Report – Scansione dei Servizi con Nmap – Target Windows

Francesco D'amora

Indice

Obiettivo

Verificare l'effetto del Windows Firewall sulla visibilità dei servizi di rete, eseguendo scansioni Nmap da Kali Linux verso una macchina Windows nelle condizioni di Firewall attivo e Firewall disattivato

Scansioni Nmap Utilizzate

Comando Nmap	Tipo di Scansione	Descrizione	Finalità
nmap -sS -Pn 192.168.50.102	TCP SYN Scan	Invia pacchetti SYN per rilevare porte aperte, ignorando il ping	Scansione stealth, utile se ICMP è bloccato
nmap -sT -Pn 192.168.50.102	TCP Connect Scan	Stabilisce connessioni complete con le porte, ignorando il ping	Scansione completa, usata se SYN non funziona
nmap -sV -Pn 192.168.50.102	Version Detection	Identifica i servizi attivi e le loro versioni, ignorando il ping	Riconoscere software e servizi in esecuzione
nmap -O Pn 192.168.50.102	OS Detection	Tenta di identificare il sistema operativo del target, ignorando il ping	Rilevare il tipo di sistema (Windows, Linux)

Risultati scansioni con Firewall Attivo

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 05:11 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0020s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:64:5E:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.07 seconds

┌──(kali㉿kali)-[~]
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -O -Pn 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 05:15 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0014s latency).
Not shown: 992 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
3389/tcp open  ms-wbt-server
8443/tcp open  https-alt
MAC Address: 08:00:27:64:5E:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
 port
Aggressive OS guesses: Microsoft Windows 10 1607 (97%), Microsoft Windows Phone 7.5 or 8.0 (94%)
, Microsoft Windows Embedded Standard 7 (93%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft
 Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%
), Microsoft Windows Server 2016 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008
SP1, or Windows 7 (91%), Microsoft Windows 11 21H2 (91%), Microsoft Windows Vista SP2, Windows 7
 SP1, or Windows Server 2008 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.87 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -Pn 192.168.50.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 05:25 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0038s latency).
Not shown: 992 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
3389/tcp open  ms-wbt-server
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 21.28 seconds
```

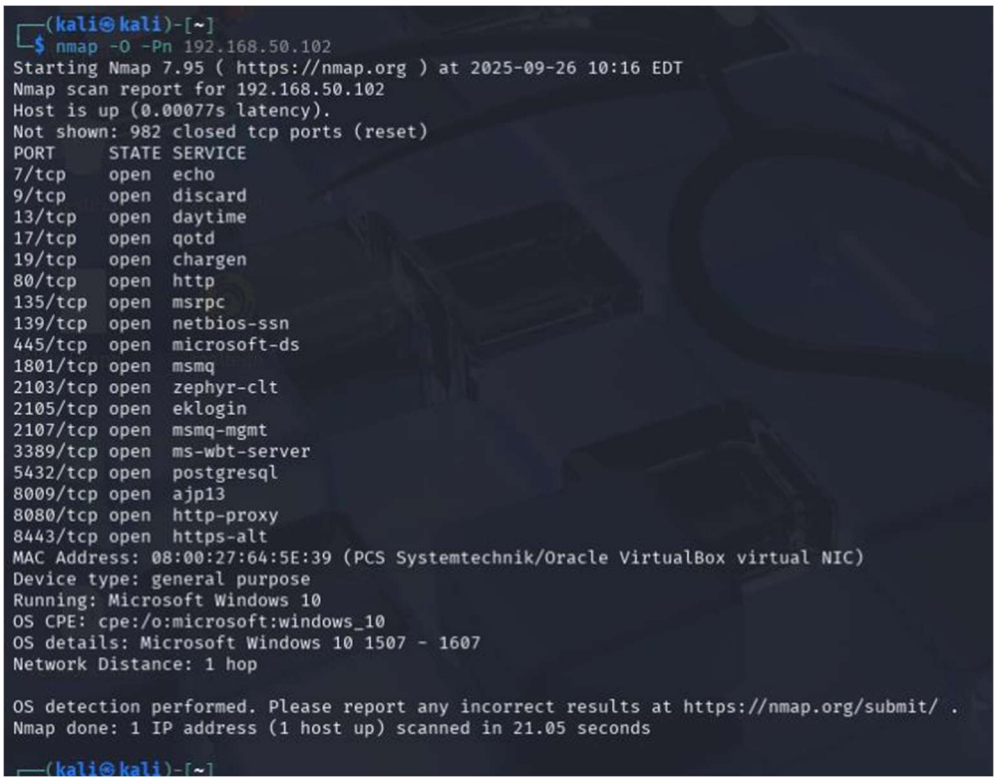
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -Pn 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 05:26 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
8443/tcp open  https-alt
MAC Address: 08:00:27:64:5E:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.81 seconds
```

Risultati scansioni con Firewall Disattivato

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -Pn 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 10:11 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00059s 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: 08:00:27:64:5E:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 20.81 seconds
```



Fase 1 – FIREWALL ATTIVATO

Attivazione del firewall con lo scopo di bloccare le connessioni in entrata non autorizzate mentre permette le connessioni liberamente in uscita

Risultati:

Porta	Servizio	Stato	Versione rilevata
135	msrpc	aperta	Microsoft RPC
445	microsoft-ds	aperta	Windows SMB
3389	ms-wbt-server	filtrata	—

FASE 2 – FIREWALL DISATTIVATO

Disattivazione del firewall in modo che ci siano comunicazioni in entrata e in uscita senza alcun filtro di protezione

Risultati:

Porta	Servizio	Stato	Versione rilevata
135	msrpc	aperta	Microsoft RPC
139	netbios-ssn	aperta	NetBIOS Session Service
445	microsoft-ds	aperta	Windows SMB
3389	ms-wbt-server	aperta	Remote Desktop Protocol
49152	unknown	aperta	—

Confronto tra le due condizioni

Porta	Firewall Attivo	Firewall Disattivato	Differenza
135	aperta	aperta	Nessuna
139	nascosta	aperta	Visibile solo senza firewall
445	aperta	aperta	Nessuna
3389	filtrata	aperta	Accessibile senza firewall
49152	nascosta	aperta	Visibile solo senza firewall

Considerazioni sulla Sicurezza

Il firewall è una barriera fondamentale contro accessi non autorizzati.
Lasciare porte aperte come 3389 (RDP) può esporre il sistema a rischi di attacco remoto.
È buona pratica mantenere il firewall attivo e configurare regole precise solo per i servizi necessari.
In ambienti di test, disattivare il firewall può aiutare nell'analisi, ma in produzione deve sempre essere attivo.
Il Windows Firewall nasconde porte e servizi, riducendo la superficie d'attacco.
Disattivandolo, Nmap rileva più porte aperte, inclusi servizi critici come RDP (3389).
Questo dimostra l'importanza del firewall nella protezione di rete.