

S9/L1

Traccia:

L'esercizio di oggi è verificare in che modo l'attivazione del firewall impatta il risultato di una scansione dei servizi dall'esterno, per questo motivo:

1. assicurarci che il firewall sia disattivato sulla macchina Windows XP
2. effettuare una scansione con il nmap sulla macchina Target
3. abilitare il firewall su Windows XP
4. effettuare una seconda scansione con il nmap
5. trovare le differenze e motivarle

Per prima cosa, come richiede la traccia configuriamo le due macchine con gli IP richiesti:

Kali 192.168.240.100

```
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 4227 bytes 274450 (268.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6305 bytes 381318 (372.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 19 bytes 1770 (1.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 1770 (1.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Windows XP 192.168.240.150

Utilizza il seguente indirizzo IP:

Indirizzo IP:	192 . 168 . 240 . 150
Subnet mask:	255 . 255 . 255 . 0
Gateway predefinito:	192 . 168 . 240 . 1

Disattiviamo il firewall su Windows XP e procediamo con una prima scansione inserendo su kali il comando “nmap –sV + l’IP target di XP”:

```
sudo su
[sudo] password for kali:
(root@kali)~[/home/kali]
# nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 09:02 EST
Nmap scan report for 192.168.240.150
Host is up (0.0013s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:40:3E:ED (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.05 seconds
```

Con questa opzione visualizziamo la scansione e la versione dei servizi aperti sul nostro host Target, per cui nmap cercherà di determinare anche la versione dei servizi che sono in ascolto sulle porte aperte di Windows XP.

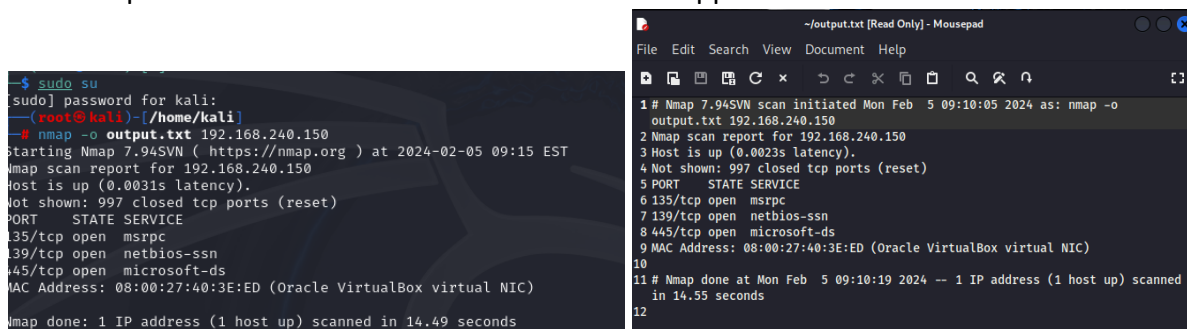
Analizziamo brevemente queste porte aperte:

Porta 135: RPC (remote procedure call); un protocollo che consente a un programma di richiamare procedure su un altro indirizzo di spazio degli indirizzi come se fossero procedure locali, senza doversi preoccupare dei dettagli della comunicazione tra i processi.

Porta 139: NETBIOS Session Service; gestisce le sessioni di comunicazione tra i dispositivi sulla rete. NetBIOS è un protocollo di rete legacy utilizzato in ambienti Windows più datati. La porta 139 è stata storicamente utilizzata per la condivisione di risorse di rete, ma è stata anche associata a problemi di sicurezza e vulnerabilità.

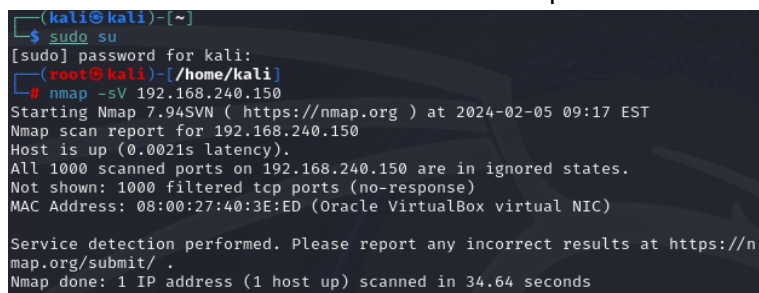
Porta 445: Microsoft Directory Services; è utilizzata dal servizio Microsoft-DS, che gestisce la condivisione di file e stampanti su reti Windows. Questa porta è spesso associata a Server Message Block (SMB), un protocollo di rete utilizzato per la condivisione di risorse, l'accesso a file e la comunicazione tra dispositivi Windows. La porta 445 è stata coinvolta in numerose vulnerabilità e attacchi, tra cui exploit noti come EternalBlue utilizzati dal ransomwar Wannacry.

Procediamo ora con un secondo comando sempre su nmap, ovvero: `nmap -o` seguito da un nome di file.txt per salvare i risultati della scansione in un apposito file di testo:



The image contains two screenshots. The left screenshot is a terminal window showing the execution of an Nmap scan. The user runs `sudo su` to become root, then `nmap -o output.txt 192.168.240.150`. The output shows the scan starting at 09:15 EST, identifying the host as up, and listing open ports: 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). The scan completes in 14.49 seconds. The right screenshot is a mousepad window displaying the saved output file. It shows the same scan results as the terminal, including the MAC address 08:00:27:40:3E:ED and the scan completion time of 14.35 seconds.

Abilitiamo ora il firewall su Windows XP e procediamo con una nuova scansione:



The image is a terminal window showing the execution of an Nmap scan with the `-sV` flag. The user runs `sudo su` to become root, then `nmap -sV 192.168.240.150`. The output shows the scan starting at 09:17 EST, identifying the host as up, and stating that all 1000 scanned ports are in ignored states due to no response. The scan completes in 34.64 seconds.

Ciò significa che tutte le 1000 porte scansionate sulla macchina target con indirizzo IP 192.168.240.150 sono in uno stato ignorato. Inoltre, non sono state mostrate tutte le 1000 porte filtrate con "no-response" (nessuna risposta).

La parte chiave di questa dichiarazione è "ignored states". Questo termine può indicare che le porte sono in uno stato che Nmap non sta considerando o non riesce a interpretare. Questo nel nostro caso deriva appunto dal fatto che il firewall è attivo, per cui Nmap non ha ricevuto risposta da queste porte durante la scansione.

In questo contesto, potrebbe essere utile esaminare la configurazione del firewall sulla macchina target e considerare se ci sono restrizioni specifiche che influiscono sulla scansione e andarle a modificare.

