INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: nel corso dell'attività è stata condotta una valutazione strutturata del sistema Metasploitable avente indirizzo 192.168.50.101, attraverso una serie di analisi di rete finalizzate a comprenderne lo stato operativo.
L'intervento ha previsto l'esecuzione di una scansione completa delle porte e dei servizi esposti, unitamente a un'osservazione approfondita dei comportamenti del nodo quando interrogato da diverse tipologie di richieste. Questa fase è servita a ottenere una fotografia chiara, affidabile e quanto più completa possibile della configurazione attuale del sistema, evidenziando la quantità e la natura dei servizi in ascolto e la loro risposta ai controlli esterni.

OBIETTIVO: identificare i servizi operativi del sistema e valutarne la struttura complessiva. In aggiunta, si è mirato a rilevare eventuali criticità che potessero suggerire un utilizzo non ordinario o non allineato agli standard attesi.

SCANSIONE PORTE

```
┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.50.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 11:47 EST
Nmap scan report for 192.168.50.101
Host is up (0.0017s latency).
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

nmap -sn 192.168.50.101 : il comando esegue una **ping scan**, una modalità in cui Nmap verifica esclusivamente se un host è attivo sulla rete senza analizzare le porte. Tecnicamente, il tool invia una serie di richieste *ICMP/ARP* e attende una risposta per confermare la presenza del dispositivo.

Nel nostro caso, il comando ha confermato che l'host 192.168.50.101 è **raggiungibile e operativo**, ha restituito un tempo di risposta estremamente ridotto e ha rilevato anche l'indirizzo MAC associato all'interfaccia di rete.
Questo indica che il sistema è correttamente connesso alla rete locale e pronto per eventuali analisi successive.

```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.50.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 11:47 EST
Nmap scan report for 192.168.50.101
Host is up (0.00098s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

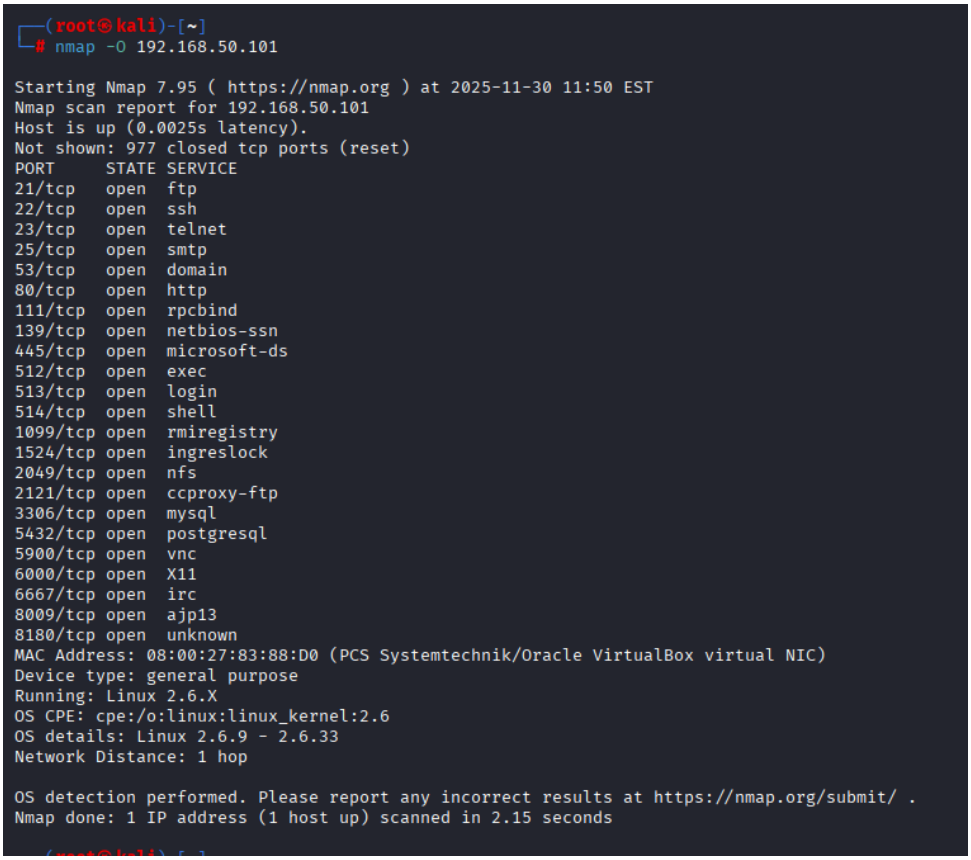
nmap -sS 192.168.50.101 : Questo comando avvia una scansione basata su SYN, la tecnica consiste nell'inviare pacchetti SYN verso ogni porta del sistema target e nell'interpretare la risposta per determinare se la porta è aperta, chiusa o filtrata.
La scansione ha rilevato un numero significativo di porte aperte sul sistema 192.168.50.101. Tra i servizi individuati figurano FTP, SSH, HTTP, DNS e altri ancora; questa esposizione estesa conferma che l'host esegue molteplici servizi attivi contemporaneamente, inclusi servizi notoriamente sensibili o obsoleti, evidenziando un potenziale rischio operativo nel caso di un'infrastruttura reale.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 11:47 EST
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.31 seconds
```

nmap -sS -sV 192.168.50.101 : Questo comando esegue una scansione delle porte del sistema combinando due funzionalità: la rilevazione delle porte aperte tramite tecnica SYN, che permette di identificare i servizi attivi in modo rapido e con un impatto minimo sul sistema analizzato, e la raccolta delle informazioni di versione dei servizi rilevati.

La scansione ha evidenziato una quantità molto ampia di servizi in ascolto sul sistema 192.168.50.101, confermando la presenza di un ambiente operativo estremamente ricco di funzionalità attive. Tra i servizi individuati sono presenti componenti legati alla gestione remota, protocolli di condivisione di file, server web, database, strumenti di comunicazione, ambienti applicativi e altri elementi di natura eterogenea. L'analisi delle versioni riportate mostra che molti servizi sono basati su software datato o non più mantenuto, condizione che, in un contesto reale, aumenterebbe in modo significativo l'esposizione del sistema e la complessità gestionale.

Complessivamente, il risultato rivela un'infrastruttura densamente popolata di elementi attivi e potenzialmente vulnerabili, offrendo una panoramica chiara della superficie operativa del sistema esaminato.

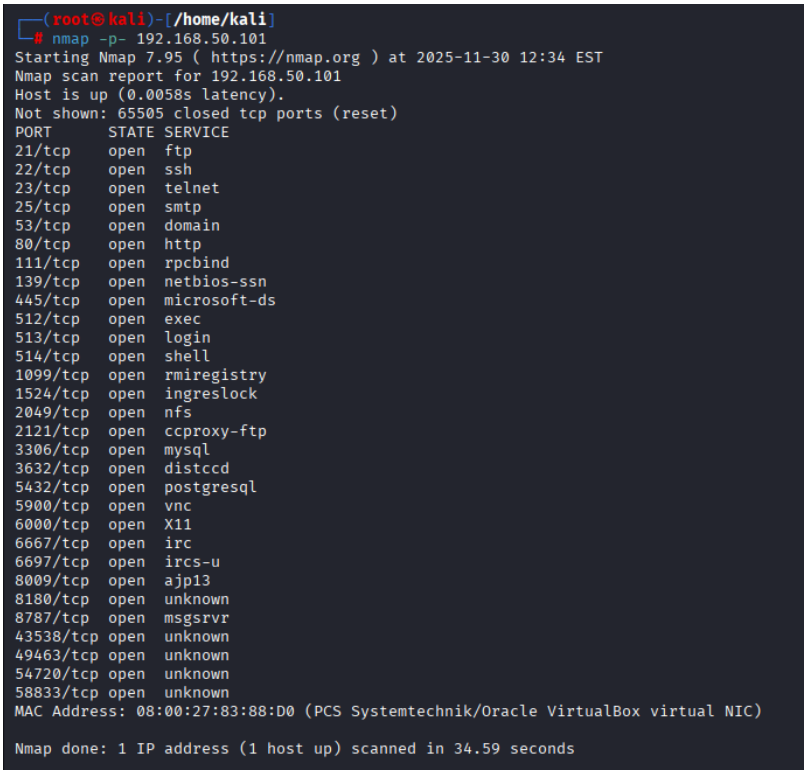


nmap -O 192.168.50.101 : esegue una scansione dell'host per identificarne il sistema operativo analizzando il comportamento dello stack TCP/IP.

L'esecuzione del comando ha restituito una mappatura estremamente dettagliata dei servizi attivi sull'host analizzato; ha identificato un numero elevato di porte TCP in stato "open", ciascuna associata a servizi reali e perfettamente raggiungibili sulla macchina.

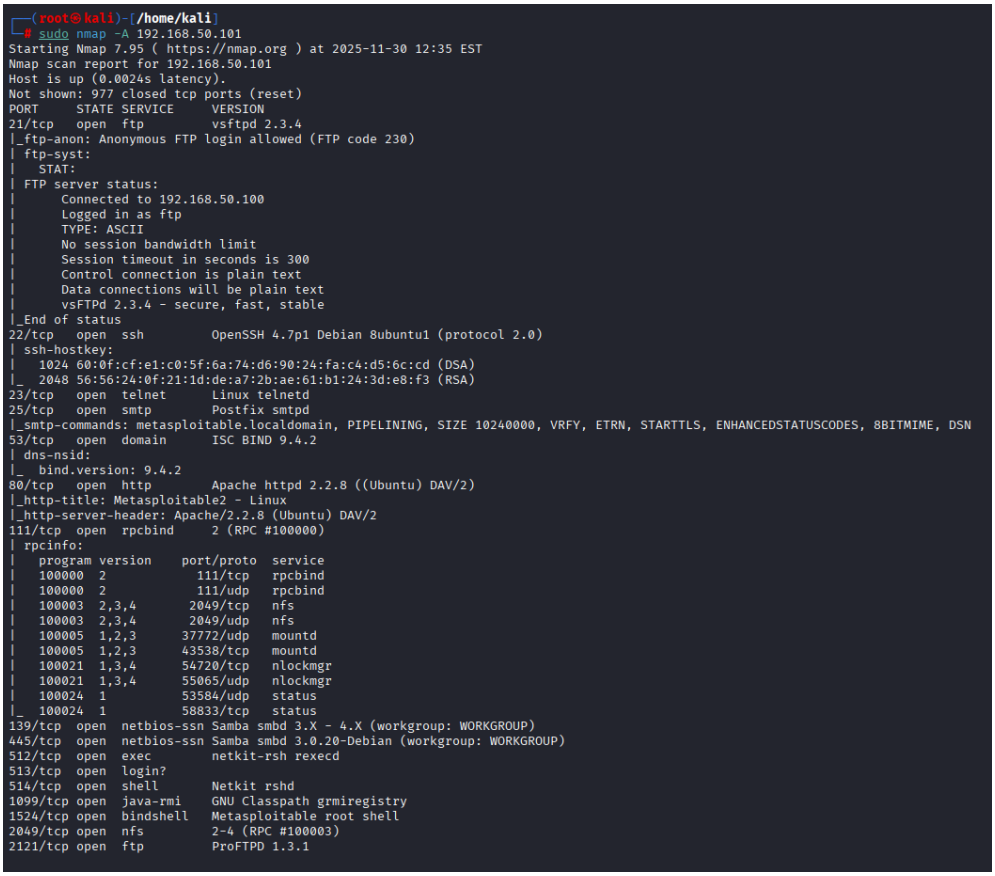
La scansione ha evidenziato la presenza di numerosi protocolli operativi e l'insieme dei risultati mostra una superficie d'attacco ampia e articolata, distribuita su tecnologie eterogenee e versioni obsolete, elemento che suggerisce una configurazione volutamente permissiva.

Nel complesso, il risultato finale descrive un sistema ricco di servizi esposti e facilmente interrogabili, offrendo un quadro chiaro della sua struttura tecnica e del potenziale livello di rischio associato.



map -p- 192.168.50.101 : il comando richiede a Nmap di eseguire una scansione completa su tutte le porte TCP dell'host, analizzando senza esclusioni ogni possibile punto di accesso per verificare quali porte risultano effettivamente aperte.

Nel caso specifico, la scansione ha rivelato che la macchina risponde attivamente su un numero molto esteso di porte, mostrando un profilo estremamente esposto e caratterizzato dalla presenza di numerosi servizi raggiungibili dall'esterno. L'esito complessivo indica quindi una configurazione poco restrittiva, con un livello di apertura insolito che suggerisce la necessità di un controllo approfondito e di eventuali interventi di contenimento.

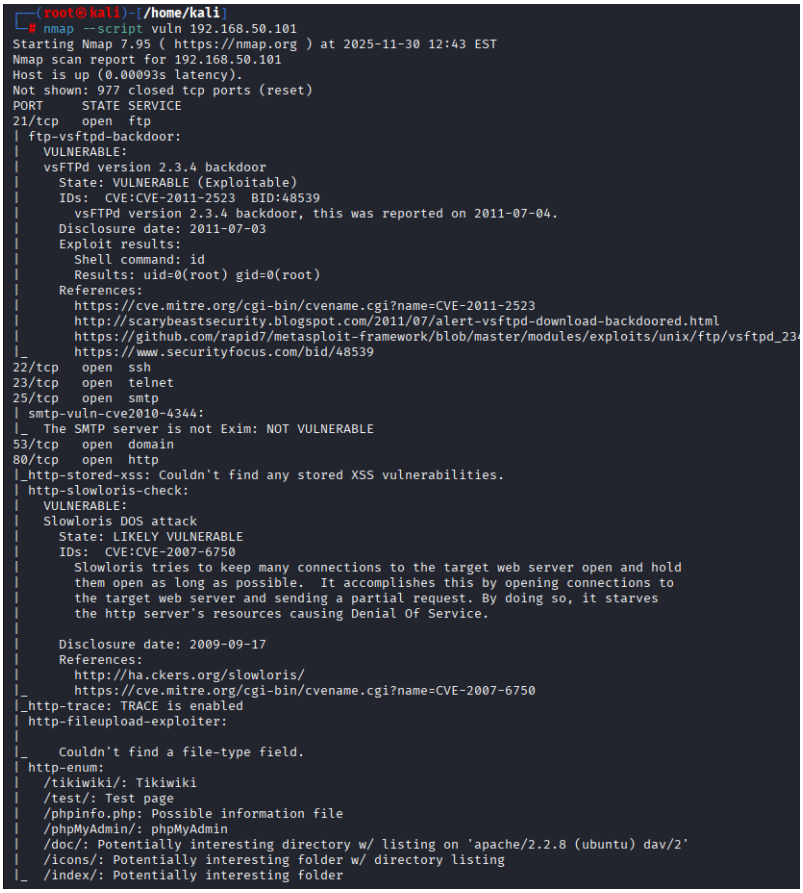


```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -A 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 12:35 EST
Nmap scan report for 192.168.50.101
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      37772/udp   mountd
|   100005  1,2,3      43538/tcp   mountd
|   100021  1,3,4      54720/tcp   nlockmgr
|   100021  1,3,4      55065/udp   nlockmgr
|   100024  1          53584/udp   status
|_  100024  1          58833/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
```

nmap -A 192.168.50.101 : questo comando effettua una scansione avanzata dell'host, combinando il rilevamento dei servizi attivi, delle versioni dei software esposti e una stima del sistema operativo, così da ottenere una visione completa del comportamento della macchina e di ciò che rende identificabili i suoi componenti interni.

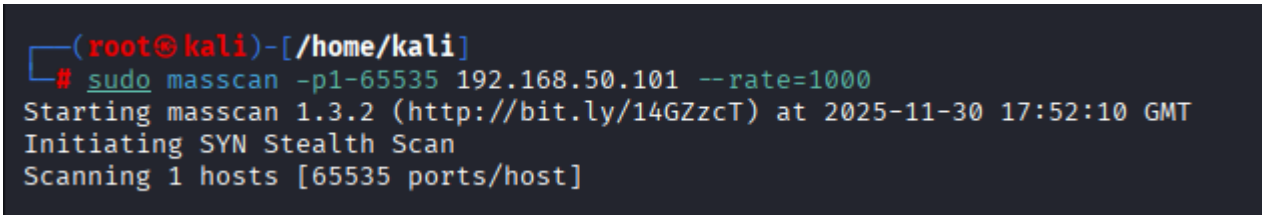
Nel caso concreto, l'esecuzione ha restituito un quadro estremamente articolato, mettendo in evidenza un sistema ricco di servizi raggiungibili, con applicazioni storiche e strutture software datate, spesso accompagnate da informazioni dettagliate che permettono di riconoscere con precisione le tecnologie adottate.

La grande quantità di risposte ricevute conferma un livello di esposizione insolito, con un ampio ventaglio di funzionalità accessibili e un'impronta complessiva che suggerisce una superficie operativa molto ampia e potenzialmente fragile, tale da richiedere una revisione attenta del perimetro digitale.



nmap --script vuln 192.168.50.101 : ha la funzione di analizzare un sistema alla ricerca di vulnerabilità note, interrogando i servizi esposti e confrontando il loro comportamento con un insieme di verifiche automatiche sviluppate per identificare debolezze già documentate. L'obiettivo è valutare in maniera immediata quali componenti risultino potenzialmente sfruttabili e quali aspetti dell'infrastruttura meritino attenzione prioritaria.

Nel caso specifico, l'esecuzione ha fatto emergere una situazione particolarmente delicata: sono stati individuati servizi obsoleti che presentano falle pubblicamente note e, in alcuni casi, pienamente sfruttabili; una delle evidenze più significative riguarda un servizio FTP che riporta la presenza di una backdoor, segno di una compromissione strutturale che espone completamente l'apparato.



sudo masscan -p1-65535 192.168.50.101 --rate=1000

Questo comando ha lo scopo di eseguire una scansione estremamente rapida dell'intero intervallo delle porte TCP, utilizzando un approccio ad alta velocità pensato per identificare in tempi molto ridotti qualsiasi servizio eventualmente esposto da un sistema.

L'idea è rilevare in modo immediato l'estensione del perimetro aperto, senza approfondire le caratteristiche dei singoli servizi ma ottenendo una mappa completa di ciò che risponde sulla macchina analizzata.

Nel caso specifico, l'operazione ha avviato un controllo su tutte le 65.535 porte dell'host target, confermando che il sistema risulta pienamente raggiungibile e predisposto a fornire risposte dall'esterno.

L'avvio della scansione mostra che l'intero pacchetto di porte è stato preso in carico senza alcuna restrizione, segnale evidente di una superficie molto ampia da verificare.

CONCLUSIONE

L’insieme delle attività svolte ha evidenziato che il sistema analizzato presenta un livello di esposizione estremamente elevato, con numerosi servizi attivi, versioni datate e vulnerabilità note che risultano facilmente identificabili anche attraverso strumenti di scansione standard. La presenza contemporanea di molteplici porte aperte, servizi non necessari e componenti con criticità documentate conferma una configurazione priva dei requisiti minimi di sicurezza attesi in un ambiente operativo moderno. L’analisi complessiva suggerisce la necessità di un intervento strutturato di riduzione della superficie di attacco, aggiornamento delle tecnologie in uso e revisione delle policy di gestione, al fine di riportare l’infrastruttura a un livello di rischio coerente con gli standard di riferimento aziendali.