

# Report sulle Azioni Preventive: Impatto dell'Attivazione del Firewall su Windows XP

---

## Introduzione

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. A livello di rete, abbiamo appreso che è possibile attivare e configurare Firewall e regole specifiche per bloccare traffico potenzialmente dannoso. In questo esercizio pratico, ho verificato come l'attivazione del Firewall su una macchina Windows XP impatti il risultato di una scansione dei servizi dall'esterno.

---

## Materiali e Metodi

Per questo esercizio ho utilizzato:

- Una macchina virtuale Windows XP
- Il tool nmap su kali linux per la scansione di rete

## Passaggi Eseguiti

### 1. Verifica dello stato del Firewall

- Ho verificato che il Firewall fosse disattivato sulla macchina Windows XP.
- Per fare ciò, ho navigato su: *Pannello di controllo -> Centro sicurezza -> Windows Firewall* e confermato che fosse impostato su "Disattivato".

### 2. Prima Scansione con nmap

- Ho effettuato una scansione iniziale con nmap sulla macchina target per rilevare i servizi attivi.
- Comando utilizzato: `nmap -sV <indirizzo IP target> -o prima_scansione.txt`
- La scansione è stata salvata nel file `prima_scansione.txt`.

### 3. Attivazione del Firewall

- Ho attivato il Firewall sulla macchina Windows XP.
- Per fare ciò, ho navigato su: *Pannello di controllo -> Centro sicurezza -> Windows Firewall* e impostato su "Attivato".

### 4. Seconda Scansione con nmap

- Ho effettuato una seconda scansione con nmap, utilizzando gli stessi parametri della prima.
  - Comando utilizzato: `nmap -sV <indirizzo IP target> -o seconda_scansione.txt`
  - La scansione è stata salvata nel file `seconda_scansione.txt`.
-

## Risultati

### Prima Scansione (Firewall Disattivato)

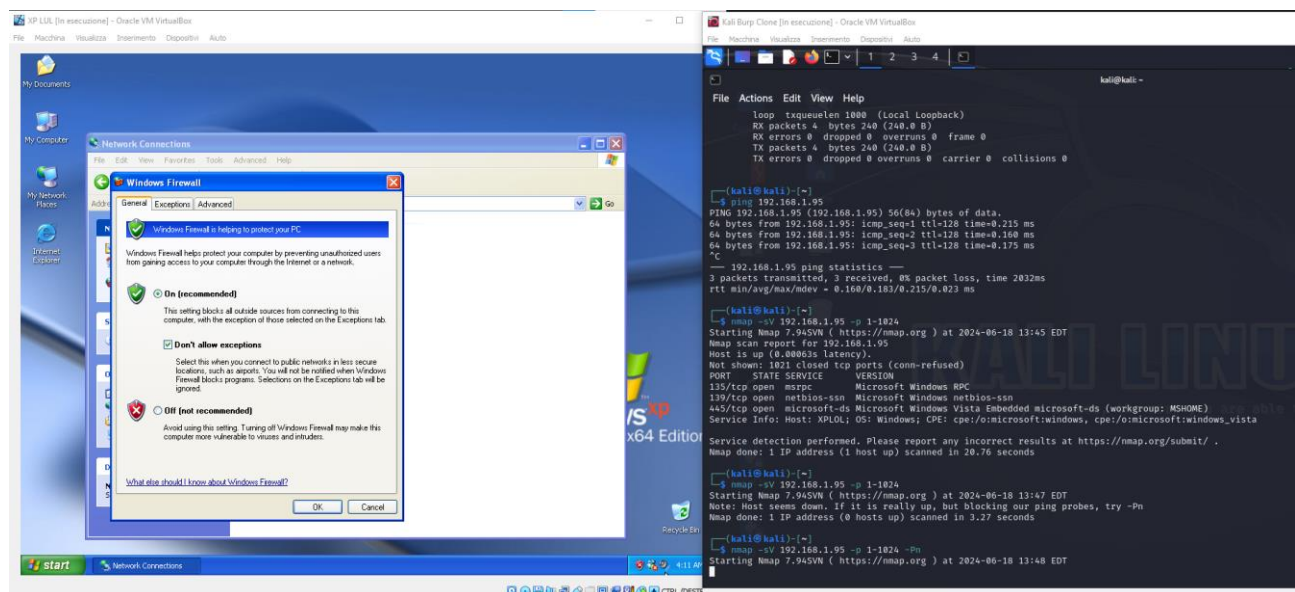
Il risultato della prima scansione ha mostrato i seguenti servizi attivi sulla macchina Windows XP:

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.95 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-18 13:45 EDT
Nmap scan report for 192.168.1.95
Host is up (0.00063s latency).
Not shown: 1021 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 Vista Embedded microsoft-ds (workgroup: MSHOME)
Service Info: Host: XPLOL; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.76 seconds

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

### Seconda Scansione (Firewall restrittivo)



## Discussione

Dall'analisi dei risultati delle scansioni, si evince che l'attivazione del Firewall su Windows XP ha bloccato la visibilità di vari servizi che erano invece rilevabili con il Firewall disattivato. In particolare, i servizi open non sono più visibili dall'esterno una volta che il Firewall è stato attivato. Questo dimostra l'efficacia del Firewall nel limitare l'esposizione dei servizi di rete a potenziali attacchi.

## Conclusione

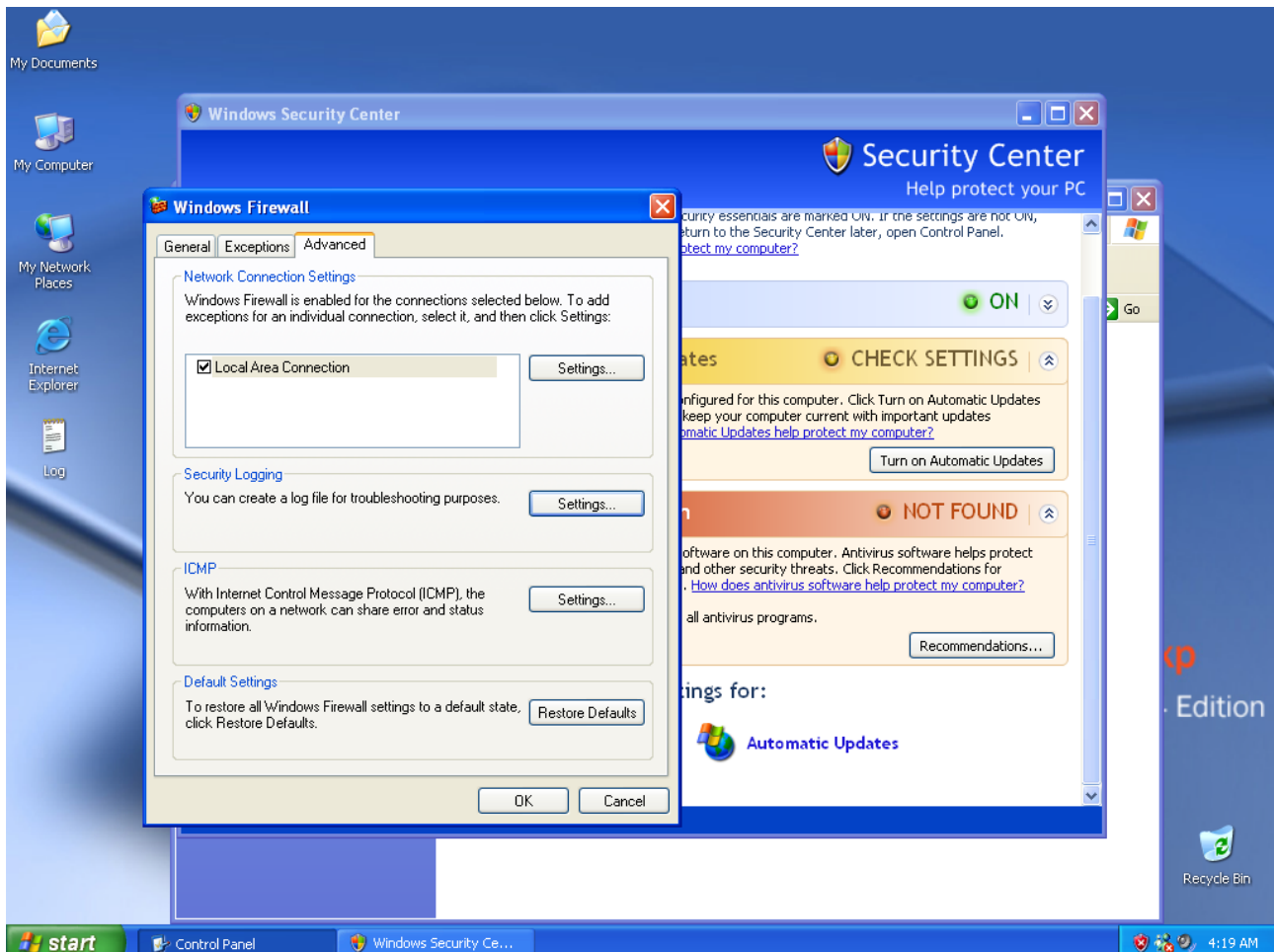
L'attivazione del Firewall sulla macchina Windows XP ha significativamente ridotto il numero di servizi visibili dall'esterno. Questo esercizio evidenzia l'importanza delle misure preventive come l'attivazione del Firewall per migliorare la sicurezza della rete.

## Bonus:

Monitorare i log di Windows durante queste operazioni.

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

Attiviamo il logging sul Firewall windows.



```
Log - Notepad
File Edit Format View Help
#Version: 1.5
#Software: Microsoft windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpsyn tcpsyn tcpsyn
2024-05-14 04:19:00 OPEN TCP 192.168.1.95 192.168.11.111 1060 4444 - - - - - - - - - -
2024-05-14 04:19:00 OPEN TCP 192.168.1.95 192.168.11.111 1061 4444 - - - - - - - - - -
2024-05-14 04:19:09 DROP TCP 192.168.1.100 192.168.1.95 40290 80 60 S 1272876695 0 64240 - -
2024-05-14 04:19:09 DROP TCP 192.168.1.100 192.168.1.95 42302 443 60 S 1318673507 0 64240 - -
2024-05-14 04:19:10 DROP TCP 192.168.1.100 192.168.1.95 42302 443 60 S 1318673507 0 64240 - -
2024-05-14 04:19:10 DROP TCP 192.168.1.100 192.168.1.95 40290 80 60 S 1272876695 0 64240 - -
2024-05-14 04:19:11 DROP TCP 192.168.1.100 192.168.1.95 42308 443 60 S 2443440106 0 64240 - -
2024-05-14 04:19:11 DROP TCP 192.168.1.100 192.168.1.95 40304 80 60 S 1331114018 0 64240 - -
2024-05-14 04:19:21 CLOSE TCP 192.168.1.95 192.168.11.111 1061 4444 - - - - - - - - - -
2024-05-14 04:19:21 CLOSE TCP 192.168.1.95 192.168.11.111 1060 4444 - - - - - - - - - -
2024-05-14 04:19:31 OPEN TCP 192.168.1.95 192.168.11.111 1060 4444 - - - - - - - - - -
2024-05-14 04:19:31 OPEN TCP 192.168.1.95 192.168.11.111 1061 4444 - - - - - - - - - -
2024-05-14 04:19:52 CLOSE TCP 192.168.1.95 192.168.11.111 1061 4444 - - - - - - - - - -
2024-05-14 04:19:52 CLOSE TCP 192.168.1.95 192.168.11.111 1060 4444 - - - - - - - - - -
2024-05-14 04:20:02 OPEN TCP 192.168.1.95 192.168.11.111 1060 4444 - - - - - - - - - -
2024-05-14 04:20:02 OPEN TCP 192.168.1.95 192.168.11.111 1061 4444 - - - - - - - - - -

C:\WINDOWS\system32\cmd.exe
Active Connections
Proto Local Address Foreign Address State PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 560
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:1028 0.0.0.0:0 LISTENING 280
TCP 127.0.0.1:1031 0.0.0.0:0 LISTENING 1928
TCP 192.168.1.95:139 0.0.0.0:0 LISTENING 4
TCP 192.168.1.95:1060 192.168.11.111:4444 SYN_SENT 1180
TCP 192.168.1.95:1061 192.168.11.111:4444 SYN_SENT 1512
TCP [::]:135 [::]:0 LISTENING 560
TCP [::]:445 [::]:0 LISTENING 4
TCP [::]:1028 [::]:0 LISTENING 280
UDP 0.0.0.0:500 *: * 280
UDP 0.0.0.0:1037 *: * 692
UDP 0.0.0.0:4500 *: * 280
UDP 127.0.0.1:123 *: * 760
UDP 127.0.0.1:1900 *: * 760
UDP 192.168.1.95:123 *: * 760
UDP 192.168.1.95:137 *: * 4
UDP 192.168.1.95:138 *: * 4
UDP 192.168.1.95:1900 *: * 760
C:\Documents and Settings\Administrator>
```

Si notano due cose, la prima il drop di tutte le scansioni nmap. La seconda che c'è una backdoor attiva sul sistema come si nota anche da netstat /ano che prova a connettersi su 192.168.11.111:444.