

Security Operation: azioni preventive

Sommario

Traccia esercizio principale	2
Svolgimento esercizio	3
Configurazione del laboratorio	3
Scansione	3
Analisi dei risultati delle scansioni	4
Analisi Log di Windows.....	4

Traccia esercizio principale

Le azioni preventive mirano a ridurre la possibilità di attacchi provenienti dall'esterno.

Abbiamo visto che a livello di rete, possiamo configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

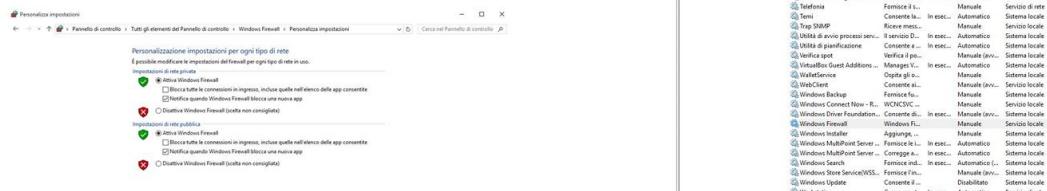
La macchina Windows, che abbiamo utilizzato, ha di default il **Firewall disabilitato**.

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. Assicuratevi che il Firewall sia disattivato sulla macchina Windows
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch `-sV`, per la service detection e `-o nomefilereport` per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch `-sV`.
5. Trovare le eventuali differenze e motivarle.

Attivazione Windows Firewall:

- andare in Servizi
- cercare il servizio Windows Firewall
- impostare il tipo di avvio in Manuale
- Applica
- Avvia
- Abilitare il firewall da Pannello di controllo\Tutti gli elementi del Pannello di controllo\Windows Firewall\Personalizza impostazioni



Per disattivare eseguire i comandi inversi

Traccia esercizio facoltativo

Monitorare i log di Windows durante queste operazioni:

1. Quali log vengono modificati? (se vengono modificati)
2. Cosa si riesce a trovare?

Svolgimento esercizio

Configurazione del laboratorio

Si è preferito impostare gli indirizzi in IP statico

- Kali Linux IP statico: 192.168.11.111
- Windows 7 IP statico: 192.168.11.107

Scansione

Si effettua una scansione con nmap.

Firewall Off: **nmap -sV -oN firewalloff.txt 192.168.11.107**

-oN: Salva l'output in un file di testo leggibile (formato standard).

```
(kali㉿kali)-[~/Desktop]
$ nmap -sV -oN firewalloff.txt 192.168.11.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-05 19:31 CET
Nmap scan report for 192.168.11.107
Host is up (0.0011s latency).

Not shown: 990 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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:9B:5C:E9 (Oracle VirtualBox virtual NIC)
Service Info: Host: CORSO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.54 seconds
```

Firewall On: **nmap -sV -oN firewallon.txt 192.168.11.107**

```
(kali㉿kali)-[~/Desktop]
$ nmap -sV -oN firewallon.txt 192.168.11.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-05 19:33 CET
Nmap scan report for 192.168.11.107
Host is up (0.00052s latency).

Not shown: 990 filtered tcp ports (no-response)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:9B:5C:E9 (Oracle VirtualBox virtual NIC)
Service Info: Host: CORSO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.87 seconds
```

Analisi dei risultati delle scansioni

The screenshot shows two terminal windows side-by-side. The left window is titled 'firewall attivo' and the right window is titled 'firewall disattivo'. Both windows display Nmap scan reports for the IP address 192.168.11.107.

firewall attivo (Left Window):

```
1 # Nmap 7.94SVN scan initiated Tue Nov 5 19:33:07 2024 as: /usr/lib/nmap/nmap --privileged -sV -oN firewallon.txt 192.168.11.107
2 Nmap scan report for 192.168.11.107
3 Host is up (0.00052s latency).
4 Not shown: 990 filtered tcp ports (no-response)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
9 5357/tcp   open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10 49152/tcp open  msrpc   Microsoft Windows RPC
11 49153/tcp open  msrpc   Microsoft Windows RPC
12 49154/tcp open  msrpc   Microsoft Windows RPC
13 49155/tcp open  msrpc   Microsoft Windows RPC
14 49156/tcp open  msrpc   Microsoft Windows RPC
15 49157/tcp open  msrpc   Microsoft Windows RPC
16 MAC Address: 08:00:27:9B:5C:E9 (Oracle VirtualBox virtual NIC)
17 Service Info: Host: CORSO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
18
19 Service detection performed. Please report any incorrect results at https://nmap.org/submit/
20 # Nmap done at Tue Nov 5 19:34:24 2024 -- 1 IP address (1 host up) scanned in 77.87 seconds
21 |
```

firewall disattivo (Right Window):

```
1 # Nmap 7.94SVN scan initiated Tue Nov 5 19:31:06 2024 as: /usr/lib/nmap/nmap --privileged -sV -oN firewalloff.txt 192.168.11.107
2 Nmap scan report for 192.168.11.107
3 Host is up (0.0011s latency).
4 Not shown: 990 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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
9 5357/tcp   open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10 49152/tcp open  msrpc   Microsoft Windows RPC
11 49153/tcp open  msrpc   Microsoft Windows RPC
12 49154/tcp open  msrpc   Microsoft Windows RPC
13 49155/tcp open  msrpc   Microsoft Windows RPC
14 49156/tcp open  msrpc   Microsoft Windows RPC
15 49157/tcp open  msrpc   Microsoft Windows RPC
16 MAC Address: 08:00:27:9B:5C:E9 (Oracle VirtualBox virtual NIC)
17 Service Info: Host: CORSO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
18
19 Service detection performed. Please report any incorrect results at https://nmap.org/submit/
20 # Nmap done at Tue Nov 5 19:32:22 2024 -- 1 IP address (1 host up) scanned in 76.54 seconds
21 |
```

A yellow arrow points from the text 'differenza' located below the windows to the line '4 Not shown: 990 filtered tcp ports (no-response)' in the left window and to the line '4 Not shown: 990 closed tcp ports (reset)' in the right window.

La differenza principale tra le due scansioni riguarda lo stato delle porte non mostrate.

- Firewall attivo: Nmap riporta che **990 porte sono filtrate** (no-response), il che significa che il firewall ha bloccato o ignorato i pacchetti di Nmap su queste porte.
- Firewall disattivo: Nmap riporta che **990 porte sono chiuse** (reset), il che significa che le porte non sono filtrate dal firewall, ma semplicemente non sono in ascolto su alcun servizio. Qui Nmap è riuscito a ottenere una risposta, anche se negativa (reset dei pacchetti).

Analisi Log di Windows

Non sono stati rilevati eventi nei log che indichino azioni specifiche del firewall in risposta alla scansione Nmap. Il firewall è stato attivato alle 20:55:41, ma non ci sono log successivi che mostrino attività di blocco o monitoraggio delle connessioni. È possibile che il firewall non sia configurato per registrare tali eventi, o che la scansione sia stata eseguita prima che il firewall fosse completamente operativo.