Report Scansioni con Nmap su Metasploitable e Windows

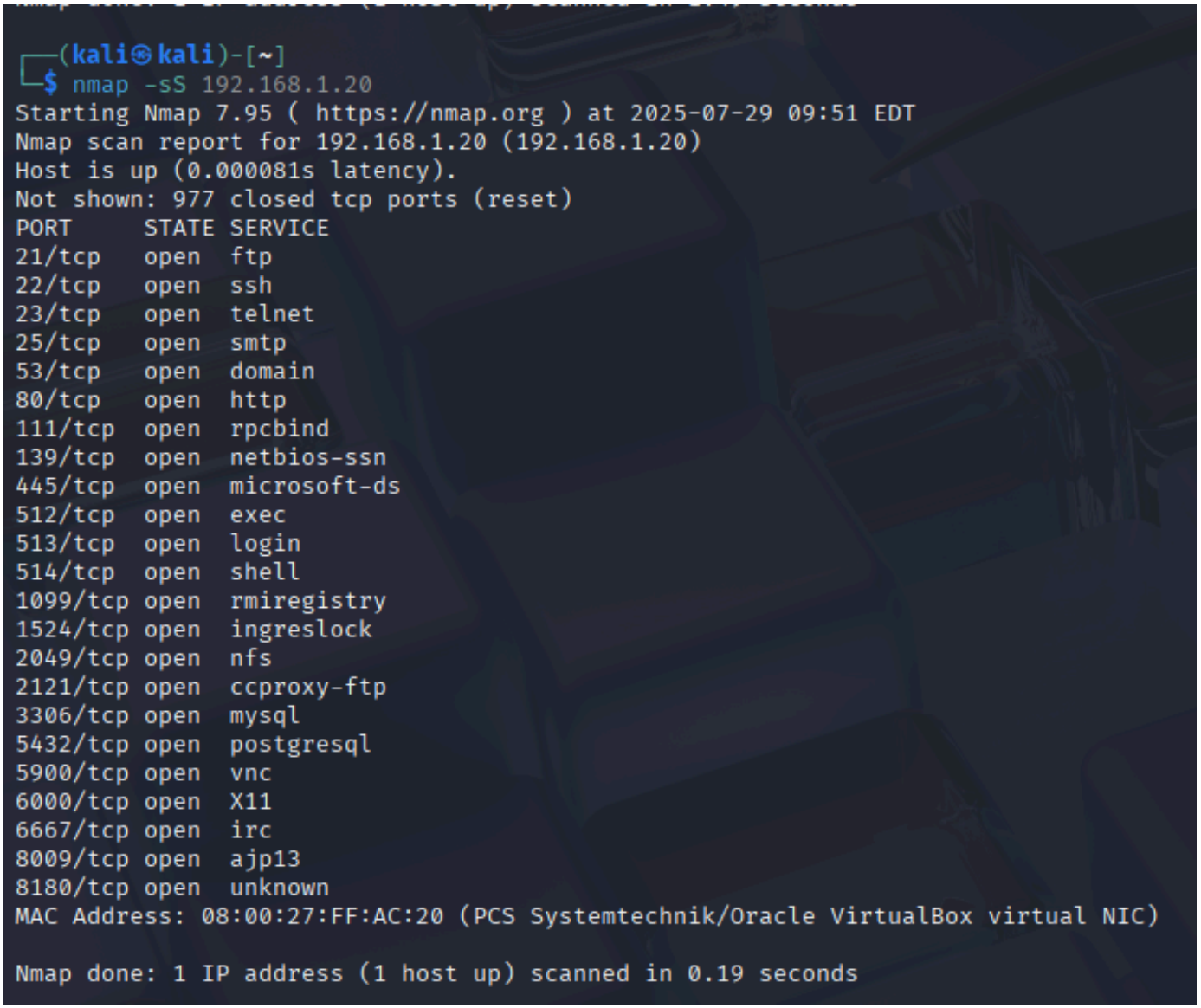
Scansione su Metasploitable

OS fingerprint:

L'OS fingerprint tamite nmap è una tecnica utilizzata per identificare il sistema operativo in esecuzione su un dispositivo remoto. Questa tecnica è utile per scopi di sicurezza, come l'individuazione di vulnerabilità. In questo caso, conoscendo l'indirizzo IP della metasploitable (192.168.1.20) siamo riusciti a risalire al suo sistema operativo da kali utilizzando il comando **nmap -O** (Linux 2.6.x tra la versione .9 e .33) vedi lo screenshot qui sotto:

SYN Scan (Stealth Scan):

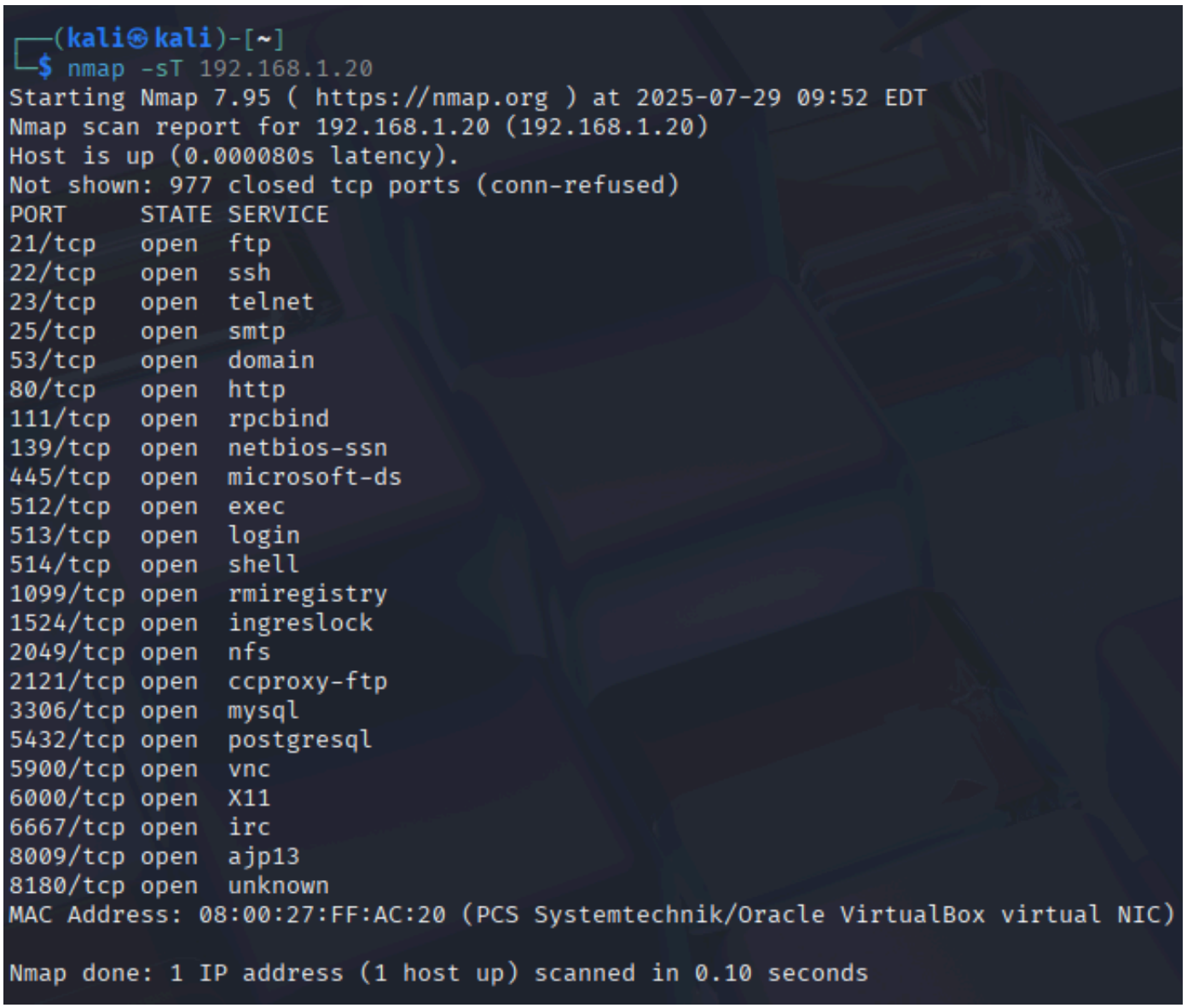
Lo SYN scan è una tecnica di scansione delle porte di rete che permette di determinare quali porte di un sistema sono aperte senza stabilire una connessione completa. In pratica, il client invia un pacchetto SYN al server, aspettandosi una risposta SYN-ACK (se la porta è aperta). A questo punto, invece di completare l'handshake TCP con un pacchetto ACK, invia un pacchetto RST (reset) per chiudere la connessione. Per questa scansione abbiamo utilizzato il comando **nmap -sS**. Andiamo a vedere nello screenshot qui sotto quali porta sono risultate aperte:



TCP Connect Scan:

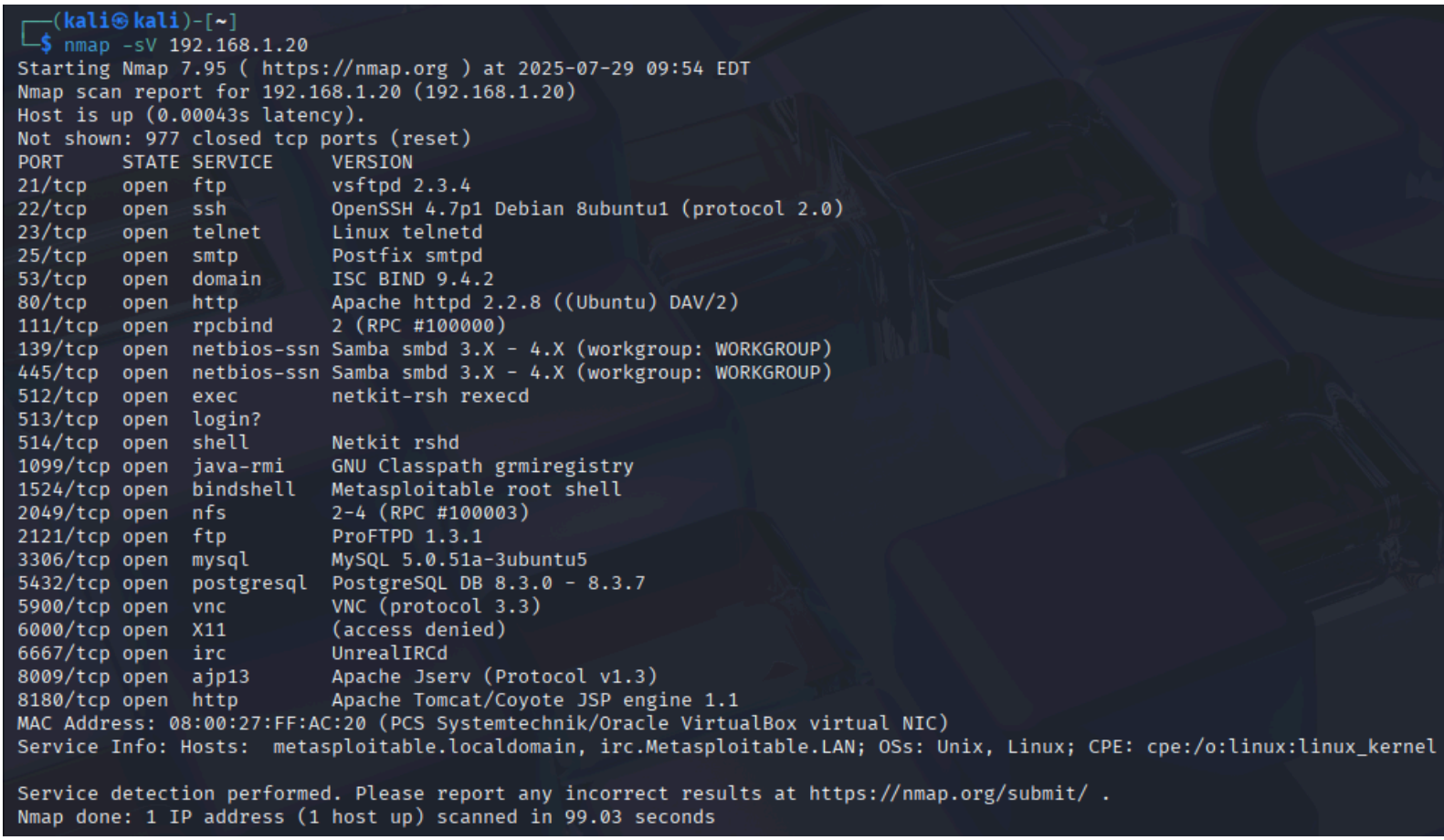
Il TCP Connect Scan è una tecnica di scansione delle porte che, a differenza dello SYN Scan, tenta di stabilire una connessione TCP completa con ogni porta target (quindi completa l'handshake SYN, SYN-ACK-, ACK senza chiudere la connessione in anticipo). Abbiamo utilizzato il comando **nmap -sT** per questa operazione. Come si può notare dagli screenshot non c'è nessuna differenza tra questa scansione e quella effettuata con il comando nmap -sS se non una leggera maggiore velocità di questa scansione con TCP Connect scan, fatto strano ma possibile quando si fanno queste operazioni su una singola macchina (Il SYN Scan dovrebbe essere più veloce e sprecare meno

risorse di rete in quanto fa un passaggio in meno). Qui sotto lo screen con il risultato della scansione:



Version Detection:

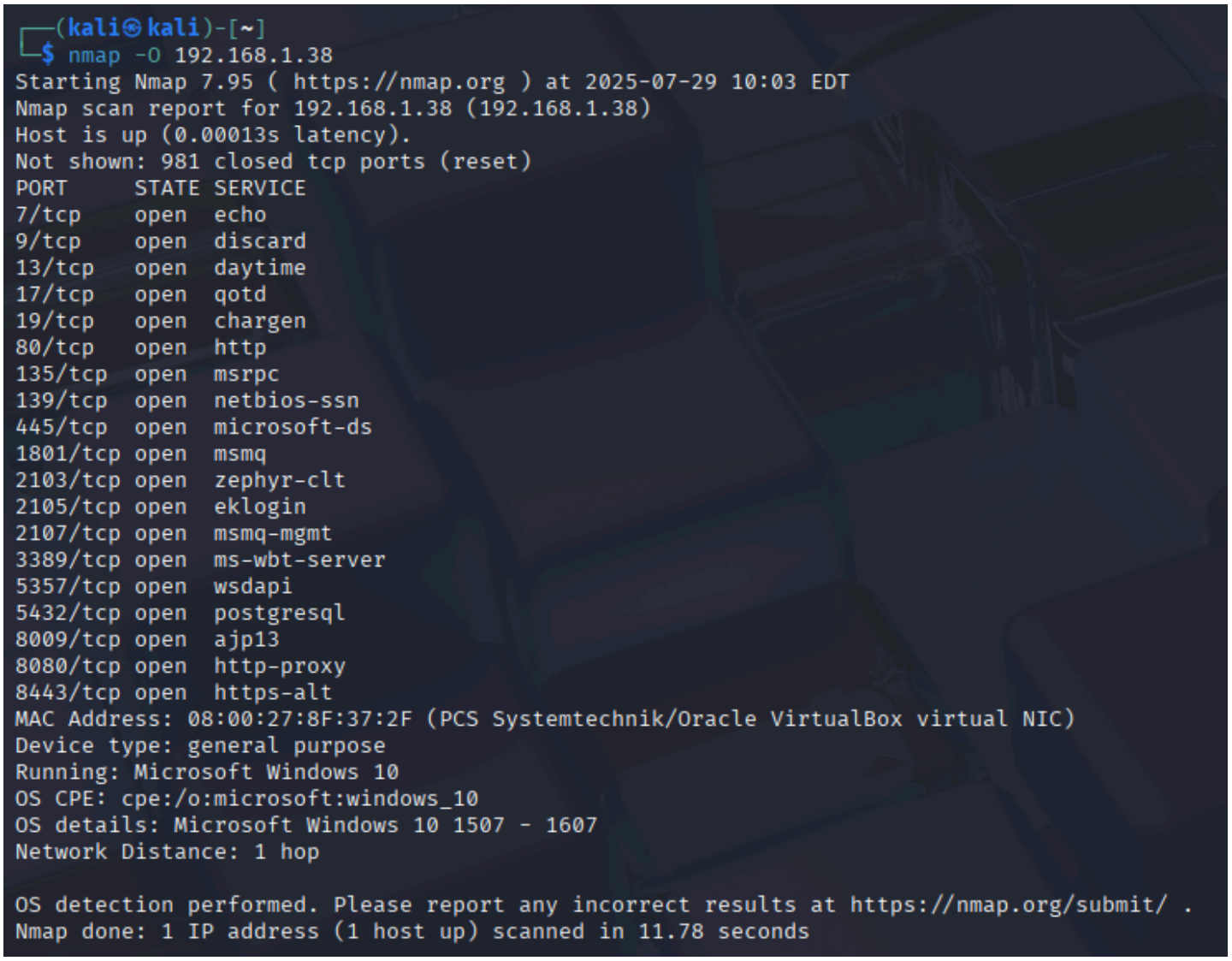
La "Version Detection" in Nmap è una funzionalità che permette di identificare il servizio in esecuzione su una porta aperta e la sua versione. In pratica, Nmap non si limita a rilevare quali porte sono aperte (come per SYN Scan e TCP Connect Scan), ma cerca anche di capire quale applicazione o servizio le sta utilizzando e che versione ha. Per questa scansione abbiamo utilizzato il comando **nmap -sV**. Qui sotto ecco lo screenshot della scansione con le porte e il relativo servizio in ascolto su ogni porta trovata aperta:



Scansione su Windows 10

OS fingerprint:

Per windows l'unico target richiesto è stato quello di risalire al sistema operativo tramite il comando **nmap -O** dalla macchina Kali. Avendo il suo indirizzo IP (192.168.1.38) siamo riusciti ad utilizzare il comando e risalire alla versione di Windows (Windows 10 tra la versione 1507 e 1607).
Nota bene: nmap-O sfrutta bug presenti in queste versioni e riesce a penetrare la macchina e risalire al sistema operativo attivo su essa, dà un range di versioni perché lo stesso bug è presente in tutte queste. Sotto lo screenshot dimostrativo:


┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.38
Starting Nmap 7.95 (https://nmap.org) at 2025-07-29 10:03 EDT
Nmap scan report for 192.168.1.38 (192.168.1.38)
Host is up (0.00013s latency).
Not shown: 981 closed tcp ports (reset)
PORT STATE SERVICE
7/tcp open echo
9/tcp open discard
13/tcp open daytime
17/tcp open qotd
19/tcp open chargen
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1801/tcp open msmq
2103/tcp open zephyr-clt
2105/tcp open eklogin
2107/tcp open msmq-mgmt
3389/tcp open ms-wbt-server
5357/tcp open wsdapi
5432/tcp open postgresql
8009/tcp open ajp13
8080/tcp open http-proxy
8443/tcp open https-alt
MAC Address: 08:00:27:8F:37:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 11.78 seconds