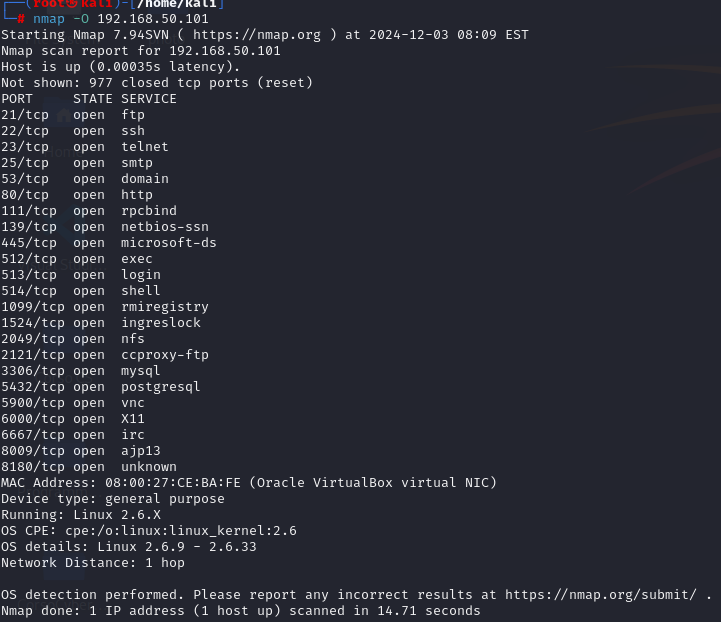
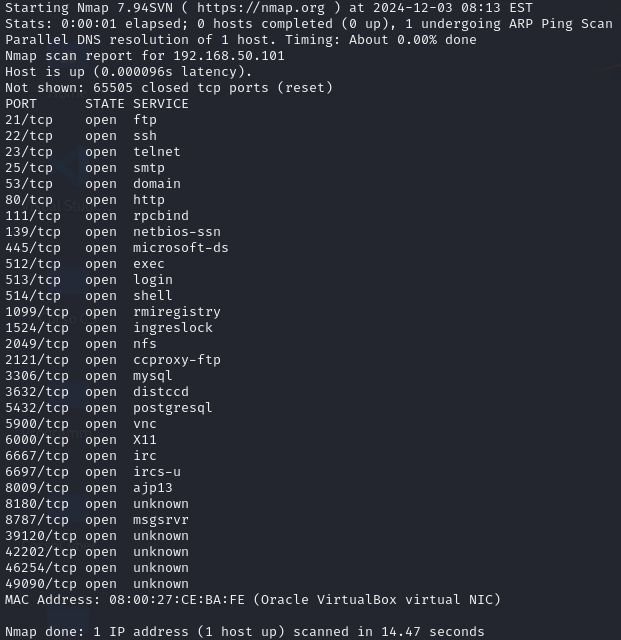
Metasploitable: 192.168.50.101

Windows xp: 192.168.50.102

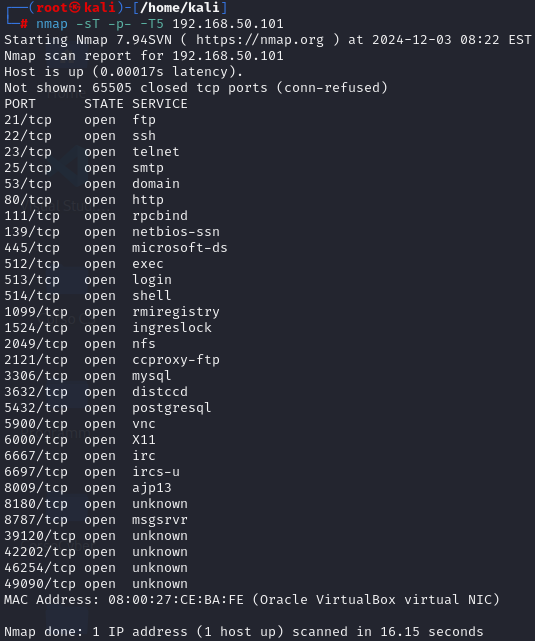
Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

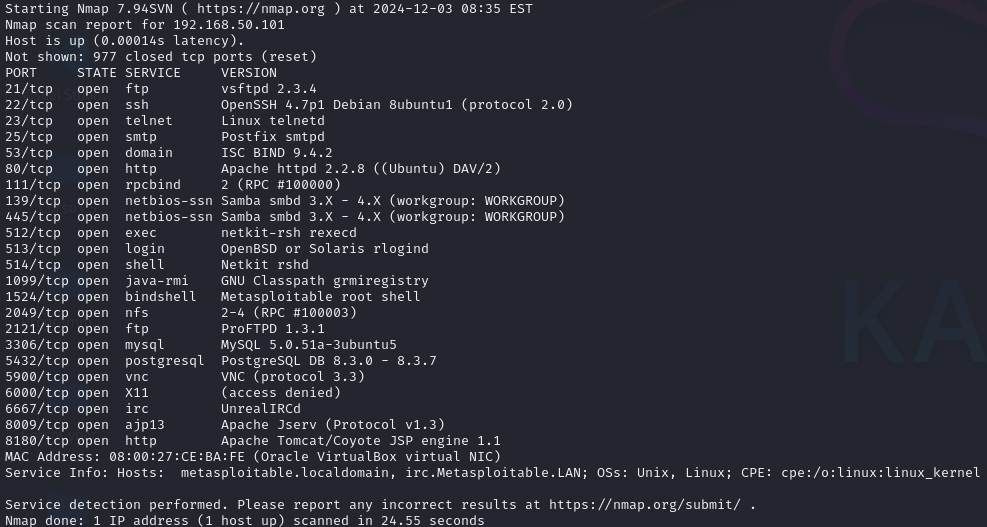
OS details: Linux 2.6.9 - 2.6.33



Porte aperte: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 3632, 5432, 5900, 6000, 6667, 8009, 8180, 8787, 39120, 42202, 46254, 49090

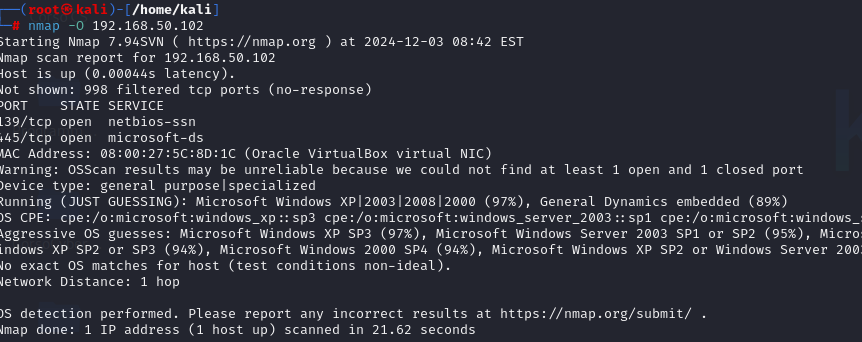


Anche lanciandoli in modalità verbosa, non ho riscontrato differenze con tra -sS e -sT, ma -sT può essere utile qualora non si abbiano accessi di root.



sS lanciato con la version detection, come output dà sempre le stesse porte aperte, ma dà anche le versioni dei rispettivi servizi

Os Fingerprint su windows xp



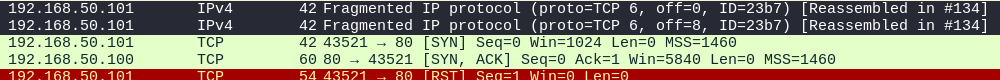
Se lanciato solo con -O, nmap dovrà tirare ad indovinare, con una certezza del 97%, ha correttamente individuato windows xp



Se lanciato con l’aggiunta di -sV, dà informazioni sul servizio

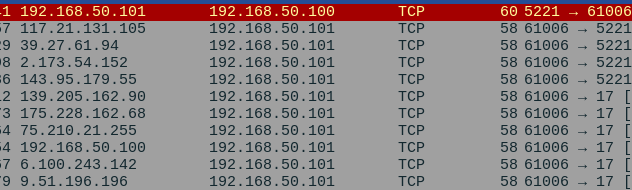


Lanciando nmap -g 53 -p80 192.168.50.101, nmap userà la porta 53 per inviare i pacchetti alla porta 80 della metasploitable, invece di una porta effimeta e, come visto da wireshark, questo può simulare che il traffico arrivi da un server DNS, rendendo più difficile il tracking e il lavoro del firewall



Utilizzando lo switch -f invece, nmap andrà a frammentare il pacchetto di dati inviato per controllare la porta 80, rendendo ancora più facile bypassare IDS e firewall che analizzano i pacchetti in base alla dimensione

-D effettua una scansione con Decoy Hosts, andando a creare ip fantoccio per confondere IDS/IPS, per rendere più difficile determinare quale host stia eseguendo la scansione, se lanciato con RND:10, andrà a generare 10 ip randomici



Qui si vedono in Wireshark gli ip randomici da cui viene lanciato lo stesso pacchetto, (wireshark evidenzia l’ip reale)

Considerazioni: senza specificare gli id decoy, la rilevazione puù essere abbastanza ovvia a occhio umano

è corretto usare -p U:53,T:200, sì, questo comando lancia lo scan per le porte 53 e 200, la u e la t specificano il protocollo per ciascuna porta, u per UDP e t per TCP, un esempio completo sarebbe

nmap -sS -sU -p U:53,T:200 192.168.50.101