S9_L1
Unit 3 - CS0424

MATTEO BELTRAMI MARZOLINI
CYBEREAGLES

GIORNO 1 - SECURITY OPERATION

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 che abbiamo utilizzato 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.

Che differenze notate? E quale può essere la causa del risultato diverso?

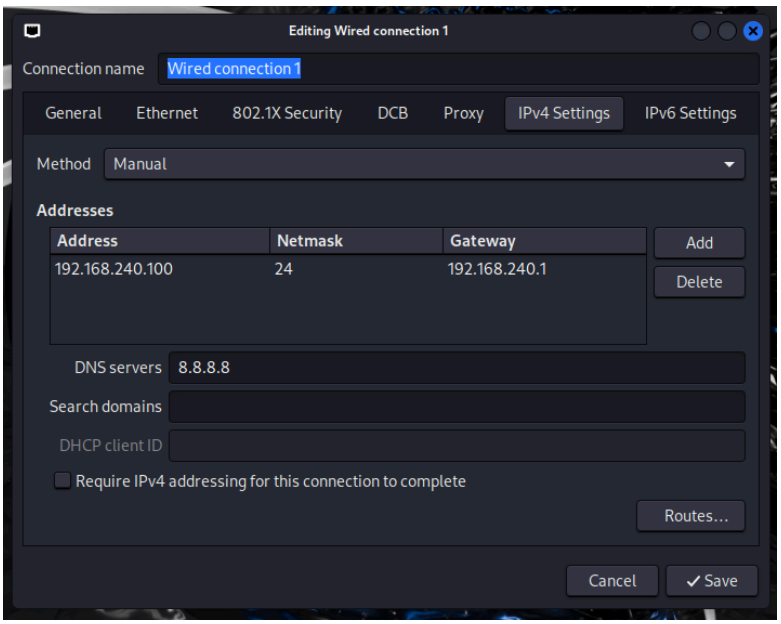
Requisiti:

- Configurate l'indirizzo di Windows XP come di seguito: 192.168.240.150
- Configurate l'indirizzo della macchina Kali come di seguito: 192.168.240.100

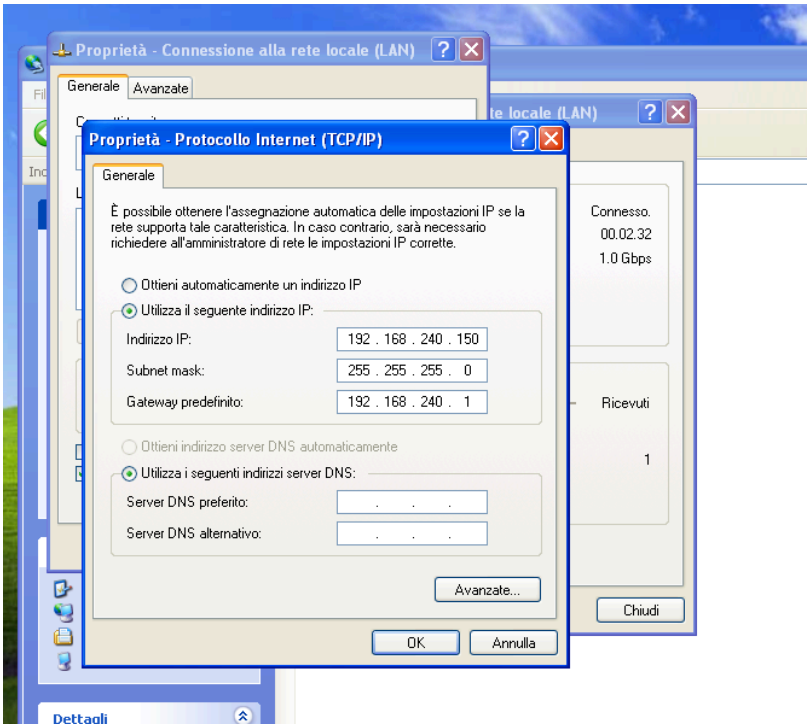
SVOLGIMENTO

Configurazione delle macchine:

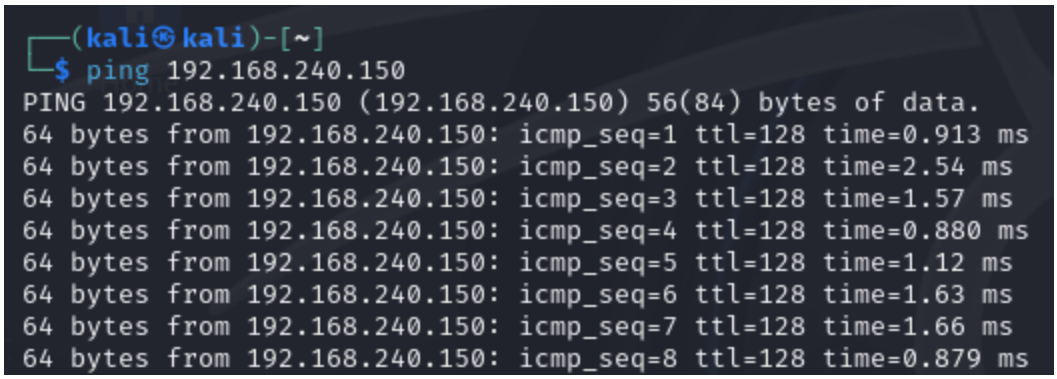
- **Kali Linux:** 192.168.240.100



- **Windows XP:** 192.168.240.150



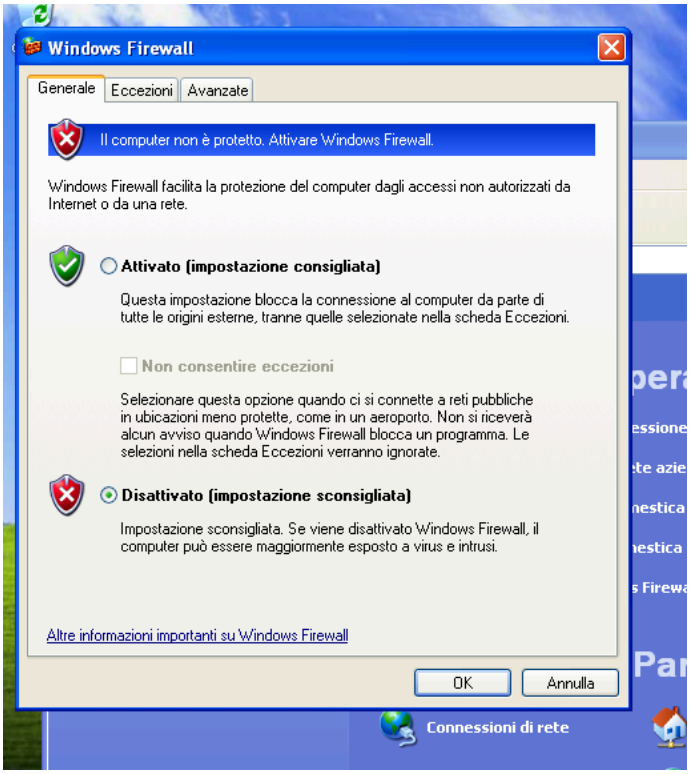
Dopo aver configurato le macchine e controllato che comunicano tra di loro correttamente,



si procede a seguire le richieste della traccia.

Si richiede di eseguire una scansione con nmap, dalla macchina Kali verso la macchina Windows XP, una volta con il firewall di Windows XP abilitato ed una volta disabilitato.

Dopo aver disabilitato il firewall di Windows, dal pannello di controllo,



Si procede, dal terminale della macchina Kali, con l'utilizzo di nmap, con il comando

nmap -sV 192.168.240.150 -o report1.txt

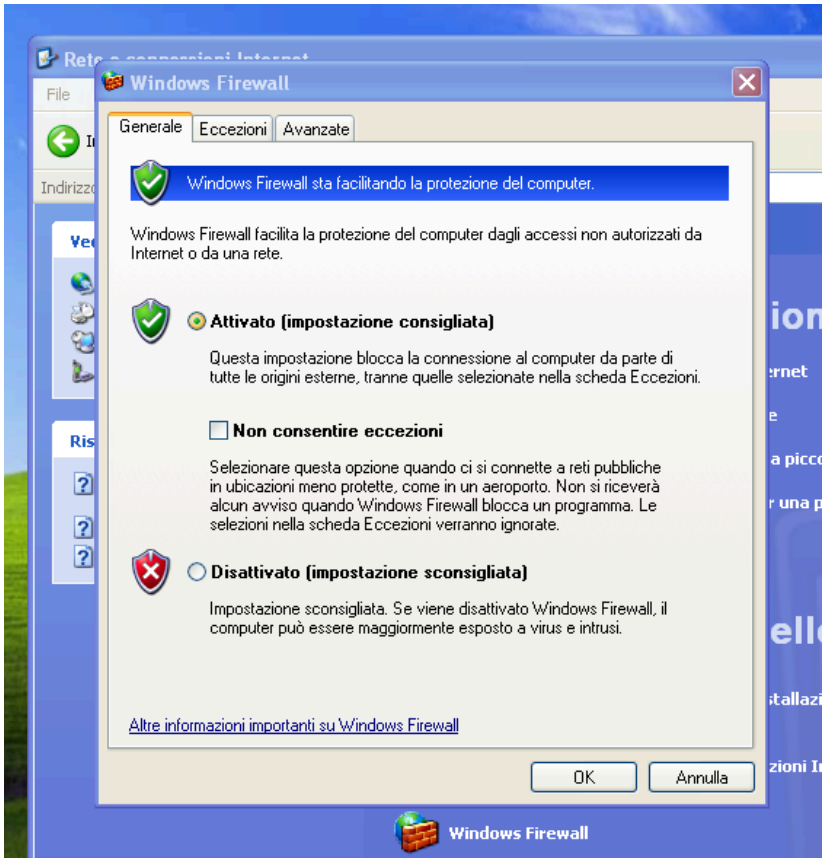
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o report1.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:21 CEST
Nmap scan report for 192.168.240.150
Host is up (0.40s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        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 8.16 seconds
```

dove:

- con **-sV** specifica le versioni dei servizi in esecuzione sulle porte aperte;
- e **-o** indichiamo di salvare l'output della scansione nel file denominato "**report1.txt**".

In allegato verranno caricati i due file txt.

Successivamente aver abilitato il firewall di Windows XP,



procedo ad eseguire un identica scansione con nmap.

Riportando, quindi, entrambi i due risultati delle scansioni, possiamo procede a valutare le eventuali differenze.

Scansione Nmap senza Firewall

- **Host**: Attivo
- **Porte aperte**:
    - 135/tcp: Microsoft Windows RPC
    - 139/tcp: Microsoft Windows netbios-ssn
    - 445/tcp: Microsoft Windows XP microsoft-ds

Scansione Nmap con Firewall

- **Host**: Sembra non attivo (Host seems down)
- **Nota**: Suggerimento di usare **–Pn** per evitare i ping probes bloccati

Differenze dei risultati

1. **Stato dell'Host**:
    - **Senza Firewall**: L'host è rilevato come attivo.
    - **Con Firewall**: L'host è rilevato come non attivo.
2. **Porte Aperte**:
    - **Senza Firewall**: Vengono rilevate tre porte aperte (135, 139, 445) con i relativi servizi.

- **Con Firewall**: Nessuna porta viene rilevata come aperta; Nmap suggerisce che l'host potrebbe essere attivo ma sta bloccando i ping probes.

Cause del Risultato Diverso

- **Firewall Abilitato**: Il firewall di Windows XP, una volta attivato, blocca i tentativi di scansione esterna, incluso il ping (ICMP Echo Request) che Nmap utilizza per determinare se l'host è attivo. Questo comportamento è standard per i firewall, che impediscono la rilevazione delle porte e dei servizi per proteggere il sistema da potenziali attacchi esterni.
- **Suggerimento di Nmap**: L'opzione -Pn bypassa i ping probes, permettendo a Nmap di effettuare la scansione delle porte anche se l'host non risponde ai ping. Questo può essere utilizzato per verificare ulteriormente la presenza di servizi sulla macchina target nonostante il firewall attivo. In questo caso non è stato utilizzato.

Nella sicurezza informatica, l'attivazione e la configurazione dei firewall sono una misura cruciale per proteggere le reti dagli attacchi. Anche se strumenti come SIEM e SOAR migliorano notevolmente la sicurezza, è di fondamentale importanza impostare in modo corretto le difese di base come i firewall.

SIEM (Security Information and Event Management)

Il SIEM raccoglie dati da varie fonti, inclusi i log dei firewall. Con il firewall attivato, il SIEM può rilevare tentativi di accesso bloccati che senza il firewall

potrebbero passare inosservati. Il SIEM normalizza e correla questi dati, identificando schemi di attacco.

Un firewall attivo fornisce dati su tentativi di scansione bloccati, offrendo una visione più completa delle minacce. Inoltre, i log dei firewall possono generare allarmi nel SIEM, segnalando tentativi di accesso non autorizzati.

SOAR (Security Orchestration, Automation, and Response)

Il SOAR può integrare i dati provenienti dai firewall e automatizzare le risposte. Con un firewall attivo, le regole del SOAR possono essere configurate per rispondere automaticamente ai tentativi di scansione bloccati. Abilitare il firewall riduce il numero di incidenti rilevabili direttamente da strumenti come Nmap, ma aumenta la rilevazione di tentativi di accesso bloccati, migliorando la capacità del SOAR di gestire gli incidenti.

Conclusione

Attivare il firewall migliora la sicurezza della rete bloccando accessi non autorizzati e fornendo dati utili per strumenti come SIEM e SOAR, che aiutano a monitorare e rispondere alle minacce in modo più efficace.