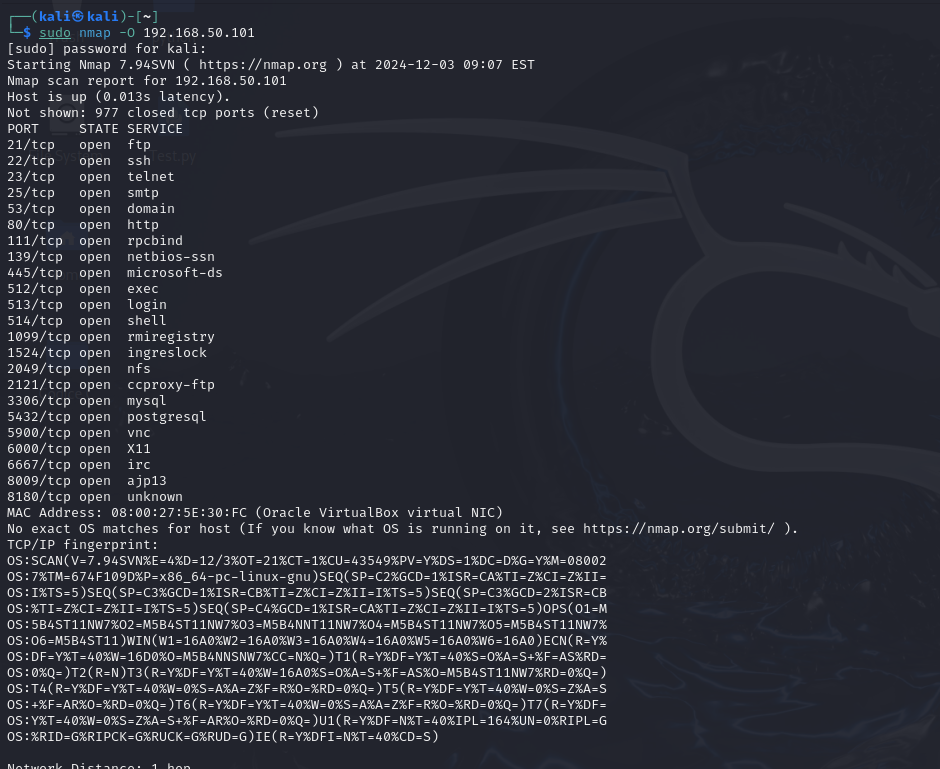
Report scansione Nmap

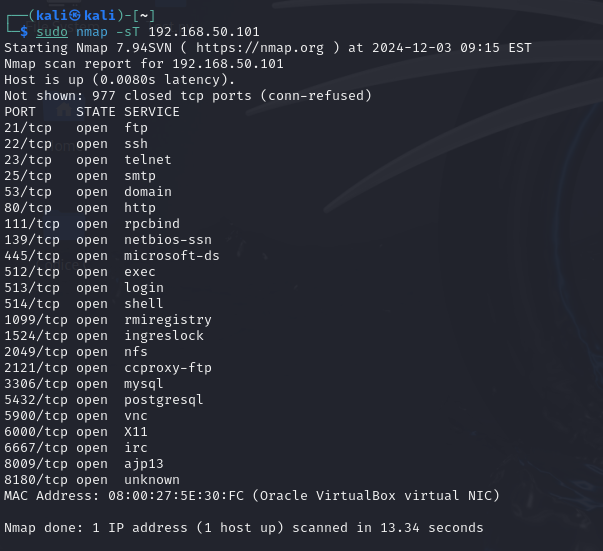
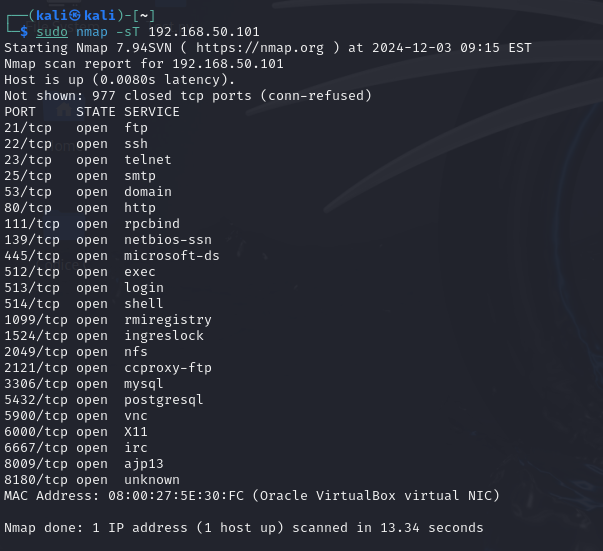
Si è partiti dallo stabilire una connessione tramite macchina Linux Kali (con indirizzo ip **192.168.50.100**) per poi andare ad esaminare le altre macchine host appartenenti alla stessa rete.   
  
**Metasploitable (192.168.50.101)**

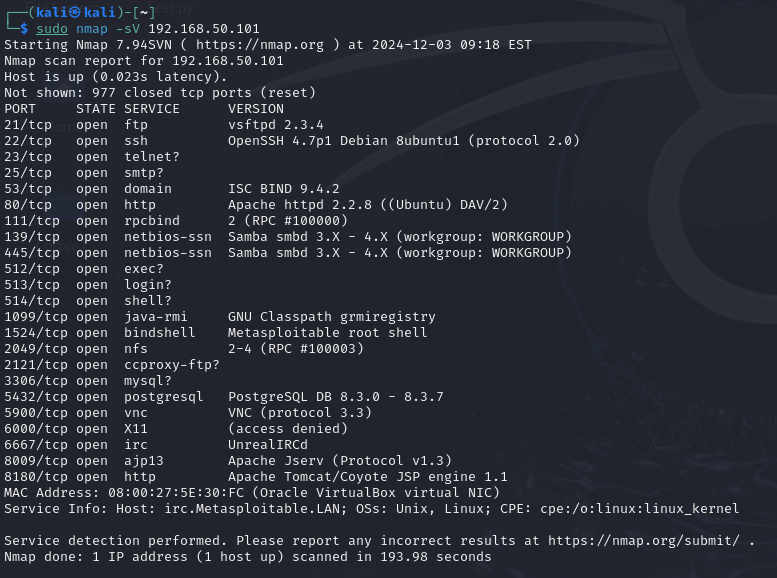
Come per primo richiesto sono andata ad effettuare la scansione della macchina Metasploitable tramite **OS fingerprint** con codice: sudo nmap -O + ip

QUesto tipo di comando determina una scansione profonda che fa capire anche che sistema operativo sta utilizzando l’host esaminato.

Tramite la scansione possiamo determinare che le porte aperte per la macchina sono: 21,22,23,25,53,80,111,139,445,512-514,1099,1524,2049,2121,3306,5432,5900,6000,6667,8009.8180. 

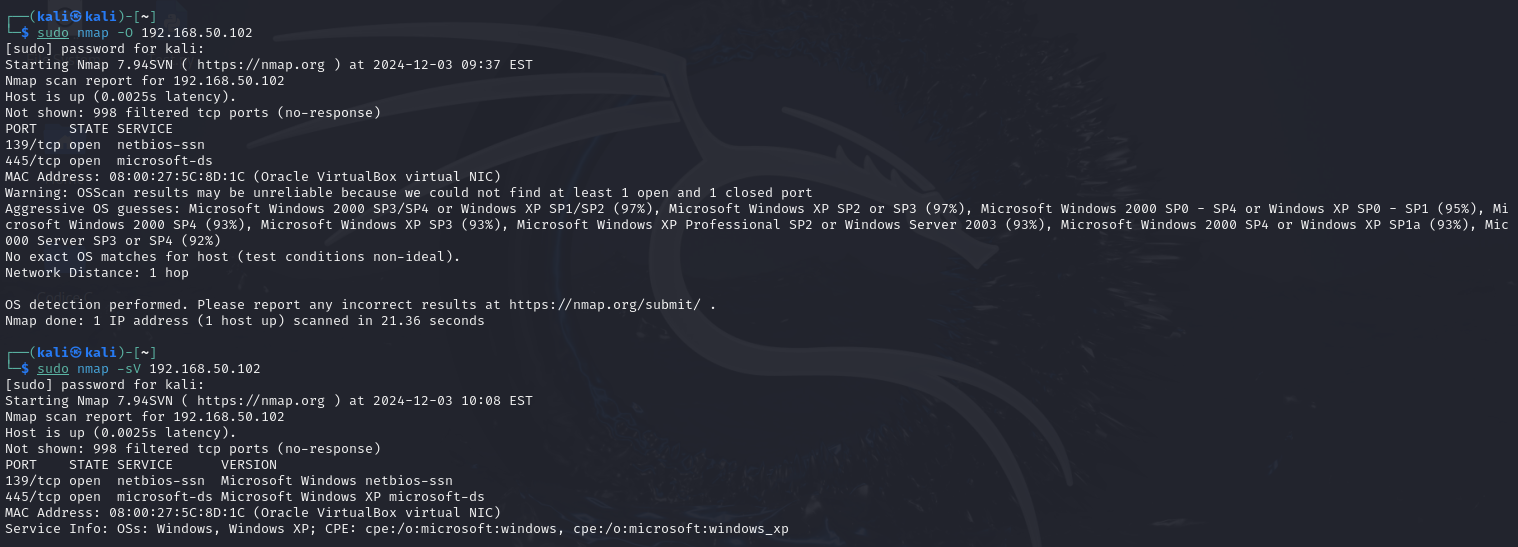
**SYN Scan e TCP Connect**Entrambi eseguono lo stesso compito ma in maniera differente. Come possiamo vedere dagli screenshot il risultato per entrambi è lo stesso, sia -sT che -sS hanno trovato lo stesso numero di porte e servizi aperti. La differenza nei due sta nella modalità di esecuzione del lavoro. -sT stabilisce connessioni TCP per intero, quindi occupa più tempo nella scannerizzazione, mentre -sS esegue una connessione SYN senza terminare il 3 way handshake, lo interrompe prima, quindi di conseguenza è più veloce.



**Version detection**

Oltre alla rilevazione delle porte e servizi aperti -sV determina anche la versione dei servizi in esecuzione sulle porte aperte nella macchina. Infatti, si possono determinare il nome dei servizi aperti e la loro versione in atto, il loro software o Sistema Operativo.

**Windows XP (192.168.50.102)**



Anche per quanto riguarda la macchina Windows XP si è andato a svolgere tramite Kali lo scanner con Os Fingerprint per andare a rilevare le porte aperte, i servizi attivi ed Il sistema operativo della macchina in questione.   
Oltre a ciò ho svolto anche una seconda verifica tramite Version Detection per dare conferma del sistema operativo ed avere anche più dettagli sul tipo di versione di quest’ultimo.