

M3 D5

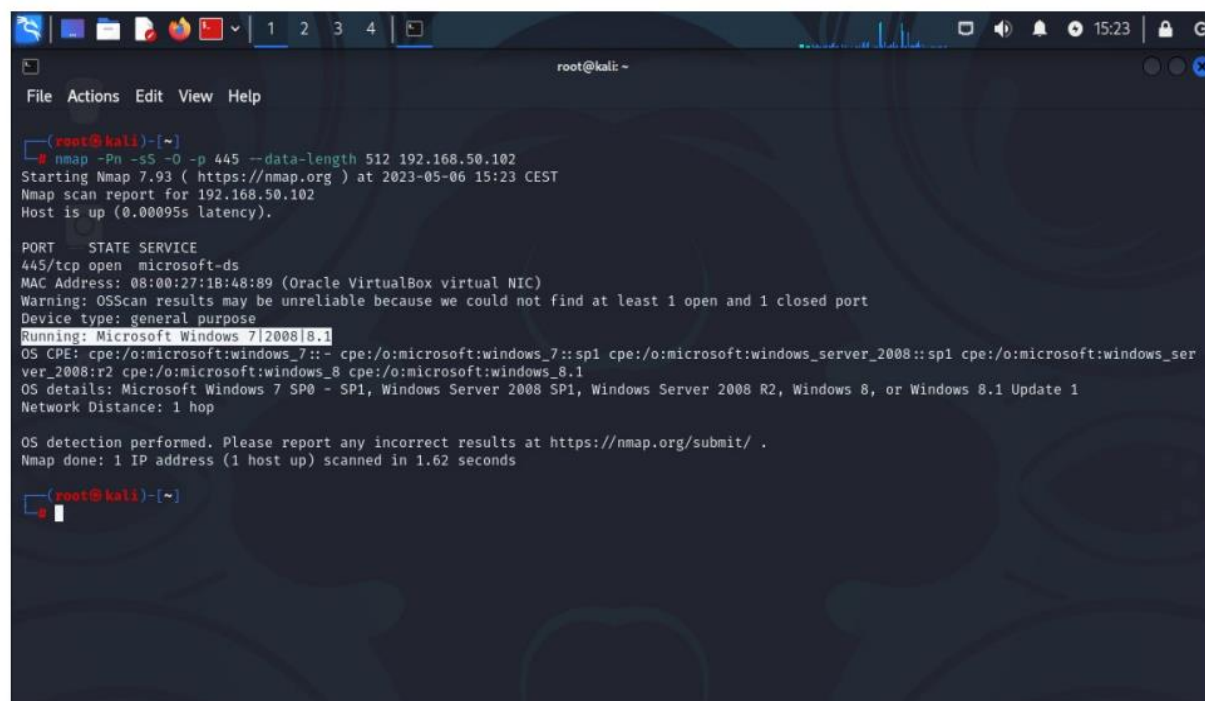
ESERCIZIO

GIORNO 3 – SCANSIONE CON NMAP

KALI VERSO WINDOWS7

Rispetto all' esercizio precedente Kali vs Metasploitable nessuna delle scansioni è andata a buon fine verso la macchina Windows a causa del firewall. Si potrebbe pensare di disattivare la protezione, ma avrebbe poco senso in un ambiente reale. Possiamo perciò provare ad utilizzare alcune opzioni avanzate di nmap per bypassare l'ostacolo come la funzione `-Pn`, la frammentazione dei pacchetti e la scansione mirata verso porte che sappiamo essere aperte.

OS Fingerprint e SYN Scan (WIN)



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~  
# nmap -Pn -sS -O -p 445 --data-length 512 192.168.50.102  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-06 15:23 CEST  
Nmap scan report for 192.168.50.102  
Host is up (0.00095s latency).  
  
PORT      STATE SERVICE  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:1B:48:89 (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Microsoft Windows 7|2008|8.1  
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1  
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds  
(root@kali)~
```

In questo modo la scansione andrà a buon fine, bypassando il firewall.