il sistema deve essere un po' vecchiotto (anche se non so' quanto).
Funziona soprattutto con i vecchi server (universita' americane).
E' lo stesso con UNIX, LINUX e OS/2.
Funziona anche con gli account anonymous che richiedono l'inserimento della email come password.

SNIFFER???

Che cos'e' uno sniffer?
Lo sniffer e' un programma che, rilasciato sopra qualche server, ne cattura le informazioni richieste e le trattiene fino a lettura o le invia ad un destinatario (ad esempio).
L'atto di catturare di queste informazioni e' chiamato sniffing.
Molte delle piu' popolari connessioni tramite computer si eseguono attraverso ethernet.
Il protocollo Ethernet lavora mandando pacchetti di informazioni a tutti gli
host dello stesso circuito.
L'inizio del pacchetto contiene l'indirizzo proprio della macchina di destrinazione.
Solo il computer con l'indirizzo uguale e' predisposto ad accettare quel pacchetto; per non fare confronti bisogna porre la macchina in modo chiamato "promiscuo".
A causa del fatto che in un normale scambio di informazioni attraverso network, account e password sono inviati attraverso ethernet in normale testo non cifrato, non e' difficile per un intruso, una volta che ha ottenuto
il livello di superuser, porre la macchina in modo "promiscuo" e, facendo lo sniffing, compromettere tutte le macchine sulla rete di quel computer.
Dove si possono trovare gli sniffer?
Lo sniffing e' una delle piu' popolari tecniche di attacco degli hackers.
Uno speciale sniffer chiamato Esniff.c, veramente piccolo, e' stato creato per lavorare sulle stazioni SunOS e riesce a catturare "solo" i primi 300 bytes delle sessioni di telnet, ftp e rlogin.
Questo e' stato pubblicato in Phrack, cioe' uno dei giornali hackers piu' letti di tutta internet.
I vari articoli del Phrack si possono trovare su diversi siti ftp.
L'Esniff.c e' rimediabile all'ftp:
coombs.anu.edu.au:/pub/net/log.
Tu, lanciando lo sniffer su di un network autorizzato, puoi vedere come questo comprometta tutte le macchine della rete.
Altri sniffer, tesi a risolvere i debug dei programmi di rete
sono:*Etherfind
sul SunOS 4.1.x
*Snoop sul Solaris 2.x e SunOS 4.1 (ftp playground.sun.com)
*Tcpdump 3.0
*Packetman, Interman, Etherman, Loadman lavorano sulle seguenti piattaforme:
S
unOS, Dec-mips, SGI, Alpha e Solaris
ft
p.cs.curtin.edu.au:/pub/netman/[sun4c|dec-
mips|sgi|alpha|solaris2]/[Etherman-1.1a|Interman-1.1|
l
oadman-1.0|packetman-1.1].tar.gz
L
o sniffer chiamato Packerman (cosi' come Etherman o Interman) e' stato creato per catturare
p
acchetti di informazioni mentre Loadman per monitorare il traffico tra i computer.

Sniffer per il DOS:
***Gobbler per macchine IBM DOS**
***Ethdump v1.03**
ft
p.germany.eu.net:/pub/networking/inet/ethernet/ethdp103.zip
***Ethload v1.04**
ft
p.germany.eu.net:/pub/networking/monitoring/ethload/ethld104.zip

Sniffer commerciali:

***Network General**
La network general produce numerosi prodotti. I piu' importanti sono gli Expert Sniffer, che non solo corrono su tutta la rete ma possono anche caricare pacchetti attraverso un sistema ad alte prestazioni diagnosticando i problemi per te.

***Microsoft's Net Monitor**

Come si individua se vi e' uno sniffer su di un sistema?

Per individuare uno sniffer che raccoglie solo dati e non risponde a informazioni bisogna fisicamente verificare tutti i propri collegamenti Ethernet, controllandoli uno ad uno.
E' impossibile verificare in modo remoto un computer mandandogli un pacchetto di informazioni o facendo un ping alla macchina se questa e' stata "sniffata".
Uno sniffer che e' stato lanciato su di una macchina, mette l'interfaccia in
modo promiscuo con il quale accetta tutti i pacchetti di informazioni. Su alcuni sistemi UNIX e' possibile individuare se una macchina e' stata messa in modo promiscuo.
E' possibile lanciare uno sniffer su di una macchina in maniera non promiscua ma questo intercettera' solamente le informazioni che sono state lanciate direttamente dalla macchina.
E' anche possibile per l'intruso eseguire una simile cattura di informazioni
lanciando alcuni trojan horse (vedi sopra) su diversi programmi come telnet, rlogin, in.telnetd e altri.
Tutti questi tipi di attacchi compromettono solo le sessioni che vengono da una macchina invece lo sniffing in modo promiscuo compromette TUTTE le sessioni su Ethernet.
Per SunOS, NetBSD e altri possibili derivati BSD dello UNIX c'e' un comando "ifconfig -a" che ti dice tutte le informazioni su tutte le interfacce
e se loro sono in modo promiscuo.
Sul DEC OSF/1 e IRIX e altri possibili OS, bisogna specificare che interfaccia si vuole verificare.
La sola via per trovare quale interfaccia e' su di un sistema e questa: eseguire:
 # netstat -r
Routing tebles

Internet:

Destination	Gateway	Flags	Refs	Use	Interface
default	iss.net	UG	1	24949	le0
localhost	localhost	UH	2	83	lo0

Poi tu puoi testare ogni interfaccia eseguendo il seguente comando:
 # ifconfig le0
le0:
flags=8863<UP, BROADCAST, NOTRAILERS, RUNNING, PROMISC, MULTICAST>
inet 127.0.0.1 netmask 0xffffff00 broadcast 255.0.0.1

Gli hackers spesso rimpiazzano comandi come ifconfig per evitare l'individuazione.

C'e' un programma chiamato cpm scaricabile a:
ftp.cert.org:/pub/tools/cpm che lavora solo sul SunOS e ispeziona

l'interfaccia per le "primiscuous flag".

L'Ultrix puo' individuare qualcuno che lancia uno sniffer usando il comando pfstat e pfconfig.
"pfconfig" ti permette di settare chi puo' usare uno sniffer.
"pfstat" ti mostra se le interfacce sono in modo promiscuo.
Questi comandi funzionano solo se lo sniffing e' abilitato linkandolo nel kernel.
Per default, lo sniffer NON e' linkato nel kernel.
Molti altri sistemi UNIX, come Irix, Solaris, SCO, ecc, non hanno indicazioni sulle flags (se sono in modo promiscuo o no) e quindi un intruso puo' fare uno sniffig sul tuo sistema senza essere individuato.

Spesso un "log sniffer" (sniffer di inserimento) diventa un grande file. Su
un network con molti computer collegati ad esso, uno sniffer puo' dar luogo a lunghi caricamenti sulla macchina sniffata. Qualche volta questo mette in allarme gli amministratori di sistema e cosi' possono arrivare a scoprire uno sniffer.
Io suggerisco di usare lsof (LiSt Open Files) scaricabile da:
coast.cs.purdue.edu:/pub/Purdue/lsof
Questo programma trova i log file e i programmi che accedono ai pacchetti di informazioni su di un sistema come il /dev/nit sul SunOS.

Non esiste un comando (per quanto ne so') per individuare una macchina IBM PC posta in maniera "promiscua", ma solitamente queste macchine non permettono comandi di esecuzione tranne che dalla console principale e quindi intrusi che operano in modo remoto non possono cambiare un computer PC in uno sniffer senza avere aiuto dall'interno.

INFORMAZIONI SUI SISTEMI OPERATIVI:

Nota:
Sotto ogni descrizione riporto una lista delle piu' comuni password e login del sistema citato.

VMS:

I computer VAX e' stato creato dalla Digital Equipment Corporation (DEC) ed usa il VMS (Virtual Memory System). Questo sistema e' caratterizzato dal prompt con la scritta "Username:".
Il "bello" di questo sistema e' che non ti dice se hai sbagliato ad inserire un
username e ti puo' disconnettere dopo tre tentativi errati di inserimento.
Il VMS registra anche le tracce di tutti i tentativi falliti di login e informa
il possessore dell'account quanti tentativi sono stati fatti sbagliati sul suo
account. Questo e' uno dei piu' sicuri sistemi operativi che sono in circolazione contro gli attacchi dall'esterno ma una volta dentro ci sono molte cose che si possono fare per evitare le barriere di sicurezza erette dal
sistema. Il VAX ha anche il migliore set di file di aiuto del mondo.
Digita HELP per vederli.

Login:
        P
assword:

SYSTEM: OPERATOR, MANAGER, SYSTEM oppure SYSLIB
OPERATOR: OPERATOR
SYSTEST: UETP
SYSMAINT: SYSMAINT, SERVICE oppure DIGITAL
FIELD: FIELD o SERVICE
GUEST: GUEST o privo di password
DEMO: DEMO o privo di password
DECNET: DECNET

DEC-10

Una linea della DEC usa il sistema TOPS-10. Queste macchine sono individuabili dal prompt "."

La serie DEC 10/20 sono dette "amiche degli hackers" in quanto permettono molti importanti comandi senza neppure aver effettuato il login.
Tu puoi prendere una lista di accounts e di process name di tutti quelli collegati al sistema senza collegarti ad esso digitando .systat (sta per SYstem STATus).
Se tu leggi una cosa tipo:
[234,1001]BOB JONES, tenta BOB o JONES o tutti e due per la password su questo account.
Gli account sono in questo formato [xxx,yyy].
Per effettuare il login digitare .login xxx,yyy e poi inserisci la password quando ti viene richiesta.
Il sistema ti permette illimitati tentativi di login su di un account e non registra le tracce di quelli falliti.
Ti informa anche se il UIC (UIC=User Identification Code) che stai tentando e' sbagliato.

```
Login:
        P
assword:

1,2:        SYSLIB, OPERATOR oppure MANAGER
2,7:        MAINTAIN
5,30:       GAMES
```

UNIX

Ci sono dozzine di differenti macchine che possono usare lo UNIX.
Sebbene per alcuni non sia il miglior sistema operativo del mondo, e' certamente il piu' usato. Un sistema UNIX ha solitamente un prompt del tipo "login:". Il sistema UNIX permette illimitati tentativi di accesso (in
molti casi) e SOLITAMENTE non registra le tracce dei login falliti.
Nota sulle password:
Il sistema operativo UNIX e' molto sensibile e quindi scrivere InfectedM al posto di infectedm e' completamente diverso.

```
Login:
        P
assword:

root:       root
admin:      admin
sysadmin:   sysadmin or admin
unix:       unix
uucp:       uucp
rje:        rje
guest:      guest
demo:       demo
daemon:     daemon
sysbin:     sysbin
```

Comunque per le password dello unix guardate anche la lista nel capitolo dedicato all'hacking di questa guida.

PRIME

Il computer centrale della PRIME usa il sistema operativo PRIMOS. Si puo' facilemente identificare con la scritta che appare cioe': "Primecon 18.23.05" o qualcosa di simile che dipende dalla versione del sistema operativo. Solitamente non da' prompt questo sistema operativo.
A questo punto digita "login". Se il sistema e' un versione pre del 18.00.00
del Primos tu puoi premere una serie di ^C al posto della password e ritrovarti dentro. Sfortunatamente la maggior parte delle persone utilizza versioni superiori alla 19+. Il sistema Primos ha anche degli ottimi file di
aiuto. Uno dei piu' utili comandi che si puo' utilizzare in questo sistema e'
chiamato: NETLINK. Una volta che ti sei inserito nel computer digita NETLINK e segui i file di aiuto. Questo ti permette di connetterti agli NUA di tutto il mondo usando il comando "nc". Per esempio per

connettersi al NUA 026245890040004 tu devi digitare @nc
:26245890040004 nel prompt del netlink.

Login:	Password:
PRIME	PRIME o PRIMOS
PRIMOS_CS	PRIME o PRIMOS
PRIMENET	PRIMENET
SYSTEM	SYSTEM o PRIME
NETLINK	NETLINK
TEST	TEST
GUEST	GUEST
GUEST1	GUEST

HP-x000

Questo sistema e' stato creato dalla Hewlett Packard ed e' caratterizzato dal
prompt con i due punti ":"
L'HP ha una delle piu' complicate sessioni di login che girino sotto computer:
1) Hello Session Name
2) UserName
3) AccountName
4) Group.
Fortunatamente qualcuno di questi campi puo' essere bianco in alcuni casi ma possono anche essere tutti protetti da password e quindi non e' un sistema semplice in cui entrare.
In generale, se il default non funziona bisogna tentare un brute force usanto la password list comune.
L'HP-x000 usa il sistema operativo MPE e il prompt e' qualcosa come ":"

Login:	Password:
MGR.TELESUP,PUB	User: MGR Acct: HPONLY Grp: PUB
MGR.HPOFFICE,PUB	privo di password
MANAGER.ITF3000,PUB	privo di password
FIELD.SUPPORT,PUB	user: FLD, others, privo di password
MAIL.TELESUP,PUB	user: MAIL, others, privo di password
MGR.RJE	privo di password
FIELD.HPPl89 ,HPPl87,HPPl89,HPPl96	privo di password
MGR.TELESUP,PUB,HPONLY,HP3	privo di password

IRIS

IRIS sta per Interactive Real Time Information System. Originariamente girava solo sotto i PDP-11 ma ora gira sotto piu' macchine.
Si puo' identificare dalla scritta 'Welcome to "IRIS" R9.14 Timesharing' e per la scritta ACCOUNT ID? nel prompt.
IRIS permette illimitati tentativi di hackeraggio e non registra i tentativi
falliti. Non conosco password di default provare quindi con le password della lista sopra.

Login:

MANAGER
BOSS
SOFTWARE
DEMO
PDP8
PDP11
ACCOUNTING

VM/CMS

Il sistema operativo VM/CMS e' funzionante sopra le International Business Machine (IBM). Quando ti connetti ad uno di questi tu puoi ricevere un messaggio tipo 'VM/370 ONLINE' e un prompt "." come il TOPS-10. Per fare il login digitare 'LOGON'.

Login:

Password:

AUTOLOG1:	**AUTOLOG or AUTOLOG1**
CMS:	**CMS**
CMSBATCH:	**CMS or CMSBATCH**
EREP:	**EREP**
MAINT:	**MAINT or MAINTAIN**
OPERATNS:	**OPERATNS or OPERATOR**
OPERATOR:	**OPERATOR**
RSCS:	**RSCS**
SMART:	**SMART**
SNA:	**SNA**
VMTEST:	**VMTEST**
VMUTIL:	**VMUTILV**
TAM:	**VTAM**

NOS

NOS sta per Networking Operating System e funziona sui computer Cyber creati dalla Control Data Corporation. Il NOS si identifica facilmente dalla scritta 'WELCOME TO THE NOS SOFTWARE SYSTEM. COPYRIGHT CONTROL DATA 1978,1987'. Il primo prompt di comandi che ti potrebbe apparire e' FAMILY:. Qua premi invio. Poi ti dovrebbe apparire lo USER NAME:.
Lo username e' solitamente lungo 7 caratteri alfanumerici ed e' ESTREMAMENTE sito-dipendente. Gli account degli operatori solitamente sono qualcosa del tipo: 7ETPDOC.

Login:	**Password:**
$SYSTEM	**unknown**
SYSTEMV	**unknown**

DECSERVER

Questo non e' realmente un sistema ma e' un server di un network che ha differenti macchine collegate a lui. Un decserver puo' dire 'Enter Username>' quando ti connetti al sistema. Questo puo' essere qualsiasi cosa e puo' non significare niente...e' solo un'identificatore. Premi 'c' a questo punto per entrare. Ora ti si presentera' la scritta 'Local>'. Da qua premi ancora 'c' per connetterti al sistema. Per prendere una lista dei nomi nel sistema, digita 'sh services' oppure 'sh nodes'. Se hai qualche problema gli aiuti online sono disponibile digitando il comando 'help'. Dai un occhio a servizi chiamati 'MODEM' oppure 'DIAL' o qualcosa di simile, questi sono spesso outdial modem e possono essere d'aiuto.

GS/1

Un altro tipo di network server. Diversamente dal Decserver tu non puoi predirre quale prompt ti dara' il gateway del GS/1. Il default e' 'GS/1>' ma questo e' ridefinibile dall'amministratore di sistema.
Per testare il GS/1 digita 'sh d'. Se questo comando stampa a video una lista di default (velocita' del terminale, prompt, parita', etc.) tu sei su un GS/1. Tu ti puoi connettere alla stessa maniera del Decserver premendo 'c'. Per trovare quali sistemi sono disponibili premi 'sh n' oppure 'sh c'. Un altro trucchettino e' 'sh m' perche' qualche volta ti stampa a video una lista di macros per effettuare il login in un sistema. Se c'e' una macro chiamata VAX, per esempio, digita 'do VAX'.

SISTEMI IRRESPONSABILI

Occasionalmente tu ti puoi connettere ad un sistema che non ti dice nulla e non fa' nulla. Questa e' una cosa abbastanza frustrante ma un approccio con metodo ad un sistema puo' farti risparmiare un sacco di tempo. La seguente lista di cosa da fare ti puo' aiutare:
1) Cambia la tua parita', lunghezza dei dati e stop dei bits. Se un sistema

non risponde con 8N1, puo' rispondere con 7E1 o 8E2 o 7S2. Se tu non hai un terminale che cambi i settaggi a EVEN, ODD, SPACE, MARK o NONE con una lunghezza di 7 o 8 e 1 o 2 stop bits vai subito a comprarne uno. Avere un buon programma e' assolutamente necesssario e, sicuramente, di aiuto.
2) Cambia il tuo baud rate (velocita' di collegamento). Ancora, se tu hai un programma che ti permette di scegliere la tua velocita' di connessione (ad esempio 600 o 1100) potresti essere capace di penetrare un sistema che, senza il cambio di velocita' di connessione non potresti hackerare. Molti sistemi dipendono dalla velocita' ed alcuni hanno una strana velocita' di connessione e questo sembra che in alcuni sia tutta la sicurezza
di cui i sistemi necessitano (almeno secondo i loro amministratori).
3) Manda una serie di 's.
4) Manda un hard break seguito da una a.
5) Manda una serie di . I Datapac network canadesi rispondono a questo.
6) Se tu ottieni un garbage premi una i. Tymnet risponde a questo come MultiLink II.
7) Inizia a mandare dei control con delle lettere a partire da ^A e findendo
^Z.
8) Cambia la tua emulazione di terminale.
9) Digita LOGIN, HELLO, LOG, ATTACH, CONNECT, START, RUN, BEGIN, LOGON, GO, JOIN, HELP e qualsiasi altra cosa tu pensi che ti possa servire.
10) Se conosci il numero della compagnia da hackerare prova a chiamarli e sparare un sacco di balle per farti dare informazioni in piu'.

PHREAKING IN ITALIA

A dir la verita' ne so' poco o nulla del phreaking in Italia ma comunque vi dico ogni cosa mi viene in mente.
Ho letto da qualche parte anche se non ricordo bene dove alcune cose riguardanti le cabine telefoniche italiane (quelle dotate di lettore schede):
Se si telefona a qualcuno e questo qualcuno alza IMMEDIATAMENTE la cornetta (quando si dice immediatamente si intende senza quasi sentire lo squillo) il lettore di schede, a volte, non "sente" l'effettivo aggancio della
linea telefonica e non fa' spendere nulla.
Questo funziona su alcune cabine NON su tutte.
Per ricaricare le tessere magnetiche invece ho sentito due versioni:
a) Prendete un televisore vecchio e accendetelo per circa due o tre ore. Trascorso tale periodo passate la tessera magnetica (con la banda magnetica rivolta verso il vetro della tv) sopra lo schermo e verificate se si
e' ricaricata almeno in parte.
b) Prima di passare la tessera magnetica sopra il televisore dategli una spruzzatina di lacca sulla banda magnatica e POI passatela sul televisore come sopra. Verificate poi anche questa.
Io personalmente non ho verificato ma nel momento in cui scrivo alcuni amici stanno provando queste teorie.
Piccola nota:
Ho sentito in giro voci di persone che avrebbero usato il bluebox (scatoletta che permette di falsificare i segnali telefonici per poter telefonare gratis) in Italia.
Ora prevedo due cose:
1) Le persone che dicono di averlo usato lo hanno davvero fatto ma magari collegandosi a centralini fuori dal nostro Paese;
2) Stanno dicendo cagate solamente per farsi belli agli occhi degli altri.
Se volete avere maggiori informazioni sul phreaking in Italia vi consiglio di leggere il N°1 di SystemDown nel quale se ne parla molto piu' che in questa guida.

NOTA AGGIUNTIVA – Non mi stanchero' mai di ripeterlo il blueboxing in Italia con la freq 2600Hz non funziona le nuocve centraline hanno un sistema molto piu complesso che si basa su piu multifrequenze codificate che oscillano parecchio e rendono impossibile il box PER ORA – FINE NOTA MrZeRo

NOTE FINALI:

Principali siti dove reperire informazioni sull'hacking:

http://www.vcalpha.com/silicon/void-f.html (nel momento in cui scrivo non e' attivo)
http://www.2600.com
http://l0pht.com
http://underground.org
http://www.mgmua.com/hackers/index.html
http://195.32.61.1:80/zo

Libri consigliati:

The Hacker Crackdown

Testi utili sull'hacking e il phreaking (tutti in inglese o quasi):

A Novice's Guide To Hacking

Alt.2600 Hack Faq

The Hacker's Handbook

The Official Phreaker's Manual

Rainbow Book

Computer Hackers: Rebel With A Cause

The Legion Of Doom Technical Journals

The Ultimate Beginner's Guide To Hacking And Phreaking

La guida italiana all'hacking :-)))

SystemDown (rivista Italiana di hacking/phreaking/cracking/virii)

Newgroups sull'hacking e il phreaking:

alt.2600 (e suoi derivati)
alt.2600.hackerz
alt.2600.hope.tech
alt.cellular
alt.cellular-phone-tech
alt.comp.virus
alt.cracks
alt.cyberpunk
alt.cyberspace
alt.dcom.telecom
alt.fan.lewiz
alt.hacker
alt.hackers
alt.hackers.groups
alt.hackers.malicious
alt.hacking
alt.hackintos
alt.security

Film da vedere sugli hackers e simili:

Wargames, giochi di guerra
Hackers
I signori della truffa

Se mi volete scrivere, lo potete fare a:

InfectedMachine@cryogen.com