

Nmap Scanner Windows XP

Richiesta: Utilizzare Nmap per effettuare due scansioni sulla macchina virtuale windows xp. 1° Scansione Firewall OFF, 2° Scansione Firewall ON.

Requisiti: Kali linux ip address 192.168.240.100

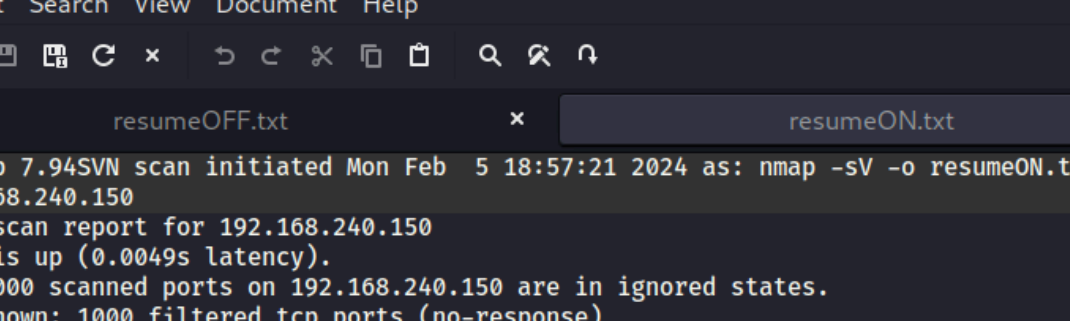
Windows xp ip address 192.168.240.150

Scansione Nmap

Effettuiamo la 1° scansione con il firewall disattivato e stampiamo il risultato in un file di testo resumeOFF.txt, utilizzando le flag -sV e -o

```
~/resumeOFF.txt [Read Only] - Mousepad
File Edit Search View Document Help
+ [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
1 # Nmap 7.94SVN scan initiated Mon Feb 5 18:56:29 2024 as: nmap -sV -o resumeOFF.txt
  192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0022s latency).
4 Not shown: 997 closed tcp ports (reset)
5 PORT      STATE SERVICE      VERSION
6 135/tcp    open  msrpc        Microsoft Windows RPC
7 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
9 MAC Address: 08:00:27:E5:48:9B (Oracle VirtualBox virtual NIC)
10 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/
   o:microsoft:windows_xp
11
12 Service detection performed. Please report any incorrect results at https://nmap.org/
   submit/ .
13 # Nmap done at Mon Feb 5 18:56:49 2024 -- 1 IP address (1 host up) scanned in 20.77
   seconds
14
```

Adesso effettuiamo la 2° scansione con il firewall attivo:



The screenshot shows a text editor window titled "~/.resumeON.txt [Read Only] - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with icons for file operations and editing. The editor displays two tabs: "resumeOFF.txt" and "resumeON.txt". The "resumeON.txt" tab is active and contains the following text:

```
1 # Nmap 7.94SVN scan initiated Mon Feb 5 18:57:21 2024 as: nmap -sV -o resumeON.txt
  192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0049s latency).
4 All 1000 scanned ports on 192.168.240.150 are in ignored states.
5 Not shown: 1000 filtered tcp ports (no-response)
6 MAC Address: 08:00:27:E5:48:9B (Oracle VirtualBox virtual NIC)
7
8 Service detection performed. Please report any incorrect results at https://nmap.org/
  submit/ .
9 # Nmap done at Mon Feb 5 18:57:55 2024 -- 1 IP address (1 host up) scanned in 34.65
  seconds
10
```

Differenze

Differenze Chiave:

- Quando il firewall è disattivato, Nmap è in grado di identificare porte aperte e servizi in esecuzione sul sistema, fornendo informazioni che possono essere utilizzate per scopi di attacco o analisi di sicurezza.
- Con il firewall attivato, le porte sono filtrate, impedendo a Nmap di determinare se le porte sono aperte o chiuse, aumentando la sicurezza del sistema ostacolando la rilevazione da parte degli scanner di porte.

La configurazione del firewall ha un impatto significativo sui risultati della scansione Nmap, come dimostrato dai due output. Un firewall configurato correttamente può nascondere le informazioni vitali sulle porte e i servizi da potenziali aggressori, riducendo così la superficie di attacco del sistema.