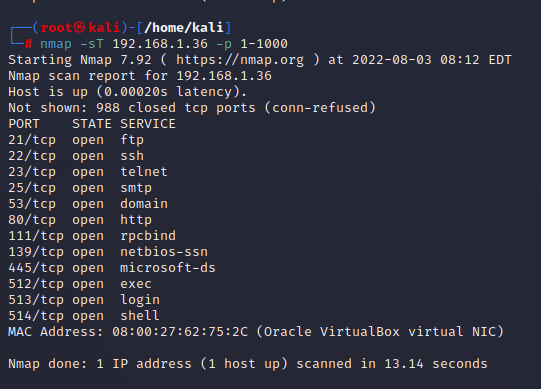
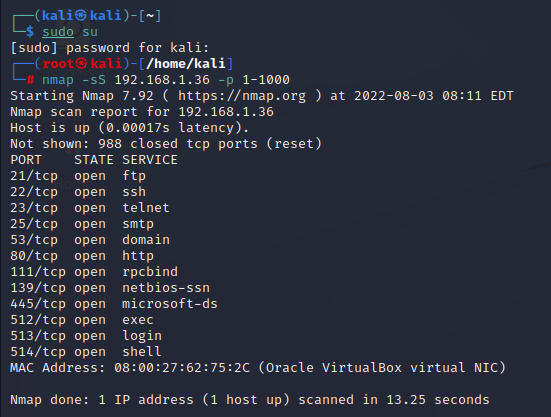
SCANSIONI CON NMAP

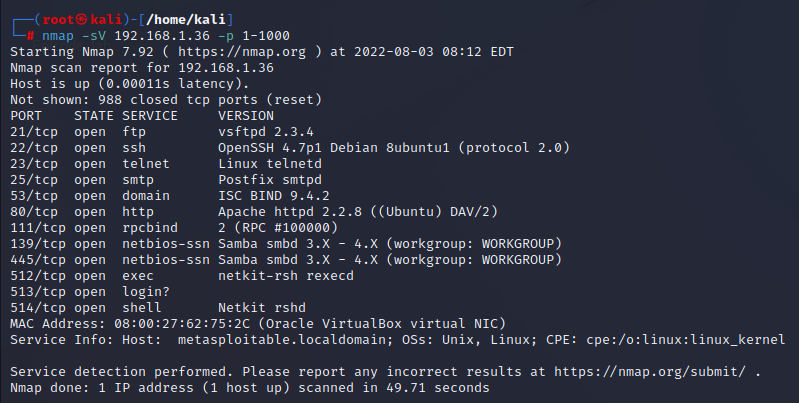
*Scansioni su Metasploitable (192.168.1.36):*

SYN scan e TCP connect:



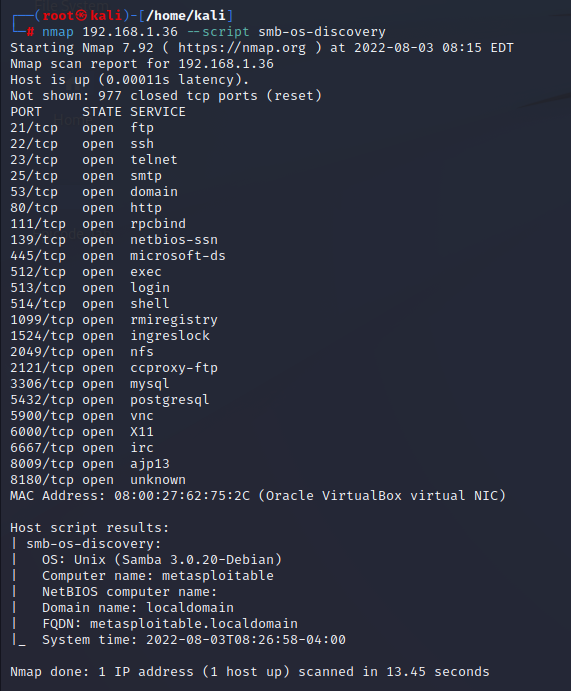
Il comando con lo switch -sS, ovvero la SYN scan, permette di fare una scansione meno invasiva ma più lenta rispetto alla TCP connect, che è eseguita tramite il comando con lo switch -sT, che al contrario è più rapida della SYN ma genera molto più “rumore”.

Version detection:



La version detection, eseguita tramite il comando con lo switch -sV, è essenzialmente una TCP connect con in più lo svolgimento di specifici test per rilevazione dei servizi in ascolto su una porta e la versione di ogni servizio. Anch’essa è molto facile da rilevare in quanto genera molto traffico di rete.

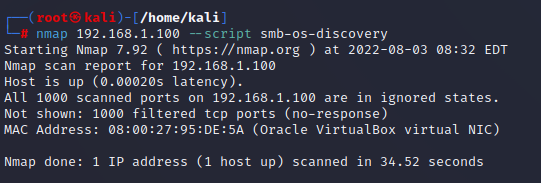
OS fingerprinting:



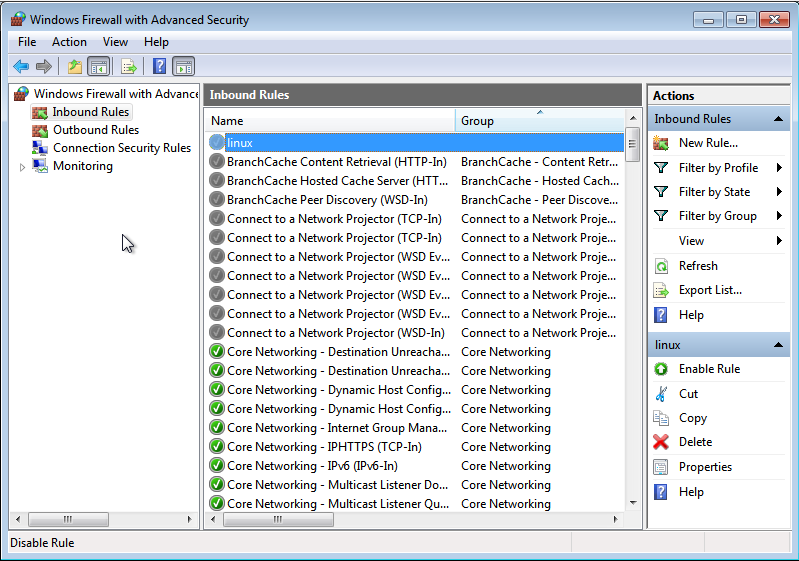
Tramite il comando di script in figura si può, oltre ad effettuare la scansione delle porte e i relativi servizi, avere in output l’host script, quindi alcune info fondamentali sul sistema operativo. Come si può vedere dall’immagine il sistema operativo è Unix (Samba 3.0.20-Debian).

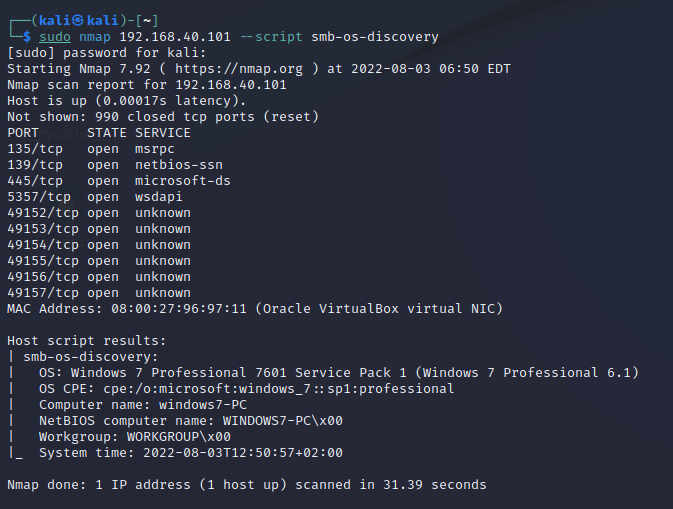
*Scansioni su Windows 7 (192.168.1.100):*

OS fingerprinting:



Come si può notare in figura, a causa del firewall ci è impedito di svolgere una scansione sul sistema operativo Windows 7. Perciò è necessario andare a creare una regola che consenta il passaggio di pacchetti da parte di Kali Linux. Per far ciò andiamo ad inserire una nuova regola da come sotto in figura:





Dopo aver risolto il problema possiamo finalmente iniziare una scansione, con il comando nmap 192.168.1.100 --script smb-os-discovery, e dai risultati si può notare che nello specifico il sistema operativo è Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1).