

SECURITY OPERATION: AZIONI PREVENTIVE

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 nomefilereport 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.

Traccia:

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

Requisiti:

Configurate l'indirizzo di Windows XP come di seguito: 192.168.240.150

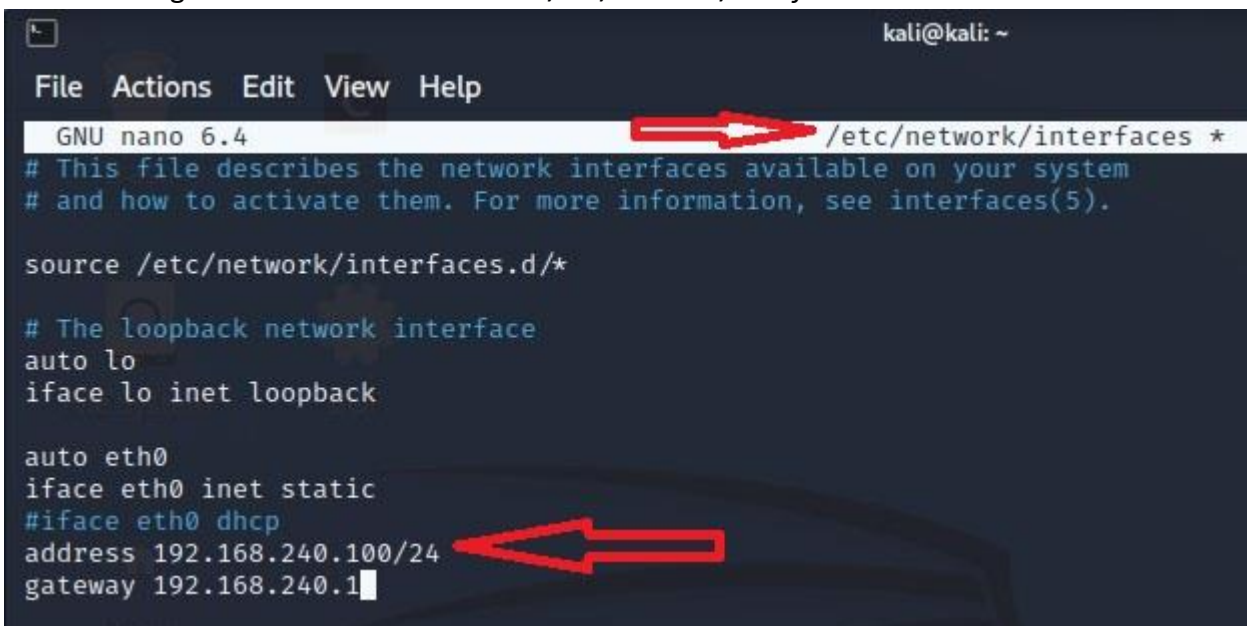
Configurate l'indirizzo della macchina Kali come di seguito: 192.168.240.100

Bonus:

Monitorare i log di Windows durante queste operazioni.

1. Quali log vengono modificati?
2. Cosa riesce a trovare?

Come richiesto, siamo andati a modificare gli IP delle macchine; per la macchina attaccante Kali, abbiamo eseguito il comando *"sudo nano /etc/network/interfaces"*.

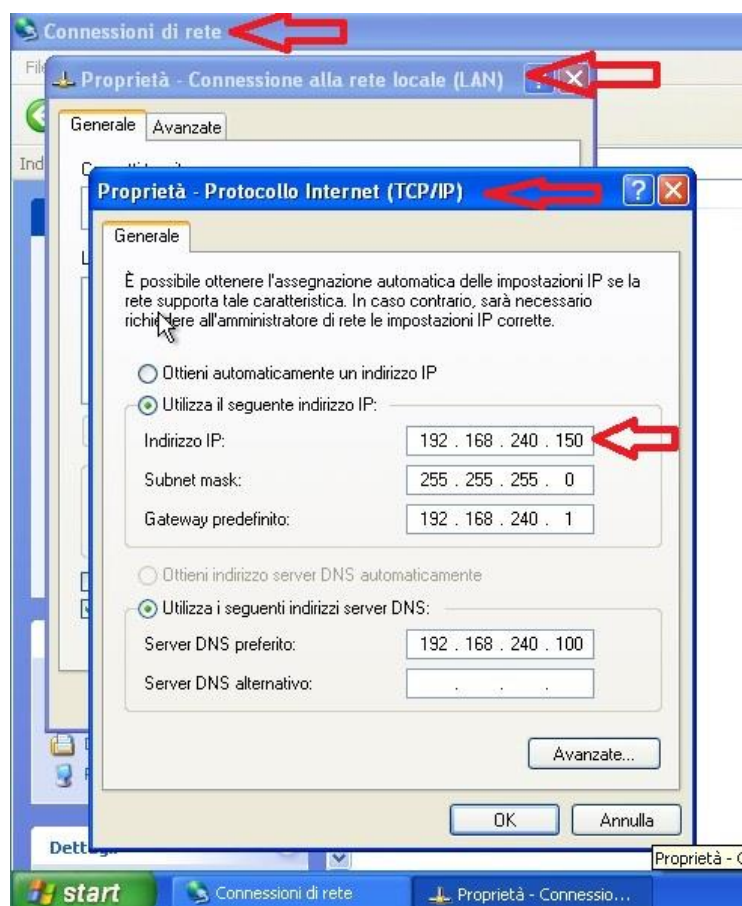


```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 6.4 /etc/network/interfaces *  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
auto eth0  
iface eth0 inet static  
#iface eth0 dhcp  
address 192.168.240.100/24  
gateway 192.168.240.1
```

Per poi riavviare il sistema con il comando “*sudo /etc/init.d/networking restart*” e controllato poi il cambio di IP tramite “*ip a*”.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nano /etc/network/interfaces  
[sudo] password for kali:  
(kali@kali)-[~]  
$ sudo /etc/init.d/networking restart  
Restarting networking (via systemctl): networking.service.  
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff  
    inet 192.168.240.100/24 brd 192.168.240.255 scope global eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fe22:464f/64 scope link  
        valid_lft forever preferred_lft forever  
(kali@kali)-[~]  
$
```

Siamo andati quindi a modificare l’indirizzo IP della macchina Windows XP tramite il percorso: *Start > Pannello di Controllo > Rete e connessioni Internet > Connessioni di Rete > Proprietà – Connessione alla rete locale (LAN) > Proprietà – Protocollo Internet (TCP/IP)*.



Abbiamo quindi controllato la giusta connessione tra le macchine con il comando di “ping”.

```
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe22:464f/64 scope link
valid_lft forever preferred_lft forever

(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=0.636 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.736 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.528 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.421 ms
64 bytes from 192.168.240.150: icmp_seq=5 ttl=128 time=0.768 ms
^Z
zsh: suspended ping 192.168.240.150

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

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ping 192.168.240.100

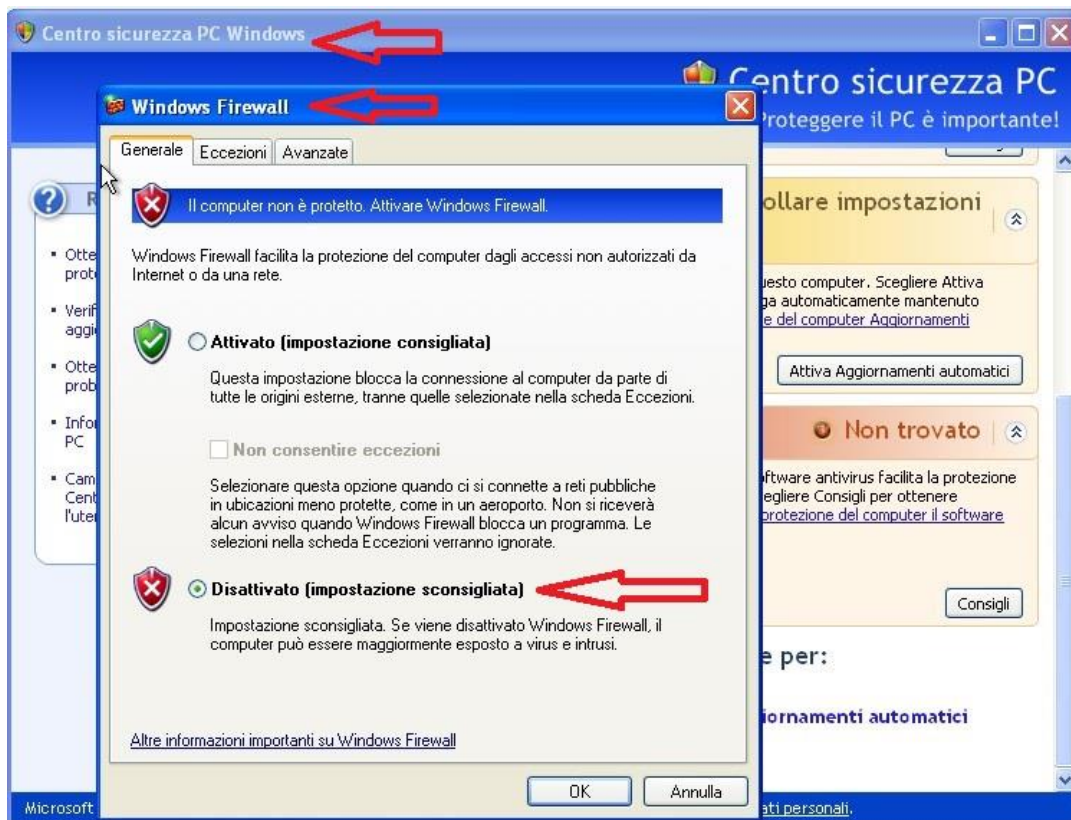
Esecuzione di Ping 192.168.240.100 con 32 byte di dati:

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<1ms 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 = 0ms, Massimo = 0ms, Medio = 0ms

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

Abbiamo quindi controllato che su Windows XP il Firewall fosse disattivato come richiesto tramite il percorso *Start > Pannello di Controllo > Centro sicurezza PC > Windows Firewall*.



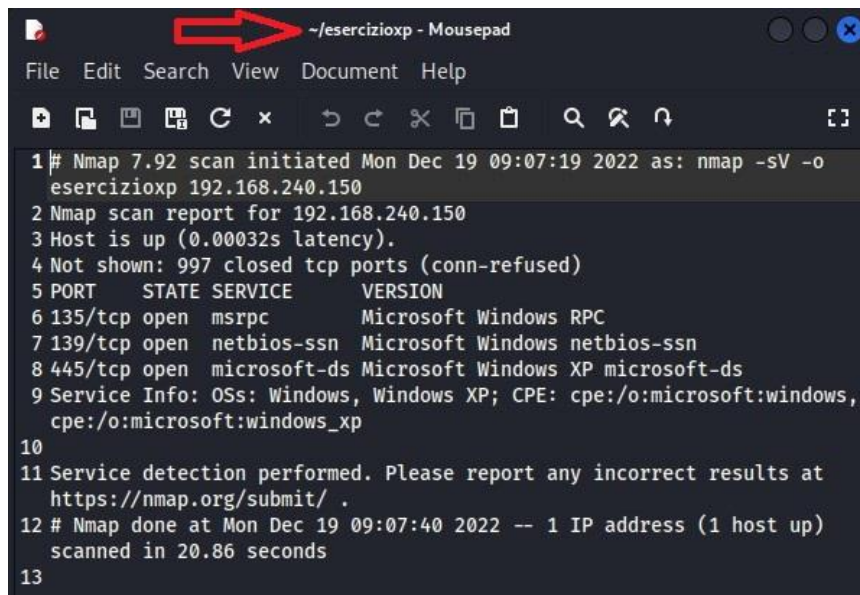
Abbiamo così avviato la nostra scansione nmap su Kali con il comando “*nmap 19.168.240.150 -sV -o esercizioxp*”.

```
(kali@kali)-[~]
$ nmap 192.168.240.150 -sV -o esercizioxp
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:19 EST
Nmap scan report for 192.168.240.150
Host is up (0.0030s 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 20.94 seconds

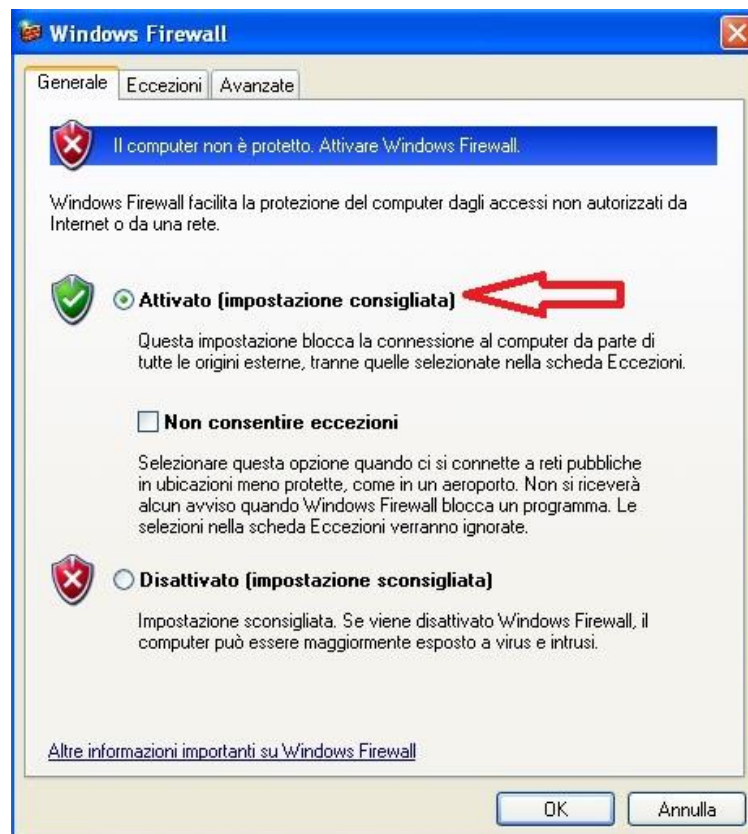
(kali@kali)-[~]
$
```


Abbiamo usato lo switch -sV per la service detection e visualizzare le versioni dei servizi attivi e lo switch -o per salvare in un file l'output.



```
1 # Nmap 7.92 scan initiated Mon Dec 19 09:07:19 2022 as: nmap -sV -o
   esercizioxp 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00032s 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 Dec 19 09:07:40 2022 -- 1 IP address (1 host up)
   scanned in 20.86 seconds
13
```

Siamo andati ad attivare il Firewall sulla macchina Windows XP, seguendo il path precedente.



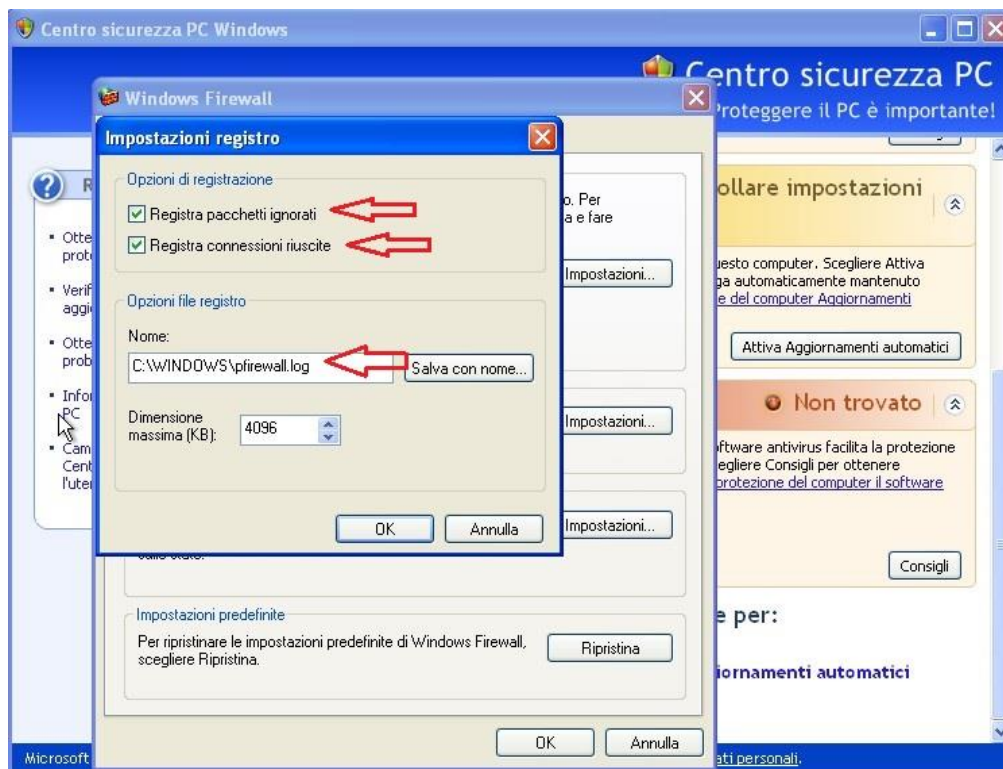
Abbiamo così riprovato la scansione con nmap.

```
(kali@kali)-[~]
$ nmap 192.168.240.150 -sV -o esercizioxp
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:21 EST
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 3.51 seconds

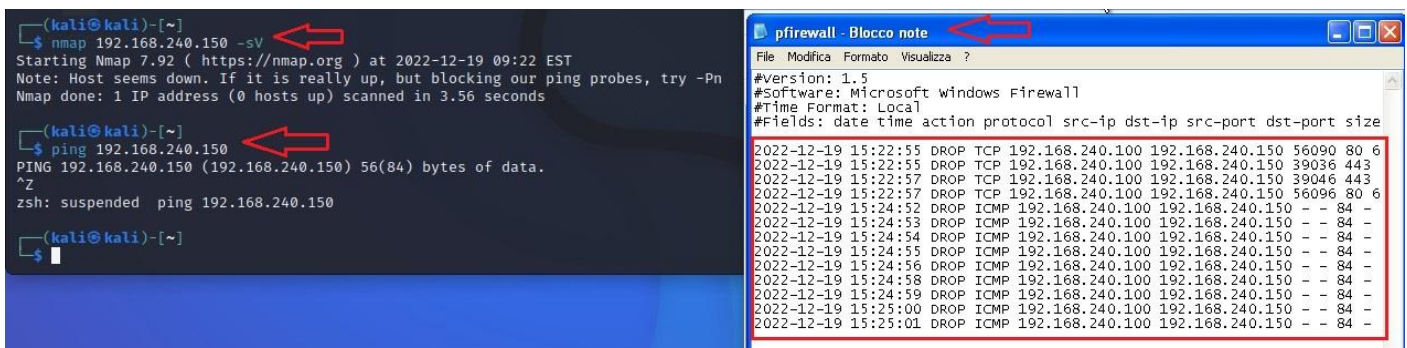
(kali@kali)-[~]
$
```

Com'è possibile vedere la seconda scansione, con il Firewall attivo non darà alcun risultato, in quanto l'host target (Windows XP) ci risulterà non attivo o non raggiungibile.

Andremo a modificare le impostazioni avanzate del Firewall per permettere alla macchina di registrare i pacchetti di connessione ignorati/riuscite.



Andremo così a verificare sul file specificato le nostre prove di connessione con nmap e ping da Kali a Windows XP.



Com'è possibile vedere le connessioni in entrata (TCP per *nmap* e ICMP per il *ping*) appariranno nel log di Windows XP come scartate (DROP) in quanto il Firewall è attivo e bloccherà tutte le connessioni in entrata, mentre con il Firewall disattivato non avremo nessun tipo di log salvato sul file. Per permettere lo scambio di pacchetti tra le macchine e consentirne il salvataggio dei log si potrebbero creare delle Firewall Policy.