Corso Epicode
SCANSIONE DEI SERVIZI CON NMAP pt2

Report a cura di Valentino Pizzi
21 settembre, 2025

Obbiettivo:
- Windows 10 ip 192.168.50.102

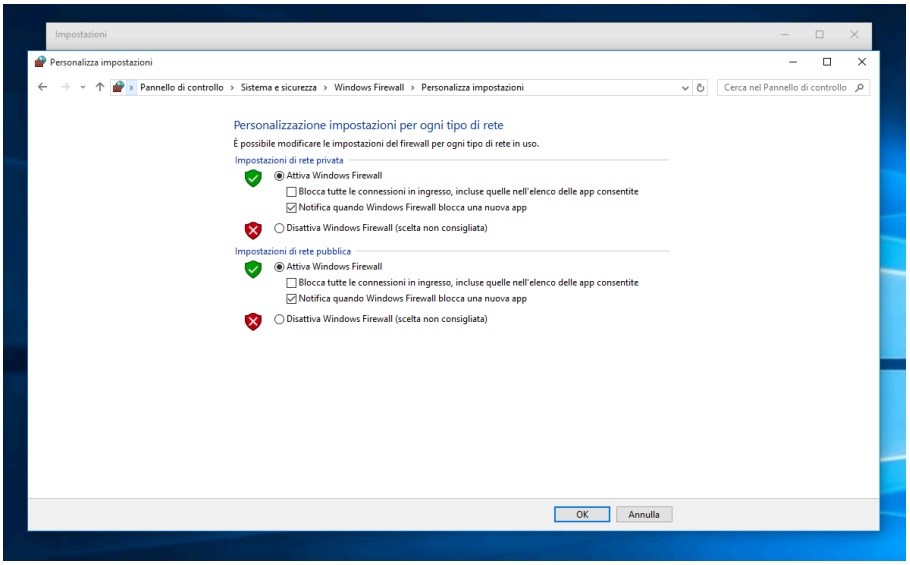
Contenuti:
- Nmap con firewall attivo
- Nmap con firewall disattivato

Obbiettivo:

Utilizzare nmap per scansire la macchina windows 10 con “IP 192.168.50.102” per raccogliere informazioni e vedere come windows firewall gestisce le richieste e protegge le porte.

Nmap con firewall attivo:

Attiviamo windows firewall sulla macchina windows 10, una volta fatto ciò mettiamo la macchina in comunicazione con la kali tramite scheda con bridge.



Avviamo la macchina kali per poter effettuare la nostra scansione usando il flag ***“-Pn”***(tratta tutti gli hosts come fossero online, salta lo step delle hosts discovery).

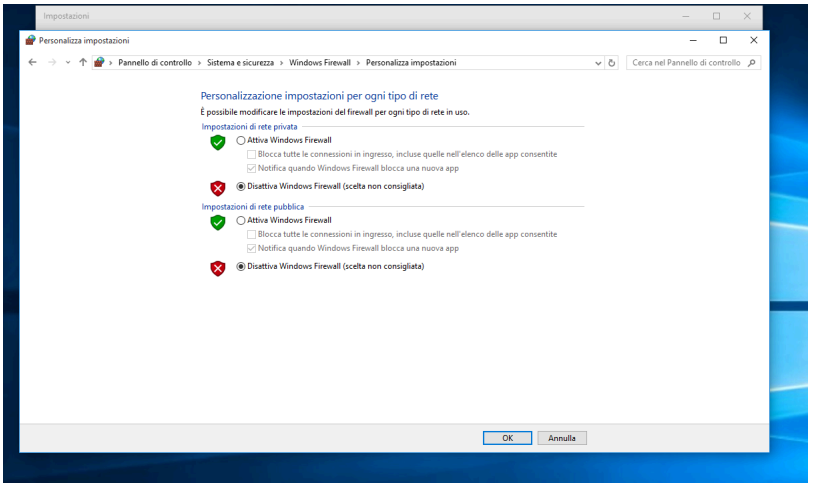
Vediamo di seguito il risultato della nostra scansione:

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 08:47 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00049s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
8443/tcp open  https-alt
MAC Address: 08:00:27:BB:1E:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.83 seconds
```

Nmap con firewall disattivato:

Disattiviamo windows firewall sulla macchina windows 10 per vedere le differenze della stessa scansione con il firewall disattivato.



Vediamo di seguito il risultato della scansione con il firewall disattivato:

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 08:59 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00044s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:BB:1E:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

Conclusioni:

Le differenze fra le scansioni eseguite sono:

- Grazie all'attivazione del firewall possiamo notare che le porte visibili con firewall attivo sono poche, ciò significa che le possibilità di penetrare la macchina sono decisamente inferiori rispetto alla disattivazione del firewall.
- Vediamo che con firewall disattivato le porte aperte sono decisamente superiori alle porte trovate con firewall attivo, possiamo constatare che le possibilità di exploiting della macchina con firewall disattivo sono ampiamente superiori.