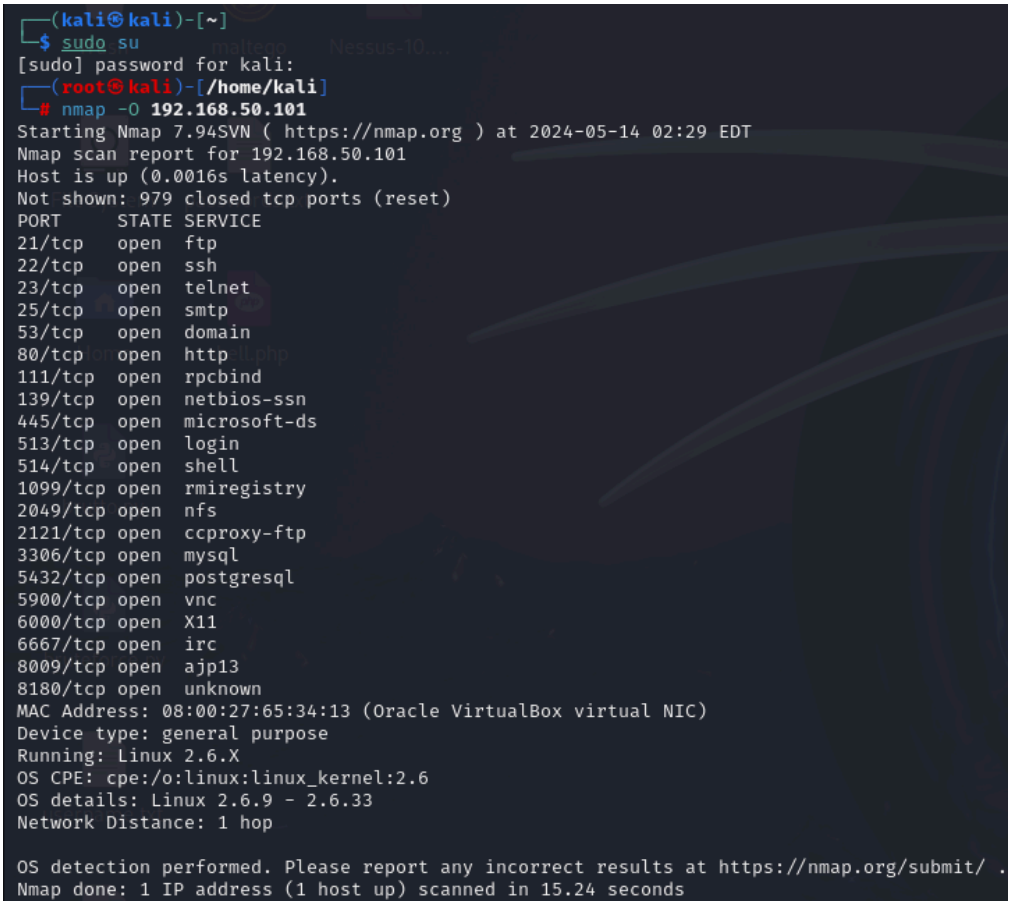
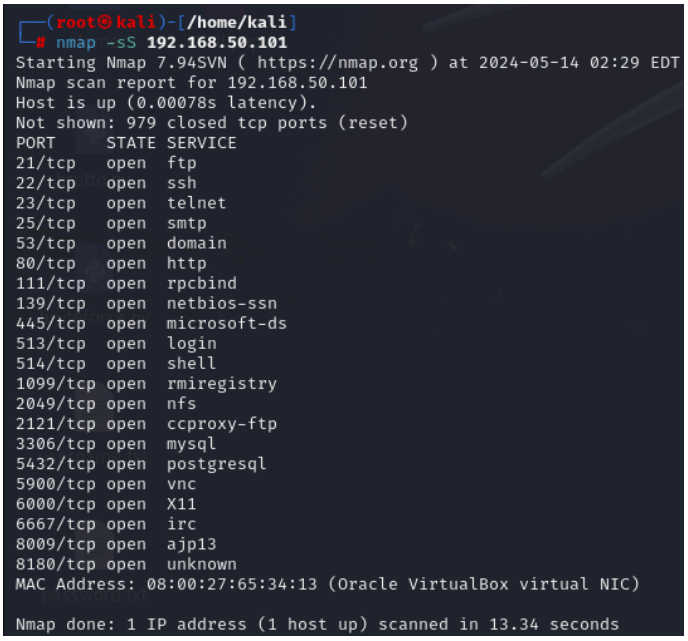
S5.L3 Mapping di rete/Nmap

OS fingerprint:



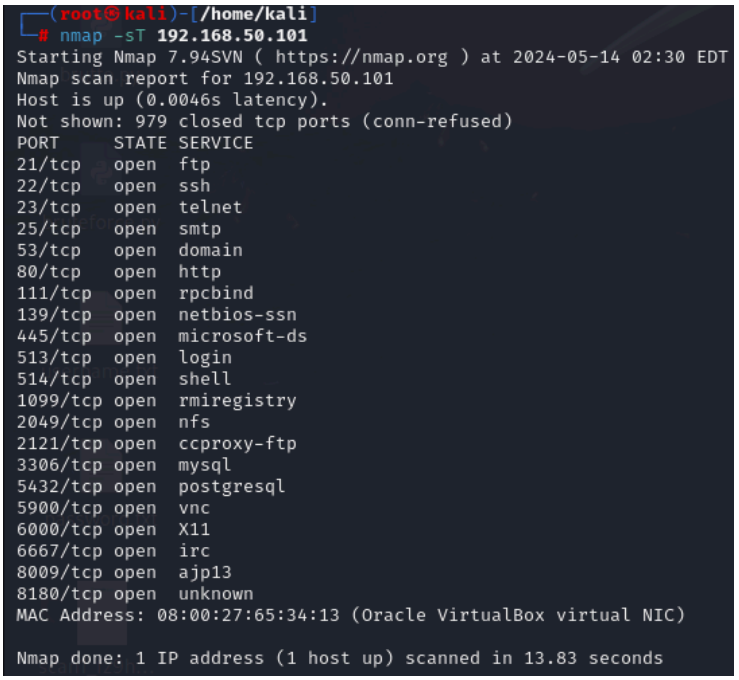
La scansione con l'opzione -O di Nmap, mostrata nell'immagine, ha permesso di identificare il sistema operativo della macchina con IP 192.168.50.101. Questo processo, noto come OS fingerprinting, ha rilevato che il sistema operativo è una versione del kernel Linux tra 2.6.9 e 2.6.33. Questa informazione è utile per determinare potenziali vulnerabilità e configurazioni specifiche del sistema target.

SYN scan:



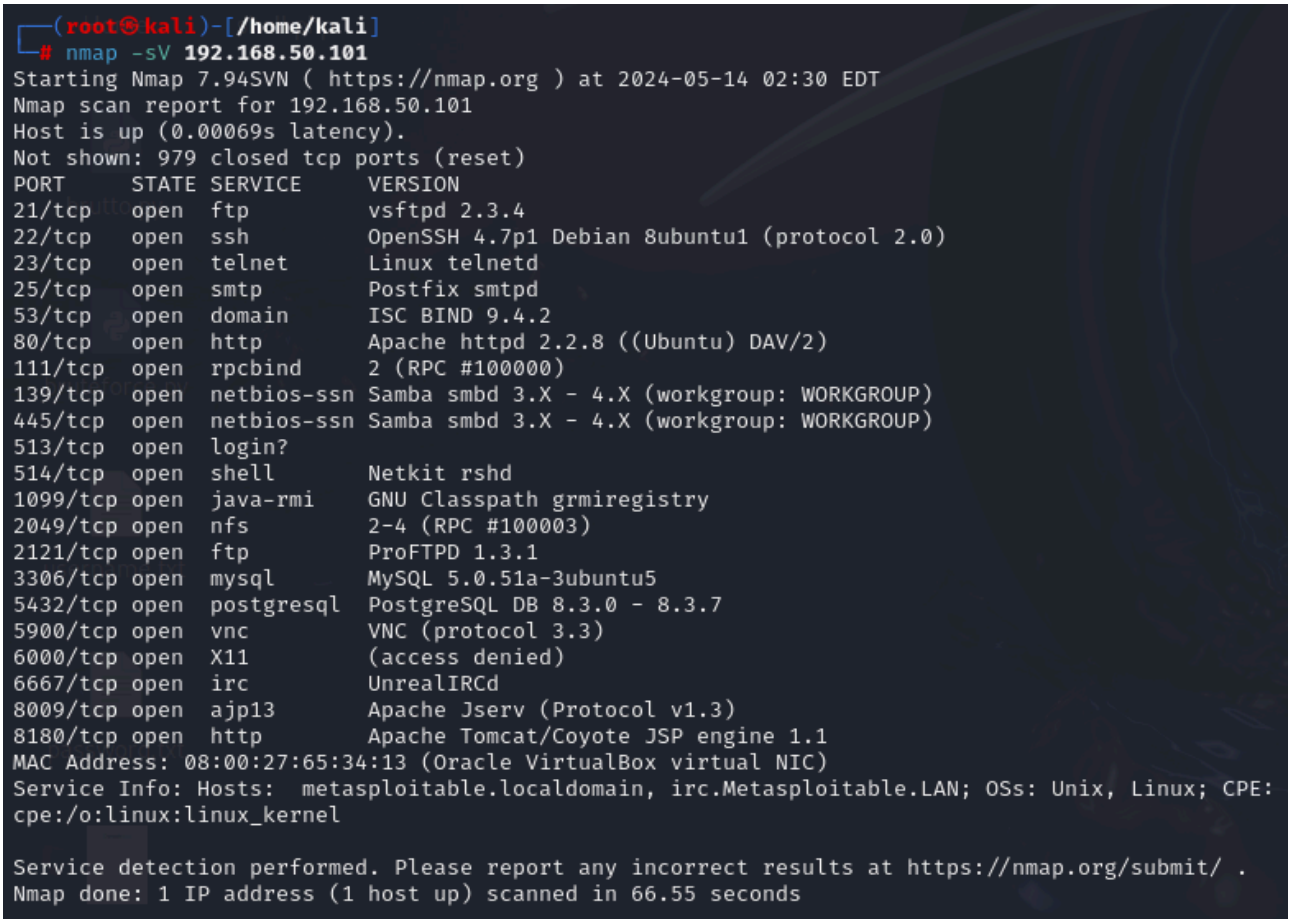
L'opzione -sS utilizzata con Nmap nell'immagine carica ha eseguito una scansione di tipo SYN, che è una delle tecniche più comuni e veloci per identificare le porte aperte su un host di rete. Questa tecnica specifica manda un pacchetto SYN (che inizia una connessione TCP) a diverse porte dell'host target. Se una porta è aperta, l'host risponde con un pacchetto SYN-ACK, altrimenti risponde con un RST per le porte chiuse.
La scansione ha rilevato diverse porte aperte offrendo servizi come FTP, SSH, Telnet, SMTP, e molti altri, indicando i vari servizi che sono attivi e ascoltano su quelle porte. Questo tipo di scansione è fondamentale per la valutazione della sicurezza, permettendo di capire quali servizi sono esposti su una rete e potenzialmente vulnerabili agli attacchi.

TCP Connect



L'opzione -sT utilizzata in Nmap per la scansione mostrata nell'immagine esegue una scansione TCP connect. A differenza della scansione SYN, la scansione TCP connect utilizza il metodo completo di connessione TCP, il che significa che Nmap completa la connessione TCP a tre vie con il host di destinazione per ogni porta scansionata. Se una porta è aperta, il sistema risponde con un SYN-ACK, seguito da un ACK da parte di Nmap, completando la connessione.
Questa tecnica è meno discreta e può essere più facilmente rilevata dai sistemi di rilevamento intrusioni, ma non richiede privilegi di amministratore per essere eseguita. La scansione ha rilevato diverse porte aperte offrendo servizi come FTP, SSH, Telnet, e altri, mostrando quali servizi sono attivi e in ascolto sulle porte del sistema target. Questo tipo di scansione aiuta nella valutazione della sicurezza, rivelando quali porte sono aperte e potenzialmente vulnerabili su un host.

Version Detection:



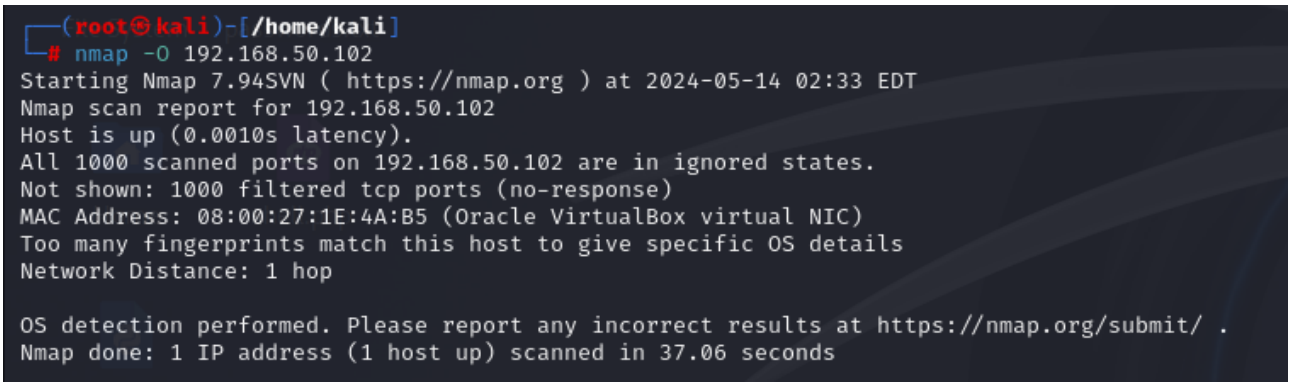
L'opzione -sV utilizzata in Nmap, come mostrato nell'immagine, serve per eseguire una scansione che determina le versioni dei servizi in esecuzione sulle porte aperte di un host. Questo tipo di scansione è molto utile per identificare specifiche versioni di software in esecuzione, che possono essere confrontate con database di vulnerabilità per scoprire potenziali punti deboli di sicurezza.
L'immagine mostra che la scansione ha identificato varie versioni di software come:

- FTP usando vsftpd 2.3.4
- SSH su OpenSSH 4.7p1
- Telnet attraverso telnetd
- SMTP con Postfix

- HTTP con Apache httpd 2.2.8 su Ubuntu
- Samba per condivisione file su NetBIOS
- MySQL versione 5.0.51a-3ubuntu5
- PostgreSQL DB 8.3.0 - 8.3.7
- Apache Tomcat su 8180/tcp

Queste informazioni sono fondamentali per un'amministrazione di sistema sicura e per attività di penetration testing, poiché permettono agli amministratori di sapere esattamente quali versioni di servizi sono in esecuzione e se esistono patch o aggiornamenti necessari per mitigare rischi di sicurezza noti.

OS Fingerprint di windows7 con firewall attivo:

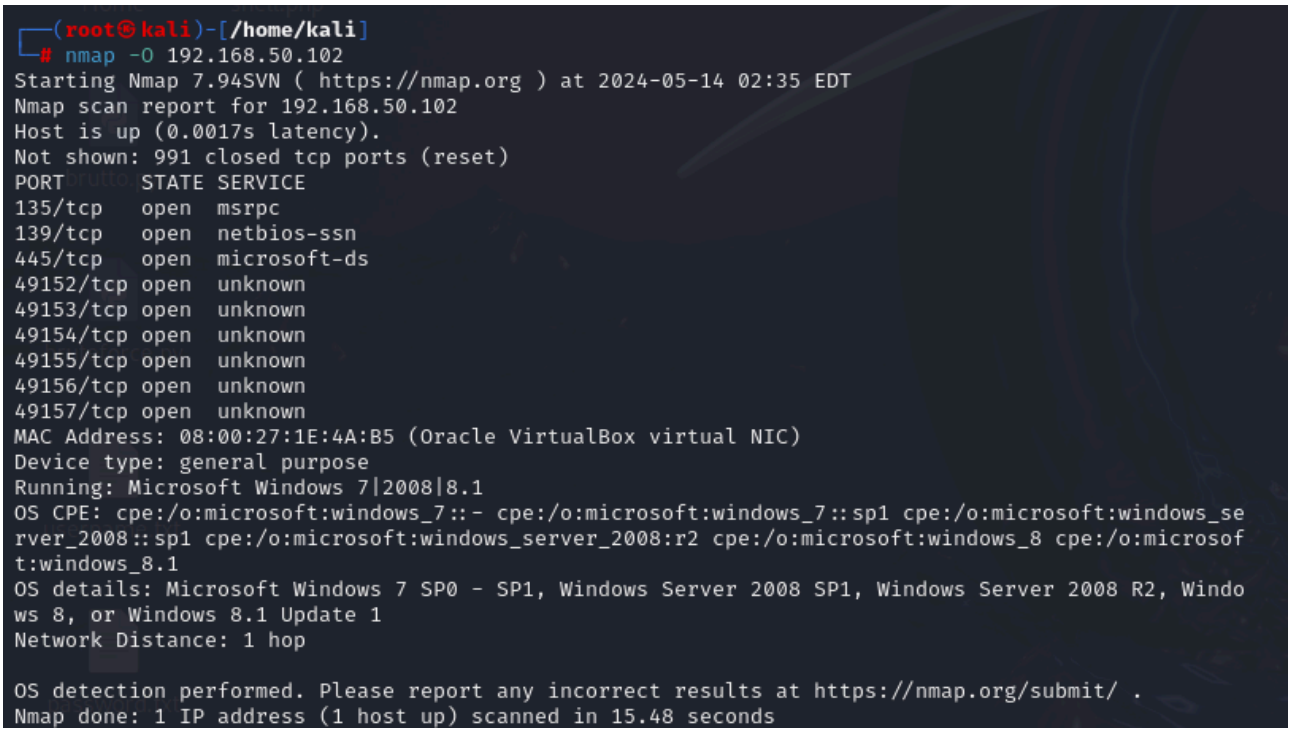


La scansione Nmap mostrata nell'immagine è stata eseguita con l'intento di identificare il sistema operativo di un host con IP 192.168.50.102. Tuttavia, il risultato dell'OS fingerprinting non è stato definitivo a causa dell'attivazione del firewall sulla macchina Windows 7 target.
Dettagli rilevanti:

- Tutte le 1000 porte TCP scansionate sono in stato ignorato perché non hanno risposto, indicando che il firewall potrebbe aver bloccato le richieste di Nmap.
- MAC Address: 08:00:27:1E:4A:B5, che appartiene a una scheda di rete virtuale Oracle VirtualBox.
- Risultato del fingerprinting: Non è stato possibile ottenere dettagli specifici sull'OS a causa di troppe corrispondenze nel database di Nmap, molto probabilmente influenzato dalla non risposta delle porte a causa del firewall.

Questa situazione dimostra come un firewall attivo possa efficacemente ostacolare tentativi di identificazione remota del sistema operativo tramite tecniche come quelle impiegate da Nmap, aumentando la sicurezza del sistema contro attività di scansione non autorizzate.

OS Fingerprint di windows7 con il firewall disattivato:



La scansione Nmap mostrata nell'immagine ha rilevato con successo informazioni dettagliate sul sistema operativo della macchina con IP 192.168.50.102, grazie alla disattivazione del firewall. Con il firewall disattivato, Nmap è stato in grado di identificare che l'host sta eseguendo una versione di Windows compatibile con Windows 7 SP0 o SP1, Windows Server 2008 SP1, o Windows Server 2008 R2, o Windows 8, o Windows 8.1 Update 1.
Differenze chiave rispetto alla scansione precedente con il firewall attivo:

1. Porte rilevate aperte: A differenza della precedente scansione, dove tutte le porte erano ignorate a causa del firewall che bloccava le richieste, questa volta Nmap ha potuto identificare diverse porte aperte come NetBIOS, Microsoft-DS, e alcune porte sconosciute.
2. Precisione nel rilevamento: Senza il firewall, Nmap ha potuto effettuare una scansione più accurata, risultando in un rilevamento più preciso del sistema operativo.

Questo dimostra come un firewall possa efficacemente proteggere una macchina impedendo il rilevamento delle porte e delle versioni di servizio, riducendo così la superficie di attacco visibile agli attaccanti. Disattivare il firewall, d'altra parte, espone più informazioni che possono essere utilizzate per identificare vulnerabilità specifiche del sistema.