

# S9L1

## 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
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch-sV.

Inoltre, definisci un'azienda cliente a cui fornirai questo servizio che rimarrà l'azienda di cui ti farai carico per tutta la settimana in termini di sicurezza informatica.

DanteNet Solutions S.r.l. è un'azienda specializzata nella fornitura di servizi di sicurezza informatica per imprese di medie e grandi dimensioni. L'azienda si occupa di proteggere le infrastrutture IT dei clienti attraverso una combinazione di consulenza, implementazione di soluzioni di sicurezza e monitoraggio continuo. I servizi offerti includono:

- Valutazione della Sicurezza di Rete: Analisi e verifica della sicurezza delle reti aziendali per identificare vulnerabilità e rischi potenziali.
- Implementazione di Firewall e Sistemi di Prevenzione delle Intrusioni (IPS): Configurazione e gestione di firewall e sistemi IPS per proteggere le reti da accessi non autorizzati e attacchi.
- Penetration Testing: Test di penetrazione per simulare attacchi reali e identificare punti deboli nel sistema di sicurezza.
- Monitoraggio e Risposta agli Incidenti: Monitoraggio continuo delle reti e risposta immediata agli incidenti di sicurezza per minimizzare i danni.
- Formazione sulla Sicurezza: Programmi di formazione per il personale aziendale per aumentare la consapevolezza e le competenze in materia di sicurezza informatica.

DanteNet Solutions S.r.l. viene ingaggiata da SwissLab S.p.A. che è una società leader nel settore medico e delle biotecnologie, specializzata nelle analisi di laboratorio sul DNA e nelle tecnologie avanzate di ricerca medica con una solida reputazione a livello internazionale grazie alla sua eccellenza nella ricerca e nello sviluppo di soluzioni innovative per la diagnosi e il trattamento delle malattie genetiche.

SwissLab S.p.A. rappresenta una realtà all'avanguardia nel settore medico e biotecnologico, con un forte impegno verso l'innovazione e la qualità.

L'azienda offre servizi cruciali per la diagnosi e il trattamento delle malattie genetiche, supportando la comunità medica e scientifica nella diagnosi e nel trattamento dei pazienti, oltre che collaborare con diverse università in tutto il mondo.

SwissLab è consapevole della necessità di proteggere le informazioni sensibili, inclusi i dati dei pazienti, i dettagli sui prodotti medici e le informazioni proprietarie.

Per garantire la sicurezza delle proprie reti e sistemi, il cliente desidera:

- Valutare l'efficacia dei firewall esistenti su diverse versioni di sistemi operativi, inclusi quelli legacy come Windows XP, ancora in uso per alcune apparecchiature mediche.
- Identificare eventuali vulnerabilità che potrebbero essere sfruttate da attori malevoli.
- Ricevere raccomandazioni per migliorare la configurazione del firewall e altre misure di sicurezza.

**NB: il preventivo che segue include soltanto i servizi richiesti nella traccia dell'esercizio di oggi e verrà implementato nel corso della settimana nel caso di servizi aggiuntivi dati nei prossimi esercizi.**

# Preventivo #1022

DanteNet Solution S.r.l

Via xxxx Milano, Italia

P.IVA: xxxxxxxxxxxxxxxxx

## Cliente:

SwissLab S.p.A.

Via xxxxxx, Mendrisio, Svizzera

P.IVA xxxxxxxxxxxxxxxxx

**Preventivo valido fino al 30.06.2024**

- **Valutazione Iniziale: €500**  
Incontro iniziale per comprendere le esigenze specifiche e definire l'ambito del progetto.
- **Esecuzione delle Scansioni: €1500**  
Disabilitazione e abilitazione del firewall sui sistemi target.  
Esecuzione delle scansioni con Nmap nelle diverse configurazioni.
- **Report e Raccomandazioni: €1000**  
Redazione di un report dettagliato con i risultati delle scansioni e raccomandazioni.  
Presentazione del report e discussione con il team IT di SwissLab S.p.A.

**Totale Preventivo: €3000**

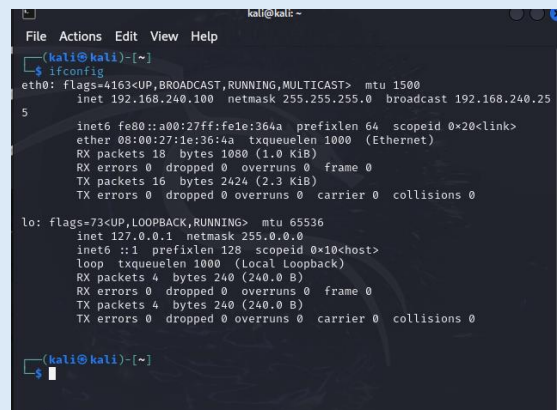
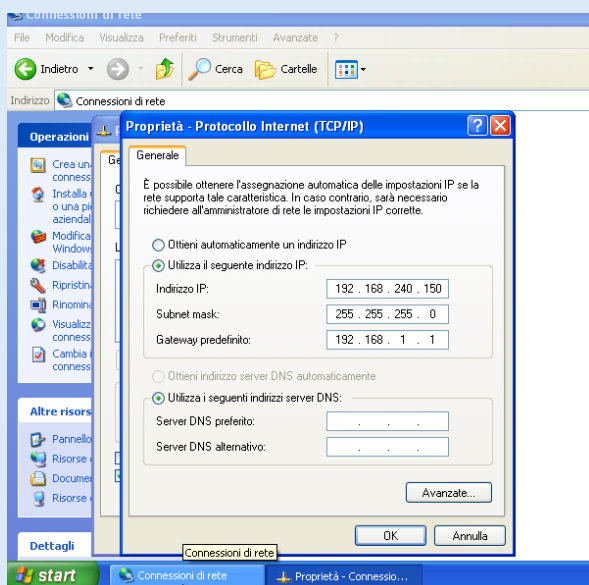
L'obiettivo dell'esercizio di oggi è quello di verificare come l'attivazione del firewall su una macchina Windows XP impatti i risultati di una scansione dei servizi effettuata dall'esterno utilizzando Nmap.

Come primo passaggio per lo svolgimento di questo esercizio, ho assegnato gli indirizzi IP richiesti alle due macchine.

Avremo quindi come da immagine

Windows XP con indirizzo IP: 192.168.240.150

Kali con indirizzo IP: 192.168.240.100.



Procedo quindi a verificare che il firewall di Windows XP sia disabilitato



Eseguo quindi la prima scansione nmap utilizzando il comando

```
nmap -sV 192.168.240.150
```

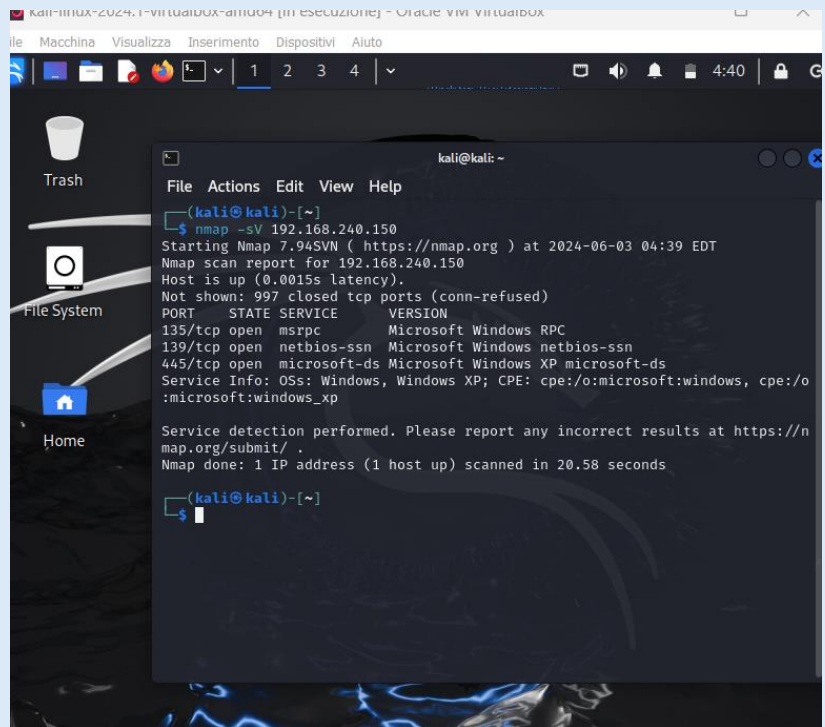
da Kali Linux per effettuare una service detection.

La scansione con il firewall disattivato ha rilevato 3 servizi in ascolto sulle seguenti porte TCP:

Porta 135: servizio Microsoft RPC

Porta 139: servizio NetBIOS-SSN

Porta 445: servizio Microsoft-DS



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:39 EDT  
Nmap scan report for 192.168.240.150  
Host is up (0.0015s 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 20.58 seconds  
  
(kali@kali)-[~]  
$
```



Tornando al pannello di controllo su Windows XP, dal centro sicurezza attivo il firewall

Eseguo nuovamente la scansione con Nmap utilizzando il comando

```
nmap -sV 192.168.240.150
```

da Kali Linux.

La scansione ha riportato che la macchina o non è accesa, oppure sta bloccando l'host discovery di Nmap.

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:41 EDT
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 3.14 seconds

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

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:43 EDT
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.29 seconds

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

Utilizzo quindi il comando

```
nmap -sV -Pn 192.168.240.150
```

per saltare il ping e passare direttamente alla service discovery.

La scansione indica che tutte le porte sembrano filtrate e non hanno risposto alle richieste dello scanner.

L'attivazione del firewall su una macchina Windows XP ha un impatto significativo sui risultati di una scansione dei servizi effettuata con Nmap.

Con il firewall disattivato, Nmap è stato in grado di rilevare tre servizi attivi sulle porte TCP 135, 139 e 445. Tuttavia, una volta attivato il firewall, la macchina ha bloccato l'host discovery di Nmap, rendendo impossibile la rilevazione dei servizi.

Utilizzando l'opzione **-Pn**, che forza Nmap a saltare il ping e procedere direttamente alla scoperta dei servizi, tutte le porte sono risultate filtrate. Questo indica che il firewall sta bloccando attivamente il traffico in ingresso, non rispondendo alle richieste di Nmap.

Questi risultati dimostrano l'efficacia del firewall di Windows XP nel bloccare tentativi di scansione esterna, aumentando significativamente la sicurezza della macchina contro possibili attacchi. L'attivazione del firewall è quindi una misura preventiva cruciale per proteggere i sistemi da traffico potenzialmente dannoso.