NMAP

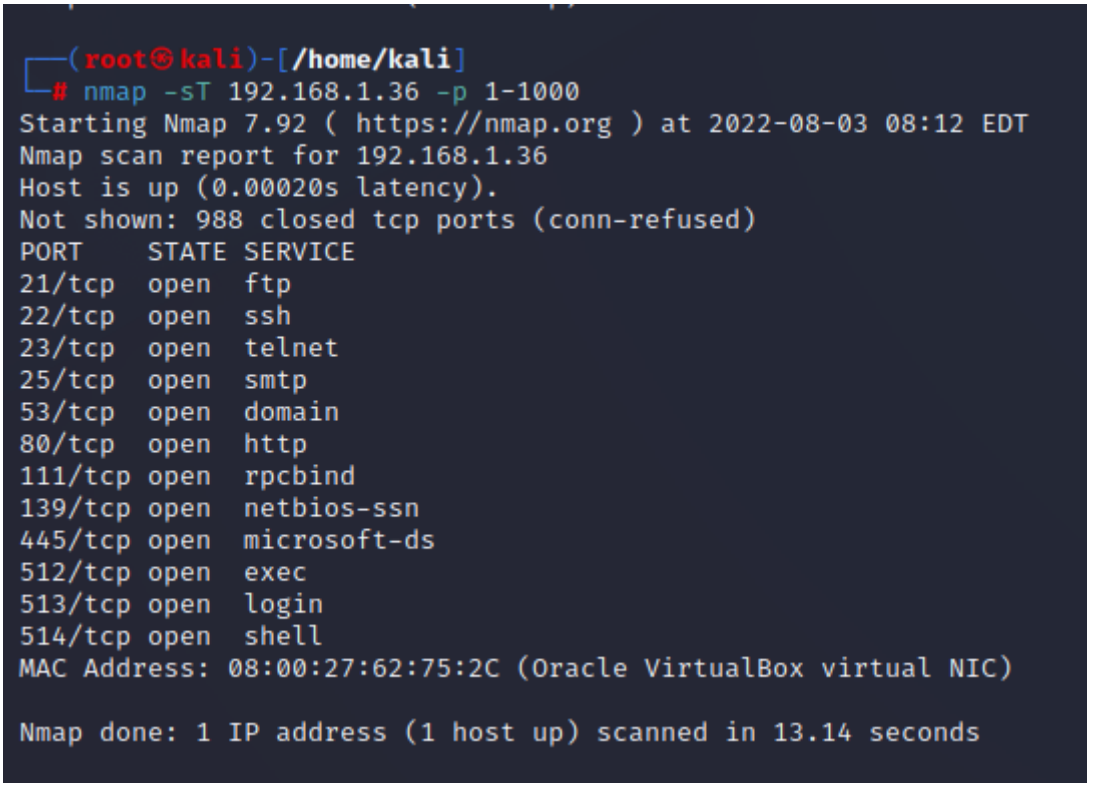
Nmap è un programma di port scanning.
Usato per scansionare le porte di possibili macchine da attaccare.
Ora andiamo a vedere alcuni comandi per fare queste scansioni effettuate sulla macchina metasploit:
nmap -sS ip -p [port range]

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.36 -p 1-1000
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:11 EDT
Nmap scan report for 192.168.1.36
Host is up (0.00017s latency).
Not shown: 988 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:62:75:2C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

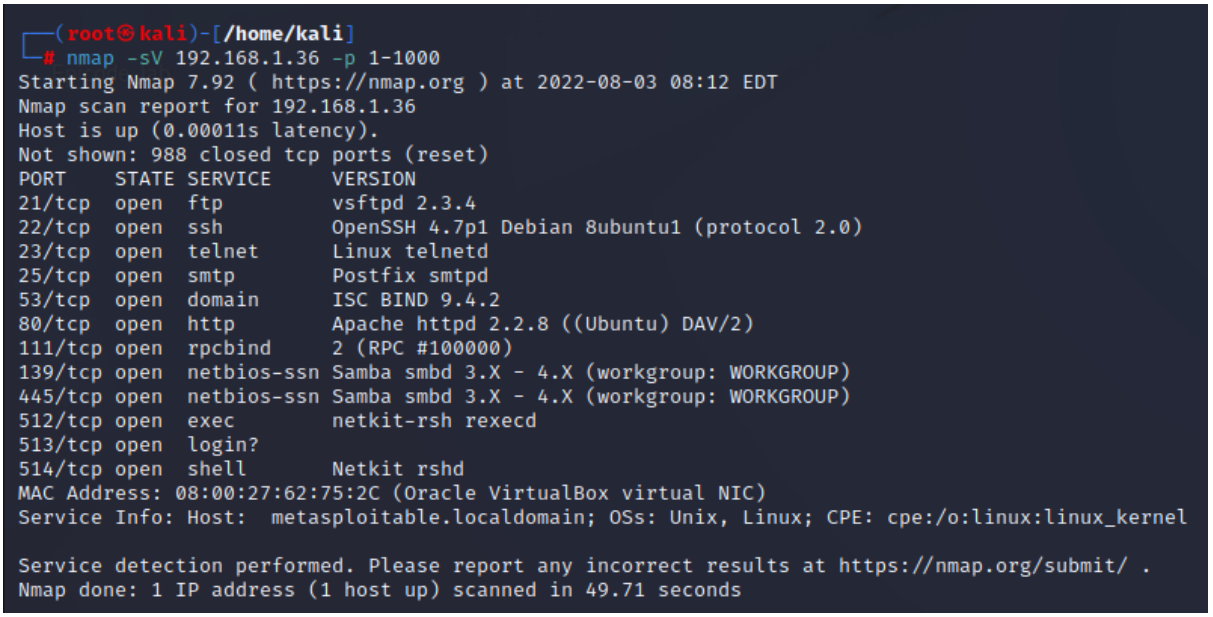
Questo comando è sS è il comando stealth.
Quindi è uno command stealth, un comando che fa poco rumore e non completa il 3WH.
In parole povere si ferma al primo SYN.

Un comando leggermente più aggressivo è il comando:
nmap -sT ip -p [port range]



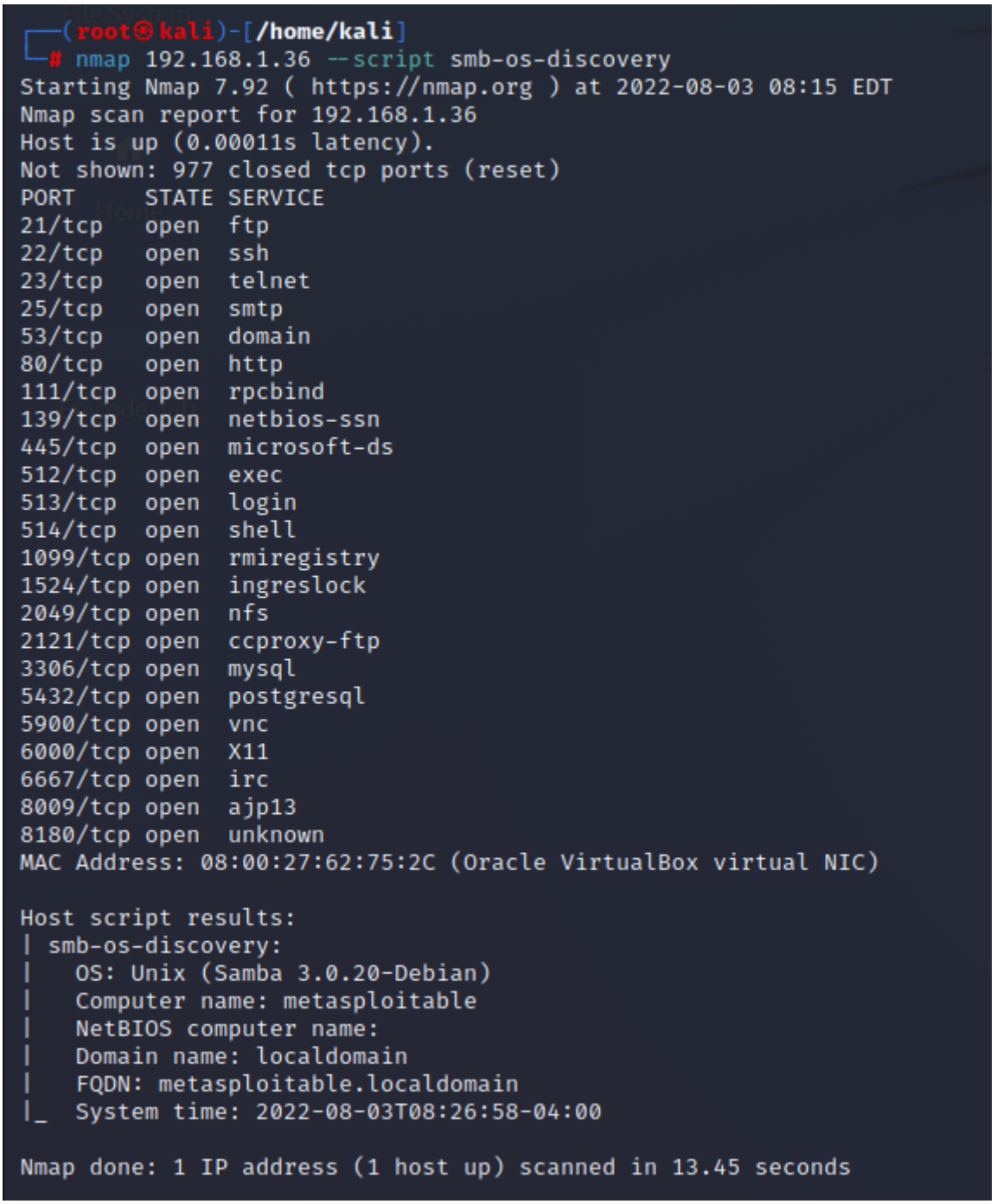
A differenza di -sS questo comando completa il 3WH e fa molto più rumore del primo, ma il funzionamento è esattamente lo stesso.
La differenza è la velocità di esecuzione -sT è più rapida rispetto -sS.
Questo comando è detto anche comando TCP.
Il tcp è proprio SYN,SYN ACK, ACK.

Il comando più aggressivo che abbiamo su nmap è nmap -sV ip -p [port range]



Questo tipo di comando oltre a chiudere il 3WH è un comando che mira a vedere anche le versioni utilizzate sulle porte aperte della macchina che stiamo scannerizzando. E' il comando che fa più rumore sulla macchina scansionata.
Come possiamo vedere appunto dall'immagine le versioni usate della porte sono ben specificate.

Ora andiamo a vedere un comando di script:
nmap ip --script smb-os-discovery



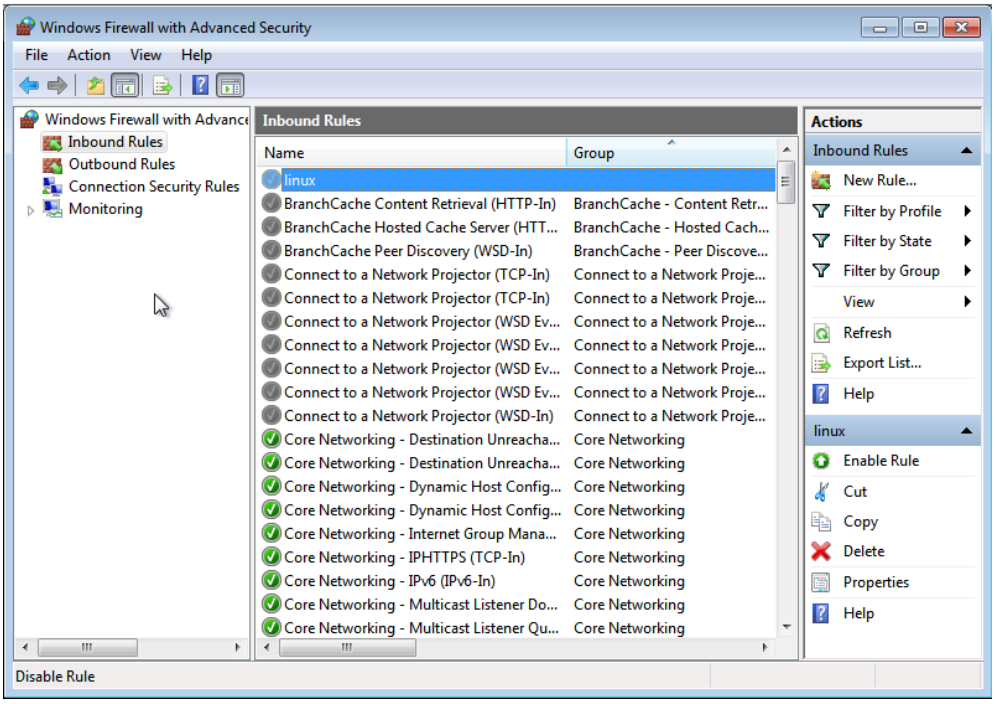
Questo comando ci permette di vedere oltre che le porte aperte anche le versione del sistema operativo usato dalla macchina scansionata.

Ora cambiamo macchina e proviamo a fare le scansioni su un macchina windows, in questo caso abbiamo usato un windows 7.
Il comando lanciato è il comando di script usato precedentemente ma il firewall di windows non ci permette di fare la scansione.

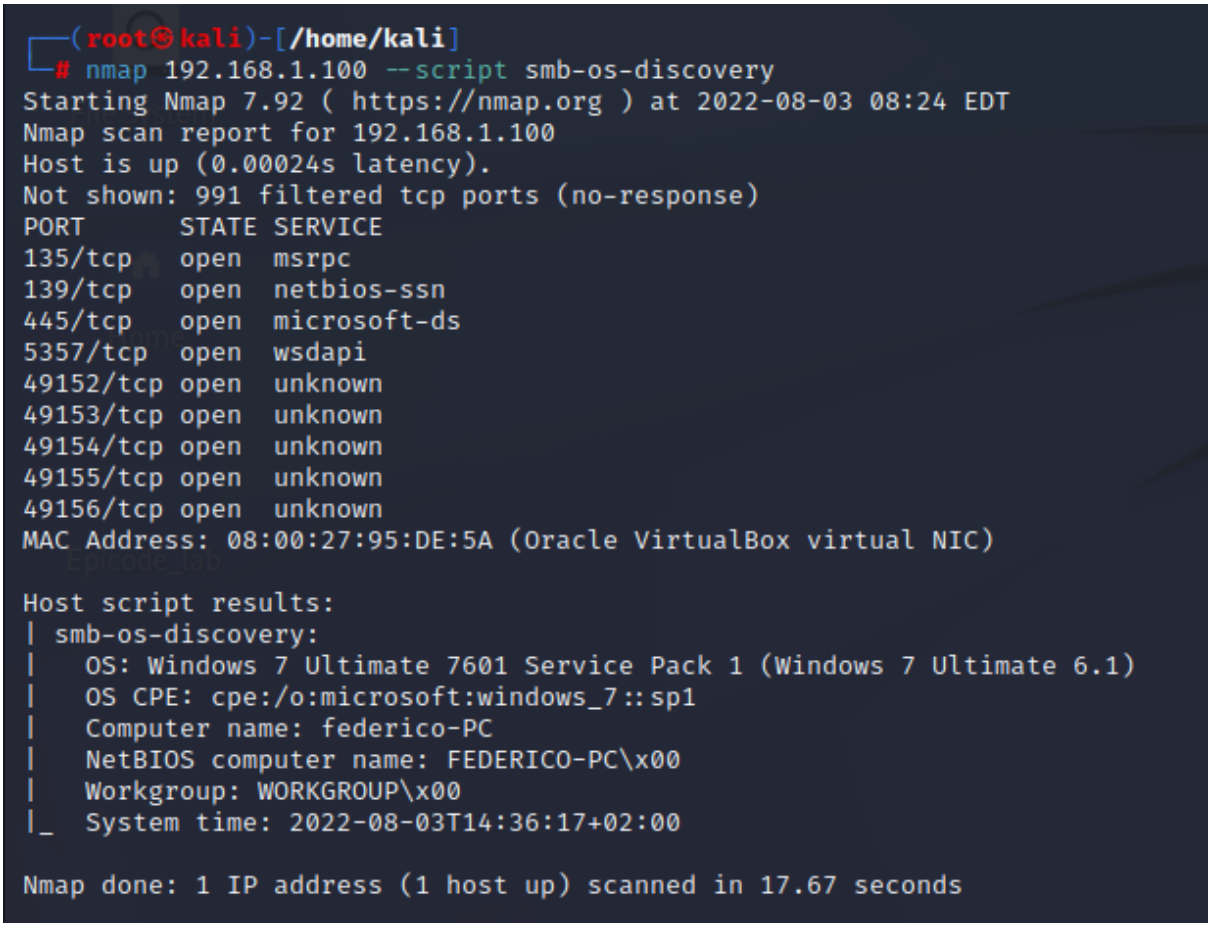
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.100 --script smb-os-discovery
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:32 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.1.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:95:DE:5A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.52 seconds
```

Quindi siamo andati sulla macchina windows 7 a cambiare le regole del firewall permettono alla macchina windows di parlare con linux.



A questo punto una volta cambiata la regola possiamo riprovare ad effettuare la scansione il risultato è completamente diverso.



Come possiamo notare ora una volta cambiata la regola del firewall abbiamo dei risultati diversi anche sulla macchina di windows.