

Esercizio 18-03-24

INDICE

1. Traccia Esercizio
2. Requisiti laboratorio
3. Inizio scansione
4. Seconda scansione
5. Ultima scansione
6. Conclusioni



EPICODE

Traccia Esercizio 18-03-24

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP 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 XP.
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch -sV, per la service detection e -o nome file report per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch -sV. 5. Trovare le eventuali differenze e motivarle.

Che differenze notate? E quale può essere la causa del risultato diverso?

Requisiti laboratorio

- Configurare l'indirizzo di Windows XP come di seguito: 192.168.240.150
- Configurare l'indirizzo della macchina Kalicome di seguito: 192.168.240.100

```
(kali㉿kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255  
    inet6 fe80::a00:27ff:fea9:39c2 prefixlen 64 scopeid 0<link>  
    ether 08:00:27:a9:39:c2 txqueuelen 1000 (Ethernet)  
    RX packets 98 bytes 13319 (13.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 31 bytes 3634 (3.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

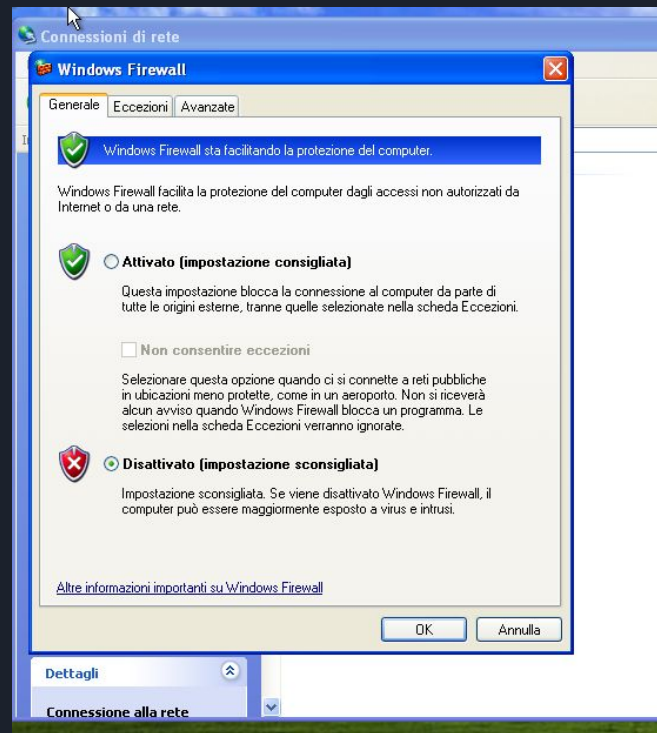
```
Prompt dei comandi  
Microsoft Windows XP [Versione 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\Documents and Settings\Administrator>ipconfig  
  
Configurazione IP di Windows  
  
Scheda Ethernet Connessione alla rete locale (LAN):  
  
    Suffisso DNS specifico per connessione: .  
    Indirizzo IP. . . . . : 192.168.240.150  
    Subnet mask . . . . . : 255.255.255.0  
    Gateway predefinito . . . . . : 192.168.240.1  
  
C:\Documents and Settings\Administrator>
```

Sulla macchina Kali Linux, utilizzando il comando “sudo nano /etc/network/interfaces”, è stato impostato l'indirizzo IP di Kali richiesto per poi riavviare il network con “sudo/etc/init.d/networking restart”; si è poi proceduto nella configurazione della macchina WindowsXP attraverso il pannello di controllo.

Inizio scansione

Come richiesto dalla traccia, con Firewall disattivato sulla macchina WindowsXP, avviamo una scansione con nmap da Kali.

```
kali@Kali: ~  
File Actions Edit View Help  
  
(kali@Kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:55 CET  
Nmap scan report for 192.168.240.150  
Host is up (0.00020s 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 20.49 seconds  
  
(kali@Kali)-[~]  
$
```



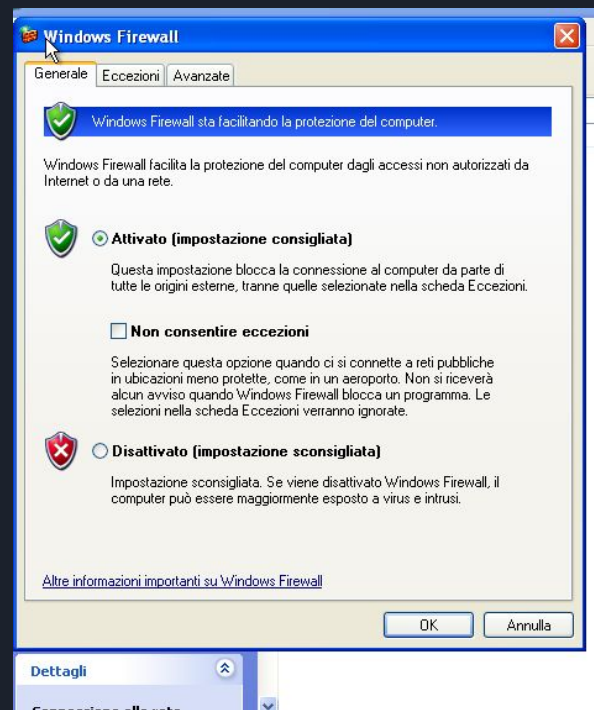
Attraverso questa scansione possiamo vedere 3 servizi in ascolto sulle porte TCP 135,139,445.

Seconda scansione

Procediamo con l'analisi con Firewall attivo sulla macchina WindowsXP, e avviamo nuovamente la scansione con nmap da Kali.

```
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:56 CET  
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 3.17 seconds
```

Con questa nuova scansione possiamo vedere una risposta diversa. Le uniche informazioni che riusciamo a reperire sono che la macchina potrebbe non essere accesa, oppure che “qualcosa” sta bloccando la mappatura di nmap. Possiamo dedurre che il Firewall sta bloccando il traffico in entrata con protocollo ICMP: ovvero il ping.



Ultima scansione

Sempre con Firewall spento, seguiamo il consiglio di nmap e proviamo ad aggiungere lo switch -Pn

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150 -Pn  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 10:04 CET  
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery  
Parallel DNS resolution of 1 host. Timing: About 0.00% done  
Nmap scan report for 192.168.240.150  
Host is up.  
All 1000 scanned ports on 192.168.240.150 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 227.88 seconds  
  
(kali㉿kali)-[~]  
$ █
```

Sfruttando lo switch -Pn - la scansione evita di procedere con il ping - e passa direttamente alla scansione dei servizi: in questo caso le porte risultano **filtrate**, questo significa che non c'è risposta alle richieste dello scanner. Possiamo concludere dicendo che il Firewall sta bloccando l'accesso alle porte.



Conclusioni

Una rete sicura blocca le tecniche di scansione e avvisa quando viene rilevata una scansione. I Firewall bloccano i tentativi di scansione o eliminano le risposte ai pacchetti di richiesta. I sistemi di rilevamento delle intrusioni (**IDS**) monitorano l'attività della rete e degli host e creano avvisi quando il traffico corrisponde a firme predefinite. La maggior parte delle tecniche di scansione sono facili da rilevare e fanno scattare facilmente gli allarmi degli IDS.

Nel nostro caso possiamo affermare che il Firewall sta preventivamente riducendo i rischi di attacchi dall'esterno, rendendo inaccessibili dall'esterno i servizi sulle porte scannerizzate in precedenza, con firewall disattivato, che sarebbero altrimenti vulnerabili.