



Esercizio S9-L1



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 in formato OVA che abbiamo utilizzato nella Unit 2 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)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch -sV.

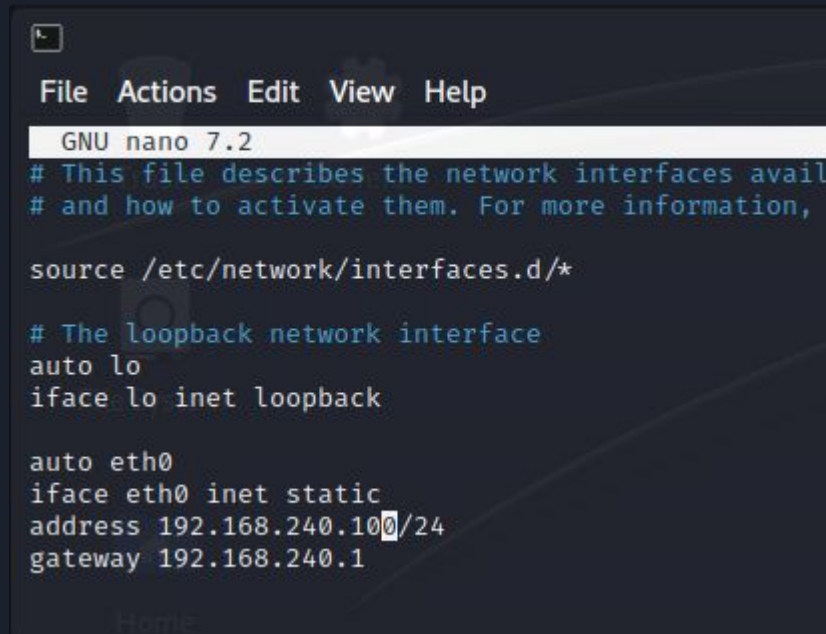
Cambio Indirizzo IP a Kali Linux:

Procediamo col cambio dell'indirizzo IP di Kali Linux; per prima cosa lanciamo da terminale il seguente comando `<<sudo nano /etc/network/interfaces>>` per accedere al file che contiene le informazioni della nostra scheda di rete e per modificare le configurazioni di rete.

Una volta fatto ciò modifichiamo il contenuto del file in modo che sia identico alle configurazioni in figura.

Le configurazioni mostrate conferiscono alla macchina il seguente indirizzo IP statico `<<192.168.240.100>>`

Quando abbiamo modificato il file lo salviamo e lo chiudiamo con `<<Ctrl + X>>` e `<<y>>` e premiamo invio. In seguito riavviamo la macchina col comando `<<sudo reboot>>` per applicare le modifiche appena effettuate.

A screenshot of the GNU nano 7.2 text editor. The editor has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The text content shows the configuration for network interfaces. It starts with a comment about the file's purpose, followed by a source directive for /etc/network/interfaces.d/*. Then, it defines the loopback interface 'lo' as 'auto lo' and 'iface lo inet loopback'. Finally, it defines the ethernet interface 'eth0' as 'auto eth0', 'iface eth0 inet static', with a fixed address of '192.168.240.100/24' and a gateway of '192.168.240.1'. The cursor is positioned at the end of the '100' in the IP address.

```
GNU nano 7.2
# This file describes the network interfaces avail
# and how to activate them. For more information,

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.1
```

Verifica del cambio dell'IP a Kali Linux:

Dopo che la macchina si è riavviata possiamo verificare che le modifiche siano state apportate correttamente digitando da terminale il comando `<<ifconfig>>` che mostra le informazioni sulla scheda di rete.

Come possiamo osservare la scheda `eth0` ha come indirizzo IP il seguente `192.168.240.100` quindi le modifiche sono state apportate correttamente.

```
File Actions Edit View Help
(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:fea7:3f55 prefixlen 64 scopeid 0<link>
    ether 08:00:27:a7:3f:55 txqueuelen 1000 (Ethernet)
    RX packets 48 bytes 5681 (5.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 2854 (2.7 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 16 bytes 1456 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 1456 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

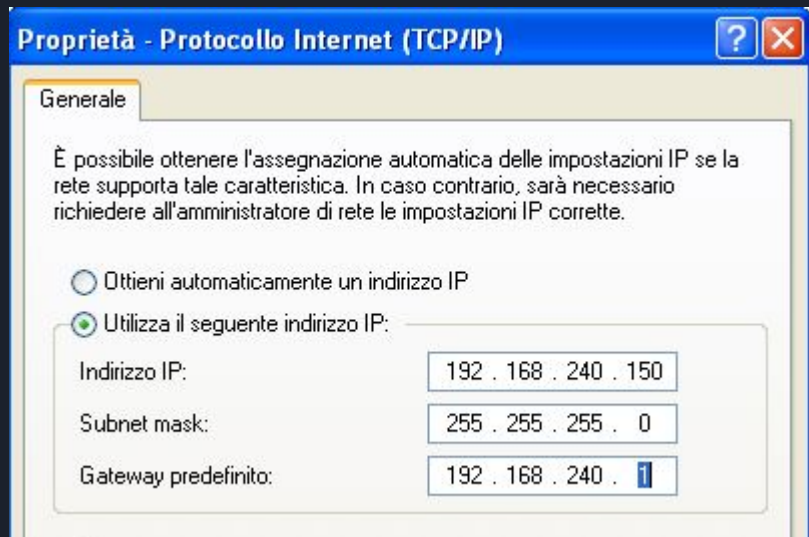
(kali@kali)-[~]
$
```

Cambio indirizzo IP a Windows XP

Per modificare l'indirizzo IP della macchina Windows XP bisogna raggiungere la finestra delle impostazioni di sistema corretta. Dopo aver acceso la macchina seguiamo il seguente path per raggiungere la finestra che ci permetterà di modificare l'indirizzo IP della macchina.

[Start>Pannello di controllo>Rete e connessioni internet>Connessioni di rete>Tasto destro sulla scheda di rete>proprietà>Tasto sinistro su Protocollo Internet(TCP/UDP)>proprietà]

Una volta raggiunta la finestra modifichiamo i valori come in figura per cambiare l'indirizzo IP al seguente <<192.168.240.150>> e riavviamo la macchina per apportare le modifiche.



Ping tra le due macchine

Dopo aver configurato entrambe le macchine dobbiamo accertarci che riescano a comunicare fra loro, per fare ciò utilizzeremo la funzione <<ping>> che ci permette di mandare dei pacchetti ad un indirizzo IP che scegliamo noi per verificare che ci sia comunicazione tra le macchine.

Da Kali mandiamo il seguente comando <<ping 192.168.240.150>> per effettuare un ping alla macchina Windows XP.

Di 5 pacchetti inviati, 5 sono stati ricevuti confermando che avviene 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=3.08 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.80 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.82 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=2.10 ms
64 bytes from 192.168.240.150: icmp_seq=5 ttl=128 time=2.02 ms
^C
— 192.168.240.150 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 1.801/2.163/3.076/0.470 ms

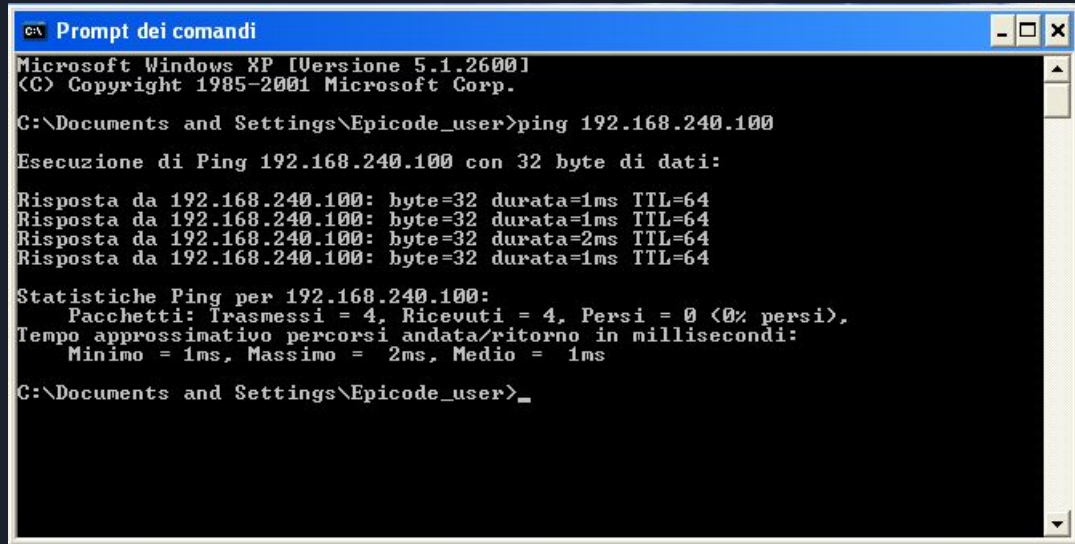
(kali@kali)-[~]
$
```

Ping tra le due macchine

Per scrupolo eseguiamo la stessa procedura anche nella direzione inversa, ovvero da Windows XP a Kali Linux.

Sulla nostra macchina Windows XP apriamo un prompt dei comandi ed inseriamo il seguente comando `<<ping 192.168.240.100>>` per eseguire un ping verso Kali Linux.

Analizzando il risultato del comando possiamo vedere che avviene lo scambio di pacchetti correttamente, confermando l'avvenuta comunicazione tra le due macchine.



```
C:\ Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>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=2ms TTL=64
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64

Statistiche Ping per 192.168.240.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 1ms, Massimo = 2ms, Medio = 1ms

C:\Documents and Settings\Epicode_user>_
```

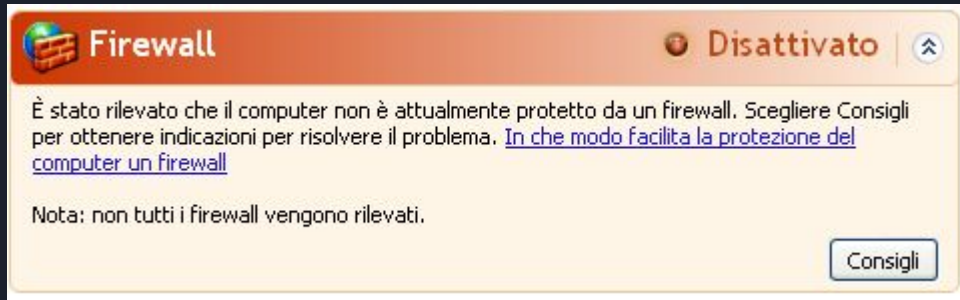
Procediamo con le scansioni

Dopo aver configurato correttamente le due macchine ed esserci accertati che comunicano fra loro senza problemi possiamo procedere con le scansioni con nmap da Kali Linux verso Windows XP.

Per prima cosa verifichiamo lo stato del firewall di Windows XP, per fare ciò apriamo il pannello di controllo e clicchiamo su Centro Sicurezza PC.

Come possiamo osservare il firewall di Windows XP è attualmente disattivato.

Preso nota dello stato del firewall torniamo su Kali e procediamo con la scansione.



Procediamo con le scansioni

Da terminale procediamo ad effettuare una scansione con nmap verso la macchina Windows XP che ci elencherà le porte attive sulla macchina target, procediamo col comando <<sudo nmap -sV 192.168.240.150>>

Osservando il risultato della scansione possiamo osservare che ci sono tre porte aperte sulla macchina Windows e sono rispettivamente la 135, la 139 e la 445.

Prendiamo nota di questi risultati e procediamo con la seconda scansione.

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.240.150
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 11:21 CET
Nmap scan report for 192.168.240.150
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
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
MAC Address: 08:00:27:E0:E6:A5 (Oracle VirtualBox virtual NIC)
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 20.06 seconds

(kali@kali)-[~]
$
```

Procediamo con le scansioni

Abbiamo appena eseguito una scansione alla macchina Windows XP mentre il suo firewall era disattivato, proviamo adesso a ripetere la scansione dopo aver attivato il firewall per osservare eventuali differenze.

Torniamo su Windows alla pagina Centro Sicurezza PC e attiviamo il firewall.

Dopo aver attivato il firewall torniamo su Kali e ripetiamo lo scan.



Firewall



Attivato



Procediamo con le scansioni

Dopo essere tornati su Kali ripetiamo la scansione col comando `<<sudo nmap -sV 192.168.240.150>>`

Osservando il risultato della scansione possiamo notare che delle 1000 porte analizzate da nmap tutte e 1000 appaiono filtrate, di conseguenza possiamo dedurre che il firewall di Windows deve avere qualche regola che dice di dropare i pacchetti quando viene effettuata la scansione. Questa ipotesi è valorizzata dal fatto che se proviamo a ripetere il ping da Kali verso Windows questa volta non andrà a buon fine e ci informerà che i pacchetti non vengono ricevuti dalla macchina Windows.

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 11:26 CET
Nmap scan report for 192.168.240.150
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E0:E6:A5 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.58 seconds

(kali@kali)-[~]
$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
^C
— 192.168.240.150 ping statistics —
25 packets transmitted, 0 received, 100% packet loss, time 24561ms
```