Traccia:

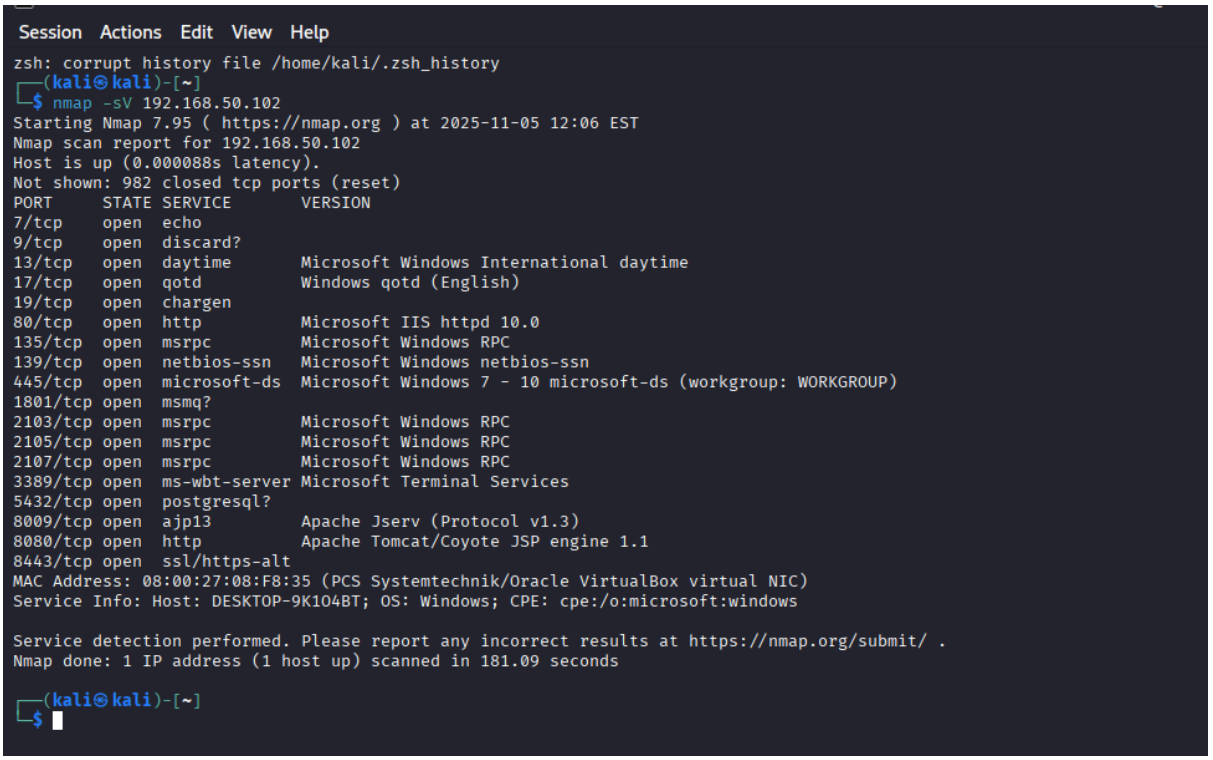
Le azioni preventive mirano a ridurre la possibilità di attacchi provenienti dall'esterno.
Abbiamo visto che a livello di rete, possiamo configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

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.

Svolgimento:
scansione su nmap con firewall disabilitato



con il windows firewall disabilitato possiamo vedere dalla scansione di nmap le diverse porte aperte i servizi e la versione dei servizi.

scansione su nmap con firewall abilitato:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 12:35 EST
Nmap scan report for 192.168.50.102
Host is up (0.0011s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: 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 93.81 seconds
```

Con il firewall abilitato possiamo vedere che rispetto all'immagine precedente ha trovato molte meno porte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 13:08 EST
Nmap scan report for 192.168.50.102
Host is up (0.00011s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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)
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; 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 93.59 seconds
```

stessa identica cosa con il comando sV -Pn

Conclusioni:
queste scansioni con nmap prima con firewall disabilitato e poi con firewall abilitato ci hanno mostrato il vero impatto che ha la nostra macchina sulla rete.
Firewall disabilitato: nmap ha rilevato un numero significativo di porte e servizi in esecuzione questo ci indica che la macchina senza protezioni può esporre servizi che potenzialmente possono essere vulnerabili ad attacchi da parte di malintenzionati che potrebbero sfruttare queste vulnerabilità per ottenere l'accesso alla macchina ed eseguire azioni non autorizzate dal proprietario della macchina.

Firewall abilitato: in questo caso abbiamo visto che nmap rileva molte meno porte e quindi molte delle porte viste in precedenza con il firewall disabilitato potrebbero essere essere filtrate o completamente nascoste, questo ci fa capire l'importanza di un firewall che blocca preventivamente il traffico in ingresso che non sia stato autorizzato impedendo a nmap di identificare alcune porte e quindi anche la natura dei servizi sottostanti a queste porte, con il firewall abilitato le possibilità di una attacco si riduce.
Quindi in conclusione possiamo dire che il firewall svolge un importante ruolo per limitare la visibilità della macchina verso l'esterno, limitando quindi i rischi associati a servizi vulnerabili a qualche attacco, ovviamente concludo col dire che impostando delle regole fatte ad hoc dalle impostazioni del firewall si può limitare ulteriormente l'esposizione garantendo quindi il traffico necessario e bloccando tutto il resto.