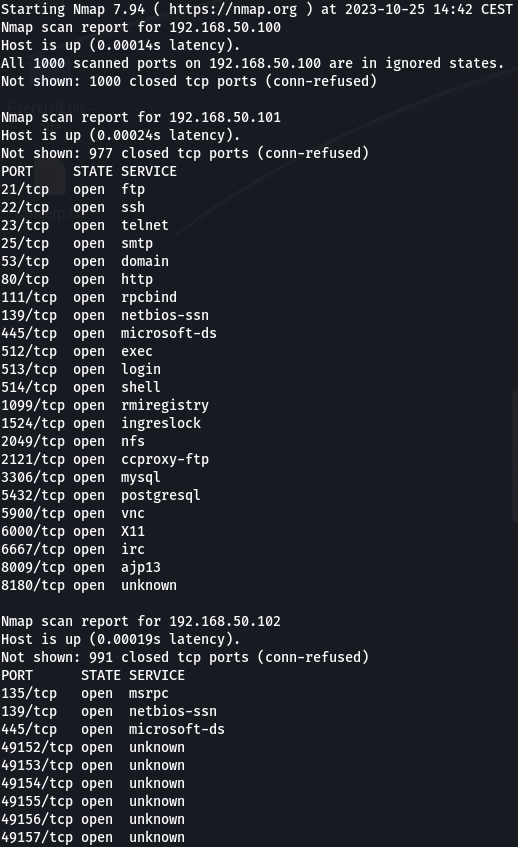
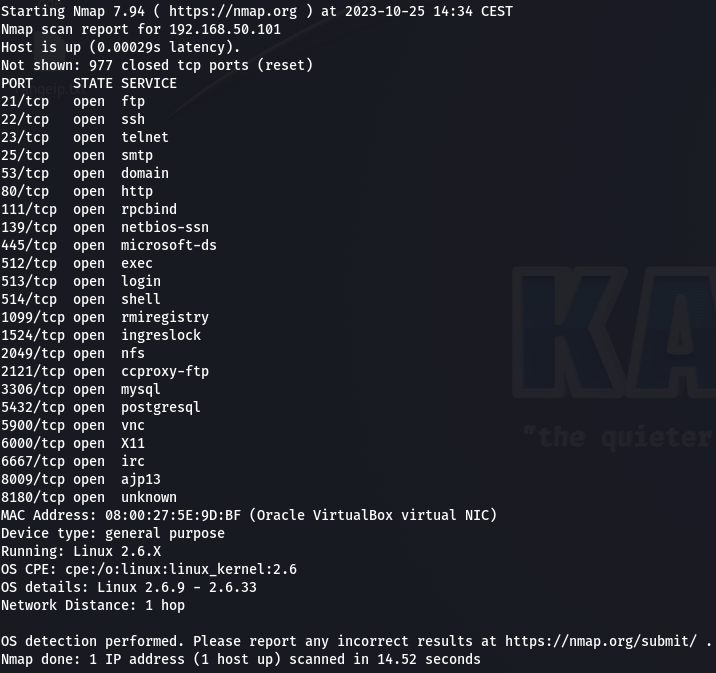
**SCANSIONE DEI SERVIZI CON NMAP**

Ci troviamo su una rete, con il nostro sistema Kali Linux e vogliamo capire quanti altri dispositivi siano presenti.

1) Tramite il comando “nmap -sS 192.168.50.\*” andiamo a cercare tutti gli IP in uso.

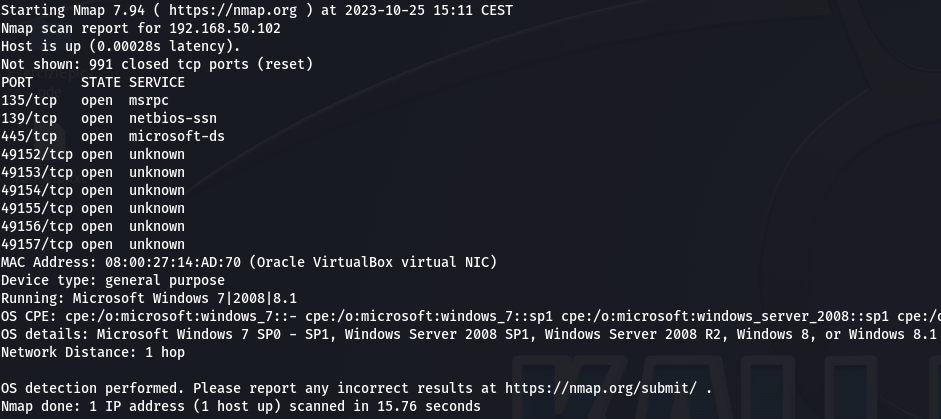


a) Troviamo il nostro IP:  
192.168.50.100.  
  
b) Un secondo IP:  
192.168.50.101.  
  
c) Un terzo IP:  
192.168.50.102.

2) Andiamo ora a capire che tipo di dispositivi siano, controllando il loro S.O. (FINGERPRINTING) tramite il comando “nmap -O 192.168.50.101 / x.x.50.102”.

Per l’IP 192.168.50.101   
troviamo che gira su un S.O.   
Linux, probabilmente tra   
la versione 2.6.9 e 2.6.33.

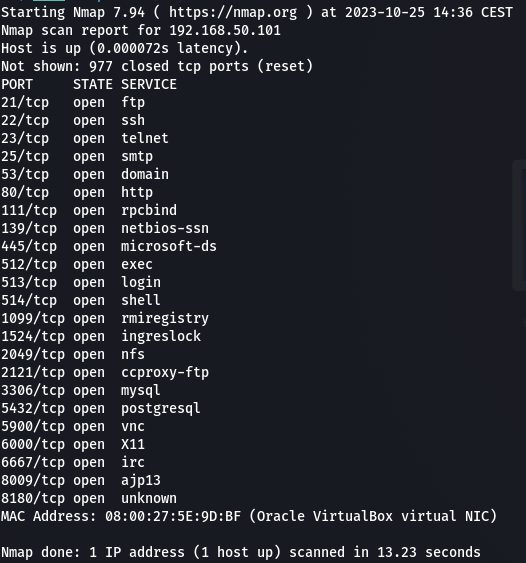






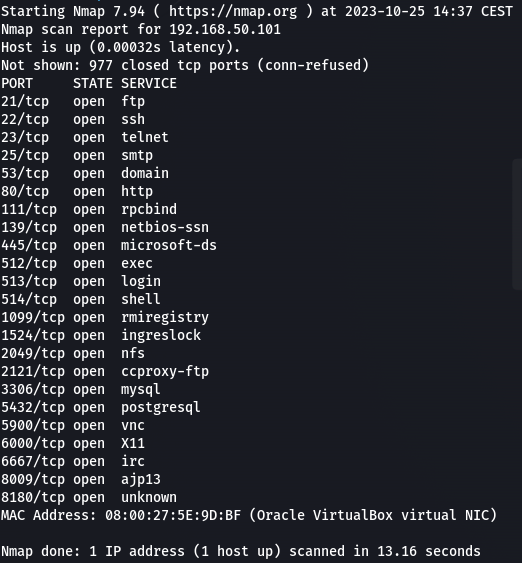
Per l’IP 192.168.50.102 vediamo che gira su un Windows, probabilmente tra 7 e 8.1, o anche Windows 2008 (una versione server di Windows).

3) Successivamente ci concentriamo sulla macchina Metaspoitable e utilizziamo i comandi “nmap -sS 192.168.50.101” e “nmap -sT 192.168.50.101” per una scansione delle porte aperte e pronte ad accettare una connessione.

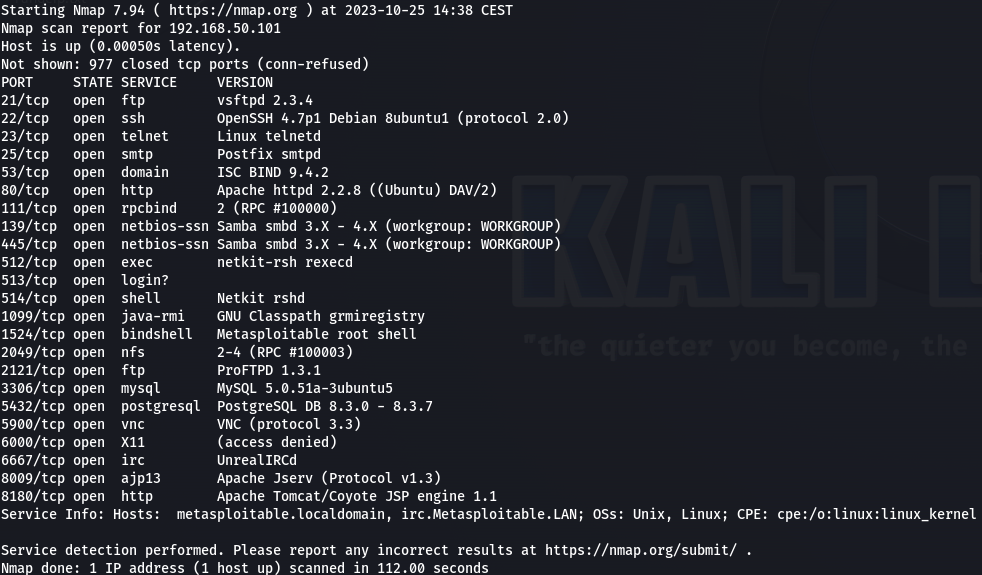


Nel SYN Scan inviamo un   
pacchetto “SYN” al dispositivo   
ricevente. Se una porta è   
aperta, il computer ricevente   
risponderà con un   
pacchetto “SYN-ACK” per   
accettare la connessione.   
Chiude la comunicazione   
inviando un pacchetto reset.  
Per questo è considerata una   
tecnica meno invasiva, meno  
rumorosa ma meno affidabile.

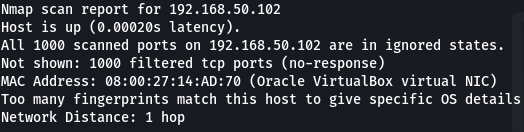


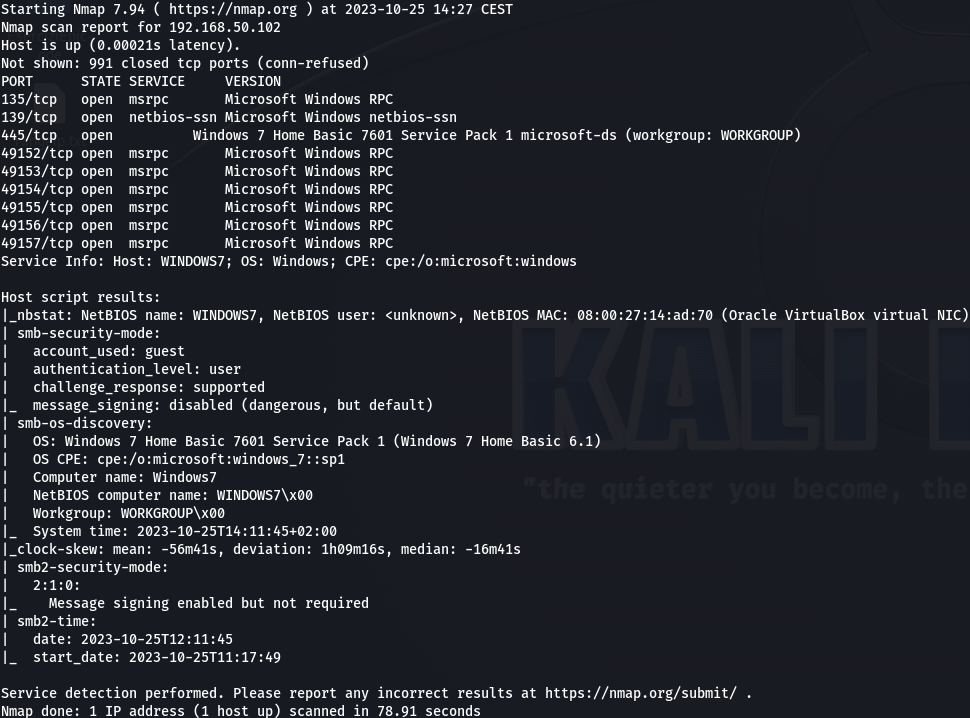


Nel TCP Scan effettuiamo il   
3-Way-Handshake, creando il   
canale di comunicazione.   
Recupera info sullo stato delle  
porte in modo più invasivo,  
fornendo informazioni più  
attendibili ma creando più   
rumore e più latenza.  
  
(In questo caso, su Metasploit,  
non notiamo differenze tra   
l’una e l’altra).

4) Infine utilizziamo il comando “nmap -sV 192.168.50.101” per verificare informazioni riguardo la versione di software e servizi.



**Quesito extra**: Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?  
  
  
Abbiamo notato come,  
inizialmente, non abbiamo  
ottenuto info riguardanti Win7



Abbiamo pensato, quindi, di disattivare il firewall di Win7 e utilizzare il comando “nmap -A -T4 192.168.50.102” (Aggressive Scan), notando come ci siano state riportate tutte le informazioni riguardanti il dispositivo.