

Report - Impatto dell'attivazione del Firewall su Windows XP

Data 29/01/23

Indice

Report - Impatto dell'attivazione del Firewall su Windows XP

Introduzione

1.1 Obiettivo dell'Esercizio

Configurazione Iniziale

2.1 Disabilitazione del Firewall su Windows XP

2.2 Configurazione degli Indirizzi IP

Prima Scansione con nmap

3.1 Utilizzo di nmap con lo switch -sV

Attivazione del Firewall su Windows XP

4.1 Procedura per Attivare il Firewall

Seconda Scansione con nmap dopo l'Attivazione del Firewall

5.1 Risultati della Seconda Scansione

5.2 Analisi delle Differenze

Conclusioni

6.1 Raccomandazioni di Sicurezza

1. Introduzione

L'esercizio odierno si propone di esaminare in che modo l'attivazione del firewall sulla macchina Windows XP influisca sui risultati di una scansione dei servizi eseguita esternamente, attraverso l'impiego dello strumento nmap. Attraverso questo studio pratico, miriamo a comprendere come la configurazione del firewall possa impattare sulla visibilità e sulla sicurezza dei servizi offerti da una macchina.

1.1 Obiettivo dell'Esercizio

L'obiettivo dell'esercizio è verificare l'impatto dell'attivazione del Firewall sulla macchina Windows XP sul risultato di una scansione dei servizi dall'esterno, utilizzando lo strumento nmap.

2. Configurazione Iniziale

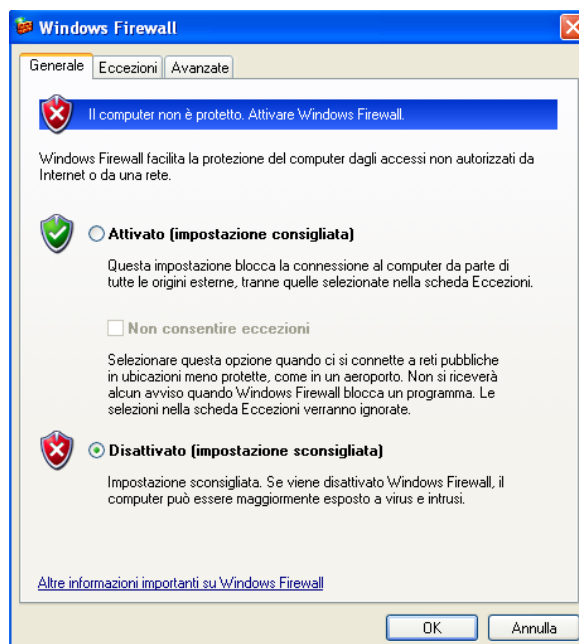
2.1 Disabilitazione del Firewall su Windows XP

Per garantire una configurazione iniziale uniforme, abbiamo disabilitato il Firewall sulla macchina Windows XP. Per farlo abbiamo seguito la seguente procedura:

Cliccato sull'icona in basso a destra (rettangolo rosso).

Selezionato "Windows Firewall" (rettangolo blu).

Impostato lo stato del Firewall su "DISATTIVATO" e cliccato su "OK".



2.2 Configurazione degli Indirizzi IP

Abbiamo assegnato gli indirizzi IP seguendo le specifiche dell'esercizio:

Dal pannello di controllo abbiamo raggiunto la sezione “rete e connessione internet”, successivamente siamo entrato nella sezione connessioni di rete e nell’unica scheda di rete configurata abbiamo configurato tramite l’opzione proprietà l’indirizzo IP del protocollo TCP/IP. L’indirizzo assegnato è stato:

Windows XP: 192.168.240.150

Nella macchina attaccante Kali linux abbiamo modificato l’indirizzo IP da terminale. Andando a modificare il file di configurazione interfaces con il comando “sudo nano /etc/network/interfaces” ed impostato il seguente indirizzo:

Kali Linux: 192.168.240.100

3. Prima Scansione con nmap

3.1 Utilizzo di nmap con lo switch -sV

Abbiamo eseguito una scansione dei servizi sulla macchina Windows XP utilizzando nmap con lo switch -sV per la rilevazione dei servizi in ascolto. Il comando utilizzato è stato il seguente:

```
- nmap -sV 192.168.240.150
```

Nell screen sottostante è visualizzato il risultato della scansione con il firewall di windows disattivato.

```
kali@kali: ~  
└─(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 08:29 EST  
Nmap scan report for 192.168.240.150  
Host is up (0.81s 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 21.50 seconds  
  
└─(kali@kali)-[~]  
$
```

4. Attivazione del Firewall su Windows XP

Con la stessa procedura effettuata per disabilitare il firewall abbiamo riattivato il firewall della macchina windows XP.

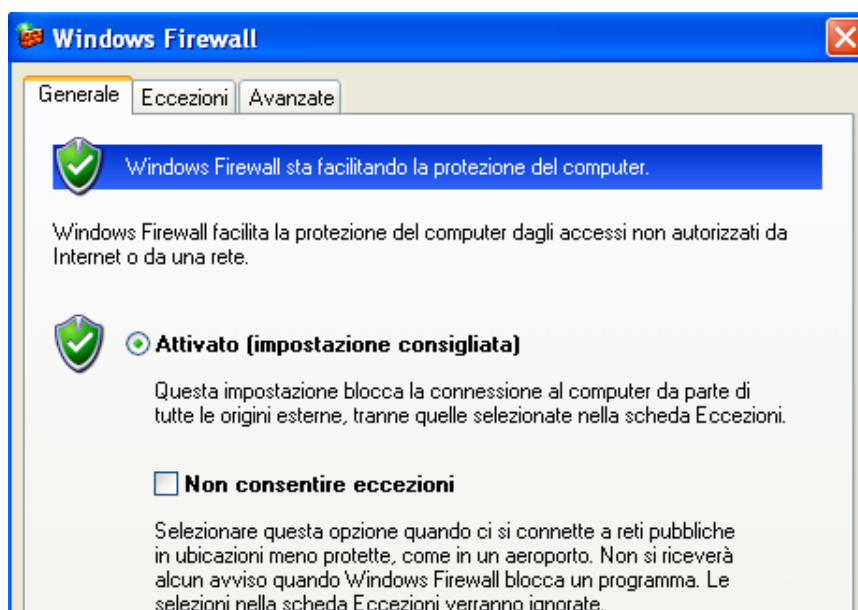
4.1 Procedura per Attivare il Firewall

Abbiamo attivato il Firewall sulla macchina Windows XP seguendo la procedura fornita:

Cliccato sull'icona in basso a destra (rettangolo rosso).

Selezionato "Windows Firewall" (rettangolo blu).

Impostato lo stato del Firewall su "ATTIVATO" e cliccato su "OK".



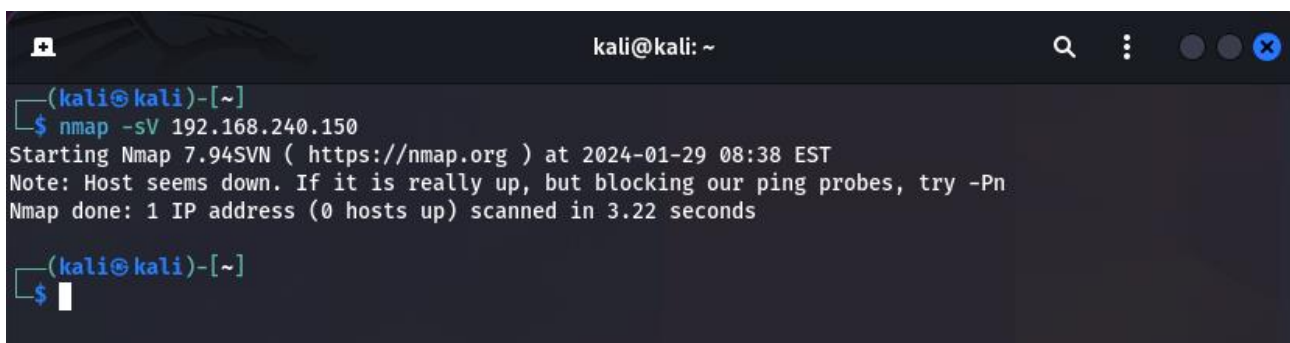
5. Seconda Scansione con nmap dopo l'Attivazione del Firewall

5.1 Risultati della Seconda Scansione

Abbiamo eseguito una seconda scansione dei servizi sulla macchina Windows XP dopo l'attivazione del Firewall, utilizzando nuovamente nmap con lo switch -sV. Abbiamo eseguito il seguente comando:

```
- nmap -sV 192.168.240.150
```

Il risultato della scansione non ha permesso di identificare i servizi esposti della macchina windows XP e neanche la connettività dell'host target.

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The prompt is '(kali@kali)-[~]'. The user has entered the command '\$ nmap -sV 192.168.240.150'. The output shows 'Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-29 08:38 EST', followed by a note: 'Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn'. The final line of output is 'Nmap done: 1 IP address (0 hosts up) scanned in 3.22 seconds'. The prompt returns to '(kali@kali)-[~]' with a new '\$' prompt character visible.

```
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 08:38 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 3.22 seconds  
  
(kali@kali)-[~]  
$
```

5.2 Analisi delle Differenze

Confrontando i risultati delle due scansioni, abbiamo identificato le differenze nel servizio e analizzato le possibili cause di tali variazioni.

Con il firewall disattivato sulla macchina Windows XP, la scansione con nmap ha rivelato i servizi in ascolto, evidenziando le porte aperte e indicando l'host come "up". Tuttavia, con il firewall attivato, la scansione non ha restituito alcun servizio in ascolto, e l'host target è stato segnalato come non raggiungibile ("down"). Questo risultato può essere attribuito al fatto che il firewall blocca le richieste di scansione in arrivo, impedendo la visualizzazione dei servizi e nascondendo la presenza dell'host dalla scansione esterna per motivi di sicurezza. Il firewall costituisce quindi una barriera protettiva che limita l'esposizione dei servizi e riduce la rilevabilità dell'host da parte di potenziali attaccanti.

6. Conclusioni

L'esperimento condotto evidenzia l'impatto significativo che l'attivazione del firewall può avere sulla sicurezza e sulla visibilità di un sistema. Con il firewall disattivato, la scansione ha fornito dettagli sui servizi in ascolto e sulle porte aperte, identificando correttamente l'host come "up". Tuttavia, con il firewall attivato, la mancanza di risposte dai servizi ha reso l'host apparentemente non raggiungibile.

Questa differenza sostanziale sottolinea il ruolo cruciale del firewall nella gestione delle comunicazioni in rete. Attivando il firewall, si limita la visibilità esterna dei servizi, riducendo le informazioni disponibili agli attaccanti e contribuendo a proteggere il sistema da potenziali minacce. Questo dimostra l'importanza di integrare adeguatamente le misure di sicurezza, come l'uso corretto dei firewall, per garantire la robustezza e la difesa dei sistemi informatici contro intrusioni indesiderate. In conclusione, la configurazione oculata del firewall è un elemento fondamentale nella strategia complessiva di sicurezza informatica, contribuendo a mitigare i rischi e a preservare l'integrità dei servizi di un sistema.

6.1 Raccomandazioni di Sicurezza

Basandoci sui risultati, sottolineiamo l'importanza di configurare correttamente i firewall per migliorare la sicurezza del sistema. Raccomandiamo una valutazione costante delle regole del firewall per adattarsi alle esigenze di sicurezza in evoluzione.