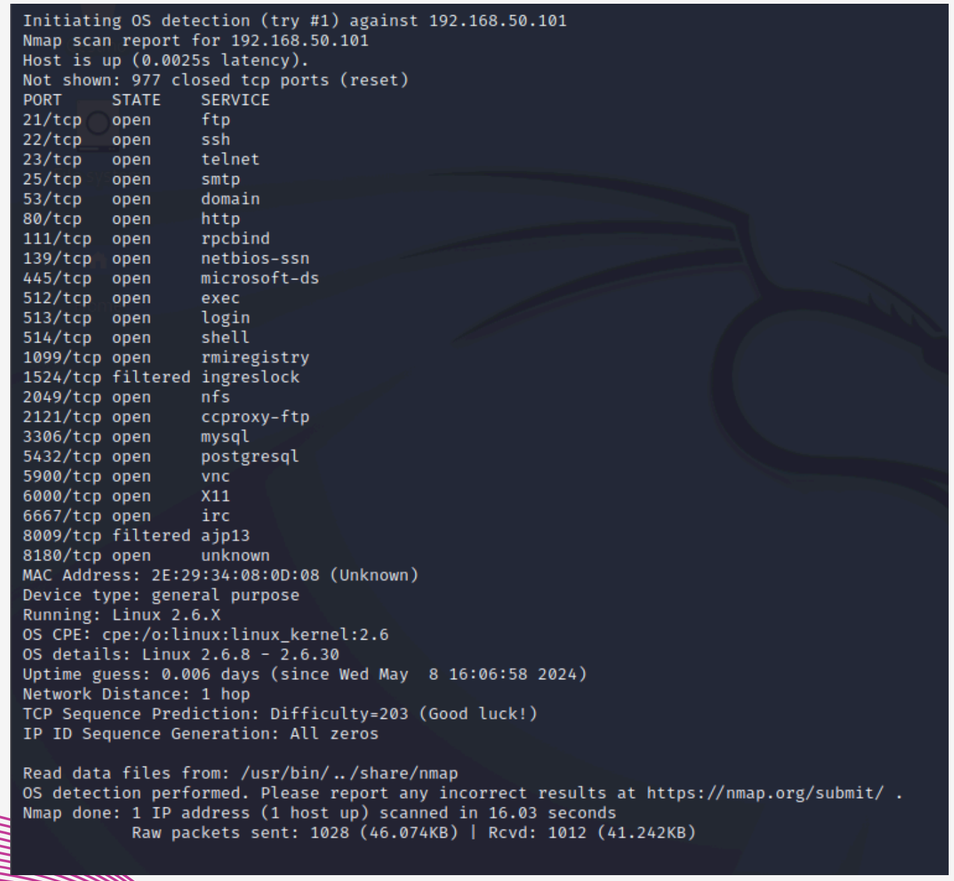
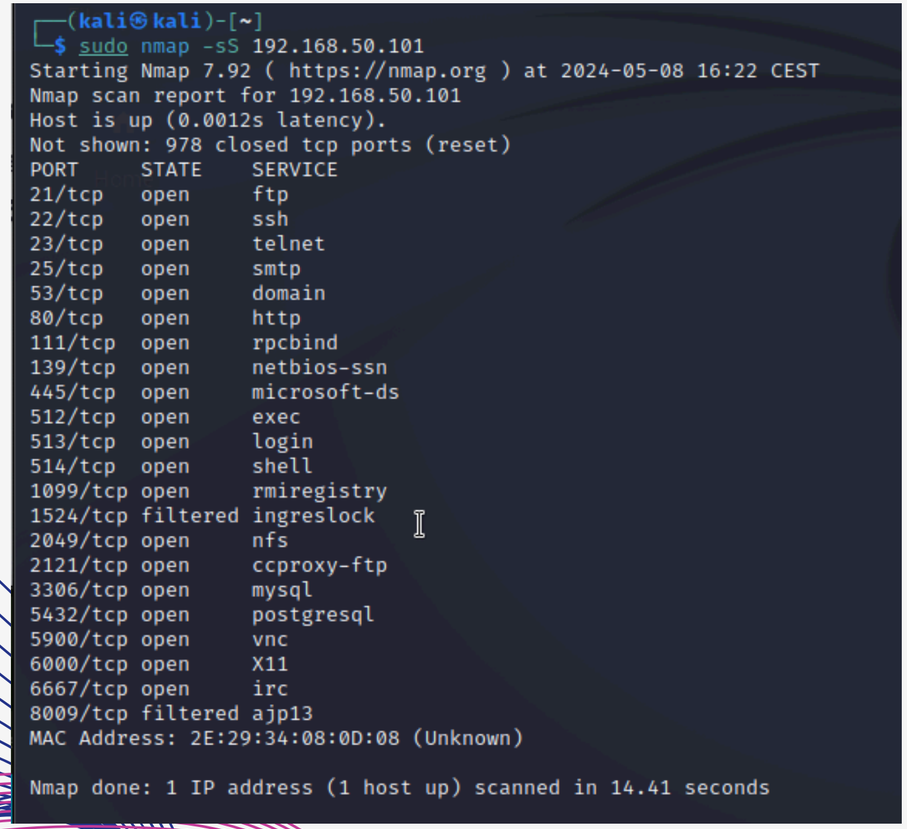
Scansione dei servizi con Nmap



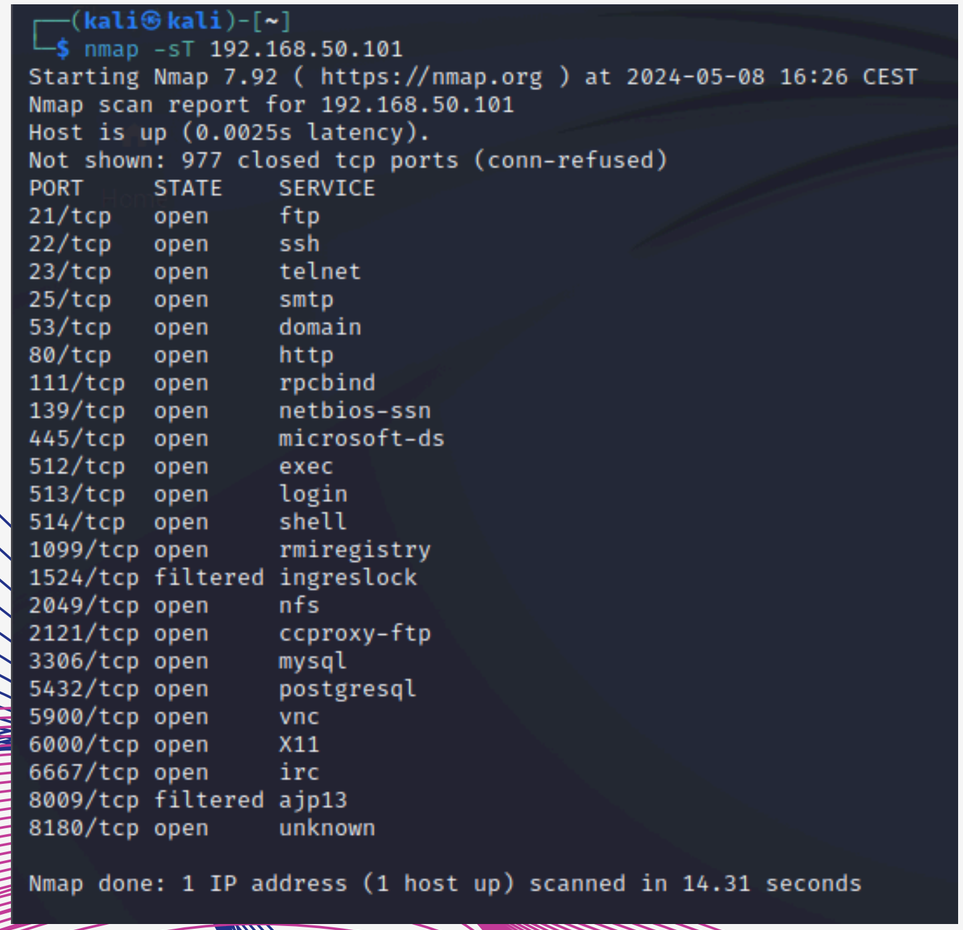
sudo nmap -O

identificare da remoto il sistema operativo di un host attraverso il fingerprint dello stack TCP/IP. Nmap invia una serie di pacchetti TCP ed UDP all'host remoto ed esamina ogni bit ricevuto in risposta.



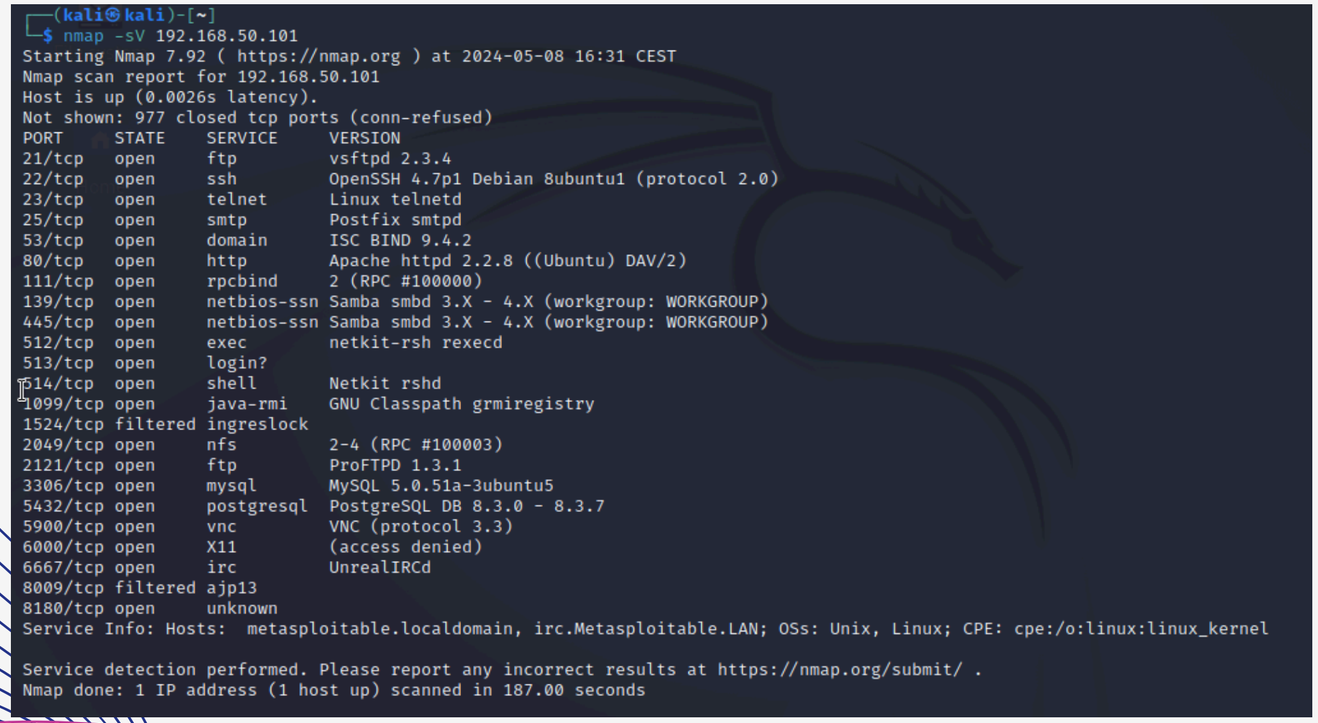
sudo nmap -sS

con l'opzione -sS, si sta specificando di eseguire una "scansione SYN". Questo tipo di scansione invia pacchetti SYN (iniziali) ai porti di destinazione e ascolta le risposte. Se viene ricevuta una risposta SYN/ACK, il porto è considerato aperto, se viene ricevuta una risposta RST, il porto è considerato chiuso.



sudo nmap -sT

L'opzione -sT in nmap specifica una "scansione TCP connect", che è una tecnica di scansione più tradizionale e meno furtiva rispetto alla scansione SYN. In questa modalità, nmap tenta di stabilire una connessione TCP completa con il target sui porti specificati. Se la connessione ha successo, il porto viene considerato aperto, altrimenti viene considerato chiuso



sudo nmap -sV

L'opzione -sV in nmap indica di eseguire una "scansione di versione". Questo tipo di scansione va oltre la semplice identificazione delle porte aperte, cercando di determinare anche le versioni dei servizi che rispondono su tali porte.
Quando si esegue sudo nmap -sV, nmap cercherà di determinare non solo lo stato delle porte (aperte o chiuse) tramite la scansione TCP, ma anche di identificare quali servizi sono in esecuzione su tali porte e, se possibile, determinare la versione di tali servizi. Questo è utile per capire quali software specifici stanno girando su una determinata macchina, il che può aiutare a valutare la sicurezza della rete e individuare potenziali vulnerabilità.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.103
[sudo] password di kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-08 16:37 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0054s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 7E:03:BE:74:74:34 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.70 seconds
```

sudo nmap -sV

L'opzione -O in nmap indica di eseguire il rilevamento del sistema operativo. Quando si utilizza questa opzione, nmap cercherà di determinare il sistema operativo del target in base alle risposte ottenute durante la scansione. Questo comando esegue una scansione del target specificato e cerca di identificare il sistema operativo del target basandosi su caratteristiche di risposta specifiche durante la scansione.