

INDICE

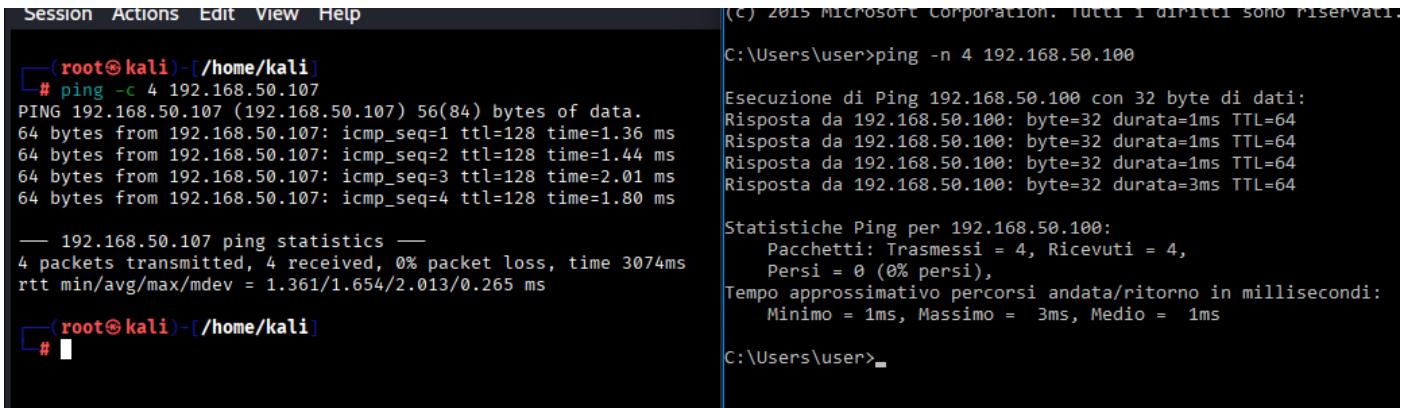
INDICE.....	1
INTRODUZIONE ED OBIETTIVO.....	2
METODOLOGIA OPERATIVA.....	3-5
CONCLUSIONE.....	6

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il presente laboratorio analizza l'impatto del **Windows Defender Firewall** sull'esposizione dei servizi di rete di una macchina Windows raggiungibile dall'esterno. L'attività è stata svolta in un ambiente controllato composto da una macchina **Kali Linux**, utilizzata per effettuare le scansioni di rete, e una macchina **Windows 10**, configurata come sistema target. Attraverso l'osservazione dei risultati delle scansioni prima e dopo l'attivazione del firewall, è stato possibile valutare come le politiche di filtraggio influenzino la visibilità delle porte e dei servizi esposti, nonché il processo di rilevamento dell'host da parte degli strumenti di analisi.

OBIETTIVO: verificare come l'attivazione del Windows Defender Firewall e il blocco del traffico ICMP incidano sui risultati di una scansione dei servizi di rete, evidenziando la riduzione della superficie d'attacco e la necessità di tecniche alternative di rilevamento quando l'host non risponde alle richieste di discovery.

METODOLOGIA OPERATIVA



```
Session Actions Edit View Help
└─(root㉿kali)-[~/home/kali]
# ping -c 4 192.168.50.107
PING 192.168.50.107 (192.168.50.107) 56(84) bytes of data.
64 bytes from 192.168.50.107: icmp_seq=1 ttl=128 time=1.36 ms
64 bytes from 192.168.50.107: icmp_seq=2 ttl=128 time=1.44 ms
64 bytes from 192.168.50.107: icmp_seq=3 ttl=128 time=2.01 ms
64 bytes from 192.168.50.107: icmp_seq=4 ttl=128 time=1.80 ms
— 192.168.50.107 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3074ms
rtt min/avg/max/mdev = 1.361/1.654/2.013/0.265 ms

└─(root㉿kali)-[~/home/kali]
# 

(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.
C:\Users\user>ping -n 4 192.168.50.100
Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=3ms TTL=64

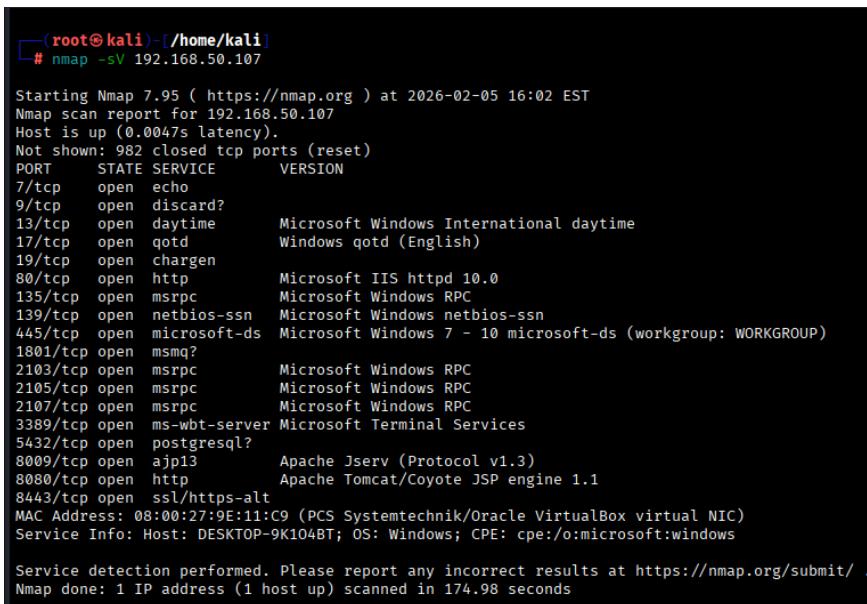
Statistiche Ping per 192.168.50.100:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 1ms, Massimo = 3ms, Medio = 1ms

C:\Users\user>
```

Prima di procedere con l'analisi dei servizi di rete, è stata verificata la corretta connettività tra le due macchine.

La verifica ha confermato che risultano correttamente raggiungibili reciprocamente, senza perdita di pacchetti e con tempi di risposta stabili.

Questo passaggio è risultato fondamentale per assicurare che i risultati delle successive scansioni fossero influenzati esclusivamente dalla configurazione del firewall e non da problemi di rete o di instradamento.



```
└─(root㉿kali)-[~/home/kali]
# nmap -sV 192.168.50.107
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-05 16:02 EST
Nmap scan report for 192.168.50.107
Host is up (0.0047s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime      Microsoft Windows International daytime
17/tcp     open  qotd        Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http         Microsoft IIS httpd 10.0
135/tcp    open  msrpc       Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
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
5432/tcp   open  postgresql?
8009/tcp   open  ajp13       Apache Jserv (Protocol v1.3)
8080/tcp   open  http        Apache Tomcat/Coyote JSP engine 1.1
8443/tcp   open  ssl/https-alt
MAC Address: 08:00:27:9E:11:C9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; 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 174.98 seconds
```

Con il Windows Defender Firewall disattivato, è stata effettuata una scansione dei servizi di rete della macchina Windows al fine di identificare le porte aperte e i servizi esposti. L'analisi ha evidenziato la presenza di numerosi servizi attivi, distribuiti su più porte TCP, inclusi servizi di rete di base, servizi di comunicazione remota e servizi web.

Il risultato della scansione mostra una superficie d'attacco ampia, caratterizzata da un'elevata visibilità dei servizi disponibili sulla macchina target.

In assenza di meccanismi di filtraggio attivi, il sistema risponde alle richieste di scansione fornendo informazioni dettagliate sui servizi in ascolto, facilitando le attività di enumerazione da parte di un potenziale attaccante.

Questa fase dell’analisi rappresenta lo scenario di riferimento iniziale, utile per confrontare in modo diretto l’efficacia delle misure di protezione introdotte successivamente tramite l’attivazione del firewall.

```
(root㉿kali)-[~/home/kali]
# nmap -sV 192.168.50.107

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-05 16:31 EST
Nmap scan report for 192.168.50.107
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.50.107 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:9E:11:C9 (PCS Systemtechnik/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 42.32 seconds
```

Dopo l’attivazione del Windows Defender Firewall sulla macchina Windows, è stata ripetuta la scansione dei servizi di rete.

A differenza dello scenario precedente, il sistema target non ha restituito informazioni sui servizi in ascolto, mostrando tutte le porte come filtrate e non rispondenti alle richieste di scansione.

Il risultato evidenzia come l’attivazione del firewall impedisca la rilevazione dei servizi di rete dall’esterno, bloccando il traffico in ingresso e limitando significativamente le informazioni ottenibili tramite attività di enumerazione.

Sebbene l’host risulti raggiungibile a livello di rete, l’assenza di risposte sulle porte scansionate indica l’efficacia delle regole di filtraggio nel mascherare i servizi attivi.

Questo confronto mette in evidenza il ruolo del firewall nella riduzione della superficie d’attacco del sistema, rendendo inaccessibili dall’esterno servizi che risultavano precedentemente visibili in assenza di protezioni attive.

```
[root@kali]~[/home/kali]
# nmap -sV -Pn 192.168.50.107

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-05 16:35 EST
Nmap scan report for 192.168.50.107
Host is up (0.0019s latency).
Not shown: 993 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
8443/tcp  open  ssl/https-alt
MAC Address: 08:00:27:9E:11:C9 (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 96.31 seconds
```

Con il Windows Defender Firewall attivo, il sistema target risulta non rispondere alle richieste di rilevamento iniziale, indicando il blocco del traffico ICMP utilizzato per l'host discovery.

In questa condizione, una scansione standard non consente di individuare servizi esposti, facendo apparire l'host come non raggiungibile o completamente filtrato.

Forzando la scansione dei servizi senza affidarsi alla fase di discovery, è stato comunque possibile rilevare un numero limitato di porte aperte; i servizi individuati risultano significativamente inferiori rispetto allo scenario con firewall disattivato e sono riconducibili a servizi esplicitamente esposti o consentiti dalle regole di filtraggio.

Questa fase evidenzia come il firewall, pur non rendendo il sistema completamente invisibile, sia in grado di ridurre drasticamente le informazioni ottenibili dall'esterno.

Il blocco del traffico ICMP contribuisce a ostacolare le attività di enumerazione, mentre la visibilità residua dei servizi dipende dalle politiche di sicurezza applicate alle singole porte.

CONCLUSIONE

L'attività svolta ha evidenziato in modo chiaro l'impatto del Windows Defender Firewall sulla visibilità dei servizi di rete esposti da un sistema Windows.

Il confronto tra le scansioni effettuate con firewall disattivato e firewall attivato mostra come l'assenza di meccanismi di filtraggio consenta una completa enumerazione dei servizi disponibili, aumentando significativamente la superficie d'attacco del sistema.

L'attivazione del firewall riduce drasticamente le informazioni accessibili dall'esterno, filtrando il traffico in ingresso e mascherando i servizi attivi; il blocco del traffico ICMP contribuisce ulteriormente a ostacolare le attività di rilevamento iniziale dell'host, rendendo meno immediata l'individuazione del sistema in rete.

Tuttavia, l'analisi ha mostrato come alcuni servizi possano rimanere accessibili qualora esplicitamente consentiti dalle regole di sicurezza, confermando che il firewall non elimina il rischio ma lo riduce in modo significativo.

Nel complesso, l'esercizio dimostra come una corretta configurazione del firewall rappresenti una misura preventiva efficace per limitare l'esposizione dei servizi e ridurre le possibilità di attacco dall'esterno, evidenziando l'importanza di politiche di sicurezza adeguate anche in contesti di rete locali e controllati.