

Introduzione

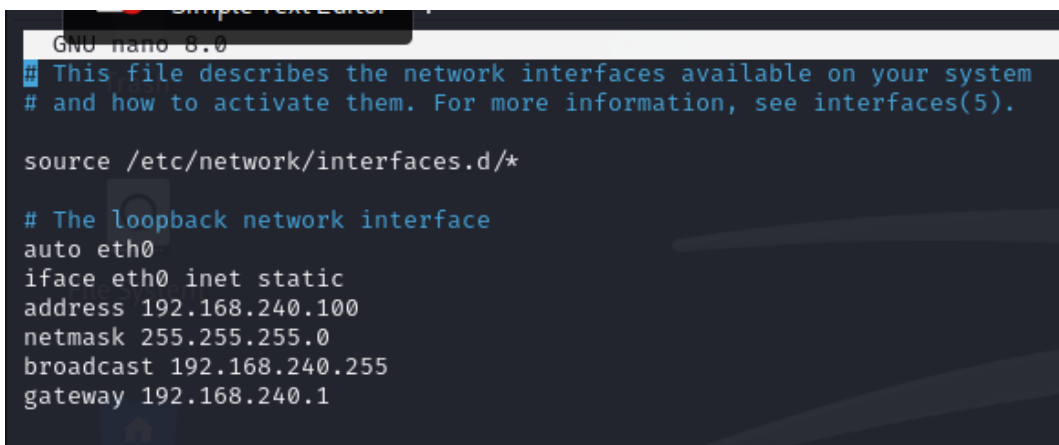
La sicurezza delle operazioni di rete è essenziale per prevenire attacchi informatici. Uno degli strumenti più importanti in questa difesa è il firewall, che controlla il traffico di rete in ingresso e in uscita. Questo report analizza l'impatto dell'attivazione del firewall sui risultati delle scansioni di rete utilizzando Nmap, confrontando i risultati ottenuti con il firewall disabilitato e abilitato.

L'esercitazione ha due obiettivi principali:

1. Configurare l'indirizzo di Windows XP come di seguito: 192.168.240.150
2. Configurare l'indirizzo della macchina Kali come di seguito: 192.168.240.100
3. Valutare come l'attivazione del firewall su una macchina Windows XP influisce sulla visibilità dei servizi di rete attraverso una scansione Nmap.
4. Analizzare i log di sistema generati durante queste operazioni per identificare eventuali modifiche e comprendere meglio il comportamento del firewall.

Configurazione Iniziale

- **Impostare indirizzo ip kali linux:**

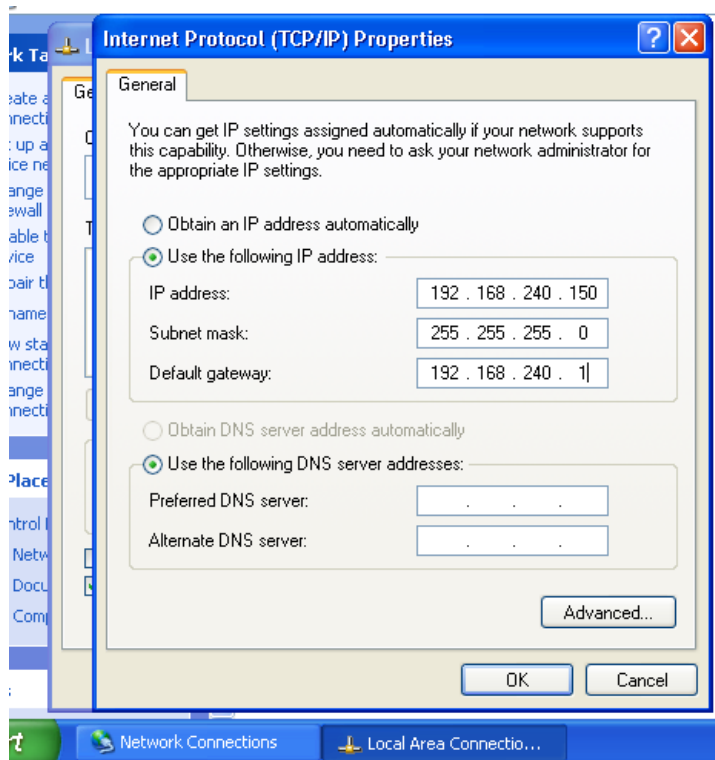


```
GNU nano 8.0
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto eth0
iface eth0 inet static
address 192.168.240.100
netmask 255.255.255.0
broadcast 192.168.240.255
gateway 192.168.240.1
```

- **Impostare indirizzo ip windows xp:**



- **Disabilitare il Firewall:** Disabilitare il firewall sulla macchina Windows XP.



- **Effettuare una Scansione Nmap:** Utilizzare Nmap con lo switch -sV per rilevare i servizi e -o per salvare l'output in un file.

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 14:17 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00073s latency).
Not shown: 997 closed tcp ports (reset)
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
MAC Address: 08:00:27:30:99:1B (Oracle VirtualBox virtual NIC)
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 19.69 seconds

(kali㉿kali)-[~]
$
```

- **Abilitare il Firewall:** Abilitare il firewall sulla macchina Windows XP.



- **Effettuare una Seconda Scansione Nmap:** Ripetere la scansione Nmap con le stesse opzioni.

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 14:22 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:30:99:1B (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.75 seconds

(kali㉿kali)-[~]
$
```

Strumenti Utilizzati

- **Nmap:** Utilizzato per effettuare le scansioni di rete.
- **Kali Linux:** Sistema operativo utilizzato per eseguire Nmap.
- **Windows XP:** Sistema operativo della macchina target con il firewall da abilitare e disabilitare.

Risultati

Scansione con Firewall Disabilitato

Con il firewall disabilitato, la scansione Nmap ha rilevato diversi servizi attivi sulla macchina Windows XP, tra cui:

- **MSRPC:** Porta 135/TCP
- **NetBIOS-SSN:** Porta 139/TCP
- **Microsoft-DS:** Porta 445/TCP

Questi risultati indicano che senza il firewall, le porte di rete possono essere scansionate liberamente, rendendo visibili i servizi attivi sulla macchina.

Scansione con Firewall Abilitato

Abilitando il firewall e ripetendo la scansione Nmap, i risultati sono stati significativamente diversi. Nessun servizio è stato rilevato, e tutte le porte risultavano filtrate. Questo conferma che il firewall blocca le richieste di scansione, proteggendo la macchina da potenziali attacchi.

Analisi dei Log di Sistema

Durante le operazioni, sono stati monitorati i log di Windows per analizzare le attività registrate dal firewall. I log salvati nel file pfirewall.log hanno mostrato numerosi pacchetti bloccati dal firewall, inclusi:

- **Pacchetti TCP Drop:** Pacchetti bloccati dalla sorgente (IP 192.168.240.100) alla destinazione (IP 192.168.240.150).
- **Porta sorgente:**
53237
- **Porta destinazione:**

```

pfirewall - 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 tcpack tc
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 3306 44 S 2263338025 0 1024 -
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 995 44 S 2263338025 0 1024 -
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 110 44 S 2263338025 0 1024 -
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 80 44 S 2263338025 0 1024 -
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 139 44 S 2263338025 0 1024 -
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 445 44 S 2263338025 0 1024 -
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 22 44 S 2263338025 0 1024 -
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 53 44 S 2263338025 0 1024 -
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 25 44 S 2263338025 0 1024 -
2024-06-19 20:30:14 DROP TCP 192.168.240.100 192.168.240.150 53237 5900 44 S 2263338025 0 1024 -
2024-06-19 20:30:16 DROP TCP 192.168.240.100 192.168.240.150 53239 5900 44 S 2263206955 0 1024 -
2024-06-19 20:30:16 DROP TCP 192.168.240.100 192.168.240.150 53239 25 44 S 2263206955 0 1024 -
2024-06-19 20:30:16 DROP TCP 192.168.240.100 192.168.240.150 53239 53 44 S 2263206955 0 1024 -
2024-06-19 20:30:16 DROP TCP 192.168.240.100 192.168.240.150 53239 22 44 S 2263206955 0 1024 -
2024-06-19 20:30:16 DROP TCP 192.168.240.100 192.168.240.150 53239 445 44 S 2263206955 0 1024 -

```

I log forniscono dettagli preziosi sulle azioni del firewall, evidenziando come vengano gestiti i tentativi di connessione non autorizzati.

Conclusioni

L'esercitazione ha dimostrato chiaramente l'importanza del firewall nella protezione delle reti. Con il firewall abilitato, la visibilità dei servizi di rete è notevolmente ridotta, diminuendo la superficie di attacco. I log di sistema offrono ulteriori approfondimenti sulle attività bloccate, aiutando a monitorare e rispondere alle minacce di rete.

Raccomandazioni

Per migliorare ulteriormente la sicurezza delle operazioni di rete, si raccomanda di:

- **Mantenere il Firewall Attivo:** Assicurarsi che il firewall sia sempre attivo e configurato correttamente.
- **Monitorare Regolarmente i Log:** Analizzare regolarmente i log di sistema per identificare e rispondere tempestivamente a potenziali minacce.
- **Aggiornare le Regole del Firewall:** Aggiornare e verificare periodicamente le regole del firewall per assicurarsi che proteggano efficacemente la rete.

Implementando queste misure, le organizzazioni possono migliorare significativamente la loro sicurezza e proteggere meglio i loro sistemi da attacchi esterni.