

# SECURITY OPERATION: AZIONI PREVENTIVE

## TASK

### 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 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.

## BONUS

Monitorare i log di windows durante queste operazioni.

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

## REQUISITI

Configurare i seguenti indirizzi IP di Kali e Windows XP:

Kali: 192.168.240.100

Windows XP: 192.168.240.150

## ANALISI E VALUTAZIONI

Per prima cosa andiamo a configurare le due macchine con gli indirizzi IP richiesti:

```
GNU nano 6.3 /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/*

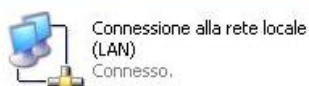
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.103
```

Per Kali andiamo sul file network con il comando ***sudo nano /etc/network/interfaces*** e dopo averlo modificato salviamo e riavviamo il sistema di rete con il comando ***sudo /etc/init.d/networking restart***

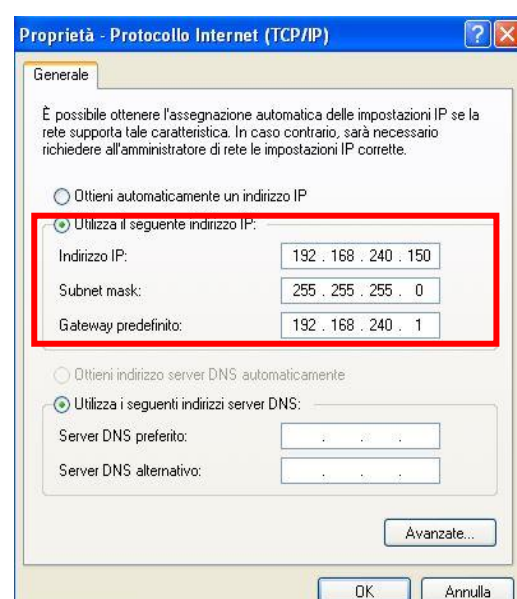
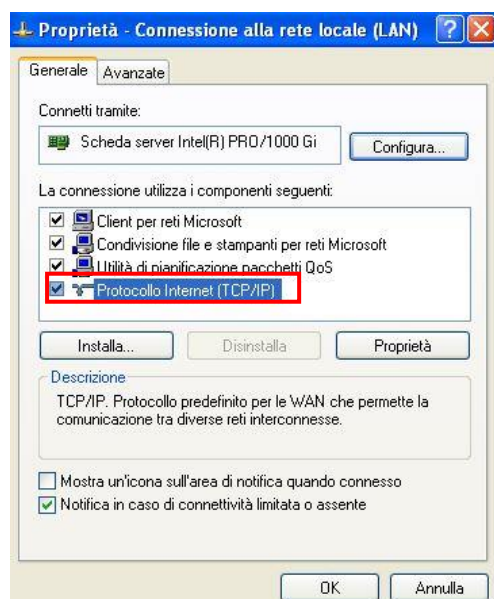


### LAN o Internet ad alta velocità



Per Windows seguiamo i seguenti passaggi:

Pannello di Controllo → Rete e Connessioni Internet → Connessione di rete → Lan (Proprietà) → Protocollo Internet (TCP/IP) → Cambiamo IP → Click su “OK”



Facciamo una prova di comunicazione tra le due macchine con il comando **ping**:

```
(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=2.47 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.739 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.889 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.853 ms
^X^Z
zsh: suspended ping 192.168.240.150

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

```
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>
```

Dopo aver testato la comunicazione andiamo ad eseguire una scansione sulla macchina in due circostanze differenti: una con il firewall attivo e l'altra con il firewall disattivato:

- **FIREWALL DISATTIVATO:**

Il firewall su Windows XP è disattivato di default quindi possiamo procedere alla scansione con nmap delle porte attive sulla macchina. Pertanto da terminale di Kali spostiamoci sulla directory Desktop e usiamo il comando

***nmap -sV -o reportnmapxp 192.168.240.150***

```
(kali@kali)-[~/Desktop]
$ nmap -sV -o reportnmapxp 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:22 EST
Nmap scan report for 192.168.240.150
Host is up (0.0048s 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 22.93 seconds

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

```
~/Desktop/reportnmapxp - Mousepad
File Edit Search View Document Help

1# Nmap 7.92 scan initiated Mon Dec 19 08:22:28 2022 as: nmap -sV -o
reportnmapxp 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0048s 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
```

-o → Switch che permette di creare un Report sulla directory in cui siamo

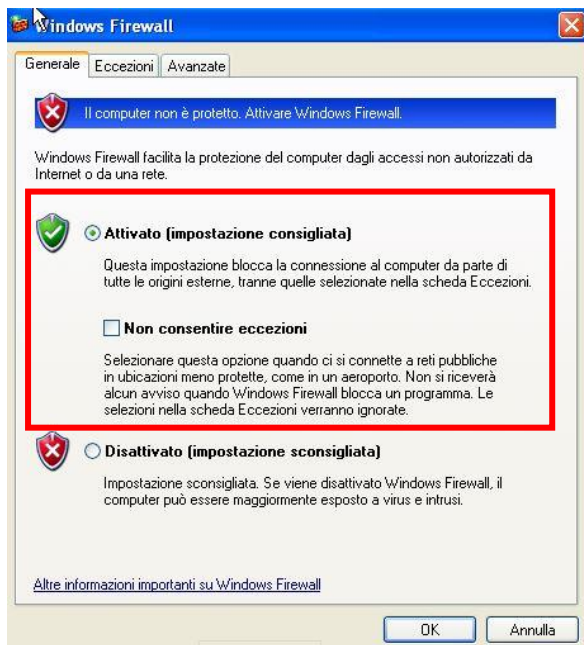
-sV → Switch che permette di scansionare le porte aperte e le loro relative versioni.

Dopo aver ottenuto il file di scansione apriamolo (come da figura in alto), e notiamo che ci verranno fornite le porte aperte con le relative versioni.

- **FIREWALL ATTIVO:**

Andiamo su Windows e procediamo per passaggi nell'attivazione del firewall:

Click Icona in basso a destra dello schermo (riquadro rosso) → Click su “Windows Firewall” (riquadro blu)  
→ Spuntare “Firewall Attivo”

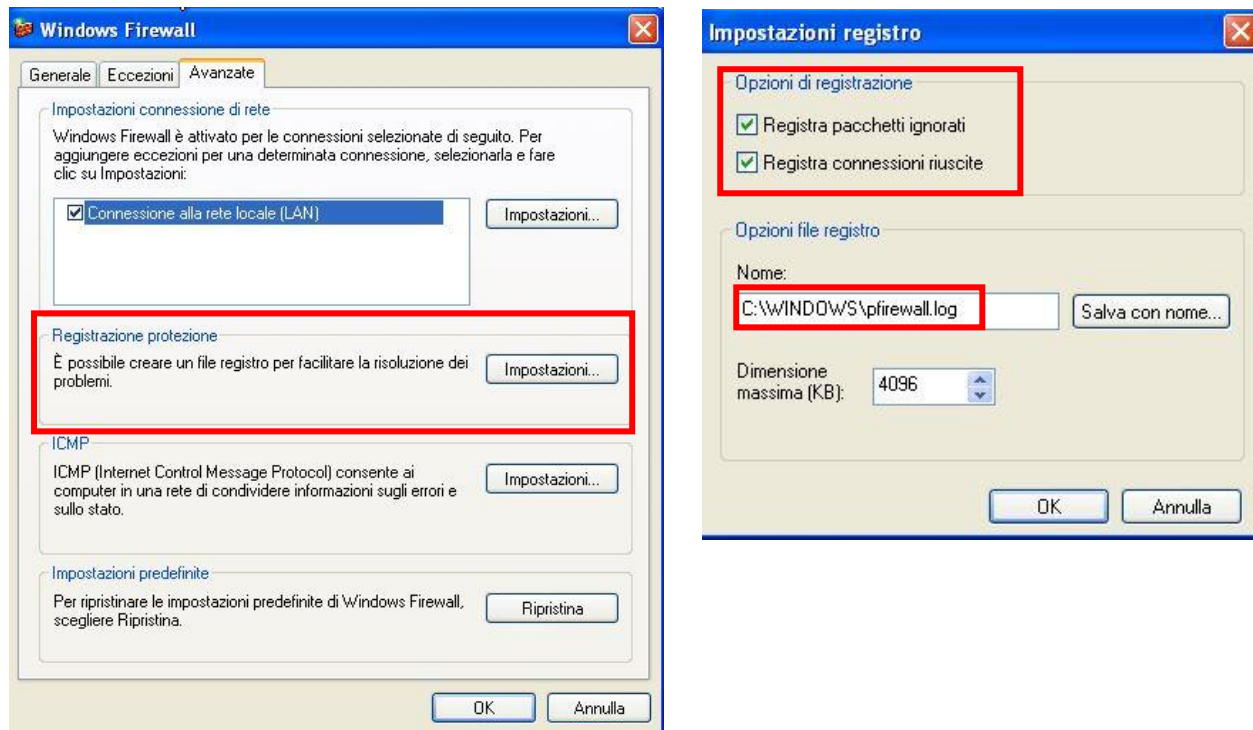


Così facendo abbiamo abilitato il Firewall, di fatti se andassimo a fare un ping da Kali a Windows esso non funzionerebbe. Se il problema non dovesse verificarsi allora spuntare anche la sezione “Non consentire eccezioni”.



Prima di proseguire con la scansione andiamo anche a spuntare il file log che ci verrà fornito da windows grazie al firewall. Per farlo andiamo seguiamo i seguenti passaggi:

Dall'ultima immagine soprastante → Avanzate → Impostazioni di Registrazione protezione → Spuntare le due caselle → Click "OK"

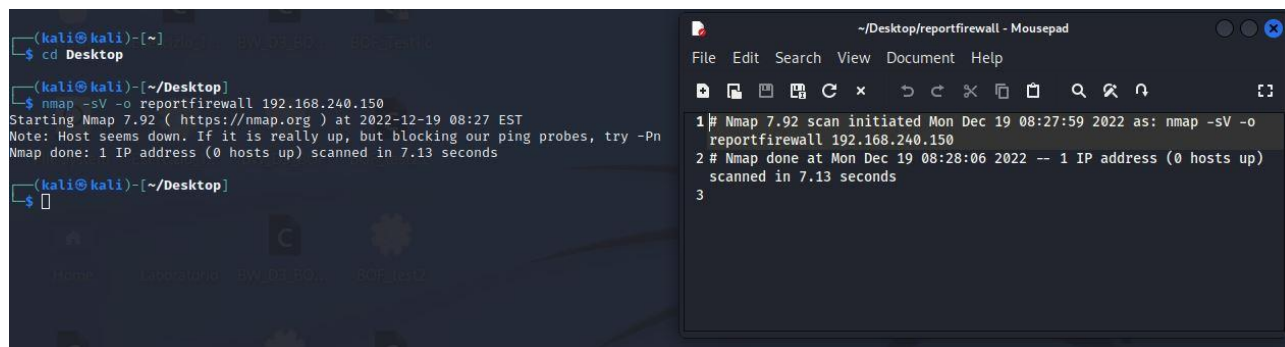


Così facendo Windows creerà un file di log in cui andrà ad inserire tutte le azioni che vengono effettuate sulla macchina. **QUESTO SARA' POSSIBILE SOLO CON FIREWALL ATTIVO.**

## SCANSIONE CON NMAP KALI - WINDOWSXP

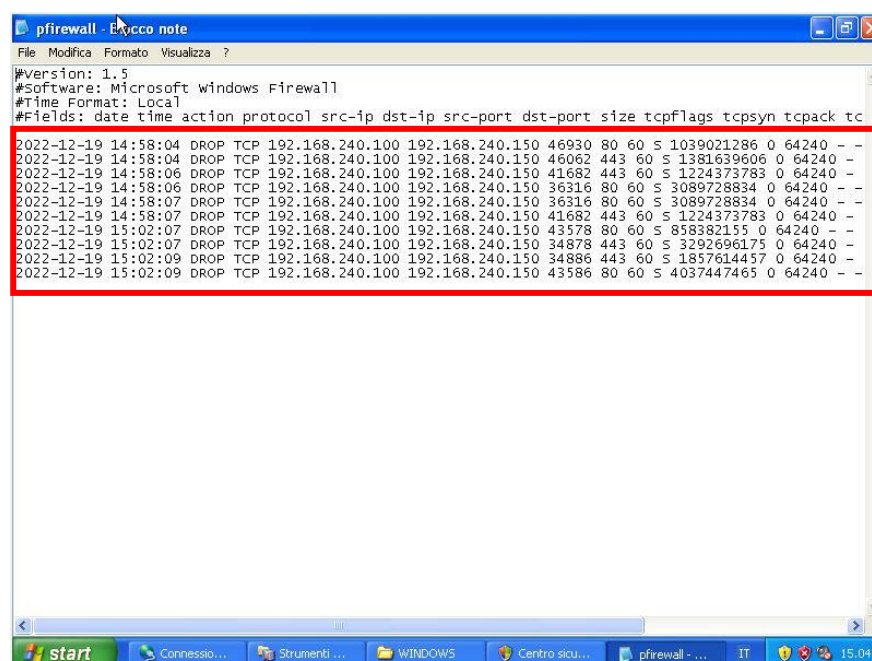
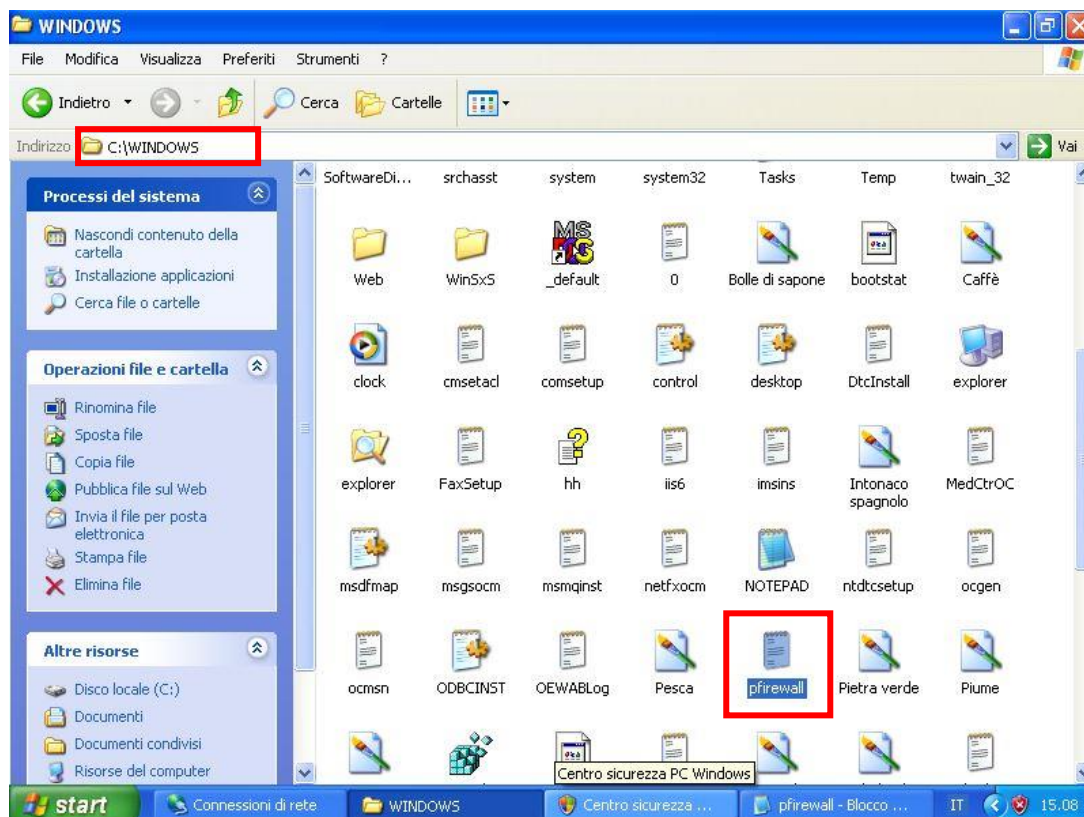
Andiamo pertanto ad eseguire la scansione da Kali con Firewall attivo con il comando:

***nmap -sV -o reportfirewall 192.168.240.150***



Come si può notare la scansione è stata sì effettuata ma non ha prodotto alcun risultato, questo a causa del Firewall che non ha permesso la conclusione della scansione.

Proprio per questo motivo possiamo andare a vedere sulla macchina Vittima (W. XP) come quest'ultima ci avvisa della scansione che è stata appena cercata di effettuare. Per vederlo infatti ci basterebbe andare nella directory del file.log che abbiamo impostato precedentemente, ovvero "C:\WINDOWS\pfirewall.log".



All'apertura del file di testo infatti ci verranno fornite tutte le informazioni a riguardo, tra cui:

- Data
- Tempo
- Azione
- Tipo di protocollo
- IP Sorgente e Destinatario
- Porta Sorg. e Dest.
- Info
- Etc.

In tal caso la scansione è stata RILASCIATA (Drop) e che un utente sconosciuto indicato da IP sorgente ha cercato di effettuare una scansione al nostro PC.

**Ogni qual volta che vogliamo leggere le azioni effettuate dobbiamo aggiornare la cartella così da far aggiornare in automatico il file di testo.**