Security Operation: azioni preventive

Sommario

Introduzione 1
Impostazione indirizzi IP statici delle macchine virtuali 1
Macchina attaccante Kali Linux 1
Macchina target Windows XP 2
Test di comunicazione tra le macchine 3
Scansione Nmap con firewall disattivato 3
Scansione Nmap con firewall attivato 4
Cosa è un firewall? 4

Introduzione

Nell'esercizio di oggi mi è stato richiesto di verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno.

Requisiti laboratorio:

IP Kali Linux: 192.168.240.100

IP Windows XP: 192.168.240.150

Impostazione indirizzi IP statici delle macchine virtuali

Macchina attaccante Kali Linux

Per modificare l'indirizzo IP come da traccia, apro il terminale e inserisco il comando **sudo nano /etc/network/interfaces**, il quale mi permetterà di modificare il file di configurazione dell'interfaccia di rete.

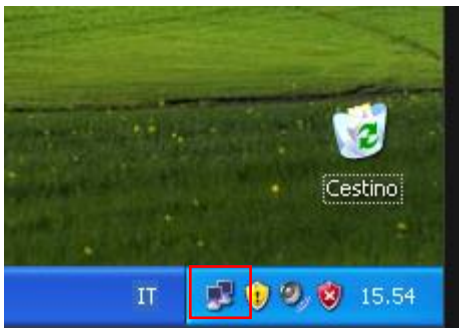
```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/network/interfaces
```

Modifico l'indirizzo accanto la voce address con 192.168.240.100

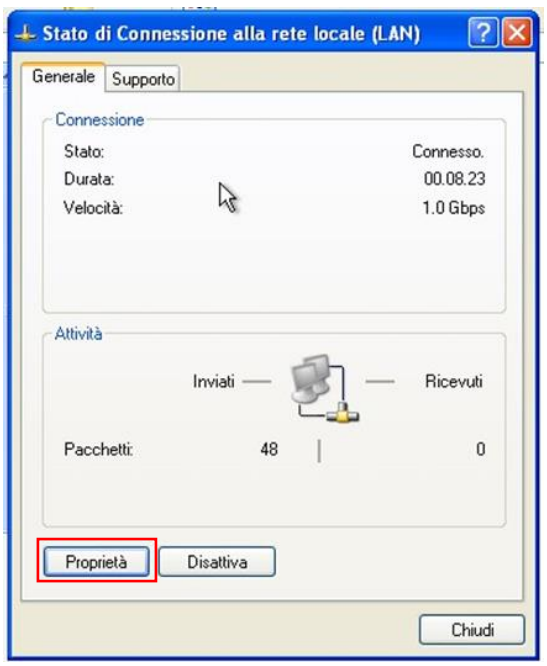
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100
netmask 255.255.255.0
network 192.168.240.0
broadcast 192.168.240.255
gateway 192.168.240.1
dns-nameservers 8.8.8.8
```

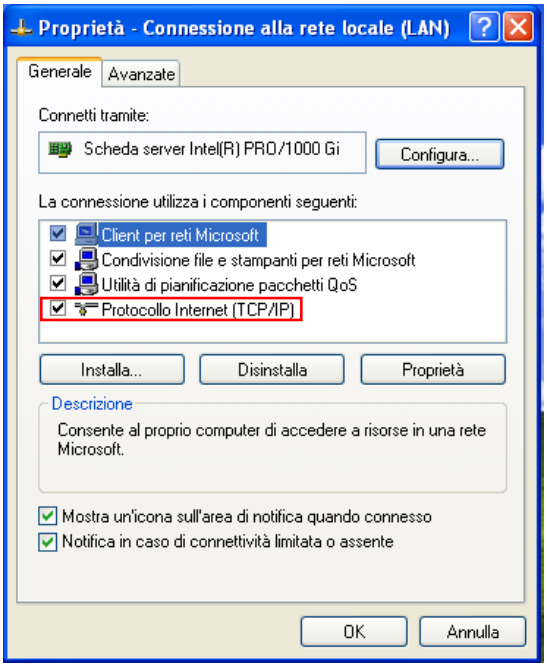
Macchina target Windows XP

Per modificare l'indirizzo IP della macchina target clicco prima sull'icona nel riquadro rosso nella barra applicazioni.

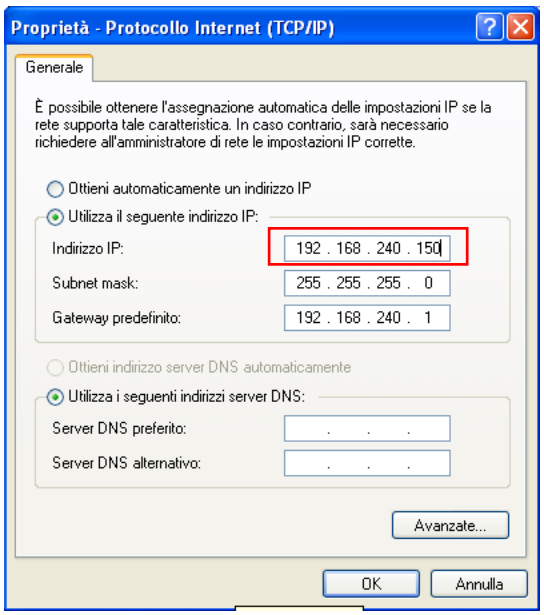


Successivamente su proprietà e infine su protocollo Internet (TCP/IP)





Inserisco quindi l'indirizzo IP 192.168.240.150 e clicco su OK.



Test di comunicazione tra le macchine

Il ping è uno strumento diagnostico che permette di verificare la connessione e la raggiungibilità di un dispositivo in una rete. Il ping invia dei pacchetti di dati chiamati echo request a un indirizzo IP e aspetta una risposta con dei pacchetti echo reply.

Quindi, verifico con il comando **ping <IP target>** se le macchine sono in grado di comunicare.

I quattro pacchetti inviati risultano correttamente trasmessi e ricevuti.

```
┌──(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=1.59 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.63 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.31 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=1.19 ms
^C
--- 192.168.240.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3014ms
rtt min/avg/max/mdev = 1.188/1.432/1.634/0.187 ms
```

Scansione Nmap con firewall disattivato

Nmap è uno strumento utilizzato per la scansione delle porte di un dispositivo. In pratica, Nmap aiuta a identificare quali porte sono aperte su un dispositivo e quali servizi di rete sono disponibili.

Per avviare la scansione inserisco nel terminale il comando **nmap -sV <indirizzo IP target>**. L'opzione -sV effettua una scansione version detection, che mi permette di recuperare anche la versione per ogni servizio attivo identificato.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 16:40 CET
Nmap scan report for 192.168.240.150
Host is up (0.0025s 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 19.81 seconds
```

Si possono notare 3 porte porte TCP sullo stato OPEN:

- TCP 135, questa porta viene utilizzata per la comunicazione tra i computer e i servizi di Windows, come il servizio di gestione remota (RPC)
- TCP 139 e 445 sono delle porte utilizzate da Windows XP per consentire ai computer di comunicare tra loro sulla stessa rete. Questa porta viene utilizzata dal protocollo SMB (Server Message Block) per la condivisione di file e stampanti.

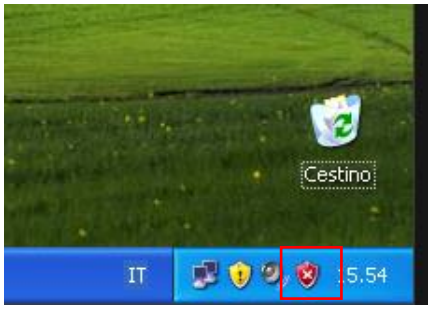
Scansione Nmap con firewall attivato

Cosa è un firewall?

Un firewall è un sistema hardware o software che monitora e protegge le reti o i dispositivi da accessi non autorizzati. Quello di Windows XP è un firewall software di tipo stateless.

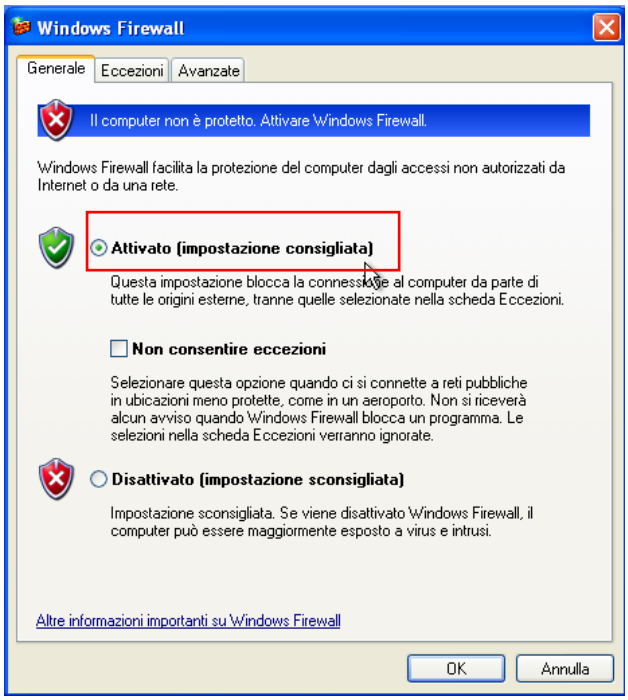
I firewall stateless utilizzano l'origine, la destinazione e altri parametri di un pacchetto di dati per determinare se i dati rappresentano una minaccia. I parametri devono essere inseriti da un amministratore o dal produttore tramite regole impostate in precedenza.

Per attivare il firewall di Windows XP clicco sull'icona nel riquadro rosso nella barra applicazioni.



Successivamente su Windows Firewall.

Infine, seleziono la spunta per attivarlo.



Ripeto la scansione con Nmap.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 16:45 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 3.18 seconds
```

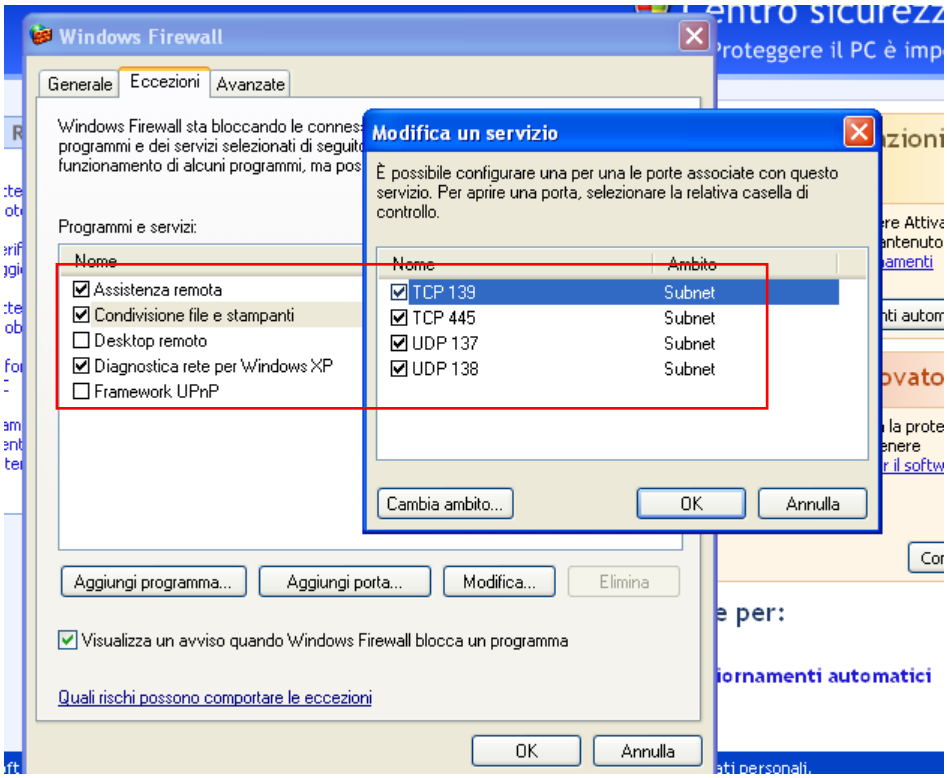
Nmap non ha effettuato la scansione perché prima di iniziarla verifica se l'host è raggiungibile con un ping. Questo succede perché il firewall ha come impostazione di default il rifiuto dei pacchetti ICMP della funzionalità ping.

Quindi aggiungo l'opzione **-Pn** per iniziare la scansione senza che verifichi col ping sia raggiungibile, essendo certo che lo sia.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 16:46 CET
Nmap scan report for 192.168.240.150
Host is up (0.0068s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
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 25.78 seconds
```

La porta 135 ora non risulta aperta perché il Firewall evidentemente è entrato in funzione. La 139 e 445 risultano ancora aperte.

Questo è dovuto a delle eccezioni presenti nel firewall che consentono appunto la condivisione di file e stampanti. Basterà disattivare la condivisione togliendo la spunta



Ed ecco che su Nmap non rileva più porte aperte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 16:53 CET
Stats: 0:01:55 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 50.50% done; ETC: 16:57 (0:01:41 remaining)
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 51.00% done; ETC: 16:57 (0:01:40 remaining)
Stats: 0:01:57 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 51.50% done; ETC: 16:57 (0:01:39 remaining)
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 215.41 seconds
```