

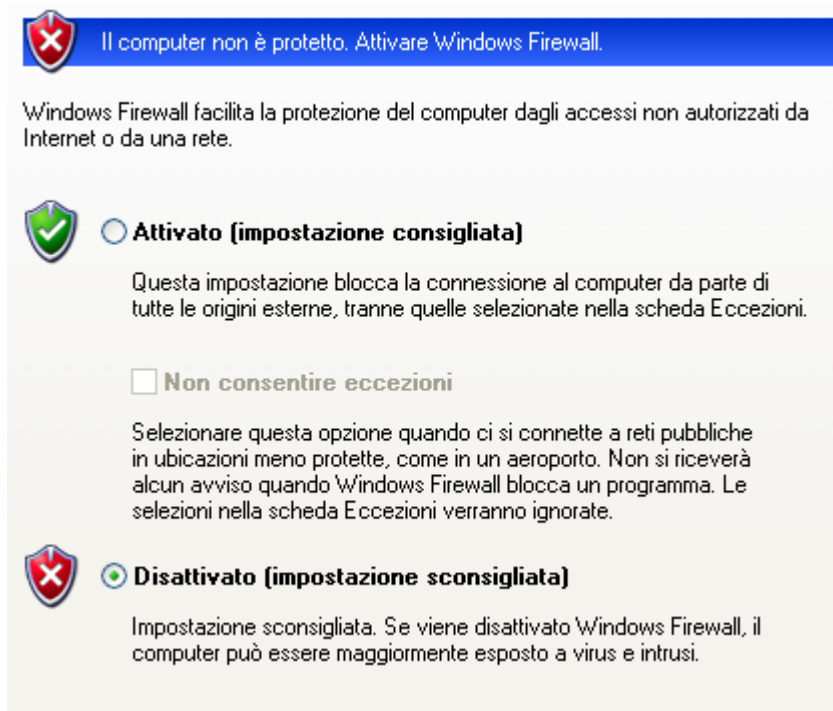
Security Operation: azioni preventive

Indirizzo IP: 192 . 168 . 240 . 150
Subnet mask: 255 . 255 . 255 . 0
Gateway predefinito: 192 . 168 . 240 . 1

```
auto eth0
iface eth0 inet static
address 192.168.11.111
netmask 255.255.255.0
gateway 192.168.11.1
```

Configurazione dell'indirizzo di Windows XP: 192.168.240.150

Configurazione dell'indirizzo della macchina Kali: 192.168.240.100



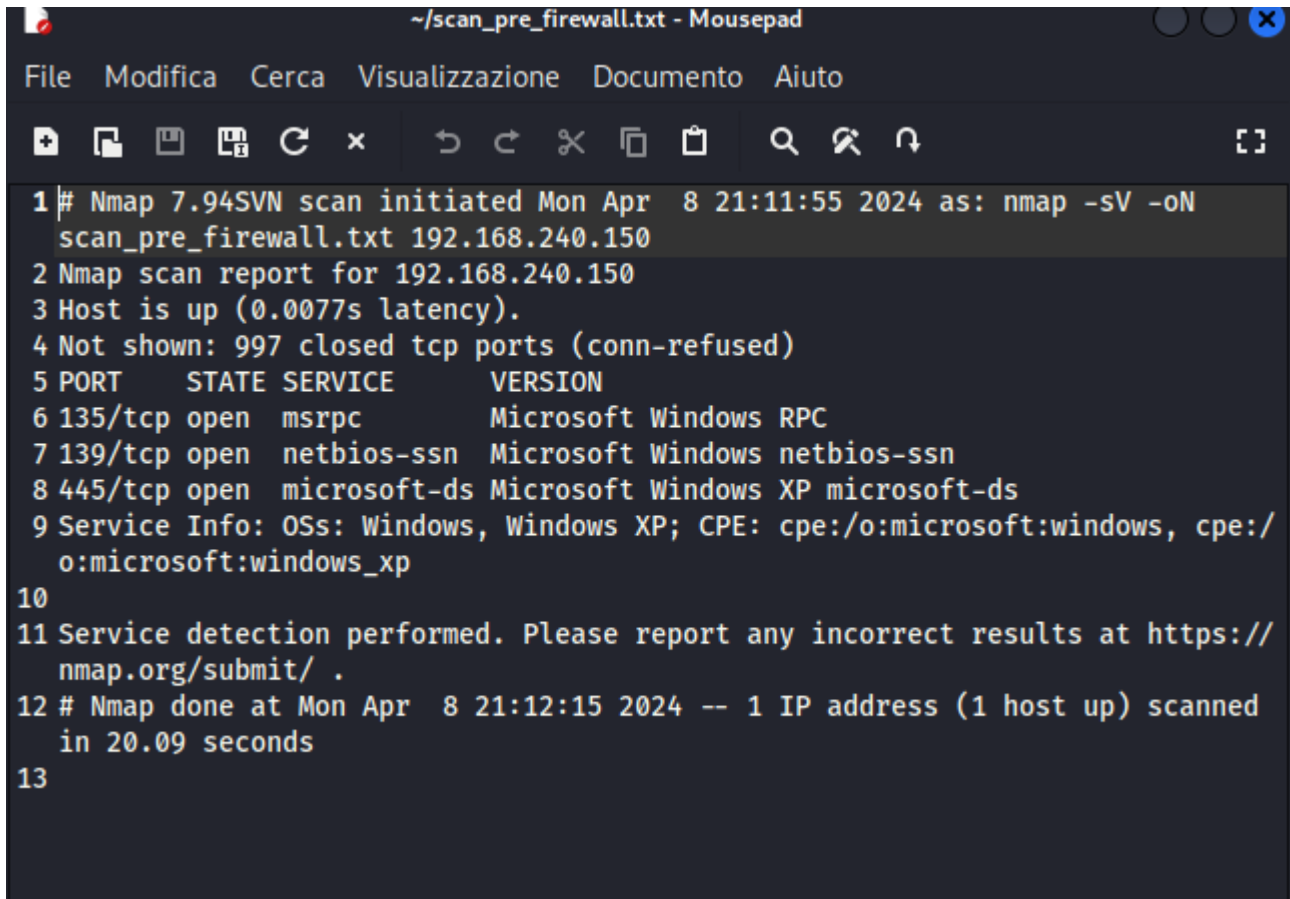
Lo screenshot mostra la finestra di dialogo del firewall di Windows XP con il firewall disattivato. Questo è lo stato richiesto per la prima parte dell'esercizio in cui la macchina deve essere scansionata senza protezione del firewall.

```
(kali@kali)-[~]
$ nmap -sV -oN scan_pre_firewall.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-08 21:11 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0077s 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 20.09 seconds
```

1. Prima dell'attivazione del Firewall:

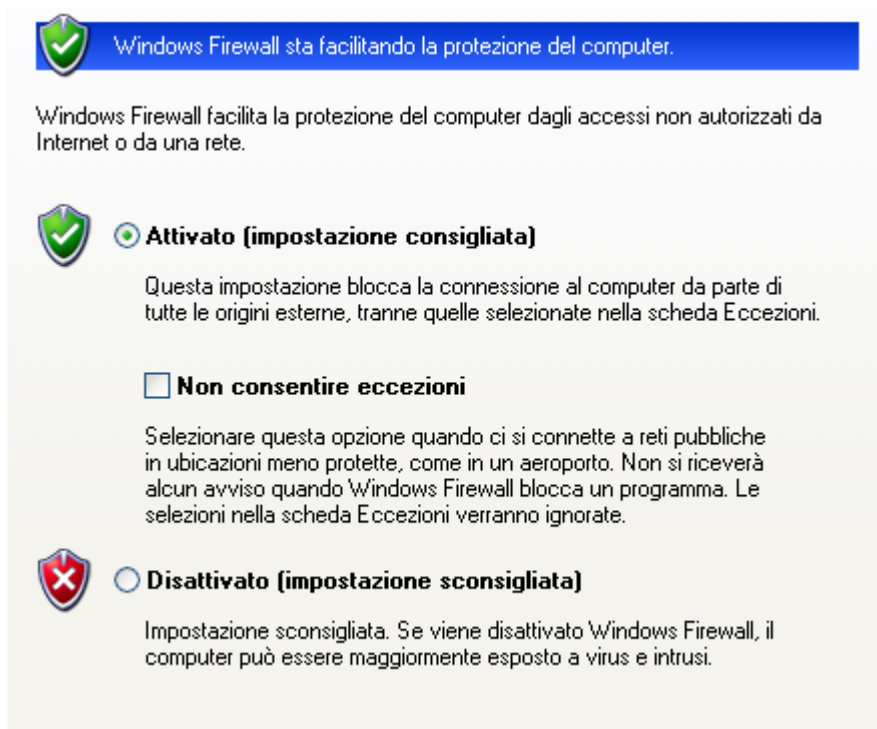
- La scansione con nmap mostra che le porte 135 (msrpc), 139 (netbios-ssn), e 445 (microsoft-ds) sono aperte e rispondono alle richieste di nmap. Questo è il risultato della macchina Windows XP con servizi di rete attivi e senza un firewall a proteggerla.



The screenshot shows a text editor window titled "~/scan_pre_firewall.txt - Mousepad". The window contains an Nmap scan report for the IP address 192.168.240.150. The report lists the open ports 135, 139, and 445, along with their corresponding services: msrpc, netbios-ssn, and microsoft-ds. The scan was performed on Monday, April 8, 2024, at 21:11:55. The report also indicates that 997 closed TCP ports were not shown.

```
1 # Nmap 7.94SVN scan initiated Mon Apr  8 21:11:55 2024 as: nmap -sV -oN
  scan_pre_firewall.txt 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0077s 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 Apr  8 21:12:15 2024 -- 1 IP address (1 host up) scanned
  in 20.09 seconds
13
```

Questo screenshot mostr un file txt, in cui sono stati salvati i dati della scansione, come da richiesta dell'esercizio.



Questo screenshot mostra che il firewall di Windows XP è stato attivato. Questo dovrebbe influenzare i risultati della successiva scansione nmap, bloccando le porte precedentemente scoperte.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ nmap -sV -oN scan_pre_firewall.txt 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-08 21:19 CEST  
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  
  
(kali@kali)-[~]  
$ cat scan_pre_firewall.txt  
# Nmap 7.94SVN scan initiated Mon Apr 8 21:19:49 2024 as: nmap -sV -oN scan_pre_firewall.txt 192.168.240.150  
# Nmap done at Mon Apr 8 21:19:52 2024 -- 1 IP address (0 hosts up) scanned in 3.18 seconds  
  
(kali@kali)-[~]  
$
```

Questo screenshot rivela che dopo l'attivazione del firewall, la macchina Windows XP non risponde più alla scansione nmap. Ciò indica che il firewall sta proteggendo il sistema da accessi non autorizzati.

In conclusione, le differenze tra i risultati delle scansioni nmap prima e dopo l'attivazione del firewall su Windows XP sono significative e chiaramente dovute al cambiamento nello stato del firewall.

Differenze Trovate:

1. Prima dell'Attivazione del Firewall: Le porte di rete erano aperte e i servizi associati a queste porte erano visibili e rilevabili dalla scansione nmap.

2. Dopo l'Attivazione del Firewall: La scansione nmap non è stata in grado di rilevare la macchina, suggerendo che le porte prima aperte sono ora nascoste o bloccate dal firewall.

Motivazione delle Differenze:

- L'attivazione del firewall ha probabilmente introdotto regole che bloccano o ignorano i pacchetti in entrata non riconosciuti o non sollecitati, come quelli inviati da strumenti di scansione come nmap. Questo è un comportamento comune del firewall progettato per aumentare la sicurezza riducendo la superficie di attacco e nascondendo i servizi interni da potenziali aggressori.

Monitoraggio dei Log di Windows:

1. Log Modificati: Durante tali operazioni, il Security Event Log su Windows XP avrebbe registrato eventi relativi a tentativi di connessione in entrata. Se il firewall è configurato per loggare tali eventi, vedresti voci relative al blocco o alla ricezione di pacchetti in entrata da specifici indirizzi IP o porte.

2. Cosa si Trova nei Log:

- Dettagli dei Tentativi di Connessione: Ogni volta che il firewall blocca un tentativo di connessione, può generare un log con informazioni sull'indirizzo IP sorgente, sulla porta di destinazione e sul protocollo utilizzato.

- Tipi di Traffico Bloccato: I log possono rivelare se il traffico era TCP, UDP o di altro tipo.

- Frequenza dei Tentativi di Accesso: Si possono notare modelli nei tentativi di accesso, come attacchi concentrati su specifiche porte o protocolli.

- Informazioni per l'Analisi Forense: In caso di un attacco reale, i log possono fornire dati cruciali per un'indagine forense sulla natura e sull'origine dell'attacco.

In assenza di log o senza la possibilità di visualizzarli direttamente, questa analisi presuppone l'uso standard di log del firewall in un ambiente Windows. Se i log non fossero configurati per registrare tali eventi, non ci sarebbero modifiche o nuove voci corrispondenti all'attività di nmap.

Questa pratica dimostra l'importanza del monitoraggio e della revisione attenta dei log di sicurezza, sia per identificare minacce potenziali sia per migliorare la sicurezza complessiva di una rete.