

# S9-L1

(Bonaldi Cristian)



## 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 nomefile` 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:

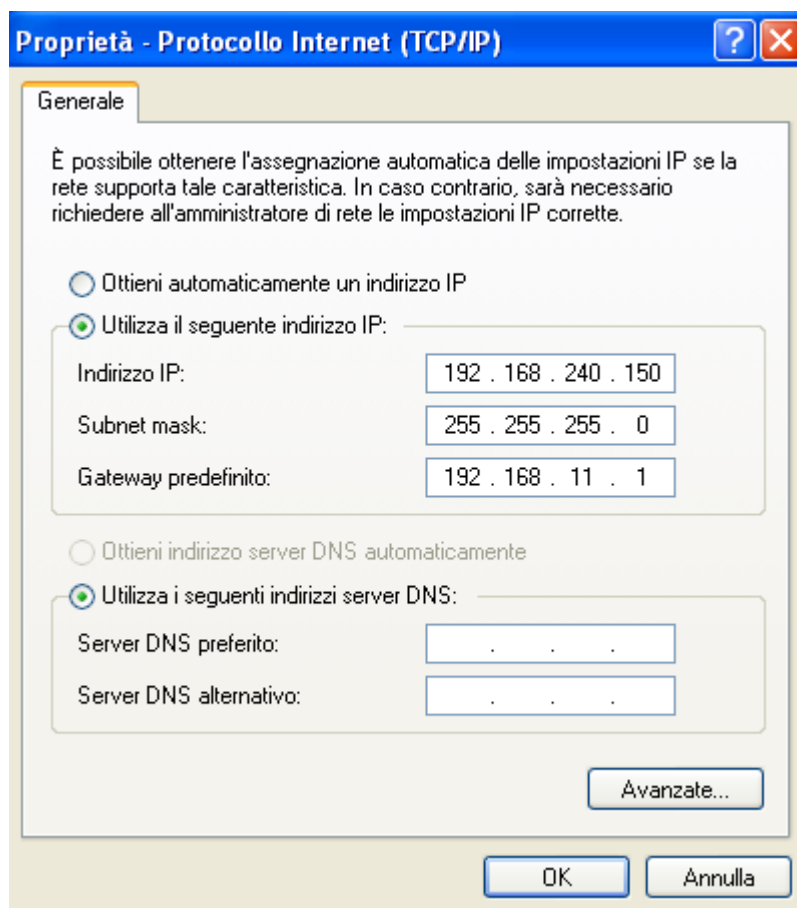
Configurate l'indirizzo di Windows XP come di seguito: 192.168.240.150

Configurate l'indirizzo della macchina Kali come di seguito: 192.168.240.100

## Esercizio:

Prima di tutto si procede alla configurazione degli indirizzi ip richiesti dalla traccia su entrambe le macchine, Windows XP e Kali Linux.

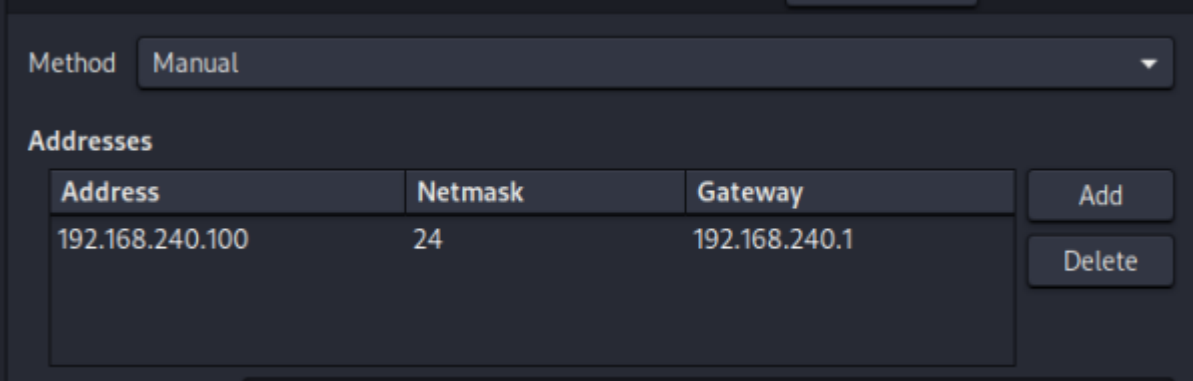
In Windows XP procediamo tramite il pannello delle configurazioni di rete, come in figura:



All'interno delle Proprietà del Protocollo Internet (TCP/IP) andiamo a configurare l'IP della macchina, la subnet mask e il gateway predefinito. Nel nostro caso l'ip sarà **192.168.240.150**.

Dopodichè andiamo ad effettuare lo stesso tipo di configurazione su Kali Linux, tramite l'interfaccia di rete sostituendo l'indirizzo IP con **192.168.240.100**.

---



The screenshot shows a network configuration window with a 'Method' dropdown set to 'Manual'. Below, the 'Addresses' section contains a table with one entry. To the right of the table are 'Add' and 'Delete' buttons.

Address	Netmask	Gateway
192.168.240.100	24	192.168.240.1

Una volta configurate le due macchine, si procede alla verifica del ping dal terminale di Kali e viceversa.

```
(kali㉿kali)-[~]  
$ ping 192.168.240.150  
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.  
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.380 ms  
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.508 ms  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.453 ms  
^C  
— 192.168.240.150 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2054ms  
rtt min/avg/max/mdev = 0.380/0.447/0.508/0.052 ms
```

---

```
Esecuzione di Ping 192.168.240.100 con 32 byte di dati:
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Statistiche Ping per 192.168.240.100:
  Pacchetti: Trasmessi = 3, Ricevuti = 3, Persi = 0 (0% persi),
  Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo = 0ms, Medio = 0ms
```

---

Stabilita la comunicazione, siamo pronti per effettuare le verifiche su Windows XP e più specificatamente cosa accade con *nmap* quando proviamo ad eseguire una scansione con firewall attivo e successivamente con firewall disabilitato sulla macchina bersaglio. Quindi ci accingiamo ad avviare nmap per scansionare l'host target con firewall disabilitato e vediamo cosa accade:

---

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150 -o scanwindowsxp.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:33 EDT
Nmap scan report for 192.168.240.150 (192.168.240.150)
Host is up (0.00030s 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: 08:00:27:5C:8D:1C (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 7.68 seconds
```

---

Il comando che andiamo ad utilizzare è:

`sudo nmap -sV 192.168.240.150 -o scanwindows.txt` , dove:

- sudo nmap**: esegue nmap con privilegi root;
- sV**: enumera i servizi attivi sulle porte aperte dell'host target;
- 192.168.240.150**: host target (Windows XP nel nostro caso);
- o scanwindowsxp.txt**: esporta il risultato della scansione in un file di testo.

Come si può notare in figura, la scansione con nmap ci restituisce le porte 135/tcp, 139/tcp, 445/tcp esposte con i relativi servizi e versioni del servizio. Questo significa che con il firewall disabilitato le porte sono visibili e i servizi vengono identificati da nmap, quindi il firewall non sta bloccando il traffico verso queste porte.

Eseguendo lo stesso tipo di scansione una volta abilitato il firewall su Windows XP:

### Funzionalità fondamentali per la sicurezza

Il Centro sicurezza PC consente di gestire le impostazioni di protezione di Windows. Per facilitare la protezione del computer, assicurarsi che le tre funzionalità fondamentali visualizzate siano contrassegnate con il valore Attivato. Se le impostazioni hanno un valore diverso da Attivato, seguire i consigli forniti. È possibile tornare al Centro sicurezza PC in qualsiasi momento, tramite il Pannello di controllo.

[Novità di Windows che facilitano la protezione del computer](#)



Accade questo:

```
(kali@kali)~$ sudo nmap -sV 192.168.240.150 -o scanwindowsxp2.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:34 EDT
Nmap scan report for 192.168.240.150 (192.168.240.150)
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.240.150 (192.168.240.150) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:5C:8D:1C (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 23.31 seconds
```

In sostanza il firewall sta filtrando il traffico verso di esse. Questo significa che nmap non riesce a rilevare né le porte esposte né i servizi attivi, contribuendo a migliorare la sicurezza dell'host target, limitando la sua esposizione a potenziali attacchi.