Manuel Di Gangi

S9_L1

Security Operation: azioni preventive

18 marzo 2024

INDICE

1. Traccia

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 -o nomefilereportper 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.

2. Nozioni Teoriche

Un firewall è un componente di sicurezza informatica progettato per monitorare e controllare il traffico di rete, sia in entrata che in uscita, tra una rete privata o un dispositivo e una rete pubblica, come Internet. Il suo scopo principale è quello di proteggere una rete o un dispositivo da accessi non autorizzati, attacchi informatici, malware e altre minacce.

Il firewall può essere implementato a livello hardware tramite dispositivi dedicati, come router o appliance firewall, oppure a livello software, utilizzando software installati direttamente sui dispositivi o sui server. Esso esamina i pacchetti di dati che attraversano la rete e applica regole di sicurezza predefinite per determinare se il traffico deve essere consentito o bloccato in base a vari criteri, come l'indirizzo IP, il tipo di protocollo o la porta di destinazione.

Nmap è uno strumento di scansione di rete ampiamente utilizzato per scoprire dispositivi e servizi in una rete, nonché per valutare la sicurezza della rete stessa. Con Nmap, gli utenti possono eseguire una varietà di scansioni, come la scansione delle porte aperte, la rilevazione del sistema operativo e molte altre attività di analisi delle reti, fornendo informazioni dettagliate sulla topologia della rete e sullo stato dei dispositivi e dei servizi in essa presenti.

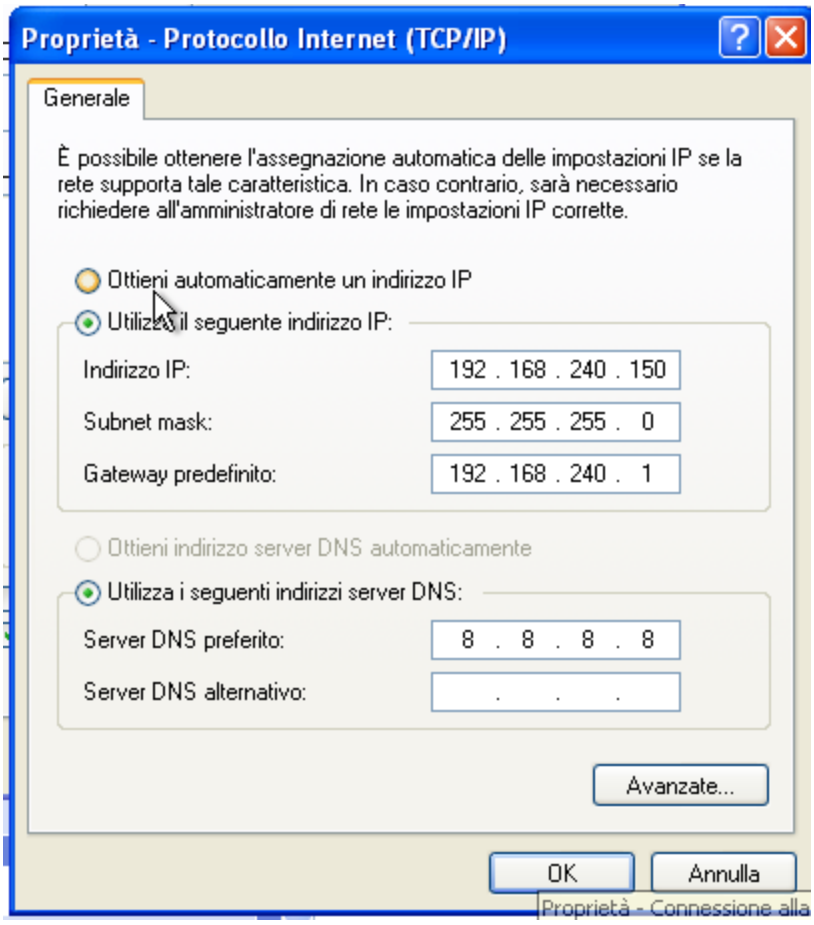
Una vulnerabilità in un sistema informatico è una debolezza o una falla nella progettazione, nell'implementazione o nella configurazione del sistema che può essere sfruttata da un attaccante per compromettere l'integrità, la disponibilità o la riservatezza dei dati, dei servizi o del sistema stesso. In sostanza, una vulnerabilità rappresenta un punto di ingresso per un attaccante che può essere utilizzato per infiltrarsi nel sistema e compiere azioni dannose o non autorizzate. Le vulnerabilità possono derivare da difetti nel software, errori di configurazione, mancanza di aggiornamenti di sicurezza o altri fattori che rendono il sistema suscettibile ad attacchi informatici.

3. Configurazione laboratorio VM

Ci rechiamo sul file “interfaces” contenente i dati delle interfacce di rete mediante il seguente comando e li modifichiamo

```
sudo nano /etc/network/interfaces
```

1. Configurazione Windows XP



2. Configurazione Kali Linux

```
┌──(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:fe83:203e  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:83:20:3e  txqueuelen 1000  (Ethernet)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 4070 (3.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Salviamo il file e riavviamo il sistema per applicare i cambiamenti con il comando:

sudo reboot

3. Verifica funzionamento rete

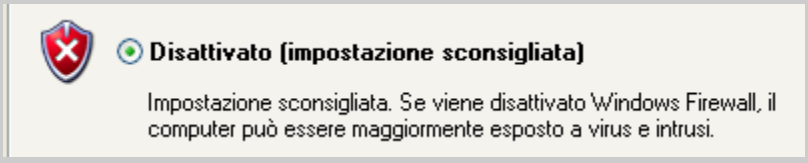
Con il comando ***ping*** verifichiamo la comunicazione tra le due macchine

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.259 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.341 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.346 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.281 ms
```

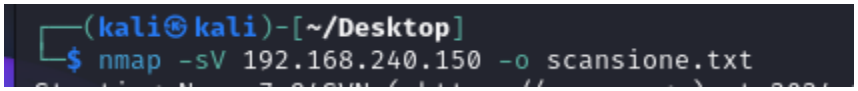
```
C:\Documents and Settings\Administrator>ping 192.168.240.100

Esecuzione di Ping 192.168.240.100 con 32 byte di dati:

Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
```

4. Scansione di Windows - Firewall Inattivo

Prima di effettuare la scansione ci rechiamo sul pannello di controllo di windows e disattiviamo il firewall.



Avviamo una scansione tramite il comando ***nmap*** e reindirizziamo l'output sul file scansione.txt

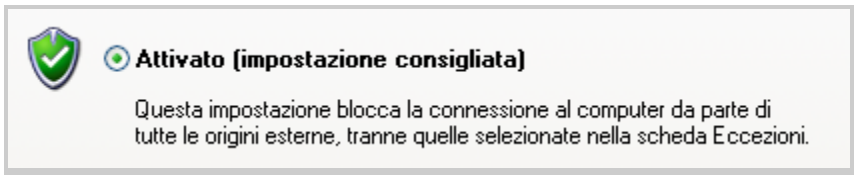



```
1 # Nmap 7.94SVN scan initiated Mon Mar 18 07:27:55 2024 as: nmap -sV -o scansione1.txt
  192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00056s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
5 PORT    STATE SERVICE      VERSION
6 135/tcp open  msrpc        Microsoft Windows RPC
7 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
9 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/
  o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/
  submit/ .
12 # Nmap done at Mon Mar 18 07:28:16 2024 -- 1 IP address (1 host up) scanned in 21.14
  seconds
13
```

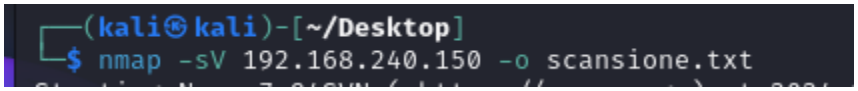
La scansione ha rilevato dei servizi attivi sulle porte 135, 139 e 445.

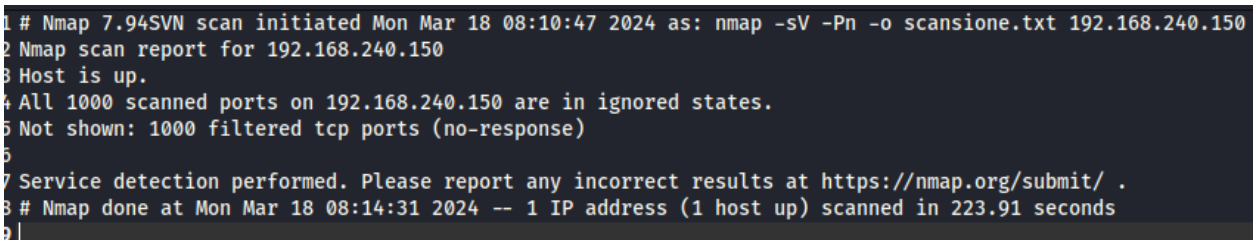
5. Scansione di Windows - Firewall Attivo

Prima di effettuare la scansione ci rechiamo sul pannello di controllo di windows e disattiviamo il firewall.



Avviamo una nuova scansione tramite il comando ***nmap*** e reindirizziamo l'output sul file scansione.txt





All'interno del file viene riportato che su tutte le mille porte analizzate, kali non ha ricevuto risposta, da qui deduciamo che le porte sono filtrate da un firewall che ignora le richieste esterne.

6. Conclusioni

L'abilitazione del Firewall di Windows XP sta di fatto bloccando la scansione dall'esterno verso i servizi attivi sulla macchina Windows XP. Come visto nelle settimane precedenti su Windows XP sono presenti diverse vulnerabilità che siamo andati a sfruttare tramite Metasploit. Possiamo affermare che il Firewall sta preventivamente riducendo rischi di attacchi dall'esterno, rendendo inaccessibili i servizi sulle porte 135,139,445.