Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable**:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

Configurazione ambiente di Test per Sicurezza Informatica

L'infrastruttura di test è costituita da tre segmenti di rete isolati, ciascuno con uno specifico ruolo nell'ecosistema di sicurezza:

1. **Rete Offensive (HOST)**
    - Sistema operativo: Kali Linux
    - Dedicata all'esecuzione di attività di penetration testing e security assessment
    - Strumenti specializzati per l'analisi delle vulnerabilità
2. **Rete Server (Target Primario)**
    - Sistema operativo: Metasploitable
    - Server volutamente vulnerabile per simulazioni di attacco
    - Predisposta con molteplici superfici di attacco
3. **Rete Client (Target Secondario)**
    - Sistema operativo: Windows 10
    - Ambiente desktop standard rappresentativo di una postazione utente aziendale
    - Macchina virtuale configurata come workstation tipica
4. **Pfsense (Router Modem)**
    - Macchina virtuale con pfSense
    - Gestisce il routing tra le diverse reti

La piattaforma di test è strutturata con tre segmenti di rete distinti.

Rete Host - Rete Offensive

- **Indirizzo IP**: 192.168.50.150
- **Subnet Mask**: 255.255.255.0
- **Gateway**: 192.168.50.1
- **Range di rete**: 192.168.50.0/24

Target Primario - Rete Server

- **Indirizzo IP**: 192.168.60.40
- **Subnet Mask**: 255.255.255.0
- **Gateway**: 192.168.60.1
- **Range di rete**: 192.168.60.0/24

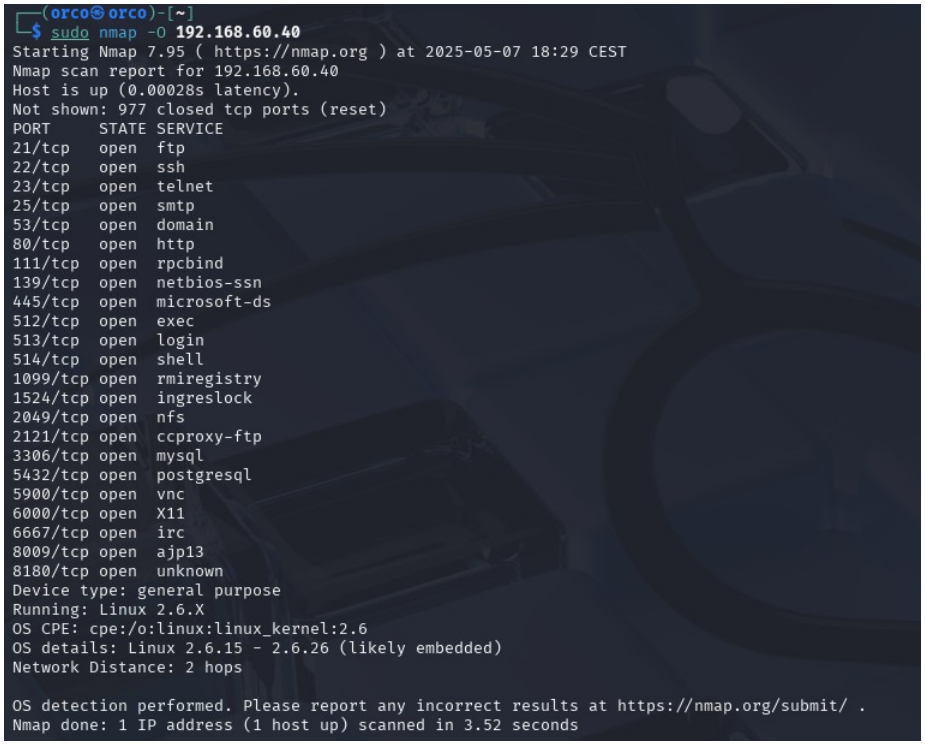
Target Secondario - Rete Client

- **Indirizzo IP**: 192.168.70.34
- **Subnet Mask**: 255.255.255.0
- **Gateway**: 192.168.70.1
- **Range di rete**: 192.168.70.0/24

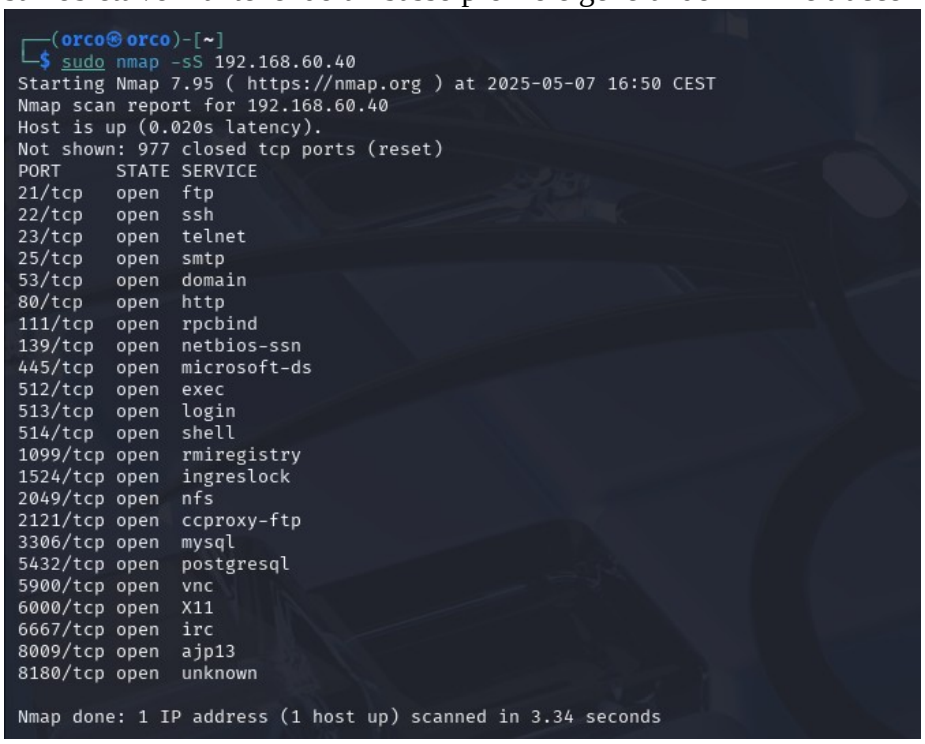
tutte gestite e configurate attraverso la PfSense

scansioni sul target **Metasploitable** (**Target Primario**)

Il comando “`sudo nmap -O 192.168.60.40`” esegue una scansione privilegiata sul sistema target (**Target Primario**) per rilevarne il sistema operativo. L'analisi delle “impronte digitali” TCP/IP permette di identificare con precisione il sistema operativo in uso, informazione fondamentale durante la fase di ricognizione di un penetration test per sviluppare strategie d'attacco mirate e specifiche.



Il comando “`sudo nmap -sS 192.168.60.40`” esegue una scansione di tipo "half-open" sul sistema target (**Target Primario**). Questa tecnica privilegiata invia pacchetti SYN senza completare l'handshake TCP, rendendola meno rilevabile dai sistemi di sicurezza. Particolarmente efficace nella fase di discovery di un penetration test, permette di identificare le porte aperte e i servizi disponibili sull'obiettivo mantenendo un basso profilo e generando minime tracce nei log di sistema.



Il comando "`sudo nmap -sT 192.168.60.40`" esegue una scansione che completa l'intero handshake TCP a tre vie con il target (**Target Primario**). Questa metodologia offre risultati altamente affidabili simulando connessioni client legittime e funziona anche senza privilegi root. Sebbene più facilmente rilevabile dai sistemi di monitoraggio rispetto ad altre tecniche, è particolarmente efficace per verificare l'effettiva disponibilità dei servizi attraverso dispositivi di sicurezza complessi come firewall stateful.

```
┌──(orco㉿orco)-[~]
└─$ sudo nmap -sT 192.168.60.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-07 16:51 CEST
Nmap scan report for 192.168.60.40
Host is up (0.020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
```

Il comando "`sudo nmap -sV 192.168.60.40`" esegue una scansione approfondita che identifica non solo le porte aperte, ma anche le specifiche versioni dei servizi in esecuzione sul target (**Target Primario**). Operando con privilegi amministrativi, NMAP invia probe specializzati che stimolano risposte contenenti informazioni identificative come banner e comportamenti distintivi dei software. Questa intelligence è fondamentale durante un security assessment, poiché la conoscenza precisa delle versioni consente di individuare vulnerabilità specifiche, rendendo possibile un'exploitation mirata ed efficace.

```
┌──(orco㉿orco)-[~]
└─$ sudo nmap -sV 192.168.60.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-07 16:52 CEST
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 16:53 (0:00:00 remaining)
Nmap scan report for 192.168.60.40
Host is up (0.00s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.34 seconds
```

Principali differenze tra `sudo nmap -sS` e `sudo nmap -sT`

1. **Completamento della connessione**
   - `-sS`: Esegue una "half-open scan" che invia solo pacchetti SYN senza completare l'handshake TCP
   - `-sT`: Completa l'intero handshake TCP a tre vie (SYN, SYN/ACK, ACK)
2. **Visibilità e rilevabilità**
   - `-sS`: Meno rilevabile dai sistemi di monitoraggio e genera meno log sui sistemi target
   - `-sT`: Più facilmente rilevabile poiché genera connessioni complete registrate nei log di sistema
3. **Requisiti di privilegi**
   - `-sS`: Richiede obbligatoriamente privilegi root/amministrativi per manipolare pacchetti raw
   - `-sT`: Può essere eseguito anche senza privilegi elevati (anche se nel comando fornito viene usato sudo)
4. **Efficacia con firewall e IDS**
   - `-sS`: Spesso può eludere firewall di base e sistemi IDS meno sofisticati
   - `-sT`: Più difficilmente aggira sistemi di protezione ma offre risultati più affidabili con firewall stateful
5. **Velocità di esecuzione**
   - `-sS`: Generalmente più veloce perché non completa le connessioni
   - `-sT`: Relativamente più lento dovendo completare l'intero handshake per ogni porta
6. **Accuratezza dei risultati**
   - `-sS`: Può generare occasionalmente falsi positivi con alcuni tipi di filtri di rete
   - `-sT`: Fornisce risultati più affidabili confermando l'effettiva capacità di stabilire connessioni

scansioni sul target **Windows 10** (**Target Secondario**)

Come per il comando sulla (**Metasploitable)** qui il comando “`sudo nmap -O 192.168.70.34`” esegue una scansione privilegiata sul sistema target (**Target Secondario**) per rilevarne il sistema operativo.