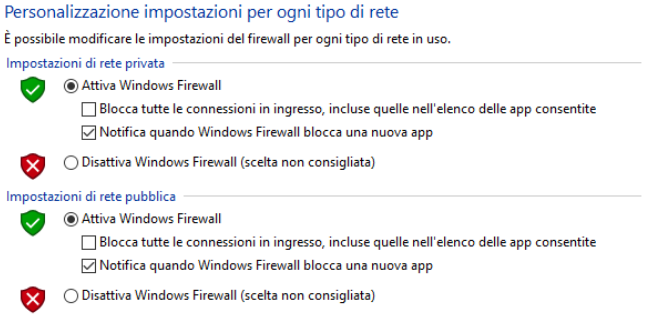
INDICE

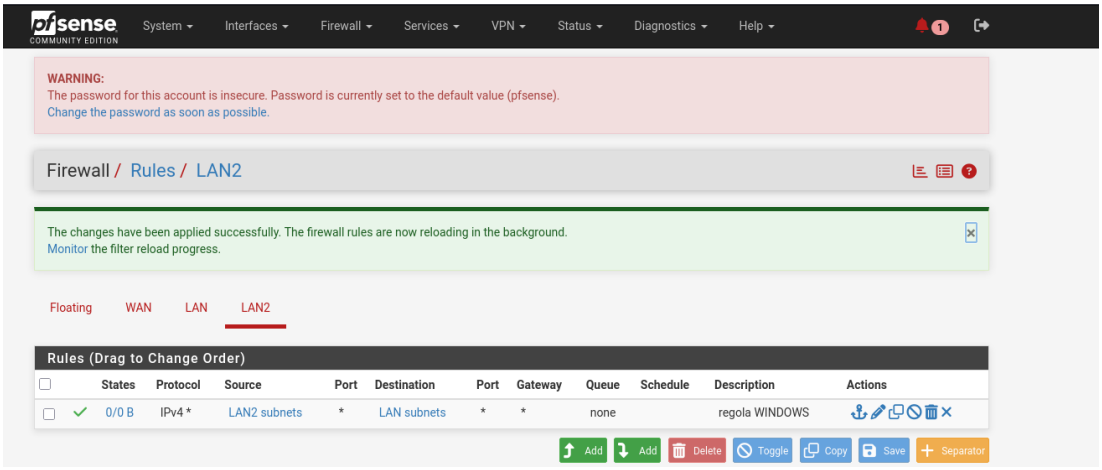
INTRODUZIONE ED OBIETTIVO

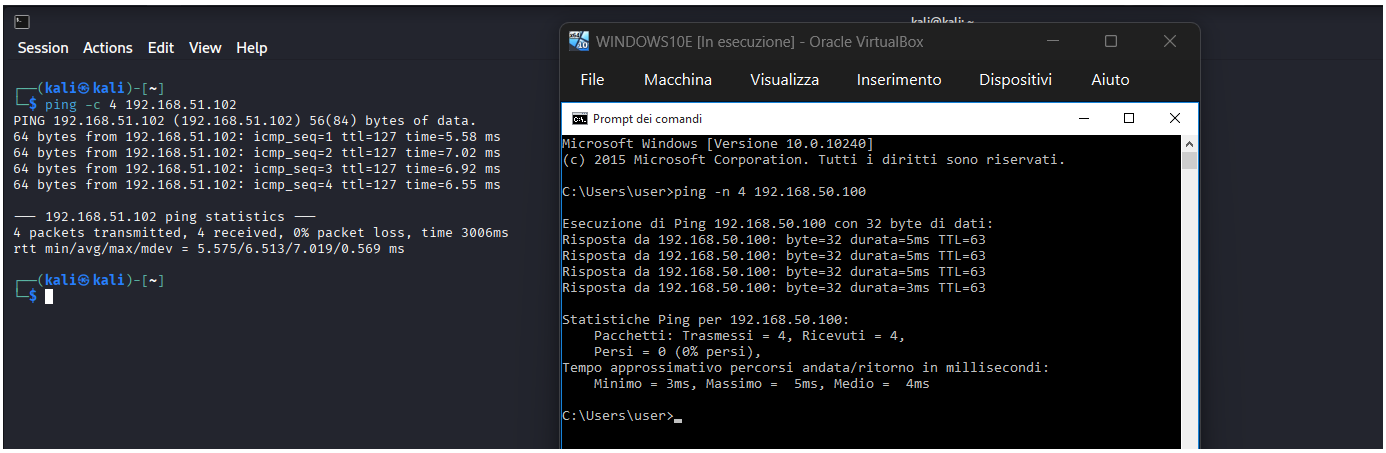
INTRODUZIONE: nel corso di questo laboratorio è stata condotta un'analisi tecnica finalizzata a osservare come un sistema Windows risponda a differenti tipologie di scansione eseguite da una macchina Linux Kali.
L'attività è stata svolta in un ambiente controllato, con le due postazioni configurate su reti distinte e collegate mediante firewall, così da poter valutare in modo realistico la superficie esposta e il comportamento dei servizi di rete in condizioni operative comuni.

OBIETTIVO: confrontare il comportamento di un sistema quando sottoposto a scansioni, osservando le differenze tra firewall attivo e disattivato.

SCANSIONE RETE DIVERSA FIREWALL ATTIVO







Per preparare l'ambiente di laboratorio è stato abilitato il firewall nativo su Windows, mantenendo il profilo attivo sia in rete privata che pubblica.
Parallelamente è stata configurata in pfSense una regola dedicata alla macchina Windows, così da consentire correttamente il traffico instradato verso le altre postazioni.
Una volta definita la regola, le due macchine sono state messe in comunicazione diretta per verificare che la rotta fosse operativa. Il test di ping ha confermato la raggiungibilità dell'host Windows da Kali e viceversa, dimostrando che la regola firewall permette il transito dell'ICMP.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:01 EST
Nmap scan report for 192.168.51.102
Host is up (0.0065s 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 4.57 seconds
```

sudo nmap 192.168.51.102 : comando utilizzato per fare uan scansione base al fine di valutare la visibilità del sistema in rete.
Il risultato ha mostrato che l'host risponde ed è correttamente raggiungibile, ma si presenta con una superficie limitata e non completamente enumerabile.
La visibilità dei servizi appare ridotta e filtrata, suggerendo che il firewall in quel momento stesse consentendo solo una parte della comunicazione mentre mascherava la restante; la macchina risulta "viva" in rete ma non libera nell'esposizione delle informazioni, indice di un controllo attivo sul traffico in ingresso.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sS 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:02 EST
Nmap scan report for 192.168.51.102
Host is up (0.0065s 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 4.75 seconds
```

sudo nmap -sS 192.168.51.102 : scansione TCP SYN per identificare servizi attivi senza instaurare una connessione completa.
Il risultato ha evidenziato che il sistema Windows espone diversi servizi in ascolto e risponde correttamente alle sonde TCP
La macchina si mostra disponibile all'interazione su più fronti applicativi, confermando che la comunicazione è aperta e che il firewall consente il traffico verso questi servizi.

In un contesto reale, questa condizione potrebbe favorire attività di enumerazione e successive analisi più approfondite.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:03 EST
Nmap scan report for 192.168.51.102
Host is up (0.010s 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
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 82.28 seconds
```

sudo nmap -sV 192.168.51.102 : scansione finalizzata al rilevamento dei servizi attivi e delle relative versioni in esecuzione sul target.
Il risultato ha evidenziato che l'host non solo è raggiungibile, ma espone applicazioni identificabili con precisione, permettendo a chi analizza la rete di comprendere quali tecnologie siano operative in quel momento.
L'acquisizione delle versioni dei servizi rende il profilo del sistema più chiaro e meno anonimo rispetto ad una scansione semplice, indicando un livello di esposizione maggiore.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -O 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:05 EST
Nmap scan report for 192.168.51.102
Host is up (0.0063s 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
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 Vista SP2, Windows 7 SP1, or Windows Server
 2008 (90%), Microsoft Windows 10 1511 (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.96 seconds
```

sudo nmap -O 192.168.51.102 : scansione orientata all'identificazione del sistema operativo tramite analisi delle risposte TCP/IP generate dalla macchina target.
L'output ha mostrato che il dispositivo è stato riconosciuto come appartenente alla famiglia Windows.
La rilevazione del SO è comunque avvenuta con un buon livello di confidenza, confermando la presenza di un host Windows attivo e permettendo di capire il contesto in cui opera. Questo risultato amplia la visibilità sulla piattaforma sottostante rispetto alla scansione precedente e dimostra che, anche in presenza di alcune protezioni o risposte filtrate, si è riusciti a ricavare indicazioni utili sul tipo di macchina, fondamentale nella comprensione dell'ambiente e nella pianificazione di analisi successive.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -p 1-1024 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:05 EST
Nmap scan report for 192.168.51.102
Host is up (0.0065s latency).
Not shown: 1022 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc

Nmap done: 1 IP address (1 host up) scanned in 4.80 seconds
```

sudo nmap -p 1-1024 192.168.51.102 : scansione mirata sul range di porte dalla 1 alla 1024.
Il risultato ha evidenziato che solo poche porte risultano effettivamente raggiungibili, mentre la quasi totalità appare filtrata o non rispondente.
Questo comportamento conferma che l'host è visibile ma espone un numero minimo di servizi, segnale di un traffico controllato e potenzialmente mediato dal firewall.
Il sistema quindi risulta presente in rete, ma con un perimetro ridotto e già parzialmente protetto, consentendo di mappare solo servizi essenziali senza rivelare dettagli più approfonditi nella fase iniziale dell'analisi.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sC -sV 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:06 EST
Nmap scan report for 192.168.51.102
Host is up (0.0063s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
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
|_ssl-date: 2025-12-06T16:08:06+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=DESKTOP-9K1O4BT
| Not valid before: 2025-09-25T19:23:17
|_Not valid after:  2026-03-27T19:23:17
8443/tcp open  ssl/https-alt
|_http-server-header: Microsoft-HTTPAPI/2.0
| ssl-cert: Subject: commonName=DESKTOP-9K1O4BT
| Not valid before: 2024-07-09T16:53:31
|_Not valid after:  2029-07-09T16:53:31
|_http-title: Not Found
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 86.72 seconds
```

sudo nmap -sC -sV 192.168.51.102: Scansione avanzata con script e rilevamento versione dei servizi per ottenere informazioni più profonde sulle applicazioni esposte dalla macchina.
In questo passaggio è stata eseguita una scansione più completa, che non si limita a verificare la presenza della macchina sulla rete, ma permette di analizzare nel dettaglio i servizi che sono attivi al suo interno.
L'output ottenuto conferma che il dispositivo è attivo, operativo e dotato di diversi servizi raggiungibili, mostrando anche informazioni aggiuntive come certificati e caratteristiche del web server.

Questo livello di approfondimento consente di capire come il sistema si presenta verso l'esterno e quali componenti sono effettivamente esposti, aumentando la comprensione generale dell'ambiente analizzato.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sC -sV -p 80,135,139,445,3389,8443 192.168.51.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:09 EST
Nmap scan report for 192.168.51.102
Host is up (0.0042s latency).

PORT     STATE    SERVICE       VERSION
80/tcp   open     http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
135/tcp  open     msrpc         Microsoft Windows RPC
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
3389/tcp open     ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DESKTOP-9K1O4BT
| Not valid before: 2025-09-25T19:23:17
|_Not valid after:  2026-03-27T19:23:17
| rdp-ntlm-info:
|   Target_Name: DESKTOP-9K1O4BT
|   NetBIOS_Domain_Name: DESKTOP-9K1O4BT
|   NetBIOS_Computer_Name: DESKTOP-9K1O4BT
|   DNS_Domain_Name: DESKTOP-9K1O4BT
|   DNS_Computer_Name: DESKTOP-9K1O4BT
|   Product_Version: 10.0.10240
|_  System_Time: 2025-12-06T16:10:38+00:00
|_ssl-date: 2025-12-06T16:10:43+00:00; +1s from scanner time.
8443/tcp open     ssl/https-alt
| ssl-cert: Subject: commonName=DESKTOP-9K1O4BT
| Not valid before: 2024-07-09T16:53:31
|_Not valid after:  2029-07-09T16:53:31
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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 83.24 seconds
```

sudo nmap -sC -sV -p 80,135,139,445,3389,8443 192.168.51.102 : scansione avanzata focalizzata su specifiche porte, con esecuzione di script e identificazione della versione dei servizi per ottenere una visione dettagliata delle applicazioni effettivamente esposte dal sistema.

Il risultato ha confermato la presenza attiva dei servizi mirati, fornendo informazioni aggiuntive come intestazioni web, certificati, nome della macchina e dettagli di dominio, aumentando nettamente la visibilità sulla configurazione reale del sistema.

Questo ha permesso di comprendere con maggiore precisione quali componenti sono pubblicamente raggiungibili e in che modo il dispositivo risponde alle richieste, evidenziando un quadro più completo rispetto alle scansioni precedenti e fornendo basi utili per eventuali analisi successive.

SCANSIONE RETE DIVERSA FIREWALL DISATTIVO

Per proseguire con la fase comparativa è stato configurato Windows con firewall disattivato sia sul profilo privato che su quello pubblico, questa scelta ha permesso di osservare il comportamento della macchina senza filtri o blocchi applicativi, lasciando il traffico in entrata completamente libero.
In questo scenario la comunicazione tra Kali e Windows avviene in modo diretto, senza interventi di controllo sulle porte, permettendo alla scansione di raccogliere informazioni in modo molto più esteso rispetto alla fase precedente.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:17 EST
Nmap scan report for 192.168.51.102
Host is up (0.062s 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

Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
```

sudo nmap 192.168.51.102 : scansione base in rete diversa con firewall disattivato per verificare la visibilità reale del sistema quando non sono presenti filtri.
Il risultato ha mostrato una risposta immediata e la presenza di un numero nettamente superiore di servizi attivi rispetto al test precedente con firewall abilitato.
Sono emerse molte più porte aperte, incluse applicazioni e componenti non rilevate in precedenza, evidenziando come l'assenza del firewall esponga la macchina quasi integralmente alla rete.
Rispetto allo scenario protetto, la superficie d'interazione risulta molto ampia e accessibile, segnale di un livello di sicurezza ridotto e di un potenziale rischio maggiore qualora il sistema fosse inserito in contesti reali o non controllati.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sS 192.168.51.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:17 EST
Nmap scan report for 192.168.51.102
Host is up (0.042s 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

Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
```

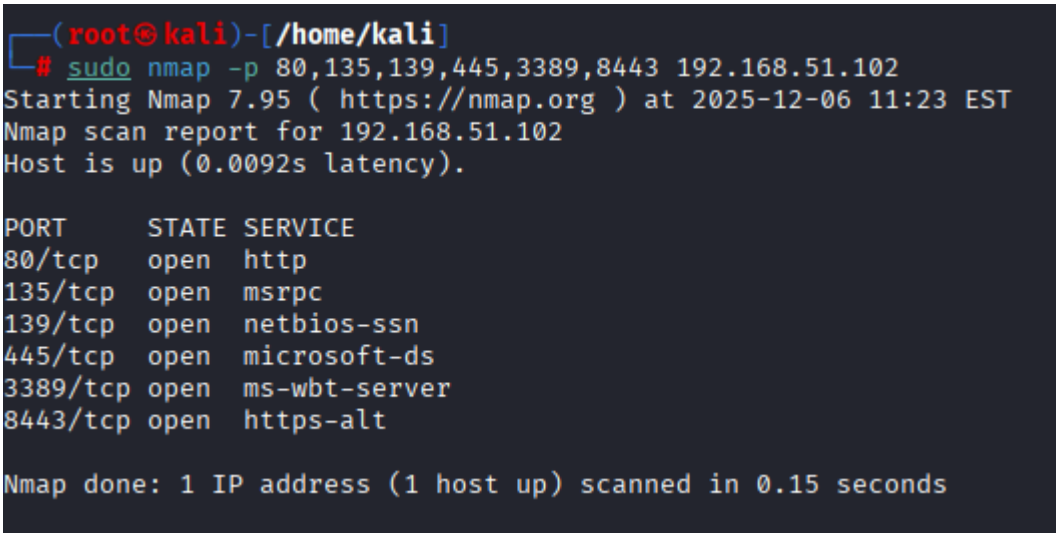
sudo nmap -sS 192.168.51.102 : scansione SYN mirata all'individuazione dei servizi effettivamente raggiungibili senza stabilire una connessione completa.
Il risultato ha evidenziato un numero elevato di porte aperte rispetto al test con firewall attivo, mettendo in chiaro che la macchina risulta pienamente visibile e interrogabile all'interno della rete.
È stato possibile riconoscere diversi servizi applicativi, confermando che la rimozione del firewall amplia drasticamente la superficie esposta e rende molto più semplice raccogliere informazioni sull'host.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -O 192.168.51.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:20 EST
Nmap scan report for 192.168.51.102
Host is up (0.025s 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
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1607
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.48 seconds
```

sudo nmap -O 192.168.51.102 : scansione orientata all'identificazione del sistema operativo tramite analisi delle risposte dell'host.
L'output ha confermato con precisione che il sistema in esecuzione è Windows 10 e ha messo in evidenza un contesto operativo completamente esposto, con numerosi servizi raggiungibili senza restrizioni.
La rilevazione è stata immediata e senza particolari difficoltà, segno che l'assenza del firewall lascia aperta la strada alla raccolta di informazioni tecniche sensibili, ampliando notevolmente la visibilità sulla macchina e sul suo profilo software.



sudo nmap -p 80,135,139,445,3389,8443 192.168.51.102 : scansione mirata verso porte specifiche di interesse per verificare rapidamente quali servizi risultano attivi e rispondenti. Il risultato ha mostrato che tutte le porte selezionate sono accessibili senza restrizioni, confermando un livello di esposizione elevato e privo di filtri difensivi.
Questo evidenzia come, in assenza di firewall, sia possibile ottenere informazioni puntuali e immediate sui servizi attivi, aumentando i rischi legati alla visibilità diretta dei punti di accesso presenti nel sistema.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:24 EST
Nmap scan report for 192.168.51.102
Host is up (0.041s 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
Service Info: Host: DESKTOP-9K1O4BT; 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 160.42 seconds
```

sudo nmap -sV 192.168.51.102 : scansione orientata all'identificazione dei servizi attivi con rilevamento della loro versione.
L'esito ha permesso di ottenere una visione estremamente dettagliata dell'infrastruttura applicativa presente sulla macchina, con informazioni precise sulle tecnologie in uso (HTTP, RPC, PostgreSQL, Terminal Services, ecc.) e sulle relative versioni software. Questo livello di dettaglio, irraggiungibile quando il firewall era attivo, dimostra come la rimozione dei filtri renda la superficie esposta molto più ampia e facilmente analizzabile, consentendo di ricostruire l'ambiente operativo in modo quasi completo e senza ostacoli.

CONCLUSIONE

L’attività ha mostrato con chiarezza quanto il firewall influenzi la visibilità di un sistema in rete e il livello di informazioni ottenibili tramite scansione.
Con il firewall attivo, la superficie esposta risultava ridotta e più difficile da interpretare, con servizi parzialmente visibili e identificazione limitata.
Ma ,una volta disabilitata la protezione, il sistema è apparso completamente aperto: le scansioni hanno restituito un quadro molto più ricco, con porte, versioni dei servizi e dettagli sul sistema operativo immediatamente disponibili.
Questo confronto evidenzia quanto un corretto controllo del traffico sia determinante nella protezione di un host, poiché anche una semplice rimozione delle regole di filtraggio consente a un osservatore esterno di ottenere informazioni critiche sull’infrastruttura interna.