Nmap Scan Report

Objective

The objective of this report is to analyze the impact of the Windows XP firewall on network scans. The scans were conducted with the firewall turned on and off to compare the visibility of open ports and services.

Environment

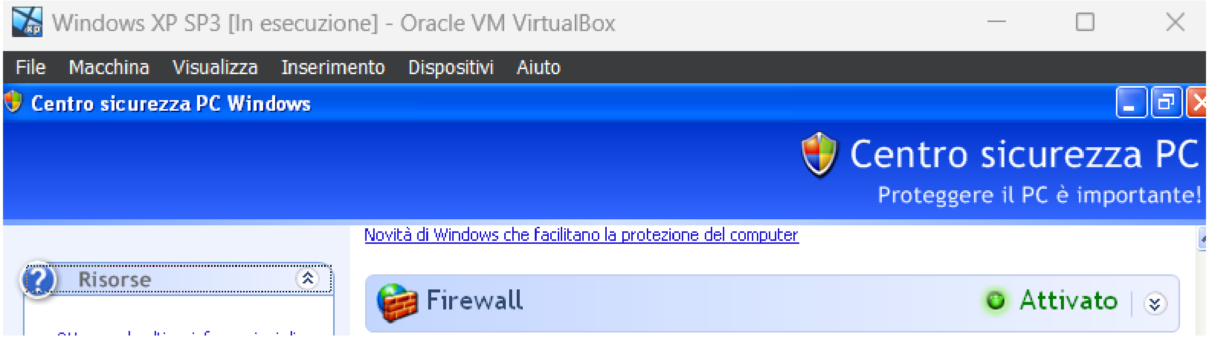
- Target Machine: Windows XP
- Scanning Tool: Nmap
- Scanner Machine: Kali Linux

Methodology

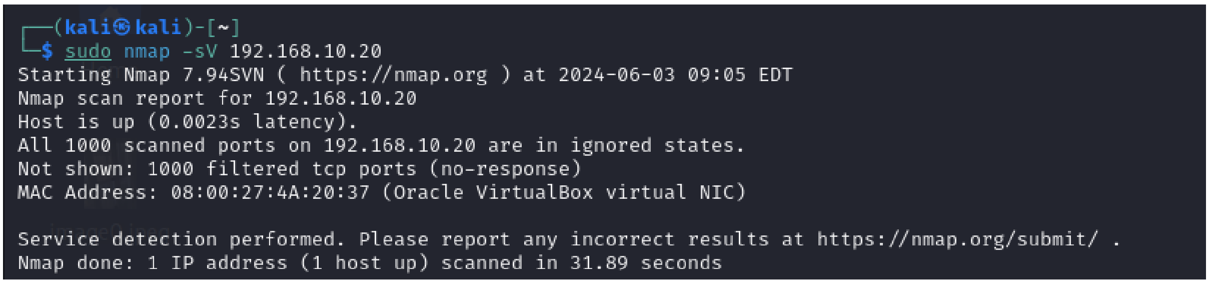
Two sets of scans were conducted:

1. With the firewall turned on.
2. With the firewall turned off.

Scan 1: Firewall On


Windows XP SP3 [In esecuzione] - Oracle VM VirtualBox
File
Macchina
Visualizza
Inserimento
Dispositivi
Aiuto
Centro sicurezza PC Windows
Centro sicurezza PC
Proteggere il PC è importante!
Novità di Windows che facilitano la protezione del computer
Risorse

Firewall ● Attivato



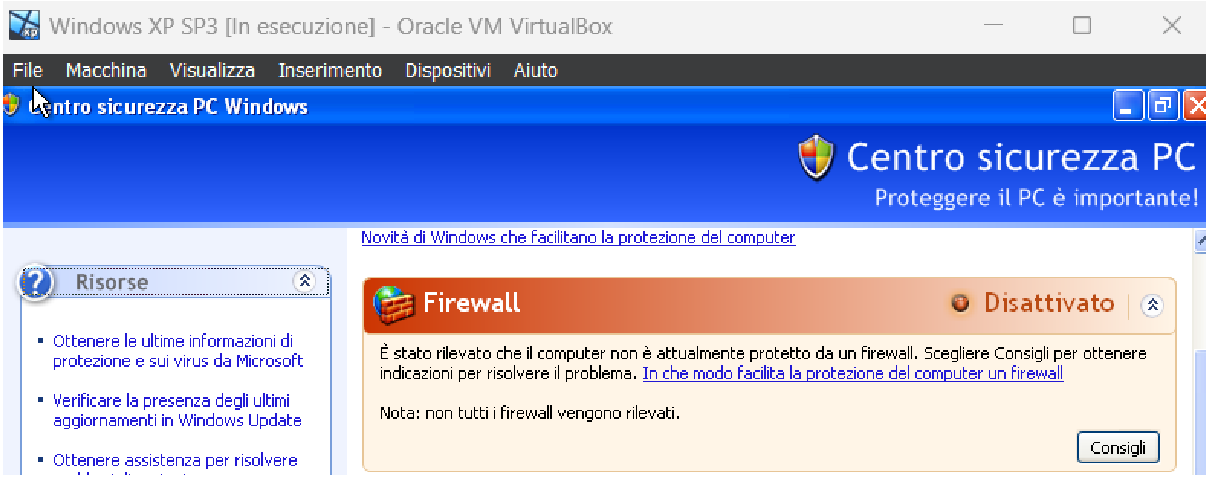
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.10.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 09:05 EDT
Nmap scan report for 192.168.10.20
Host is up (0.0023s latency).
All 1000 scanned ports on 192.168.10.20 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:4A:20:37 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.89 seconds
```

Analysis

- Visibility: All 1000 scanned TCP ports were filtered, indicating that the firewall is blocking or filtering incoming scan requests.

- Conclusion: The firewall on the Windows XP target machine effectively hides the open ports and services from the Nmap scan, preventing any useful information from being gathered.

Scan 2: Firewall Off

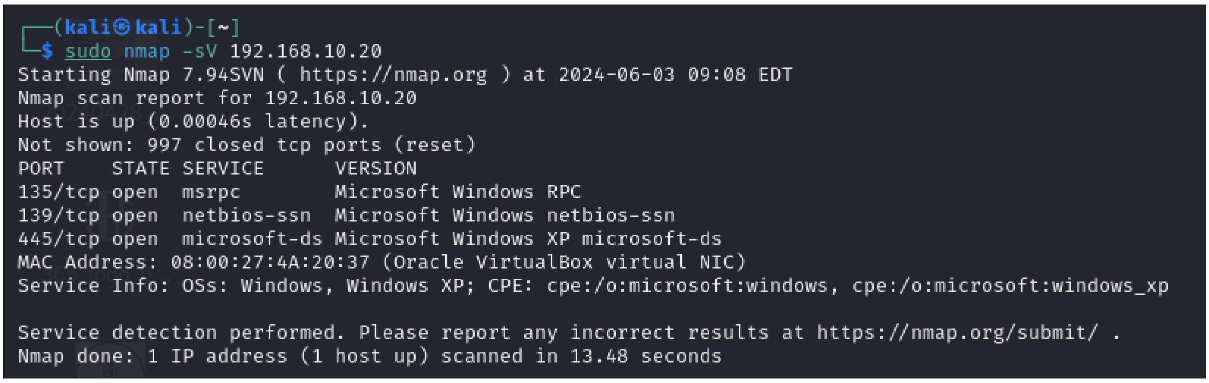

Windows XP SP3 [In esecuzione] - Oracle VM VirtualBox
File
Macchina
Visualizza
Inserimento
Dispositivi
Aiuto
Centro sicurezza PC Windows
Centro sicurezza PC
Proteggere il PC è importante!
Risorse
Firewall
Disattivato
Consigli

Novità di Windows che facilitano la protezione del computer

- Ottenere le ultime informazioni di protezione e sui virus da Microsoft
- Verificare la presenza degli ultimi aggiornamenti in Windows Update
- Ottenere assistenza per risolvere

È stato rilevato che il computer non è attualmente protetto da un firewall. Scegliere Consigli per ottenere indicazioni per risolvere il problema. In che modo facilita la protezione del computer un firewall

Nota: non tutti i firewall vengono rilevati.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.10.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 09:08 EDT
Nmap scan report for 192.168.10.20
Host is up (0.00046s 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: 08:00:27:4A:20:37 (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 13.48 seconds
```

Analysis

- Visibility: With the firewall turned off, Nmap was able to detect several open ports and services:

  -Port 135 (MSRPC): Microsoft RPC endpoint mapper.

  - Port 135 (MSRPC): Microsoft RPC endpoint mapper.

  - Port 445 (Microsoft-DS): Indicates file sharing and SMB services.

- Conclusion: Disabling the firewall exposes the open ports and services, allowing Nmap to gather detailed information about the running services on the target machine.

Comparative Analysis

Firewall On	All ports filtered	No services detected	Low
Firewall Off	Ports 80, 135, 445	HTTP, MSRPC, Microsoft-DS	High

Conclusion

The experiment clearly demonstrates the effectiveness of the Windows XP firewall in concealing open ports and services from network scans. When the firewall is enabled, Nmap is unable to detect any open ports, resulting in all scanned ports being marked as filtered. Conversely, with the firewall disabled, Nmap successfully identifies multiple open ports and associated services.

This highlights the importance of a properly configured firewall in enhancing the security posture of a system by reducing its visibility to potential attackers conducting reconnaissance activities.