Relazione sui Parametri di Scansione di Nmap

Nmap è uno strumento molto usato nella cybersecurity per esplorare le reti e scoprire informazioni utili su computer e dispositivi collegati. Tra i comandi principali, ci sono **-O**, **-sS**, **-sT** e **-sV**, ognuno con un compito specifico.

Il comando **-O** serve a scoprire quale sistema operativo (OS) sta usando il computer che stiamo analizzando. Per farlo, Nmap invia dei pacchetti speciali e analizza come il computer risponde. In questo modo, riesce a capire se sta usando, ad esempio, Windows o Linux. Questo comando è utile per conoscere meglio l'ambiente del sistema target e prepararsi per lavorarci o fare dei test.

Il comando **-sS**, chiamato anche SYN Scan, è uno dei metodi più usati per vedere quali porte sono aperte su un computer. Le porte sono come "porte d'ingresso" che i programmi usano per comunicare. Questo tipo di scansione è veloce e un po' "furtivo", perché non apre completamente la connessione, quindi è più difficile che venga notato. Per usarlo, però, bisogna avere i permessi di amministratore.

Un'altra opzione è il comando **-sT**, noto come TCP Connect Scan. Anche questo serve a vedere lo stato delle porte, ma in modo diverso. Qui la connessione viene completata, come se ci si collegasse davvero al servizio. Questo metodo è più facile da usare (non servono permessi speciali), ma lascia tracce più evidenti sul computer che stiamo analizzando.

Differenze tra SYN Scan e TCP Connect Scan

Caratteristica	SYN Scan (`-sS`)	TCP Connect Scan (`-sT`)
Richiede privilegi root	Sì	No
Stealth	Alta (meno rilevabile)	Bassa (più rilevabile)
Velocità	Veloce	Più lenta
Tipo di connessione	Parziale (non completa il 3-way)	Completa (stabilisce connessioni)

Un altro comando importante è **-sV**, che ci aiuta a scoprire quali servizi stanno girando su quelle porte aperte e, soprattutto, quale versione di quei servizi è in uso. Ad esempio, potremmo scoprire che su una porta è in esecuzione un server web, come Apache, e che usa una versione specifica. Questo è importante perché versioni vecchie o non aggiornate potrebbero avere problemi di sicurezza.

Se mettiamo tutto insieme, possiamo fare una scansione completa con un comando tipo:

```
nmap -O -sS -sV <IP_TARGET>
```

Questo comando ci dirà:

- Quali porte sono aperte.
- Quali servizi stanno girando su quelle porte.
- Quale sistema operativo sta usando il computer.

Nelle immagini in allegato si trovano tutti questi comandi sopra elencati, prima lanciati separatamente e poi in un unico comando come mostrato qui sopra. In questo caso per l'esercitazione è stata utilizzata una metasploitable impostata su connessione statica con IP:192.168.50.102; netmask:255.255.255.0; gateway:192.168.50.1. Quanto dimostrato si potrebbe fare anche settando in connessione statica(nella stessa stanza) un qualsiasi dispositivo con sistema operativo windows. In sintesi, questi comandi di Nmap sono molto utili per imparare a conoscere una rete o un computer.