Scansione con NMAP della macchina Meta

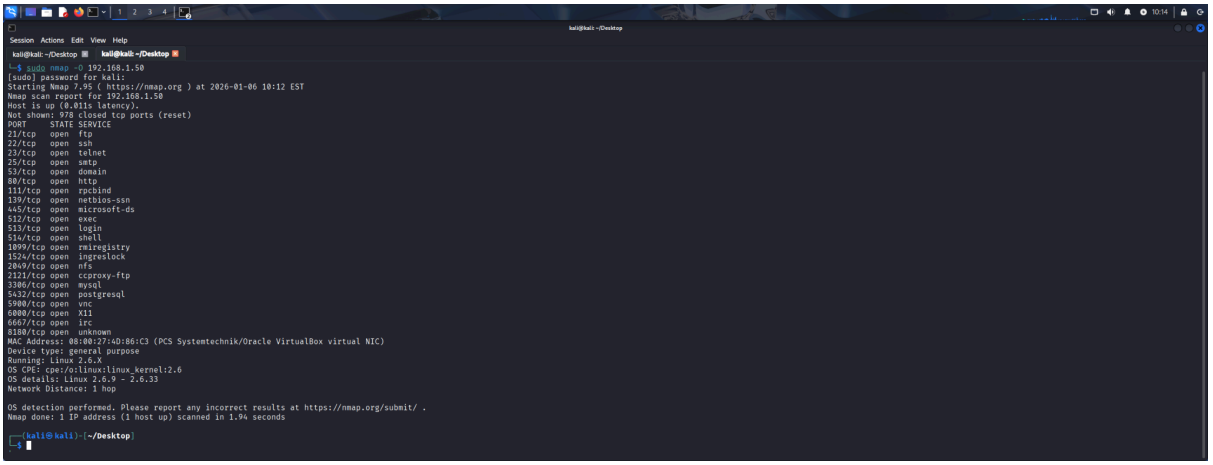
IP Meta:192.168.20.2

```
No mail.
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4d:86:c3
          inet addr:192.168.20.2  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4d:86c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4382 (4.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22873 (22.3 KB)  TX bytes:22873 (22.3 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

<u>Scansione per capire quale sistema operativo utilizza Meta</u>



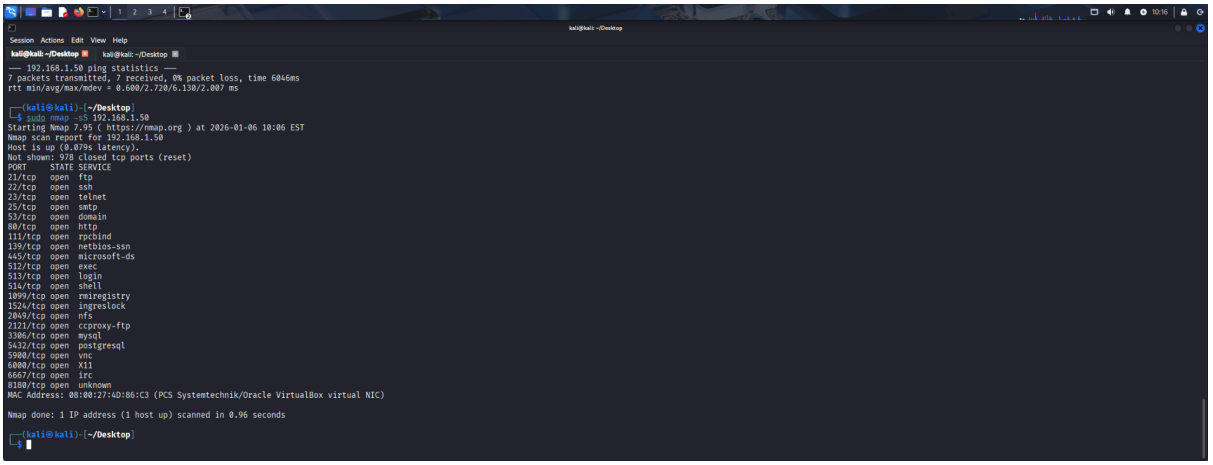
Per capire quale OS utilizza Meta usiamo nmap con il flag -O. Come si può evidenziare dallo screen il sistema operativo che usa Meta è Linux 2.6.9 - 2.6.33.

Ora vogliamo effettuare una scansione Syn Scan. Questo tipo di scansione ci permette di individuare porte aperte senza stabilire una connessione TCP completa, cioè non completa il three-way-handshake. E una scansione che fa meno rumore perchè:

- Non completa la connessione
- Non crea una sessione applicativa
- Molti servizi non registrano la connessione nei log applicativi
- Rimane rilevabile da firewall e sistemi IDS/IPS

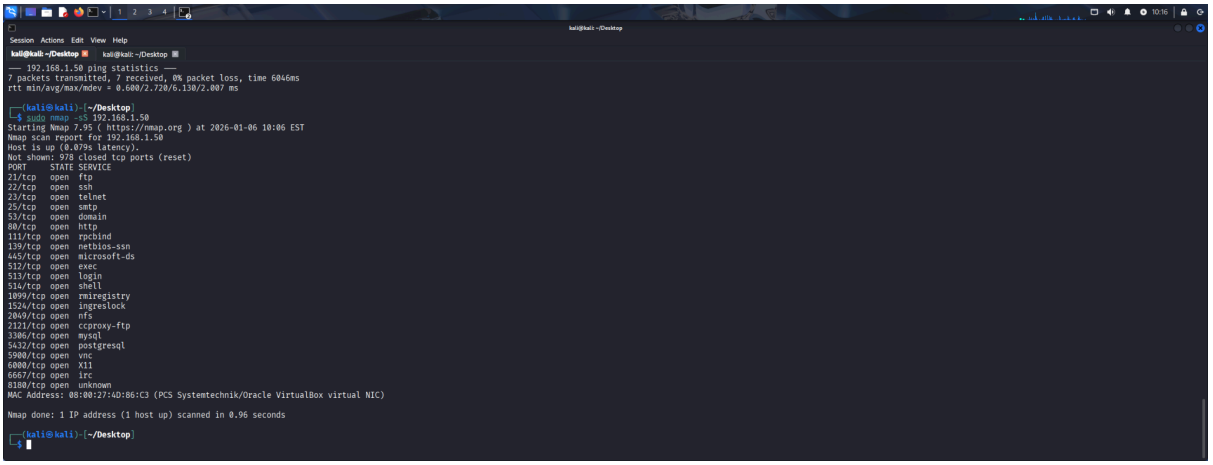
Requisiti richiesti:

- Richiede privilegi di root
- Usa pacchetti TCP raw
- E' più veloce e più "stealth" di -sT



Ora effettuiamo una scansione Nmap con il flag -sT, detta TCP Connect Scan.
Questa tipologia di scansione utilizza la chiamata di sistema connect() per stabilire una connessione TCP completa con il target, completando il three-way handshake (SYN, SYN-ACK, ACK).

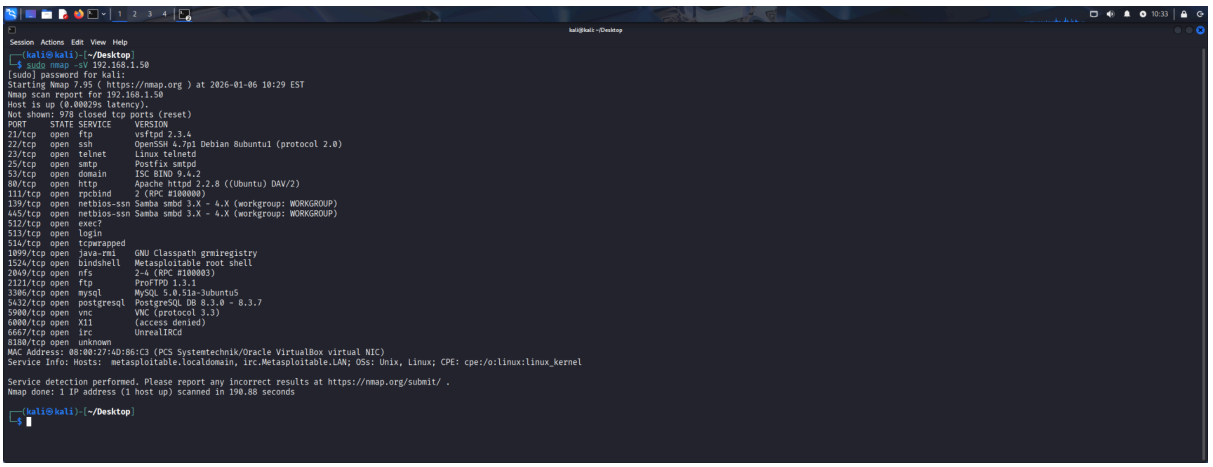
La scansione -sT consente di individuare le porte TCP aperte, chiuse o filtrate ed è la modalità utilizzata da Nmap quando non sono disponibili privilegi di root.
A differenza della SYN Scan (-sS), la TCP Connect Scan genera una connessione reale verso il servizio remoto, risultando più rumorosa e generalmente registrata nei log applicativi del sistema target.



Considerazioni di sicurezza

La TCP Connect Scan è meno stealth rispetto alla SYN Scan, ma garantisce maggiore affidabilità nei risultati, in quanto utilizza il normale stack TCP del sistema operativo.
Per questo motivo viene spesso utilizzata in contesti di test autorizzati e di analisi preliminare della superficie di attacco.

Ora facciamo una Version Detection utilizzando il flag -sV per capire quali servizi sono in ascolto sulle porte, individuare la versione software.
E’ importante perchè permette di correlare i servizi a vulnerabilità note.

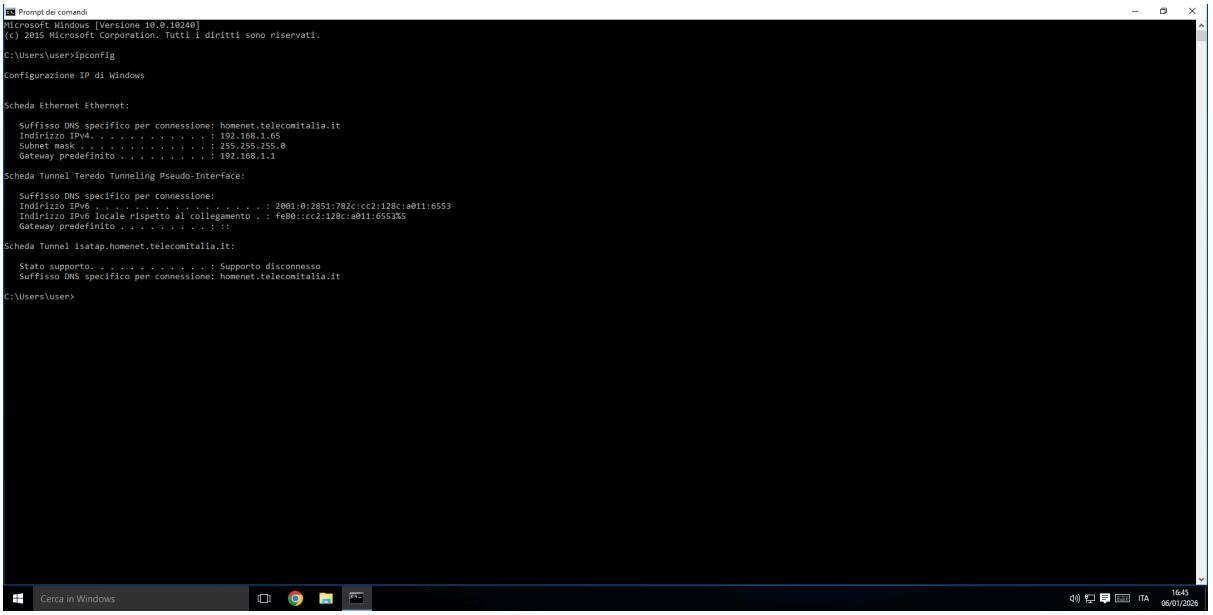


La scansione -sV interagisce attivamente con i servizi individuati, inviando specifiche sonde applicative per ottenere informazioni dettagliate come il nome del servizio, la versione del software e, in alcuni casi, il sistema operativo o il banner del servizio.
La Version Detection ha ampliato l’analisi della superficie di attacco, permettendo di passare dalla semplice individuazione delle porte aperte all’identificazione puntuale dei servizi e delle versioni installate.

Considerazioni di sicurezza

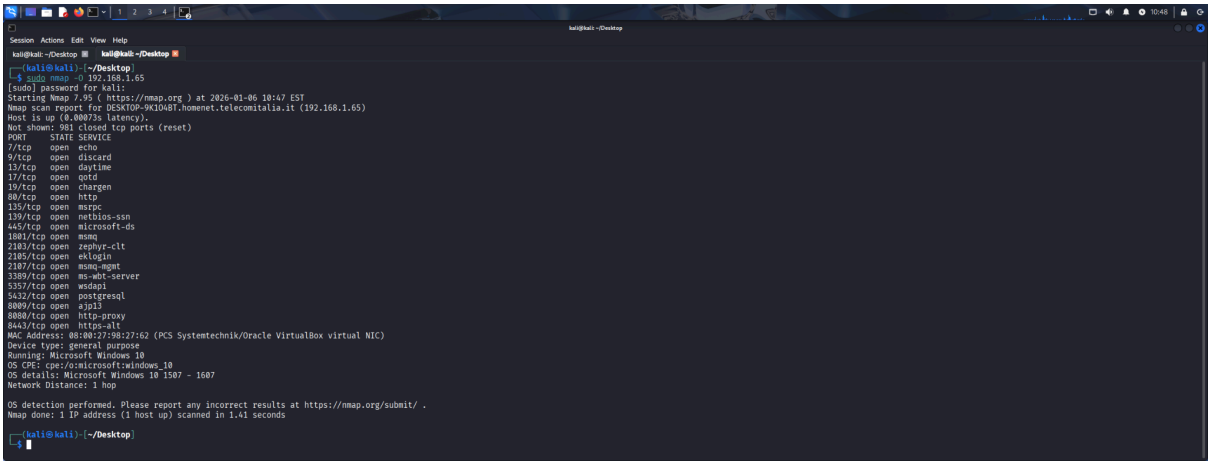
L’identificazione delle versioni dei servizi rappresenta un passaggio critico per un attaccante, in quanto consente di associare i software rilevati a vulnerabilità pubbliche note (CVE). Tuttavia, trattandosi di una scansione più invasiva rispetto a una semplice port scan, può essere rilevata e registrata nei log del sistema target.

Scansione con NMAP della macchina Windows



IP Windows 192.168.1.65

Scansione per capire quale sistema operativo utilizza Windows



Per capire quale sistema operativo utilizza questa macchina windows abbiamo utilizzato il flag -O.
Come si può osservare dallo screen il sistema operativo che utilizza windows è windows_10.