Esercizio 18-03-24

INDICE

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:

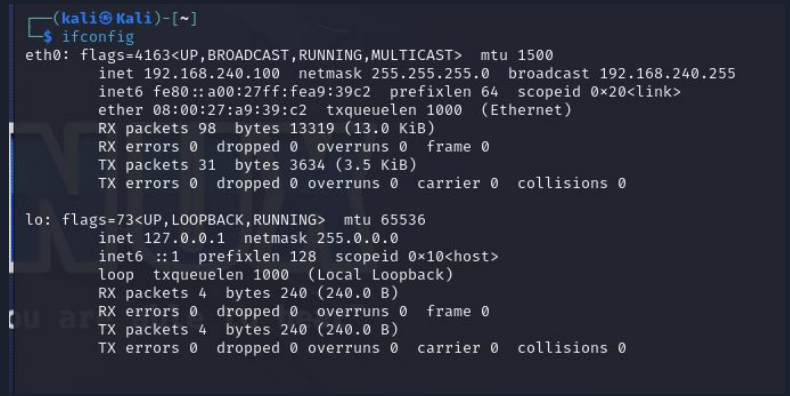
1. Assicuratevi che il Firewall sia **disattivato** sulla macchina Windows XP.
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch–sV, per la service detection e -o nome file report per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate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

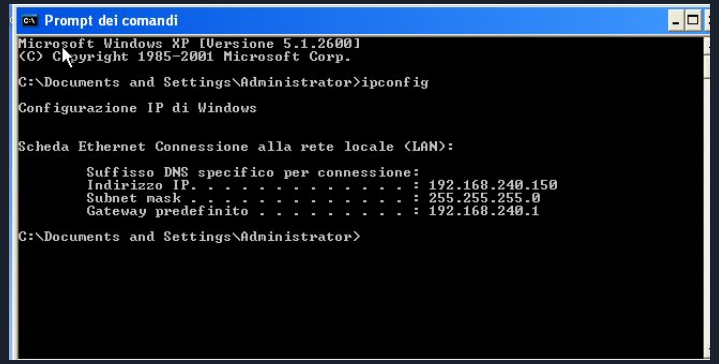
Che differenze notate? E quale può essere la causa del risultato diverso?

EPICODE

Requisiti laboratorio

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

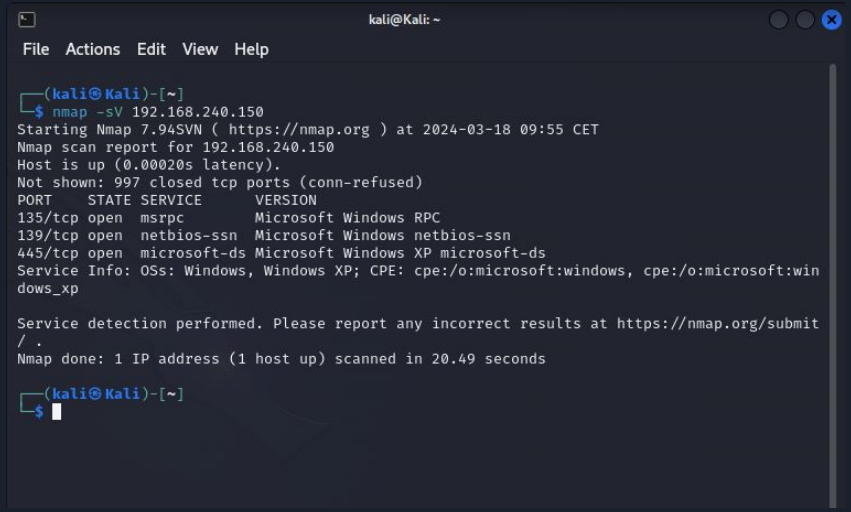


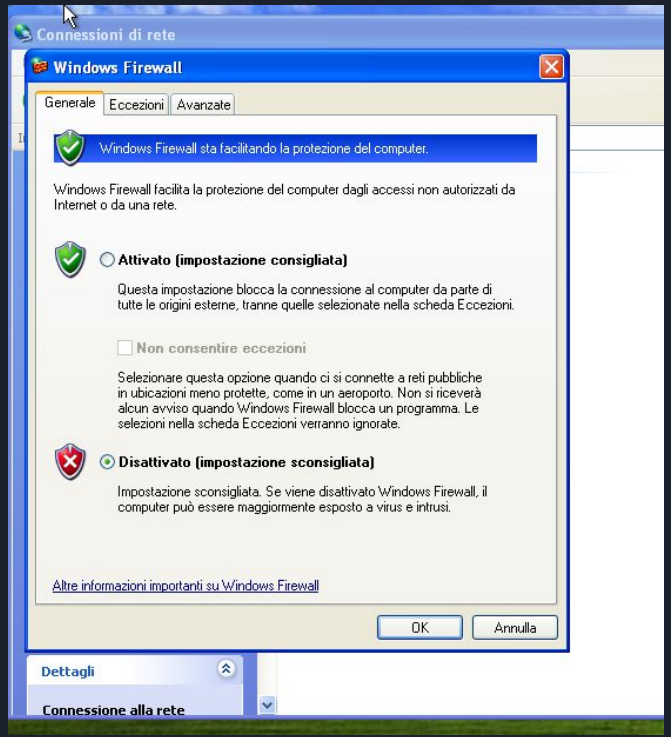


Sulla macchina Kali Linux, utilizzando il comando "sudo nano /etc/network/interfaces", è stato impostato l'indirizzo IP di Kali richiesto per poi riavviare il network con "sudo/etc/init.d/networking restart"; si è poi proceduto nella configurazione della macchina WindowsXP attraverso il pannello di controllo.

Inizio scansione

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



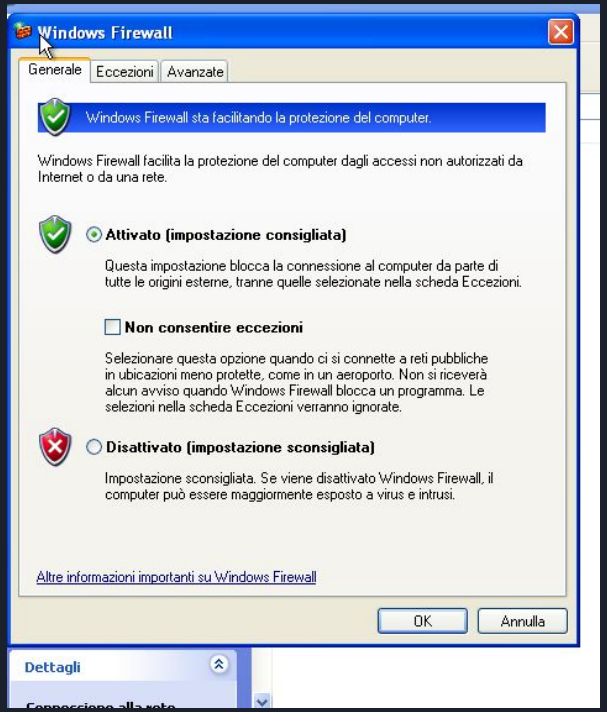


Attraverso questa scansione possiamo vedere 3 servizi in ascolto sulle porte TCP 135,139,445.

Seconda scansione

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

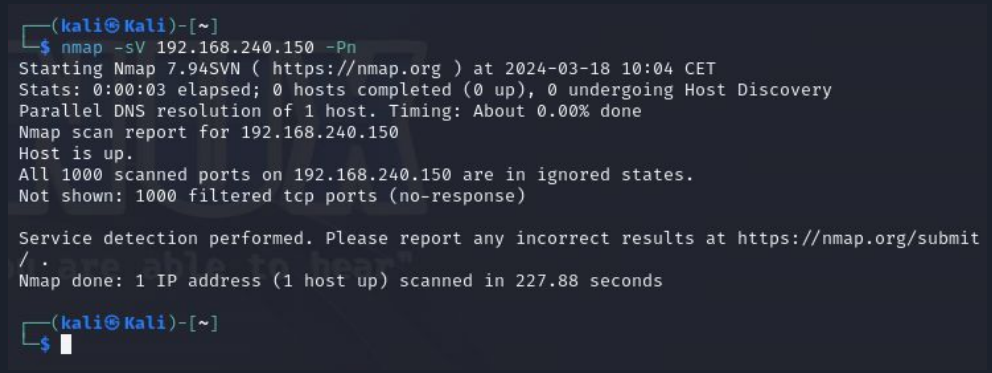
```
┌──(kali㉿Kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:56 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.17 seconds

┌──(kali㉿Kali)-[~]
└─$
```



Con questa nuova scansione possiamo vedere una risposta diversa. Le uniche informazione 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



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 scannerizzare in precedenza, con firewall disattivato, che sarebbero altrimenti vulnerabili.