

ESERCITAZIONE WEEK 18 DAY2

1. Firewall di Windows XP disattivato

```
└─$ nmap -sV 192.168.50.100 -o /home/kali/report1.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-05 12:17 EST
Nmap scan report for 192.168.50.100
Host is up (0.00022s 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 7.43 seconds
```

La macchina attaccante è in grado di rilevare le 3 porte aperte e i relativi servizi con versione.

Rileva anche il sistema operativo.

Non mostra le 997 porte tcp chiuse.

2. Firewall di Windows XP attivato

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.50.100 -o /home/kali/report2.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-05 12:19 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
```

Non riesce ad eseguire la scansione perché il ping è bloccato. Allora si usa la option -Pn:

```
(kali@kali)-[~]
└─$ nmap -Pn -sV 192.168.50.100 -o /home/kali/report2.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-05 12:20 EST
Stats: 0:02:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 66.00% done; ETC: 12:23 (0:01:09 remaining)
Nmap scan report for 192.168.50.100
Host is up.
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

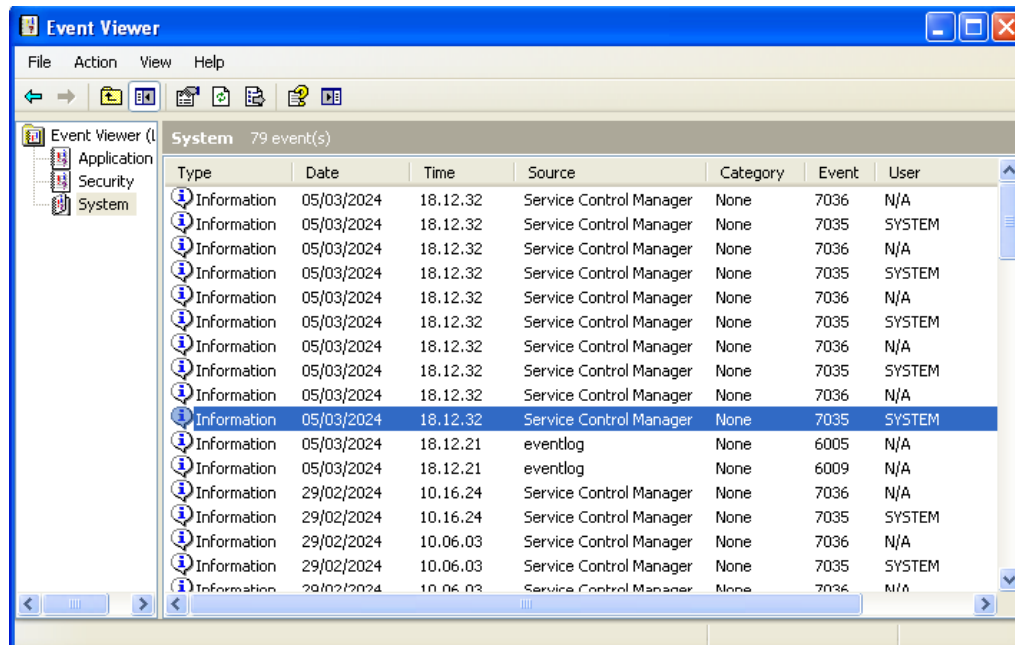
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.56 seconds

(kali@kali)-[~]
```

Stavolta ovviamente non riesce a rilevare le porte precedentemente trovate, rilevando la presenza di 1000 porte filtrate.

Probabilmente le regole del firewall sono tali che su tutte le porte viene bloccato il traffico dalla sorgente attaccante.

Log di eventi:



Type	Date	Time	Source	Category	Event	User
Information	05/03/2024	18.12.32	Service Control Manager	None	7036	N/A
Information	05/03/2024	18.12.32	Service Control Manager	None	7035	SYSTEM
Information	05/03/2024	18.12.32	Service Control Manager	None	7036	N/A
Information	05/03/2024	18.12.32	Service Control Manager	None	7035	SYSTEM
Information	05/03/2024	18.12.32	Service Control Manager	None	7036	N/A
Information	05/03/2024	18.12.32	Service Control Manager	None	7035	SYSTEM
Information	05/03/2024	18.12.32	Service Control Manager	None	7036	N/A
Information	05/03/2024	18.12.32	Service Control Manager	None	7035	SYSTEM
Information	05/03/2024	18.12.32	Service Control Manager	None	7036	N/A
Information	05/03/2024	18.12.32	Service Control Manager	None	7035	SYSTEM
Information	05/03/2024	18.12.21	eventlog	None	6005	N/A
Information	05/03/2024	18.12.21	eventlog	None	6009	N/A
Information	29/02/2024	10.16.24	Service Control Manager	None	7036	N/A
Information	29/02/2024	10.16.24	Service Control Manager	None	7035	SYSTEM
Information	29/02/2024	10.06.03	Service Control Manager	None	7036	N/A
Information	29/02/2024	10.06.03	Service Control Manager	None	7035	SYSTEM
Information	29/02/2024	10.06.03	Service Control Manager	None	7036	N/A

Non sono visibili eventi relativi alle attività svolte.