

SECURITY OPERATIONS

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 in formato OVA che abbiamo utilizzato nella Unit 2 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.

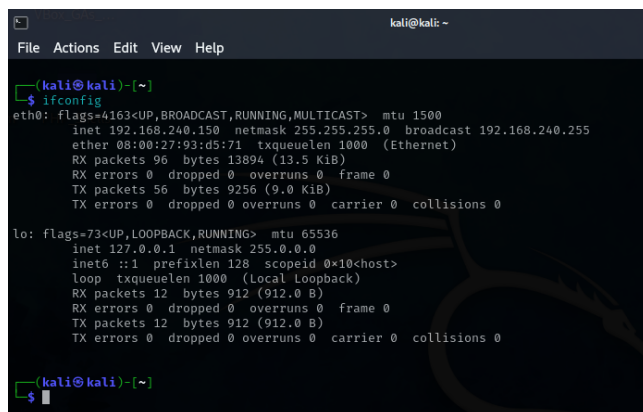
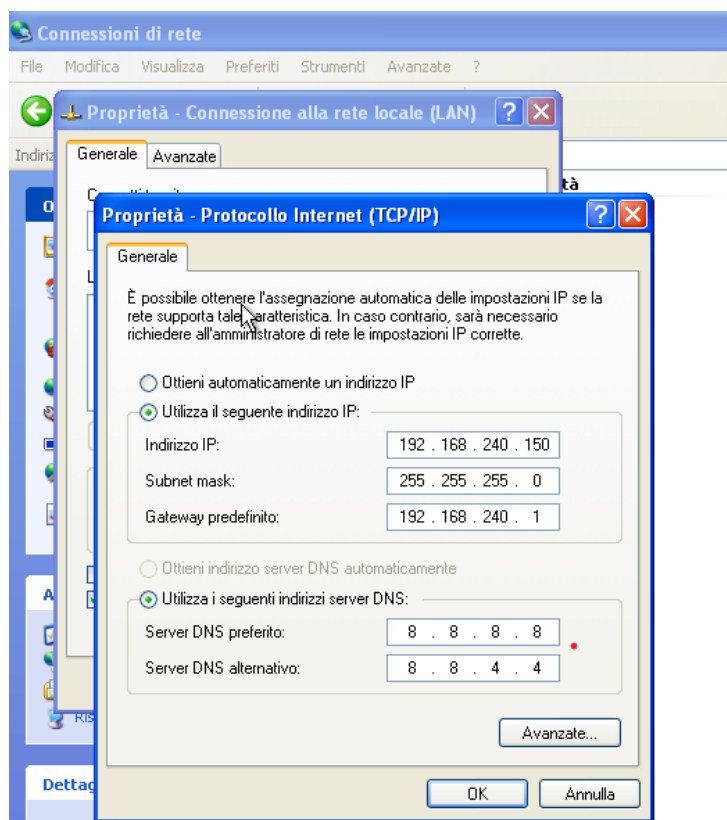
Che differenze notate? E quale può essere la causa del risultato diverso?

Requisiti:

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

Esecuzione:

Effettuiamo i cambiamenti come richiesto dalla traccia.



Primo Test: scansione con disattivazione del Firewall di Windows Xp

Disattiviamo il firewall come richiesto dalla traccia.

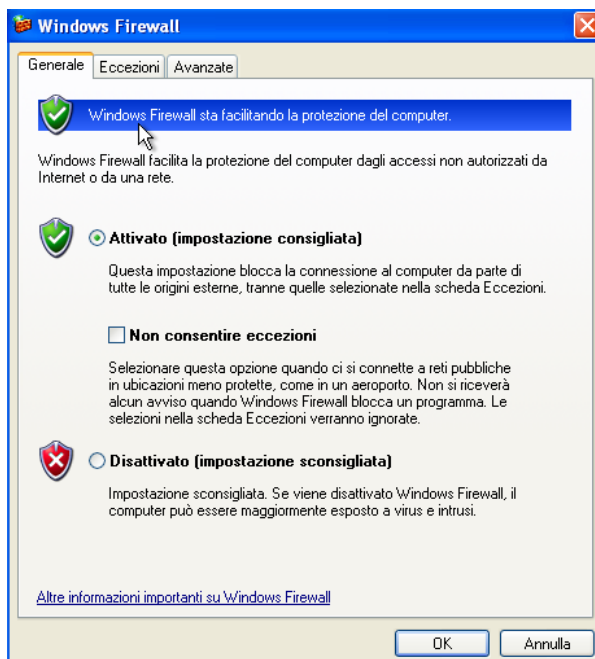


Una volta fatto, passiamo sulla macchina Kali ed effettuiamo una scansione con il comando **nmap** verso la macchina target.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-13 16:32 EDT  
Nmap scan report for 192.168.240.150  
Host is up (0.00016s 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: 08:00:27:30:69:32 (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 20.65 seconds  
  
(kali@kali)-[~]  
$
```

Secondo test: scansione con attivazione del Firewall di Windows Xp

Attiviamo il firewall come richiesto dalla traccia.



Una volta fatto, passiamo sulla macchina Kali ed effettuiamo una scansione con il comando **nmap** verso la macchina target.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
$ sudo nmap -sV 192.168.240.150  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-13 16:30 EDT  
Nmap scan report for 192.168.240.150  
Host is up (0.00032s latency).  
All 1000 scanned ports on 192.168.240.150 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:30:69:32 (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 34.70 seconds  
  
(kali@kali)~  
$
```

Differenze

Dalle scansioni effettuate in precedenza si evince che se viene abilitato un Firewall sulla macchina target (o in protezione esterna allo stesso) questo impedisce di effettuare operazioni da parte di un potenziale attaccante.

Se invece questo risulta disattivo o non presente, un'attaccante potrebbe tranquillamente effettuare scansioni ed individuare delle potenziali vulnerabilità presenti nella macchina (come nel secondo test).

La differenza principale è che nonostante vi siano delle vulnerabilità di sistema presenti nella macchina XP:

- se il firewall risulta disattivato, la macchina è esposta a rischi
- se il firewall risulta attivato, nonostante siano ancora presenti, queste vengono difese, tutelando così la macchina da accessi malevoli.

