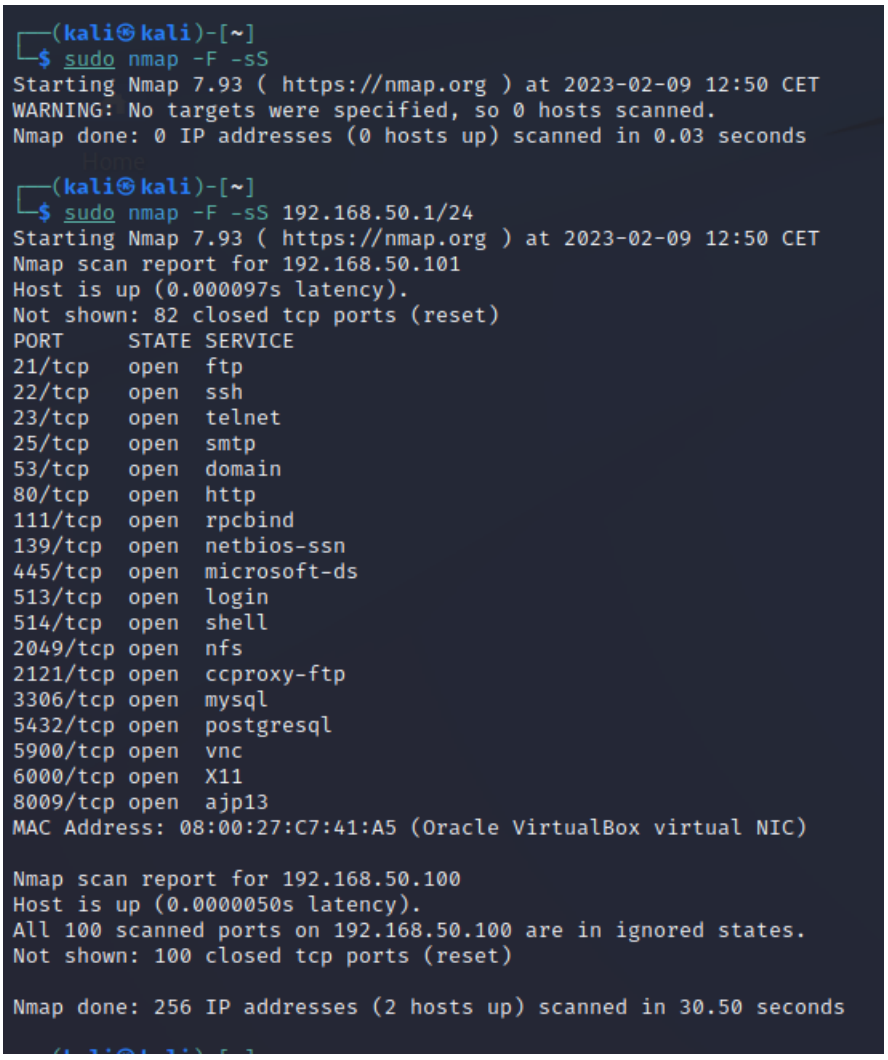
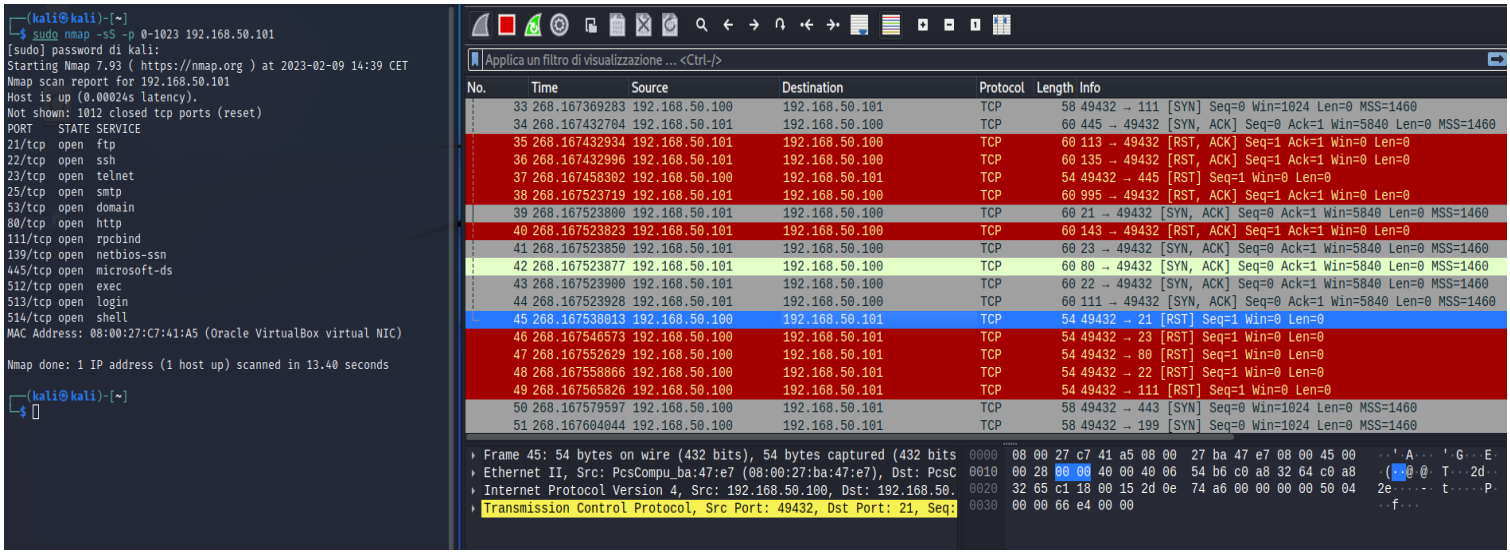
# Host discovery



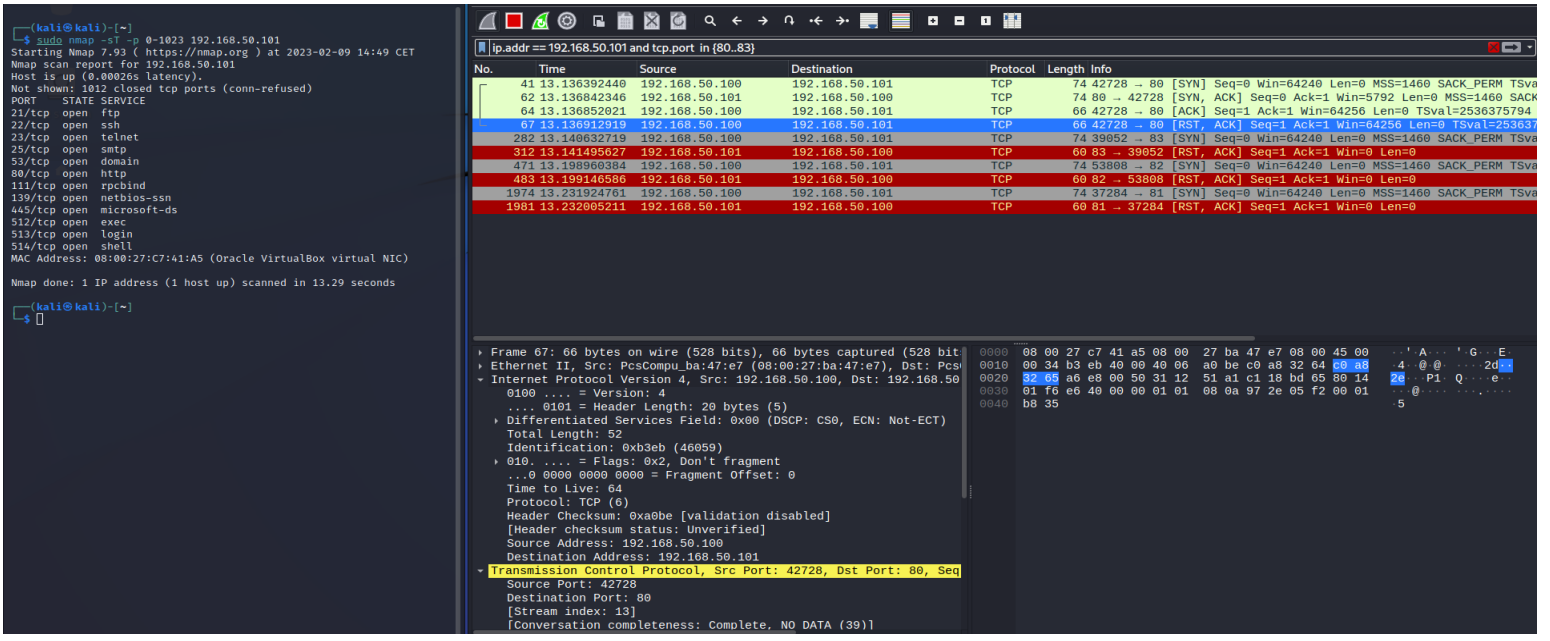

Ho scannerizzato la rete con nmap ed è stata correttamente individuata la macchina metaesploitable. Utilizzando lo switch –F, nmap testa le 100 porte di solito più utilizzate , e in questo caso sono state trovate 18 aperte.

# Sys scan su porte well-know



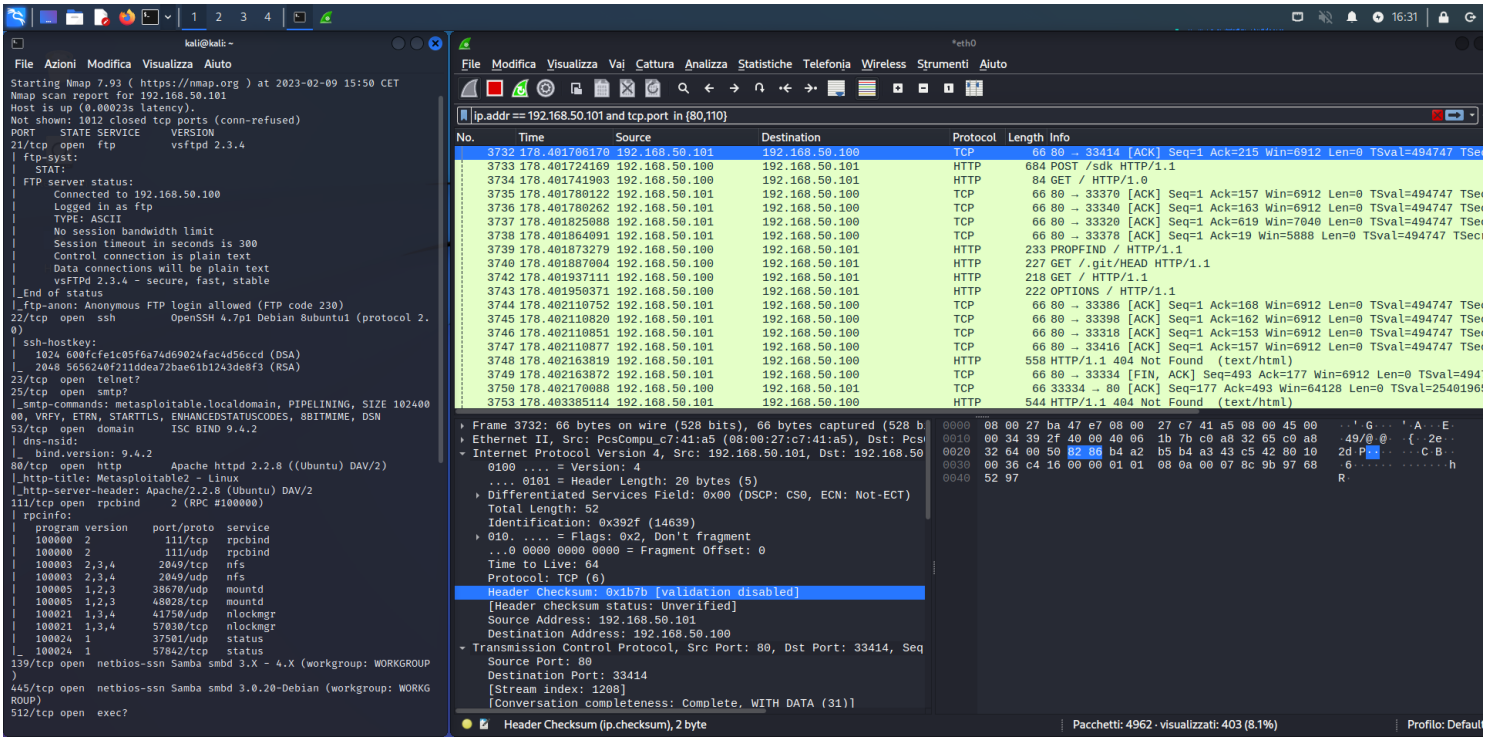

| Fonte | Target | Tipo Scan | Risultato |
|---|---|---|---|
| Kali(192.168.50.100) | Metasploitable(192.168.50.101) | sS | 12 servizi attivi su porte 0-1023 |

# Tcp Scan su porte well-know



| Fonte | Target | Tipo Scan | Risultato |
|---|---|---|---|
| Kali(192.168.50.100) | Metasploitable(192.168.50.101) | sT | 12 servizi attivi su porte 0-1023 |

# Scan con switch –A




| Fonte | Target | Tipo Scan | Risultato |
|---|---|---|---|
| Kali(192.168.50.100) | Metasploitable(192.168.50.101) | sT -A | 12 servizi attivi su porte 0-1023, incluse versioni e info sui servizi e S.O. |