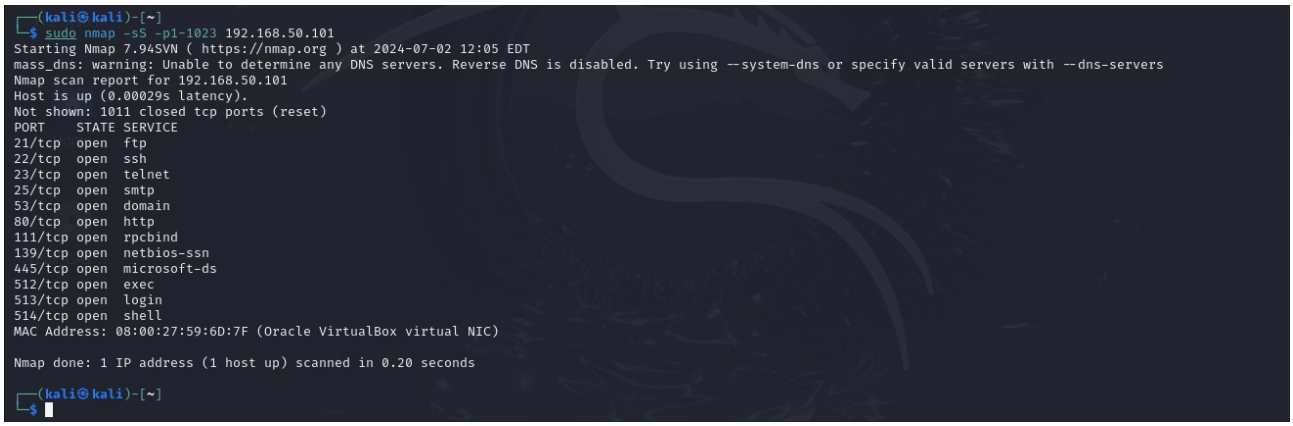
Consegna M3 – week 9 day 1 – Daniele Rufo

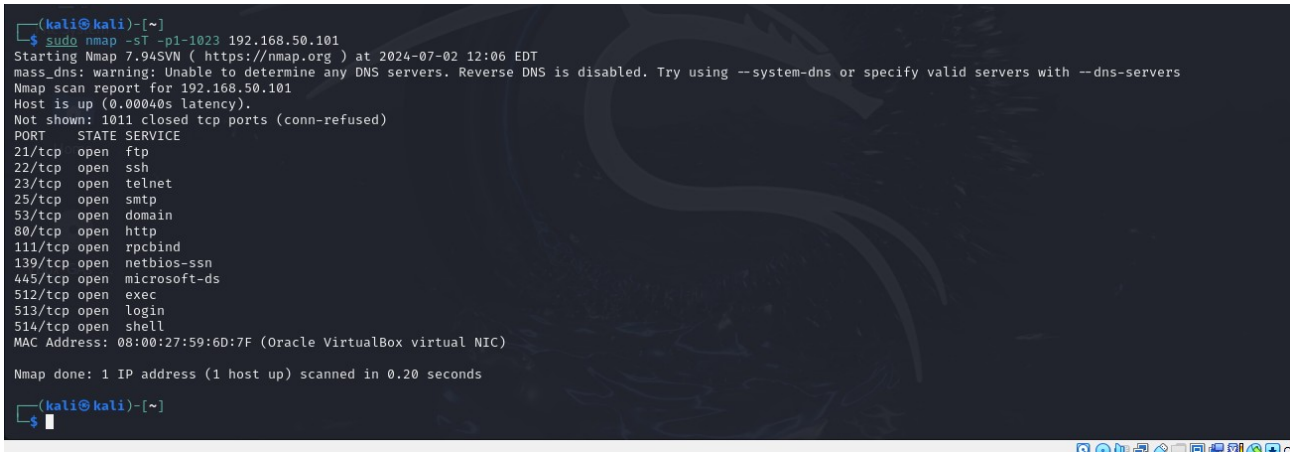
Ho eseguito le scansioni richieste dall'esercizio e raccolto i dati in una tabella. Sotto ho aggiunto anche gli screenshot delle scansioni cosi da avere anche l'output mandato al prompt da nmap e poter verificare le osservazioni.

| Fonte | Target | Metodologia | Osservazioni |
|---|---|---|---|
| 192.169.50.100 | 192.169.50.101 | -sS | -sS (SYN) è una scansione in modalità stealth. È più rapida e genera meno rumore perché non conclude il 3wayhandshake (si ferma al syn/ack e poi manda un rst per chiudere il canale). Ha più possibilità quindi di passare i controlli di IDS/Firewall e non essere rilevato, inoltre, aiuta a non sovraccaricre la linea con molte richieste tcp. La scansione -sN (TCP NULL) è ancora meno invasiva perché invia pacchetti senza flag (SYN,ACK, RST, PSH, FIN, URG, CWR) |
| 192.169.50.100 | 192.169.50.101 | -sT | -sT (TCP) invece per ogni porta controllata chiude il 3wayhandshake e quindi lascia traccia. Il risultato a video risulta uguale a quello del comando -sS |
| 192.169.50.100 | 192.169.50.101 | -A | Metodologia di scan aggressiva (A) e completa. Impiega più tempo, ma recupera molte più informazioni sui servizi in uso. Basta paragonare infatti i risultati delle scansioni: con -sS e -sT sappiamo che la porta 80 è aperta per un servizio http, ma con -A anche il nome della macchina, l'OS ed il server (Apache). Vediamo ancora come l'analisi sia più approfondita infatti con "ftp -anon IP" controlla anche se sono permessi login anonimi e ne riporta lo stato (beccata la nostra kali di cui riporta l'IP). |

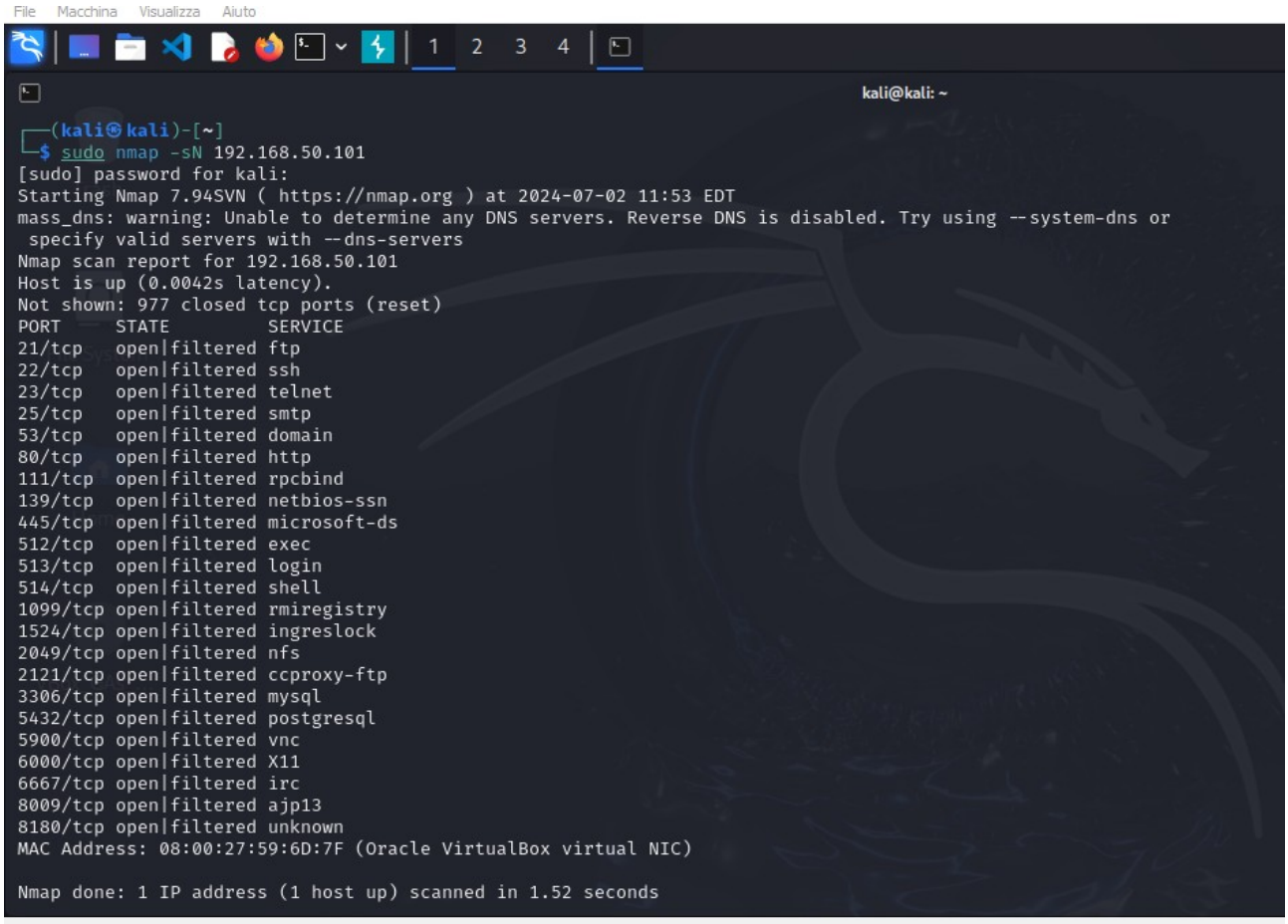
Scansione con -sS



Scansione con -sT

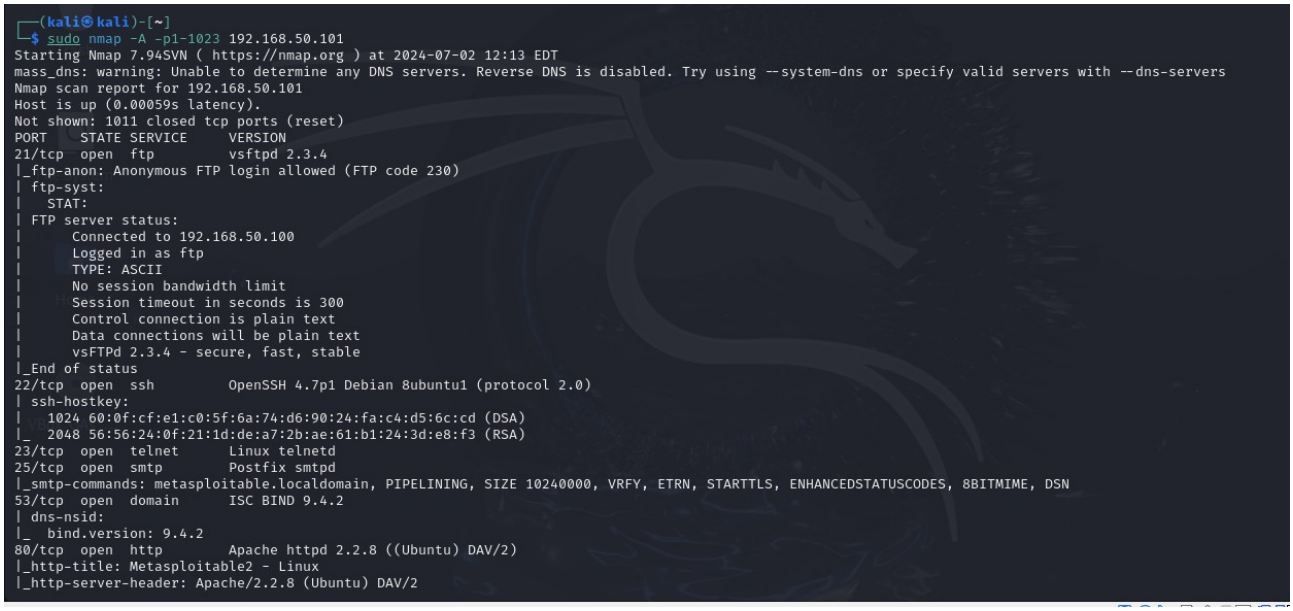



Scansione con -sN

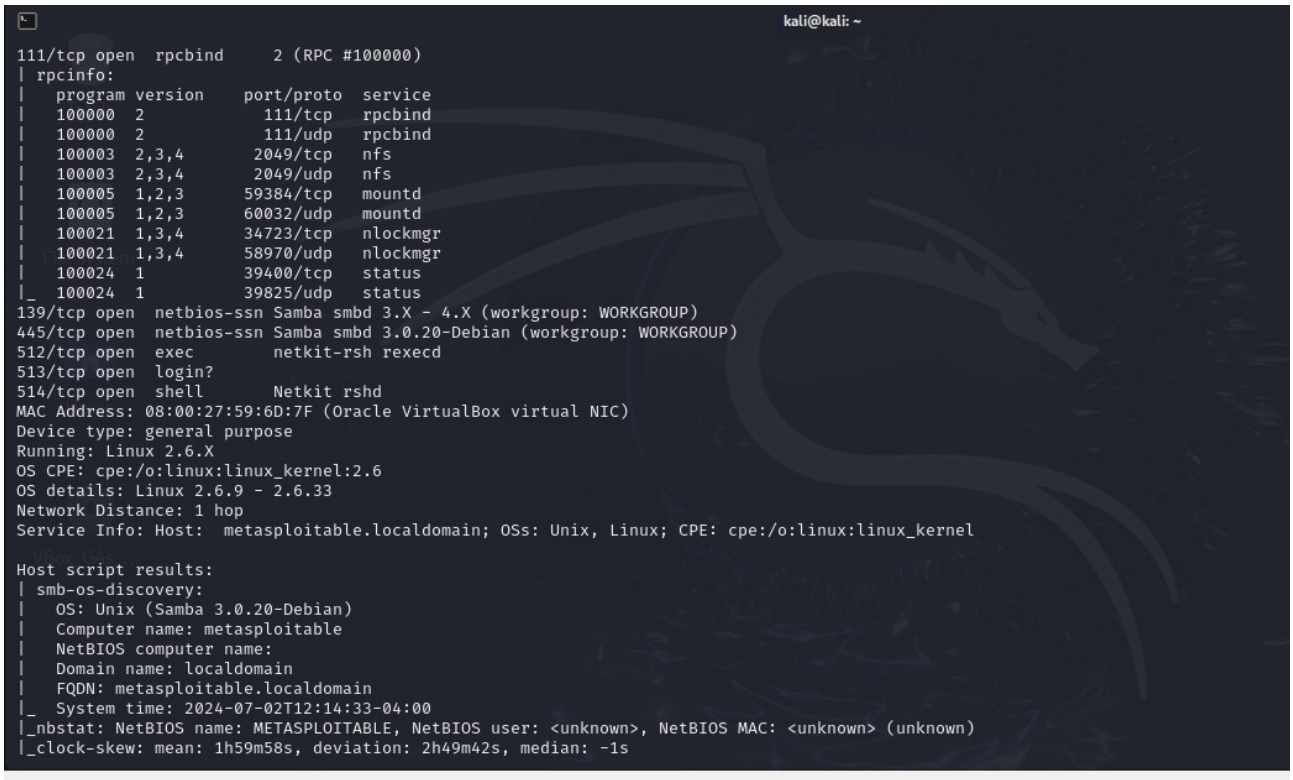


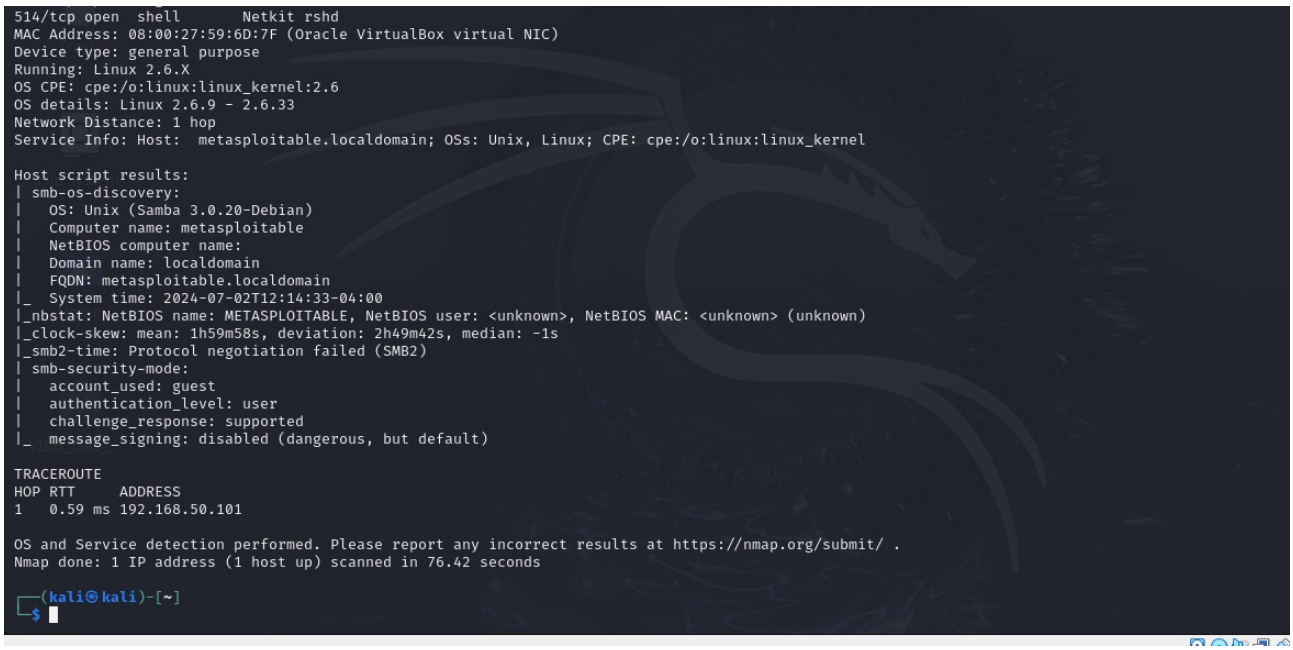
Scansione con switch -A (3screenshot)

1/3




2/3




514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:59:6D:7F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-07-02T12:14:33-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h59m58s, deviation: 2h49m42s, median: -1s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
TRACEROUTE
HOP RTT     ADDRESS
1   0.59 ms 192.168.50.101
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.42 seconds
(kali㉿kali)-[~]
$