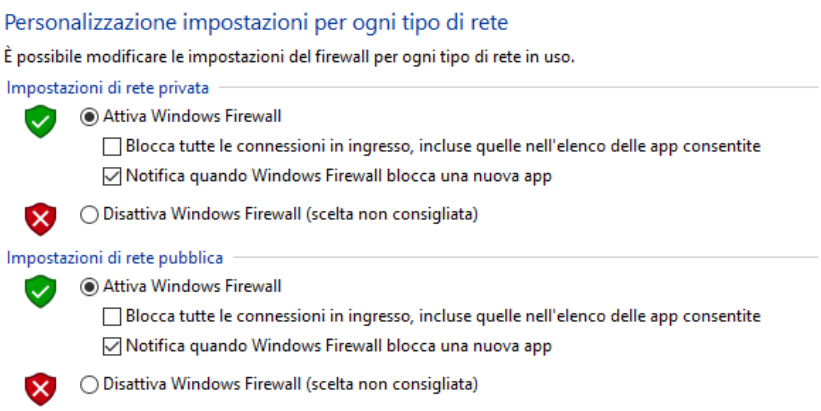
INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: in questo laboratorio è stata analizzata la comunicazione tra due macchine, Kali Linux e Windows, configurate all'interno della stessa rete.
Una volta confermata la raggiungibilità tramite ping, è stata avviata una serie di scansioni Nmap per verificare quali servizi risultassero visibili.

OBIETTIVO: verificare come un host risulti visibile e interrogabile da una macchina , quando entrambi operano nello stesso segmento di rete.



Per avviare la sessione di test interna è stato verificato che il sistema Windows avesse il firewall attivo su entrambi i profili di rete (privata e pubblica).
In questa configurazione la macchina mantiene un livello di protezione predefinito, consentendo solo connessioni ritenute sicure e bloccando tentativi non autorizzati.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap 192.168.50.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 14:24 EST
Nmap scan report for 192.168.50.102
Host is up (0.0094s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE
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
5357/tcp open  wsdapi
8443/tcp open  https-alt
MAC Address: 08:00:27:4E:73:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

sudo nmap 192.168.50.102: Il comando ha permesso di verificare la visibilità dell'host e osservare quali servizi risultano accessibili senza impiegare tecniche approfondite.
L'analisi ha mostrato che la macchina risponde regolarmente, segno della corretta comunicazione in rete locale, ma con un'esposizione controllata: alcuni servizi risultano disponibili ma non in modo completamente esteso, lasciando intuire che il firewall continui a filtrare parte del traffico. In sintesi, la macchina è individuabile e raggiungibile, ma rimane protetta da un livello di controllo che limita ciò che viene esposto all'esterno.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sS 192.168.50.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 14:26 EST
Nmap scan report for 192.168.50.102
Host is up (0.0027s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE
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
5357/tcp open  wsdapi
8443/tcp open  https-alt
MAC Address: 08:00:27:4E:73:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.31 seconds
```

sudo nmap -sS 192.168.50.102: scansione SYN più approfondita eseguita nella stessa rete, utile per ottenere una visione più dettagliata dello stato delle porte aperte senza completare la connessione TCP.

Rispetto alla scansione base, emergono più servizi attivi e correttamente raggiungibili, con una risposta più chiara sulle porte disponibili. Il risultato conferma che il sistema espone diversi servizi di comunicazione, indicando una superficie di rete più ampia e verificabile internamente, pur rimanendo in un contesto controllato in cui l'host risponde in modo diretto e stabile ai tentativi di contatto.

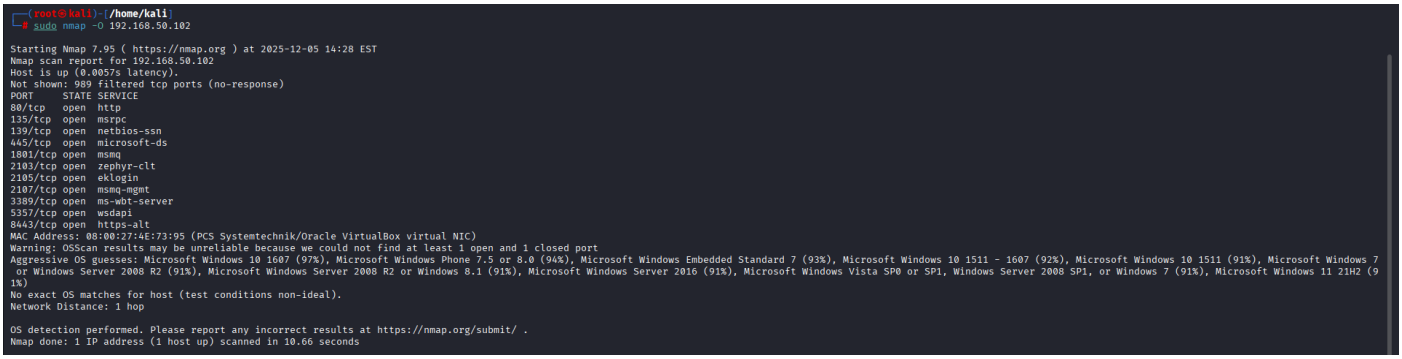
```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV 192.168.50.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 14:26 EST
Nmap scan report for 192.168.50.102
Host is up (0.0023s latency).
Not shown: 989 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
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
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:4E:73:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 81.83 seconds
```

sudo nmap -sV 192.168.50.102 : scansione orientata all'identificazione delle versioni dei servizi presenti sulla macchina, utile per associare ogni porta aperta alla relativa applicazione in esecuzione.

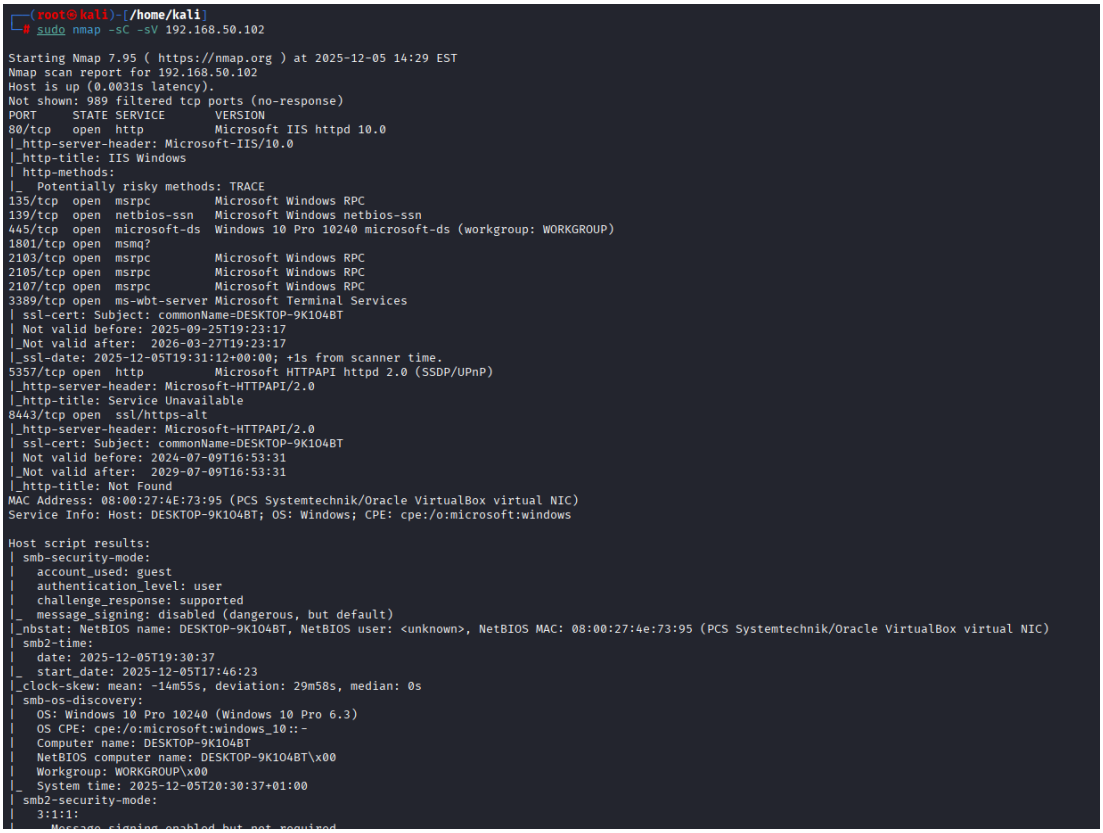
Il risultato ha permesso di distinguere in modo chiaro quali servizi rispondono sul sistema e con quale tecnologia, riconoscendo componenti Microsoft e servizi attivi tipici dell'ambiente Windows; questa visibilità più approfondita aggiunge contesto rispetto alle scansioni precedenti, evidenziando la natura dei servizi esposti e confermando che la macchina è operativa e fruibile in rete con un set definito di applicazioni raggiungibili.



sudo nmap -O 192.168.50.102: scansione mirata all'identificazione del sistema operativo tramite analisi delle risposte di rete, utile per ricavare informazioni sul tipo di piattaforma in esecuzione.

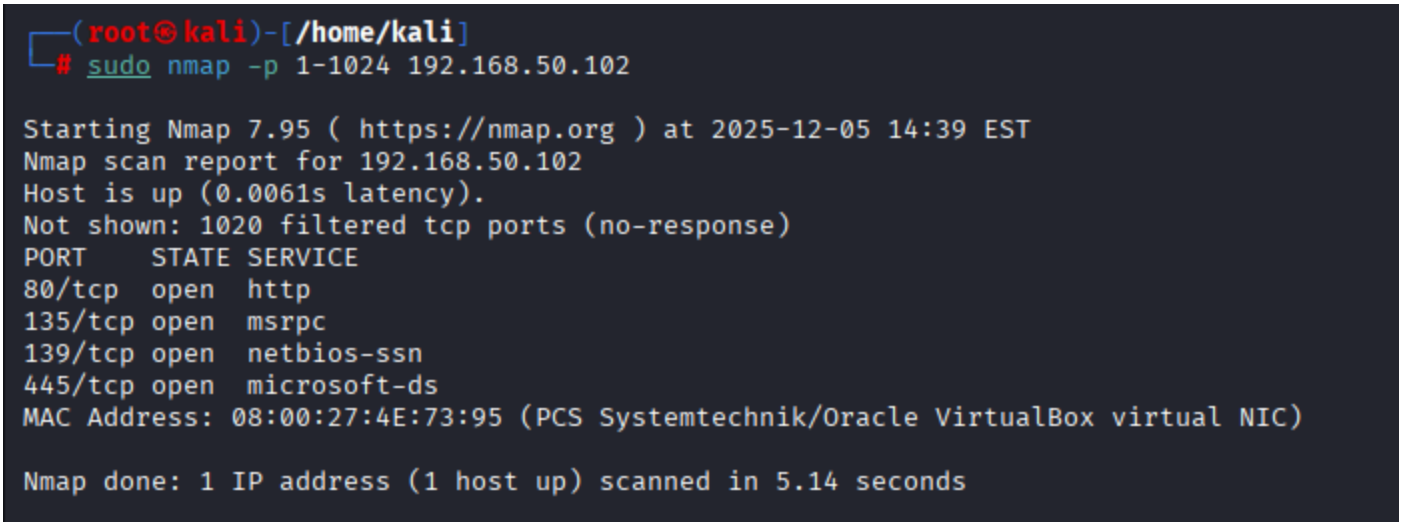
L'output ha suggerito con buona accuratezza che l'host appartiene alla famiglia Windows, restituendo diverse possibili versioni compatibili e confermando la natura del sistema analizzato.

Questo permette di contestualizzare meglio l'ambiente e di comprendere quali tecnologie è plausibile trovare attive sulla macchina, ampliando la visibilità rispetto a una semplice scansione delle porte.

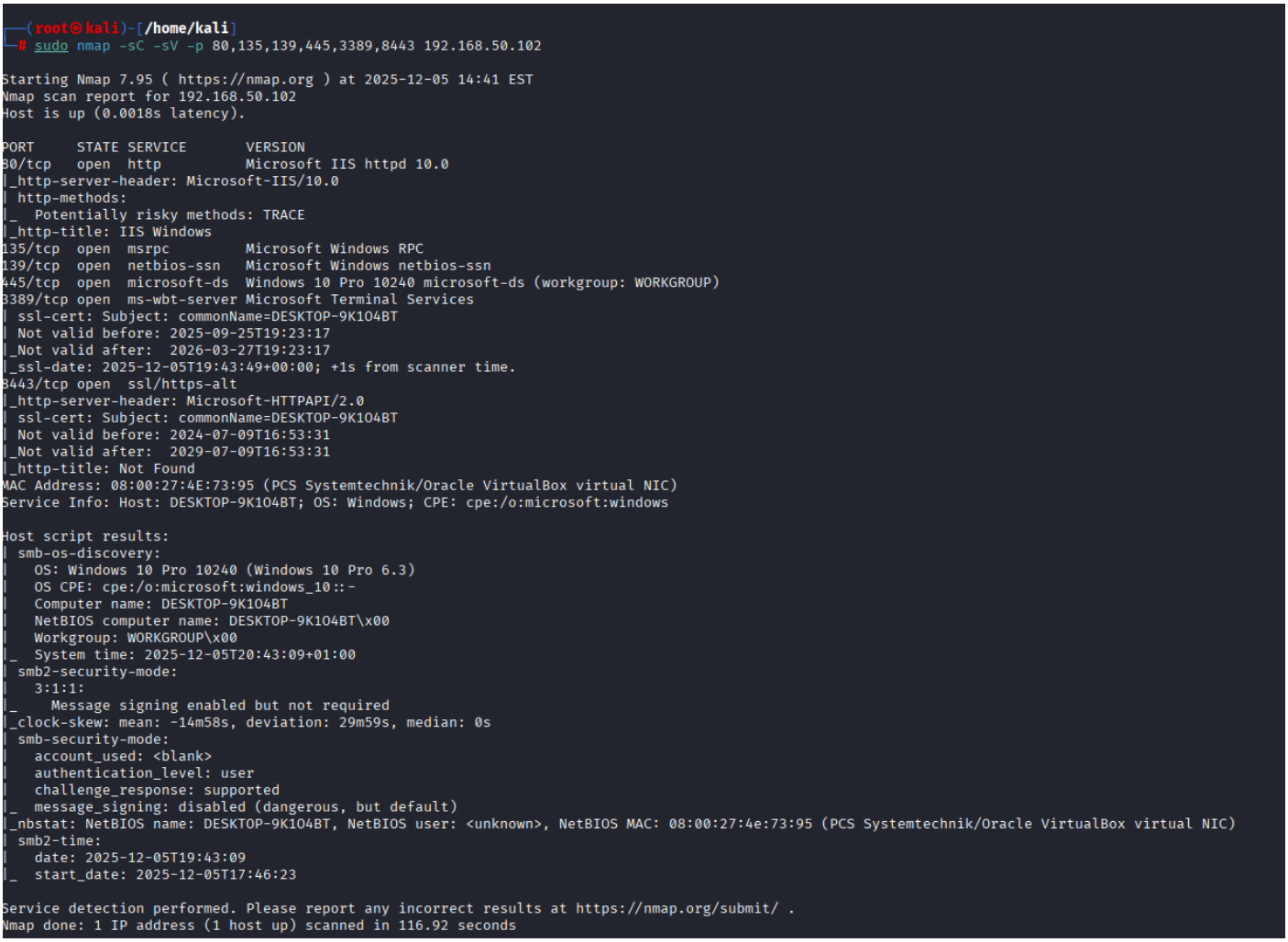


sudo nmap -sC -sV 192.168.50.102: scansione avanzata con script e rilevamento versione dei servizi per ottenere informazioni più profonde sulle applicazioni esposte dalla macchina. L'output ha mostrato non solo le porte aperte ma anche i servizi attivi, le versioni associate e ulteriori dettagli come certificati SSL, intestazioni HTTP ecc.

Questo livello di dettaglio offre una fotografia molto più completa del sistema, permettendo di comprendere quali componenti software sono presenti e quanto l'host risulti esposto o potenzialmente interrogabile da altri dispositivi presenti nella stessa rete.



sudo nmap -p 1-1024 192.168.50.102: scansione mirata sulle porte comprese nel range 1–1024, con l'obiettivo di verificare quali servizi fondamentali risultassero attivi sulla macchina. Il risultato ha evidenziato solo un numero ristretto di porte aperte, segnale di una superficie esposta contenuta e presumibilmente protetta.
Questo comportamento conferma che l'host espone solo i servizi essenziali, riducendo la visibilità esterna rispetto a una scansione completa e lasciando intendere che il sistema mantenga un livello di controllo sui servizi pubblicamente raggiungibili.



sudo nmap -sC -sV -p 80,135,139,445,3389,8443 192.168.50.102: scansione avanzata concentrata su porte specifiche, con l'obiettivo di identificare non solo quali servizi risultassero attivi ma anche quali versioni fossero in esecuzione.

L'analisi ha restituito un quadro molto dettagliato della macchina: sono stati riconosciuti servizi web, servizi di comunicazione Microsoft e componenti legati all'infrastruttura Windows, inclusi certificati e metadati di sistema.

Oltre alla semplice rilevazione delle porte aperte, lo scan ha evidenziato informazioni interne quali hostname, dominio di lavoroecc.

Questo risultato ha permesso una visione più profonda del sistema, utile per comprenderne il contesto operativo e l'eventuale livello di configurazione interna.

CONCLUSIONE

Nel contesto interno con firewall attivo, Windows è risultato raggiungibile ma solo parzialmente esplorabile.
Le scansioni hanno rilevato la presenza del sistema e alcuni servizi in ascolto, ma con una visibilità limitata e filtrata, segno che il firewall ha ridotto l'esposizione del dispositivo e impedito una rilevazione completa.
L'analisi evidenzia quindi un livello di protezione efficace all'interno della rete locale: la macchina risulta presente e operativa, ma mantiene un profilo contenuto e meno trasparente, permettendo l'accesso solo a ciò che è consentito dalle policy di difesa attive.