Consegna S9/L1

Traccia

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

1. Assicurati che il firewall sia disattivato sulla macchina Windows XP.
2. Effettua una scansione con nmap sulla macchina target (utilizzando lo switch -sV per la service detection e -o seguito dal nome del file report per salvare l'output in un file).
3. Abilita il firewall sulla macchina Windows XP.
4. Effettua una seconda scansione con nmap, utilizzando ancora una volta lo switch -sV.
5. Trova eventuali differenze e motivarle.

Firewall disattivato

1. Questi risultati indicano che senza il firewall, è possibile ottenere informazioni più dettagliate sui servizi in esecuzione sulla macchina.
2. La presenza di porte aperte può indicare la disponibilità di determinati servizi di rete

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -o report.txt 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 05:54 EST
Note: Host seems down. If it is really up, but blocking our ping probes, tr
y -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -o senzafirewall.txt 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 05:56 EST
Nmap scan report for 192.168.240.150
Host is up (0.0036s latency).
Not shown: 997 closed tcp ports (conn-refused)
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
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 19.64 seconds
```

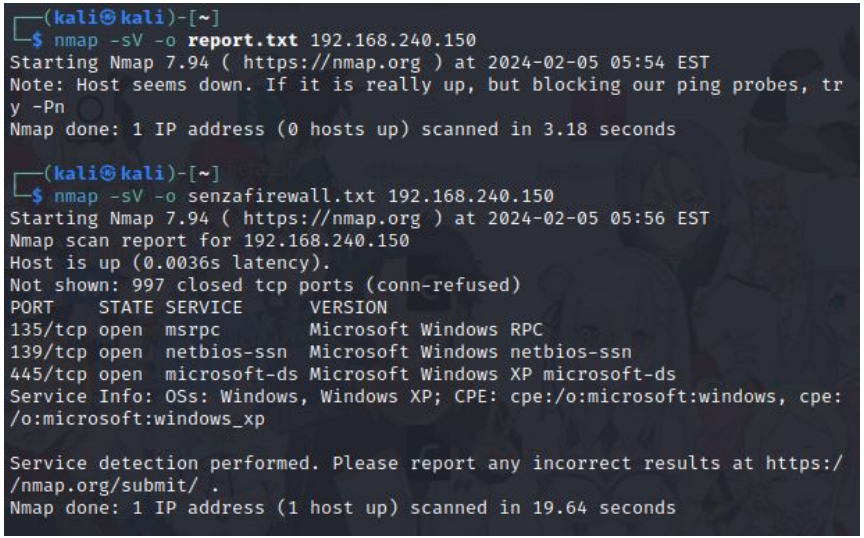
```
# Nmap 7.94 scan initiated Mon Feb  5 05:56:32 2024 as: nmap -sV -o senzafirewall.txt 192
.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.0036s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:w
indows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
# Nmap done at Mon Feb  5 05:56:51 2024 -- 1 IP address (1 host up) scanned in 19.64 seco
nds
```

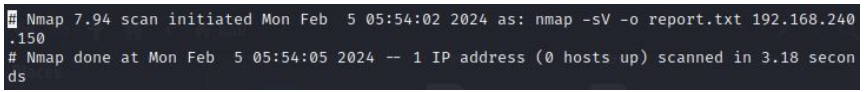
file.txt

Firewall attivato

1. Nessuna informazione rilevata con la scansione standard.
2. Suggerimento di provare l'opzione "-Pn" per bypassare la politica di non risposta del firewall, senza inviare un ping.

In questo caso, la differenza principale tra i due scenari sembra essere il fatto che il firewall blocca la scansione standard, ma con l'opzione "-Pn" puoi provare a bypassare questa politica e ottenere risultati più dettagliati. La scansione senza firewall fornisce informazioni più complete sulle porte aperte e i servizi associati.





file.txt

Firewall attivato

Questo è il mio tentativo con -Pn, ma come possiamo vedere, le regole del firewall sono impostate in modo tale da bloccare la nostra scansione anche in questo modo.