Syn scanning & Nmapping

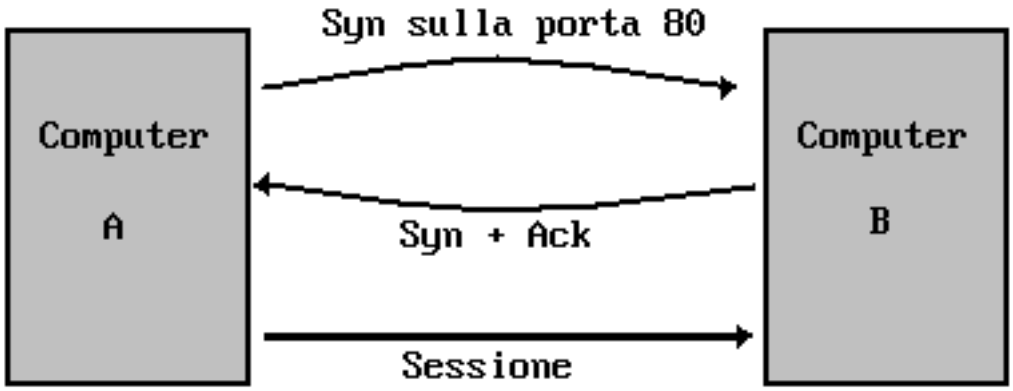
evilsocket
http://evilsocket.altervista.org/

.: Introduzione

In questo paper andremo a vedere le basi dei protocolli di comunicazione di rete al fine di capire cosa è il syn-scanning, come funziona e come usarlo per identificare vari servizi di un sistema remoto .

Quando un computer deve comunicare con un altro, viene eseguito un insieme di operazioni preliminari per inizializzare la sessione TCP, tale sequenza si chiama “handshake” .

Vediamo nella seguente figura come avviene l'handshake tra una postazione che vuole connettersi alla porta 80 di un sistema remoto .



Come possiamo vedere, nella prima fase dell handshake il computer A invia un pacchetto al computer B settando ad uno il bit SYN del header TCP del pacchetto stesso (per i riferimenti sulla struttura del header tcp vedere http://www.freesoft.org/CIE/Course/Section4/8.htm) .

Successivamente, se la porta è aperta (in questo caso la 80), il computer B risponde con un altro pacchetto, settando a 1 i bit SYN e ACK .

Da questo momento la sessione TCP ha inizio e i due pc possono procedere ad inviarsi i dati veri e propri .

.: Syn-Scanning

Il syn scanning sfrutta proprio questa particolarità del protocollo TCP in quanto, al contrario delle tecniche di scanning

basate su una connessione vera e propria alla porta, si appoggia su un livello più vicino alla macchina nello strato ISO/OSI risultando la tecnica più efficace in velocità, invisibilità e funzionamento bypassando il più delle volte un eventuale firewall che protegge il computer remoto .

Invece di stabilire una connessione vera e propria, che in molti casi potrebbe essere rifiutata da un firewall, un syn scanner si limita ad inviare un pacchetto SYN ad una determinata porta e a determinare se è aperta o meno in base alla risposta del sistema remoto (ricordate il SYN+ACK no ? ^^) .

.: Nmap

Il syn scanner per eccellenza è il noto nmap, reperibile all'indirizzo http://insecure.org/nmap/ .
Basandosi proprio su questa tecnica, nmap offre oltre ad ottime funzionalità di port scanning, anche un sistema di riconoscimento del sistema operativo remoto e dei vari servizi chiamato "fingerprinting" .

Per provare uno scanning di test sul proprio computer, potete provare la seguente riga di comando :

```
nmap localhost
```

Il che produrrà un output del tipo :

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2007-08-06
01:03 CEST
Interesting ports on Wiki (127.0.0.1):
Not shown: 1672 closed ports
PORT     STATE SERVICE
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
830/tcp  open  unknown
832/tcp  open  unknown
864/tcp  open  unknown
2049/tcp open  nfs

Nmap finished: 1 IP address (1 host up) scanned in 0.241 seconds
```

Come potete vedere, nmap in meno di un secondo ha identificato tutte le porte aperte e i relativi servizi sul vostro computer .
Se volete ottenere qualche informazione in più, come ad esempio la versione dei vari servizi, usate :

```
nmap -A localhost
```

Ottenendo una cosa del tipo :

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2007-08-06
01:05 CEST
Interesting ports on Wiki (127.0.0.1):
Not shown: 1672 closed ports
PORT     STATE SERVICE     VERSION
111/tcp  open  rpcbind      2 (rpc #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: MYGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: MYGROUP)
631/tcp  open  ipp         CUPS 1.2
830/tcp  open  status       1 (rpc #100024)
832/tcp  open  rquotad      1-2 (rpc #100011)
864/tcp  open  mountd       1-3 (rpc #100005)
2049/tcp open  nfs          2-4 (rpc #100003)

Nmap finished: 1 IP address (1 host up) scanned in 11.327 seconds
```

Ed ecco la versione di ogni servizio balzar fuori come per magia ^^ .

In questo caso, ancora non stiamo usufruendo di tutte le potenzialità di nmap .
Provate ad lanciare lo scanner usando la seguente linea di comando :

```
nmap -A -F -sS -P0 localhost
```

Dove :

-A : Indica, come abbiamo visto, di identificare la versione dei servizi .

-F : Considera solamente le porte di maggior uso e salta quelle meno note, risparmiando così tempo .

-sS : Attiva il syn-scanning (vedi sezione **Syn-Scanning**) .

-P0 : NON generare pacchetti ICMP, utilissimo per bypassare i firewall .

Il che produrrà (nel caso del mio computer) il seguente output :

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2007-08-06
01:13 CEST
Interesting ports on Wiki (127.0.0.1):
Not shown: 1672 closed ports
PORT     STATE SERVICE     VERSION
111/tcp  open  rpcbind      2 (rpc #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: MYGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: MYGROUP)
631/tcp  open  ipp         CUPS 1.2
830/tcp  open  status       1 (rpc #100024)
```

```
832/tcp  open  rquotad      1-2 (rpc #100011)
864/tcp  open  mountd       1-3 (rpc #100005)
2049/tcp open  nfs          2-4 (rpc #100003)
MAC Address: 00:17:C2:A8:xx:xx
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.7 - 2.6.11

Nmap finished: 1 IP address (1 host up) scanned in 16.830 seconds
```

In questo modo, oltre ad identificare la versione dei servizi, possiamo vedere come nmap ha identificato anche il sistema operaitvo della macchina e il mac address della sua scheda di rete .

evilsocket