

Esercizio 1 Settimana 9

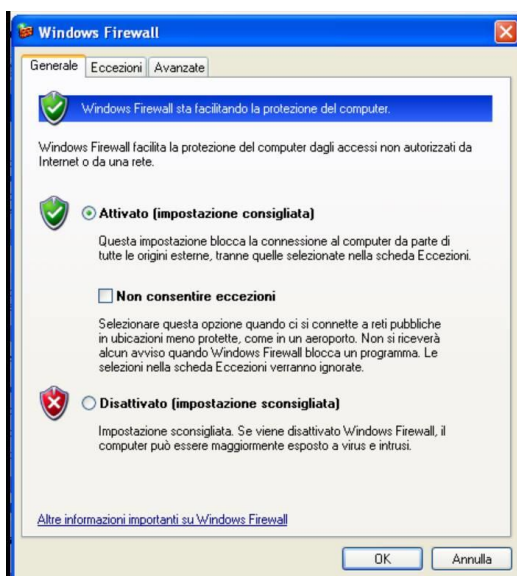
Security Operations: azioni preventive

Tra le azioni preventive per ridurre la possibilità di attacchi, abbiamo esaminato quelle relative alla rete.

Possiamo quindi andare ad attivare e/o configurare un Firewall che permetta solo a determinati indirizzi IP di generare del traffico non desiderato nella nostra rete.

Andiamo quindi ad effettuare una scansione con 'nmap' delle porte e dei relativi servizi attivi con lo switch '-sV' per la service detection sulla macchina Windows con e senza Firewall attivo.

FIREWALL ON:

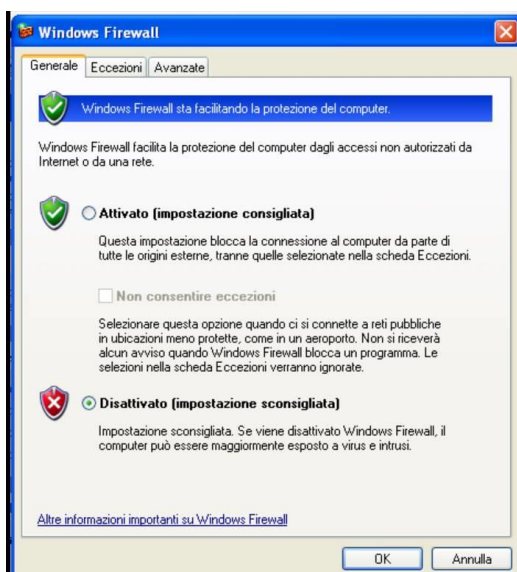


```
(root@Andrea) ~# nmap -sV 192.168.13.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 15:29 CET
Nmap scan report for 192.168.13.200
Host is up (0.00063s latency).
All 1000 scanned ports on 192.168.13.200 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:5C:59 (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 35.52 seconds

(root@Andrea) ~#
```

FIREWALL OFF:



```
(root@Andrea) ~# nmap -sV 192.168.13.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 15:27 CET
Nmap scan report for 192.168.13.200
Host is up (0.00026s 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:C6:5C:59 (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 21.04 seconds
```

Come possiamo notare, nella situazione con Firewall attivo 'nmap' non ci mostra in output alcuna informazione riguardo lo stato delle porte e i servizi attivi su di esse. Di contro ci comunica che tutte le porte scansionate su quell'IP sono in stato 'filtered': significa che per quelle determinate porte è impossibile determinarne lo stato (aperto, chiuso, etc.) a causa di restrizioni dovute, in questo caso, al Firewall. Questa casistica potrebbe sorgere anche nel momento in cui l'utente disattivi il protocollo ICMP che permette la ricezione del ping; per poter distinguere le due casistiche (ICMP o Firewall) si potrebbe utilizzare lo switch '-Pn' di 'nmap' per escludere il ping dalla scansione ed inviare le richieste direttamente senza prima preoccuparsi dello stato attivo o meno del target.

Caso contrario per la situazione di Firewall disattivato, dove 'nmap' ci restituisce le porte aperte e la relativa versione dei servizi attivi in quanto non ci sono limiti o restrizioni sulla macchina vittima.