Alessandro Olivero *Nunzio Onorati* *Leonardo Pio Petrillo*

01QZD

Laboratorio di Internet e Comunicazioni

Internet - Laboratorio 4

Port Scan - Using nmap

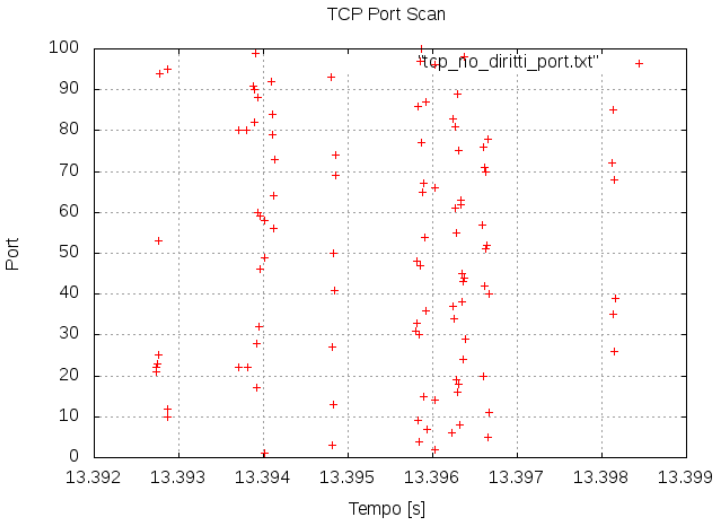
Abbiamo eseguito una Port Scan sulle prime 100 porte di un host in rete per vedere quali servizi erano attivi su quell'host

La Port Scan è stata eseguita in 4 modalità:
- TCP senza diritti di root
- UDP senza diritti di root
- TCP con diritti di root
- UDP con diritti di root

TCP senza diritti di root

```
nmap 192.168.2.15 -p 1-100 -v
```

Nmap prova ad effettuare una risoluzione DNS del client che dopo 13s di timeout fallisce.
A questo punto esegue la Port Scan che completa in pochi millisecondi.



Ogni porta viene contattata una sola volta e, sfruttando la connessione TCP capisce quali servizi sono attivi sull'host target.

Se sulla porta non sono presenti servizi attivi la conversazione consiste in due pacchetti: un [SYN] mandato dall'host locale e un [RST, ACK] mandato dall'host target.

Se sulla porta vi sono servizi attivi la connessione viene stabilita. In questo modo nmap sa che c'è un'applicazione pronta ad ascoltare e quindi può chiudere la connessione.

Si può notare che ogni connessione viene aperta da una porta differente perchè tante connessioni attivate dalla stessa porta potrebbero essere sospette.

UDP senza diritti di root

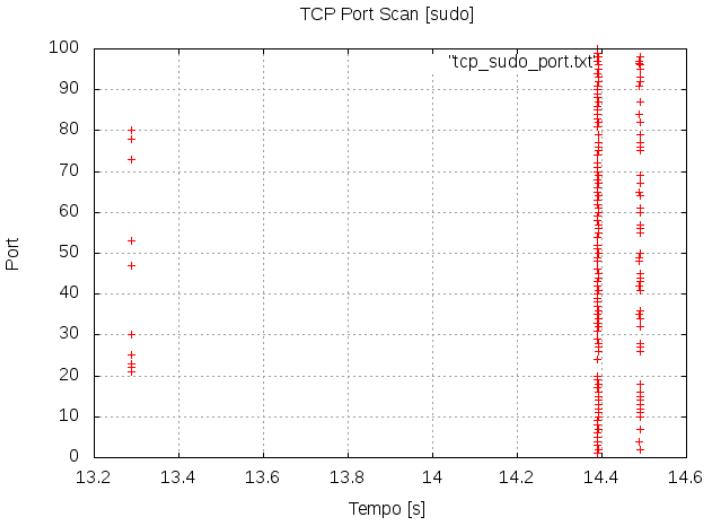
```
nmap 192.168.2.15 -p 1-100 -v -sU
```

Nmap ci avverte che per eseguire questa scan ha bisogno dei diritti di root, senza i quali non può osservare i pacchetti ICMP di ritorno.

TCP con diritti di root

```
sudo nmap 192.168.2.15 -p 1-100 -v
```

Come nel caso senza diritti di root, nmap prova una risoluzione DNS che fallisce dopo 13s.
A questo punto esegue la Port Scan.



Ogni porta viene contattata 1 o 2 volte.

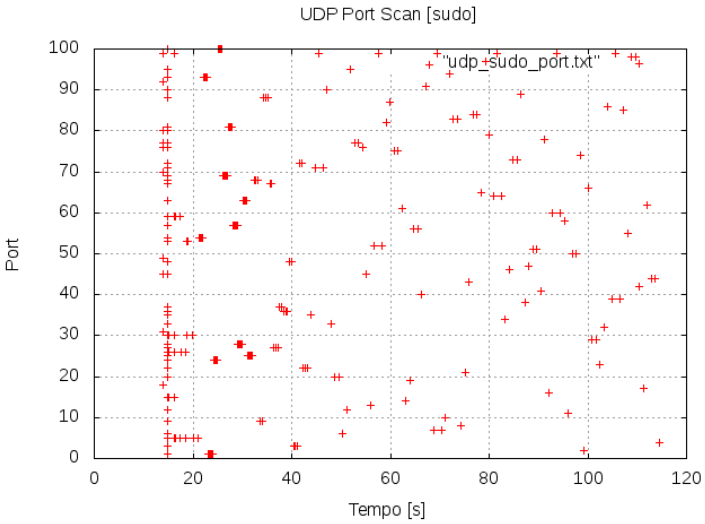
Se sulla porta non sono presenti servizi attivi, la conversazione si svolge esattamente come nel caso del TCP senza i diritti di root: un [SYN] mandato dall'host locale e un [RST, ACK] mandato dall'host target.

Invece se sulla porta vi sono servizi attivi, potendo intervenire su livelli più bassi rispetto al livello 4 del TCP, la conversazione è più breve e si compone di: [SYN], [SYN, ACK], [RST].
In questo modo la connessione non viene mai aperta, sono richiesti meno pacchetti per ottenere le informazioni e soprattutto vi sono meno probabilità che l'host target segnali la conversazione come sospetta in quanto non è mai stata aperta una connessione vera e propria. Ogni SYN viene sempre inviato dalla stessa porta.

Nmap fornisce inoltre l'indirizzo MAC dell'host target.

UDP con diritti di root

```
sudo nmap 192.168.2.15 -p 1-100 -v -sU
```



Se sulla porta sotto esame vi è un servizio attivo nmap presume che questo servizio, quando interpellato, risponda qualcosa.
Se non ottiene nessuna risposta non è possibile concludere nulla in quanto può essere andato perso il pacchetto UDP, può essere stato bloccato da un firewall, l'applicazione può aver deciso di non rispondere, è andato perso il pacchetto ICMP di risposta, ecc…

Se riceve un pacchetto ICMP Destination Unreachable (Port unreachable) allora significa che su quella porta non vi è nessuna applicazione UDP in ascolto.

Le porte vengono contattate più volte (entro un numero massimo) finché non viene ottenuta una risposta. Questa è una grande differenza rispetto alla scan effettuata tramite TCP (protocollo affidabile) rispetto ad UDP (protocollo non affidabile).
La velocità di questa scan è molto bassa in quanto l'host target invia solamente un pacchetto ICMP al secondo circa. Nmap capendo questo meccanismo rallenta l'invio dei pacchetti.

Considerazioni

Con qualsiasi protocollo si effettui la Port Scan l'ordine delle porte è casuale in quanto l'host target non deve capire di esserne bersaglio.

L'operazione effettuata tramite TCP è molto più veloce rispetto a quella effettuata tramite UDP in quanto si sfrutta la caratteristica del TCP di essere un protocollo affidabile.

Se il TCP viene utilizzato con i diritti di root si aumenta l'efficienza e soprattutto la capacità di rimanere "nascosto" di nmap.
La connessione non stabilita non viene registrata a differenza di una connessione stabilita e chiusa senza effettivo passaggio di dati.