Intrusioni: Aquisizione di Informazioni

 1

Evoluzione di un'intrusione

1. Acquisizione di informazioni
2. Uso di vulnerabilita'
3. Upload di programmi
4. Download di dati
5. Garantire un successivo accesso
6. Cancellare le tracce dell'intrusione

 2

Un'intrusione spesso non si compone di un semplice atto di uso di una vulnerabilita' di un sistema, ma e' un insieme di atti che permettono di:

1. Identificare l'obiettivo riconoscendone il Sistema Operativo, i servizi di rete abilitati, versioni dei software installati. Maggiori in numero e in precisione sono le informazioni che un intrusore riesce a ricavare e piu' facile sara' realizzare l'intrusione;
2. La specifica vulnerabilita' viene sfruttata per acquisire l'accesso al sistema;
3. Acquisito il controllo del sistema vengono spesso copiati in locale ed eseguiti programmi che facilitano il possesso del sistema o permettono ulteriori attacchi diretti ad altri sistemi;
4. Avendo il controllo del sistema possono essere acceduti dati (es. file delle password, dati proprietari dell'organizzazione);
5. L'intrusore si garantisce la possibilita' di successivi accessi con modalita' apparentemente lecite (es. creazione di nuovi account, abilitazione di nuovi servizi per l'accesso remoto);
6. Le tracce del'intrusione vengono cancellate (es. dai log di sistema) o nascoste (es. Directory nascoste, etc.)

Acquisizione di Informazioni

Whois: (whois.networksolutions.com) Dati della persona che ha registrato il dominio (es. unimi.it), ***Domain Name Servers*** (esterni);

NsLookup : (nslookup dns-server) ***Indirizzi IP*** (Web Server, Firewall …) di un dato dominio.

ARIN Web Search (USA) / RIPE Web Search (EU) : (www.arin.net - www.ripe.net) Dati sulla ***classe di indirizzi assegnati*** ad un certo dominio.

Traceroute : Visualizza tutti i ***router*** attraversati per consegnare un pacchetto ad una data destinazione (oppure fino a quando non viene rigettato)

Ping : Verifica se un dato indirizzo IP corrisponde ad un ***host in ascolto e raggiungibile***.

 3

Importante minimizzare le informazioni che si rendono disponibili pubblicamente.

DNS Esterni : listare solo gli host accedibili via Internet (indispensabile per essere raggiungibili) ma non altri, che andranno listati in un DNS interno, non interrogabile da Internet e whois.

Traceroute e Ping : Puo' essere bloccato dal router di frontiera o dal firewall tutto il traffici ICMP in entrata. Si perdono pero' funzionalita' utili.

ARIN (American Registry for Internet Numbers) e RIPE Web Search : non c'e' nulla da fare per poter limitare le informazioni ricavabili interrogando questi database

```
[root@gigan /root]# whois network-defense.com
[rs.internic.net]

Registrant:
Company Name (NETWORK-DEFENSE-DOM)
   9305 Sun Down Pl
   Nowhere, MD 21047, US

   Domain Name: NETWORK-DEFENSE.COM
   Administrative Contact, Technical Contact, Zone Contact:
      Gula, Ron  (RG15449)  rjgula@HOME.COM
      410-212-9898
   Billing Contact:
      Gula, Ron  (RG15449)  rjgula@HOME.COM
      410-212-9898
   Record last updated on 24-Nov-98.
   Record created on 24-Nov-98.
   Database last updated on 7-Apr-99 12:28:52 EDT.

   Domain servers in listed order:
   NS.AUTONO.NET               209.48.2.11
   NS10.AUTONO.NET             206.86.247.30
```


Esempio di uso del **whois**.

Esempio di ricerca su ARIN per l'indirizzo IP 24.3.17.92:

```
@Home Network (NETBLK-ATHOME)
ATHOME           24.0.0.0 - 24.7.255.255

@Home Network (NETBLK-MD-COMCAST-HWRD-1)
MD-COMCAST-HWRD-1       24.3.16.0 - 24.3.23.255
```

Da qui ricaviamo che:
L'indirizzo IP appartiene all'Internet Service Provider @Home;
@Home ha le classi B 24.0 - 24.7 assegnate;

Le classi C 24.3.16 - 24.3.23 sono usate da @Home per accessi locali
(Comcast e' una societa' di connessioni locali via cavo);

PORTMAPPING

Una informazione necessaria a preparare molte intrusioni consiste nel conoscere quali porte sono aperte (servizio abilitato) e quali sono chiuse (servizio non abilitato)

Perche' e' una informazione importante?

Perche' molti servizi (http, ftp, ssh, telnet …) hanno vulnerabilita' che possono rendere un attacco efficace.

 6

TCP scanning

- il metodo piu' semplice;
- uso della system call `connect()` fornita da Unix per aprire una connessione verso una data porta;
- se la connessione ha successo, allora la porta dell'host destinatario e' in ascolto;
- i log dell'host di destinazione mostreranno queste connessioni completate, seguite dalla loro interruzione.

 7

TCP SYN scan

- Detta **HALF-OPEN scanning**, perche' viene iniziata una regolare connessione TCP (il primo SYN dell'handshake);
- se si riceve il SYN/ACK (secondo messaggio dell'handshake), allora la data porta dell'host destinatario e' in ascolto, la connessione viene quindi resettata con un RST;
- Se la porta dell'host destinatario e' chiusa, verra' risposto con un RST;
- Non tutti gli host riportano nei log i casi di connessioni half-open

 8

```
scan.net.34567 > server.com.23: S 3900690:3900690(0)
server.com.23 > scan.net.34567 : S
                    1379776:1379776(0) ack 3900691
scan.net.34567 > server.com.23: R

scan.net.34567 > server.com.80: S 405812:405812(0)
server.com.80 > scan.net.34567 : S 423800:423800(0)
                    ack 405813
scan.net.34567 > server.com.80: R

scan.net.34567 > server.com.53: S 465834:465834(0)
server.com.53 > scan.net.34567 : R
```


TCP FIN, Xmas e Null scan

- FIN scan: invia un pacchetto isolato con il flag FIN a 1;
- Xmas scan : flag FIN, URG e PSH a 1;
- Null scan : tutti i flag a 0;
- Le specifiche di TCP (RFC 793) prevedono che questi pacchetti vengano scartati senza risposta se la porta di destinazione e' **aperta**, venga risposto un **RST** se la porta e' **chiusa**;
- Alcuni sistemi operativi (es. Windows, HP/UX, IRIX) non rispettano le specifiche del TCP e rispondono con un RST in ogni caso;
- Spesso non compaiono nei log.

 10

```
scan.net.34567 > server.com.23: F 3900690:3900690(0)

scan.net.34567 > server.com.80: F P
                    405812:405812(0) (urg)

scan.net.34567 > server.com.53:
server.com.53 > scan.net.34567 : R
```

 11

ACK scan

- ACK scan: invia un pacchetto isolato di ACK;
- Le specifiche di TCP (RFC 793) prevedono che questi pacchetti vengano scartati senza risposta se la porta di destinazione e' **aperta**, venga risposto un **RST** se la porta e' **chiusa**;
- Usato anche in combinazione con altri tipi di scan per verificare se esiste un firewall che analizza lo stato della connessione (***stateful fw***) o considera solo i singoli pacchetti (***packet filter***).

 12

Consideriamo meglio l'ultimo punto.

```
abc.com.telnet > efg.net.telnet: ack 1379777
abc.com.telnet > hil.org.telnet: ack 1379777
abc.com.imap > efg.net.imap: ack 1379777
abc.com.imap > hil.org.imap: ack 1379777
abc.com.ssh > efg.net.ssh: ack 1379777
abc.com.ssh > hil.org.ssh: ack 1379777
abc.com.telnet > mno.it.telnet: ack 1379777
mno.it.telnet > abc.com.telnet : R
abc.com.telnet > pqr.it.telnet: ack 1379777
pqr.it.telnet > abc.com.telnet : R
```

 13

Elementi da notare:

- Non rispetta l'handshake del protocollo TCP;
- Porta del client < 1024 ed uguale a quella di destinazione;
- Sequence Number sempre uguale;

Come e' possibile? I pacchetti sono stati manipolati ('crafted') volutamente, non sono frutto di una implementazione TCP.

Per quale motivo? Che cosa ricavo?

Se non ottengo risposta significa che il destinatario e' irraggiungibile (inesistente, sconnesso, etc.).

Se ricevo un RESET significa che il destinatario esiste (non so pero' se la porta sia CLOSE o LISTEN).

Se usati insieme l'ACK scan e un altro tipo di scan, ad esempio il SYN scan, posso ottenere:

```
scan.net.34567 > server.com.22: S 465834:465834(0)
fw.server.com > scan.net: icmp: host target.host
unreachable - admin prohibited

scan.net.34567 > server.com.22 : ack 1379777
server.com.22 > scan.net.34567 : R
```

Da qui deduco che il firewall esegue solo un filtraggio a livello di singolo pacchetto e non mantiene lo stato della sessione.

 14

UDP scan

- Serve per determinare quali porte UDP sono aperte;
- Viene inviato un pacchetto UDP di 0 byte di dati, se la porta e' **chiusa** viene risposto con un messaggio **ICMP port unreachable**, diversamente si assume la porta **aperta**;
- Spesso trascurato, erroneamente:
  - esistono vulnerabilita' anche per servizi UDP (es. snmp, nfs);
  - molti Trojan Horse attivano backdoor su porte UDP.
- Molto lento perche', secondo specifiche (RFC 1812), la frequenza di messaggi di errore ICMP viene limitata da molti sistemi operativi (Microsoft ignora il suggerimento e non la limita!!!).

SCANNER

Esempio di output

```
Service     State    Port
ftp         open     21/tcp File Transfer [Control]
ssh         open     22/tcp Secure Shell
telnet      open     23/tcp Telnet
smtp        open     25/tcp Simple Mail Transfer
finger      open     79/tcp Finger
http        open     80/tcp World Wide Web
pop3        open     110/tcp Post Office Protocol - Version 3
sunrpc      open     111/tcp rpcbind SUN Remote Procedure Call
login       open     513/tcp remote login
cmd         open     514/tcp shell like exec, but automatic
```

nmap e' il piu' diffuso. Presente anche in distribuzioni standard di sistemi operativi (es. Linux Red Hat 7.x).

 16

Gli scanner sono programmi che automatizzano l'attivita' di scanning.

Sono strumenti indispensabili per garantire la sicurezza (non solo per chi la vuole violare), poiche' permettono di testare con molte modalita' diverse una intera rete, verificare le politiche di sicurezza dei firewall e monitorare che gli host non presentino porte anomale attive ed in ascolto.

Obiettivo di uno scanning

Obiettivo predefinito : lo scanning e' mirato ad uno specifico sito od organizzazione (IP specifici o classe C);

Scanning ad ampio spettro : lo scanning viene effettuato su intere classi A o B di indirizzi IP;

Scanning mirato ad un servizio : lo scanning puo' essere ad ampio spettro ma concentrato a verificare le risposte da una porta predefinita.

 17

Obiettivo predefinito : qualcuno vuole raccogliere informazioni relative ad una ben precisa organizzazione;

Scanning ad ampio spettro : vengono costruiti database con lo scopo di mappare i servizi attivi su intere classi A o B di indirizzi.

Scanning mirato ad un servizio : Questo puo' indicare:

- ricerca di host con un servizio molto esposto a vulnerabilita' (tipico porta 80, http);
- nuova vulnerabilita' resa nota associata alla specifica porta;
- backdoor in ascolto sulla specifica porta;
- senza spiegazione (vulnerabilita' non nota? Backdoor non conosciuta?)

Uno scanning e' un segnale di allarme, non un'intrusione:

- Raccogliere informazioni, determinare il target (singolo, generico, servizio);
- Analizzare le propria vulnerabilita';
- Monitorare l'evoluzione;

Possibili reazioni:

- Contattare l'originatore;
- Bloccare gli indirizzi di origine.

 18

ATTENZIONE alle reazioni, come ad esempio bloccare tutte le connessioni dagli indirizzi di origine di uno scan!!!

OS Fingerprinting
(Identificazione del Sistema Operativo)

Tool come **`nmap`** e altri, utilizzano sequenze di pacchetti anomali, non rispondenti alle specifiche del TCP, oppure noti per provocare reazioni dipendenti dalle singole implementazioni dello stack TCP.

In questo modo riescono a predire, con ottima approssimazione, il sistema operativo e talvolta la specifica versione dell'host contattato.

 19

OS Fingerprinting : sequenza usata da nmap

Descrizione del test

1. **Una serie di pacchetti con SYN vengono inviati per analizzare come vengono generati i numeri di sequenza;**
2. **Un pacchetto NULL (nessun flag) viene inviato ad una porta TCP aperta;**
3. **Un pacchetto con SYN,FIN,PSH,URG viene inviato ad una porta TCP aperta;**
4. **Un pacchetto con ACK viene inviato ad una porta TCP aperta;**
5. **Un pacchetto con SYN viene inviato ad una porta TCP chiusa;**
6. **Un pacchetto con ACK viene inviato ad una porta TCP chiusa;**
7. **Un pacchetto con FIN,PSH,URG viene inviato ad una porta TCP chiusa;**
8. **Un pacchetto viene inviato ad una porta UDP chiusa;**

 20

OS Fingerprinting : esempi

```
Port     State     Service
21/tcp   open      ftp
22/tcp   open      ssh
23/tcp   open      telnet
80/tcp   open      http

...
Remote operating system guess: WinNT4 / Win95 /Win98
```

```
Port     State     Service
21/tcp   open      ftp
22/tcp   open      ssh
23/tcp   open      telnet
80/tcp   open      http

...
Remote operating system guess: Linux 2.1 - 2.4
```


Con l'uso di scanner (es. Nmap) o altri tool disponibili liberamente (sia open source, freeware che commerciali) e' possibile verificare il tipo di sistema operativo remoto (con ottime possibilita' di individiazione).

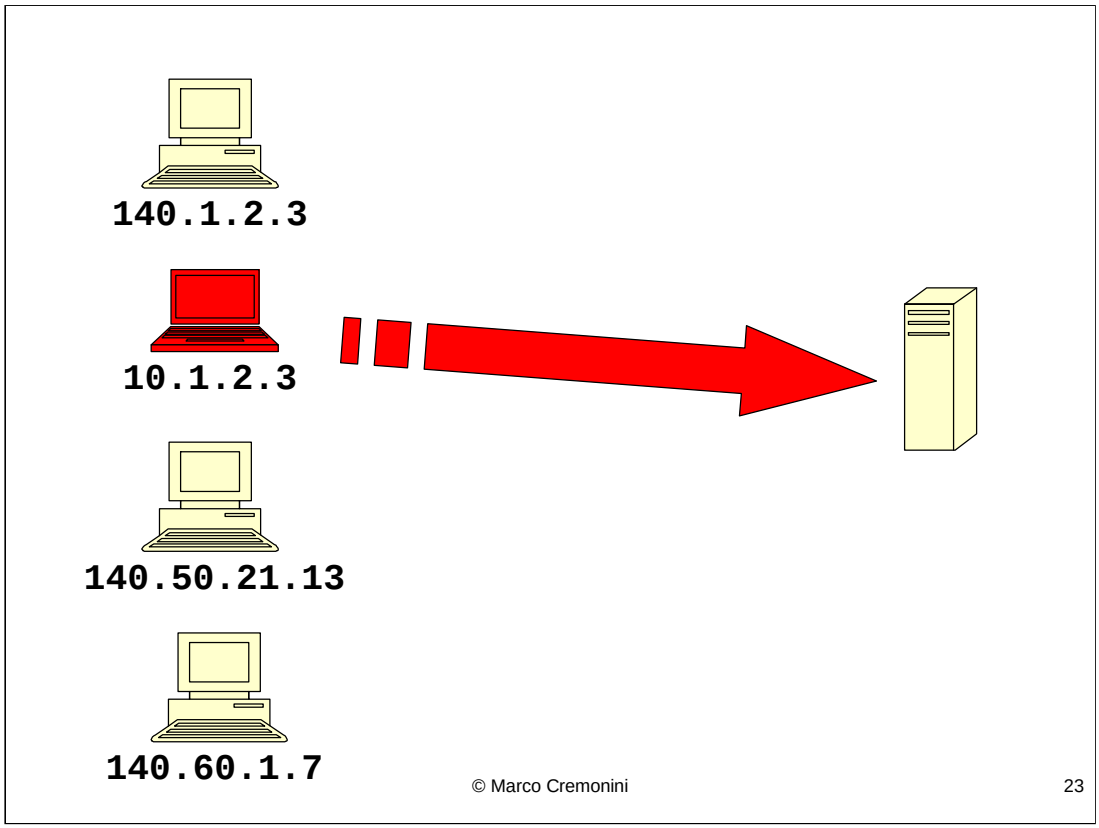
La conoscenza del sistema operativo indica anche il tipo di implementazione del generatore di numeri di sequenza.

In allcuni casi puo' essere molto semplice (incrementi fissi a intervalli temporali regolari), in altri puo' essere estremamente difficile.

```
140.1.2.3.34567 > server.com.23: F
140.1.2.3.34567 > server.com.23: F
140.1.2.3.34567 > server.com.23: F
…
10.1.2.3.2594 > server.com.23: F
10.1.2.3.2594 > server.com.23: F
…
140.50.21.13.5675 > server.com.23: F
140.50.21.13.5675 > server.com.23: F
…
140.60.1.7.8322 > server.com.23: F
140.60.1.7.8322 > server.com.23: F
140.60.1.7.8322 > server.com.23: F
```


Apparente scan da 4 indirizzi IP.

Cosa succede se decido di filtrarli tutti, impedendo quindi qualunque connessione da essi?



Potrei commettere un errore: i pacchetti possono essere stati manomessi e gli indirizzi IP che rilevo come mittenti potrebbero non corrispondere al siti che hanno effettivamente eseguito uno scanning nei nostri confronti (solo uno di essi e' il mittente).

--> operazione di **SPOOFING**