Come un cracker attacca una macchina

a) raccolta informazioni
- scanning
- finger
- packet sniffing

b) ottiene accesso non privilegiato
- sfrutta un baco del SO
- indovina o si fa dire una password

c) ottiene accesso privilegiato

d) nasconde le sue tracce
- back door
- rootkit

Scanning the internet

ICMP scanning

nmap -sP 212.121.*.*

port scanning

nmap -v target.example.com

nmap -p 1-65535 target.example.com

stealth port scanning

SYN stealth, FIN stealth, Xmas tree

timing

randomizing

analisi del SO della macchina

TCP fingerprint

Contromisure

- logging dei pacchetti
- analisi
- firewall

I risultati di un port scan

So che sistema operativo usa

So quali servizi sono attivi su una macchina

So come concentrare i miei sforzi successivi

Molte macchine sono configurate con servizi inutili
- tutto quello che non serve va chiuso!

Analisi automatizzata delle vulnerabilità

Nuove vulnerabilità sono scoperte ogni giorno

Difficile restare aggiornati

Il sistema *nessus*

- database di *exploit*
- macrolinguaggio per esprimere gli exploit
- prova tutti gli exploit uno dopo l'altro
  - exploit "sicuri" o "pericolosi"

Esempio di codice NASL (Nessus Attack Scripting Language)

```
if(description)
{
 script_id(10343);
 name["english"] = "MySQLs accepts any password";

 desc["english"] = "
You are running a version of MySQL which is
older than (or as old as) version 3.22.30 or 3.23.10

If you have not patched this version, then
any attacker who knows a valid username can
access your tables without having to enter any
valid password.

Risk factor : High
Solution : Upgrade to a newer version, or
edit the file mysql-xxx/sql/password.c, and
search for the 'while(*scrambled)' loop. In front
of it, add : 'if(strlen(scrambled) != strlen(to))return 1'";

 summary["english"] = "Checks for the remote MySQL version";
 script_category(ACT_GATHER_INFO);
 exit(0);
}
```



```
#
# The script code starts here
#

include("misc_func.inc");

port = get_kb_item("Services/mysql");
if(!port)port = 3306;

ver = get_mysql_version(port);
if (ver == NULL) exit(0);
if(ereg(pattern:"3(22(2[6789]|30)|23([89]|10))", string:ver))security_hole(port);
```

Installazione di back door

In ordine di "visibilità" crescente:

- creazione di nuove login
- lasciare un server TCP in ascolto
- associare un processo a una socket di un server esistente
  - es. httpd, ftpd
  - quando arriva una richiesta che contiene una stringa prefissata il processo si risveglia...
  - ... e apre una porta in ascolto, oppure
  - ... apre una connessione verso la macchina del cracker
- installare un programma di login troiano (o un httpd troiano...)

Cancellare le proprie tracce

i file del cracker sono in directory nascoste o dai nomi strani ". ", "..."

cancellazione dei log
- /var/log/wtmp, /var/log/messages...
- tool per la cancellazione selettiva

installazione di versioni troiane di ps(1), top(1), ls(1), who(1), netstat(8), syslogd(8)...

script kiddies n. The lowest form of *cracker*

script kiddies do mischief with scripts and programs written by others, often without understanding the *exploit* they are using.

Used of people with limited technical expertise using easy-to-operate, pre-configured, and/or automated tools to conduct disruptive activities against networked systems.

Sono pericolosi perché attaccano i sistemi poco sorvegliati

Rootkit: la manna dello script kiddie

Un singolo package, che installa
- versioni troiane dei programmi di sistema
- back door
- programmi di monitoraggio

tutto quello che digiti su un sistema compromesso può essere trasmesso silenziosamente a terzi

Contromisure

Essere paranoici (*c'è davvero* una cospirazione ai tuoi danni!)

Logging remoto

Disinstallare i servizi inutili

Monitorare la rete, e i file di log

Installare un firewall

Usare *tripwire*
- quando il sistema è appena installato, salvare l'impronta md5 di tutti i file su un floppy
- periodicamente verificare l'integrità dei file chiave

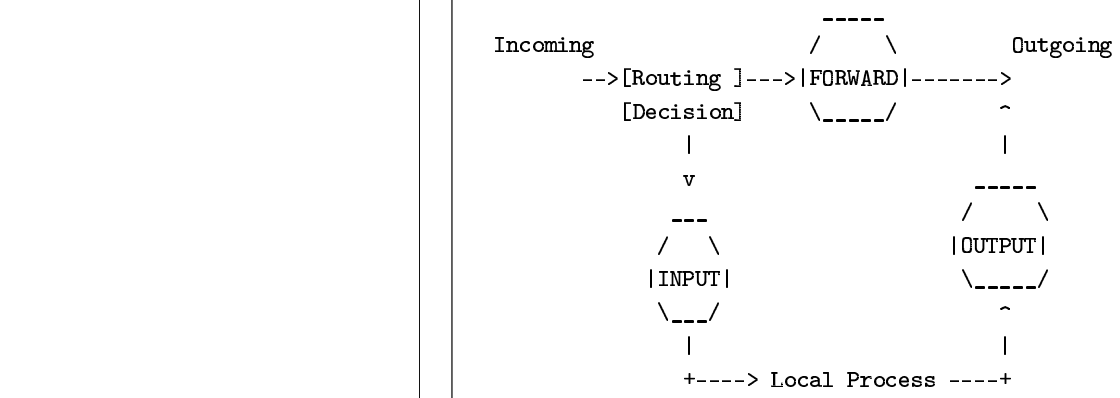
Usare *chkrootkit*

Firewall

Tipi di firewall

- packet filter
- tcp proxy
- application proxy

Netfilter: il firewall incorporato nel kernel di Linux



Esempio di firewall configurato in Linux

scopi

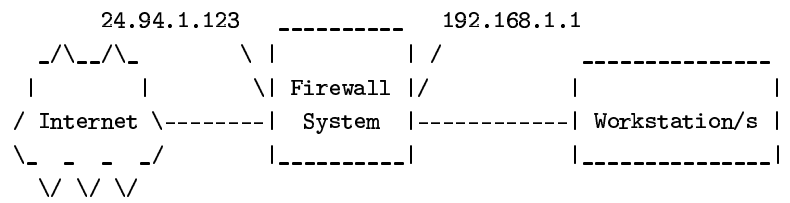
- permettere di accedere dall'esterno ai servizi HTTP e SSH
- permettere agli utenti locali di accedere a Internet
- negare tutto il resto


```
# Flush all chains
/sbin/iptables -F

# Unlimited traffic on the loopback interface
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT

# Set the default INPUT and FORWARD policy to DROP
/sbin/iptables --policy INPUT DROP
/sbin/iptables --policy OUTPUT DROP
/sbin/iptables --policy FORWARD DROP

# Use connection state to bypass rule checking
/sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# Allow port 22 (ssh) and 80 (http) TCP traffic
/sbin/iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
/sbin/iptables -A INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT

# Drop all other traffic
/sbin/iptables -A INPUT -p all -j DROP
```

NAT: uno strumento utilissimo

Network Address Translation (NAT)

- risolve il problema della scarsità di indirizzi IP pubblici
- nasconde la struttura della rete locale



Il firewall non è una panacea

- molte applicazioni non web usano il protocollo HTTP
- se espongo web applications, un errore in una di esse può essere sufficiente a compromettere il sistema
- molti attacchi provengono dall'interno
- il punto debole spesso è il personale (vedi social engineering)
- ci sono tecniche (decisamente esoteriche) per eludere i firewall
- è possibile manomettere il firewall o i router

Attacchi su una web application (i)

L'applicazione contiene questo codice:

```
$sql = "insert into quotations (insertion_date, author_name, quote)
        values                 (now(), '$_POST[author_name]', '$_POST[quote]')";
```

E se la variabile `$_POST["quote"]` contiene "What's up, doc" ?
⇒ la query sql diventa non valida!

```
insert into quotations (insertion_date, author_name, quote)
       values          (now(), 'Bugs Bunny', 'What's up, doc')
```

E se contiene...

```
'); insert into users (username, password, is_admin)
              values ('hax0r', md5('secret'), 1);
```

→ qualcuno riesce a crearsi un utente amministratore!

Attacchi su una web application (ii)

Altro esempio:

```
$user = $_POST["username"];
$pwd =  $_POST["password"];
$sql =  "select * from users where username = '$user' and password = '$pwd';
```

L'utente usa

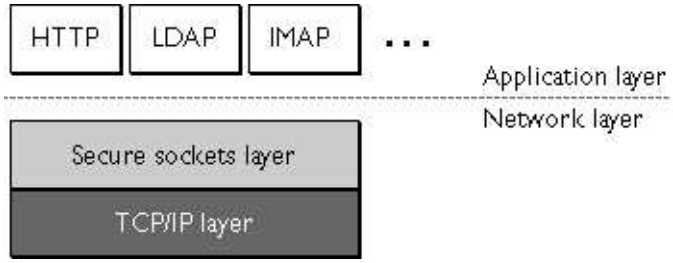
```
' or 'b'=b'
```

come username e password; risultato:

```
select * from users where username = '' or 'b'='b' and password = '' or 'b'='b'
```

→ questa where è sempre vera

Il protocollo SSL



- server authentication
- client authentication (optional)
- encrypted connection

Mai trasmettere la propria password in chiaro

Il protocollo SSH usa SSL per fornire
- remote login
- remote program execution
- file transfer

sshd(8): server daemon

ssh-keygen(1): genera una coppia di chiavi pubbliche-private

ssh(1): remote execution, remote login

scp(1), sftp(1): file transfer

ssh-agent(1): authentication agent (mi salva dal digitare la mia passphrase 100 volte al giorno

.ssh/authorized_keys: chiavi pubbliche di utenti autorizzati a usare il mio account senza password

social engineering n. Term used among *crackers* and *samurai* for cracking techniques that rely on weaknesses in *wetware* rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.

An example of social engineering by _A&T

Good morning sir, I am (insert faked name here), I am willing to speak with mr. (insert victim's name here)

Yes, hold on please

....

Hello, I am (victim's name)

Good morning sir, I am an employee of the local Hotmail agency (btw, I don't think Hotmal has 'local agencies'), I am sorry I am calling you so early...

Uh, hotmail, well, I was having breakfast, but it doesn't matter (victim is surprised)

I was able to call you because of the personal data form you filled when creating your account, so don't be surprised (with eye-blinking tone)

My pers.. oh, yes

I have to inform you that we had a hard disk crash tonight, and we are trying to restore all our user's mail.

A crash? Is my mail lost?

Oh no, sir, we can restore it. But, since we are simple employees, and we are

not allowed to mess with our user's mail, we need your password, otherwise we cannot take any action(first try, probably unsuccessfull)

Er, my password? Well...

Yes, I know, you have read on the license agreement that we will never ask for it, but it was written by the legal department, you know, all law stuff that's needed to open business and such. (effort to gain victim's trust)

Your username is (insert victim's username), isn't it? Legals gave us your username and telephone, but, as smart as they are, not the password. See, without your password nobody can access your mail, even we hotmail employees. But we have to restore your mail, and we need access. You can be sure we will not use your password for anything else, well, we will forget it. (smiling)

Well, it's not so secret (also smiling! it's amazing...), my pass is xxxxxx

Thank you very much, sir. We will restore your mail in a few minutes

But no mail is lost, isn't it?

Absolutely, sir. You should not experience any problems, but do not hesitate to contact us just in case. You will find contact numbers on our web page (which our victim has probably never read from begin to end)

Thanx, you are very efficient, goodbye

Goodbye

Mobile code

Problema: aggiungere contenuto eseguibile a una pagina web

- stock tickers
- animations
- news tickers
- direct manipulation interfaces

Ricordate: se permetto a un estraneo di eseguire codice sul mio computer, diventa il *suo* computer

Possibili tecniche:

- sandboxing
- interpretation
- code signing