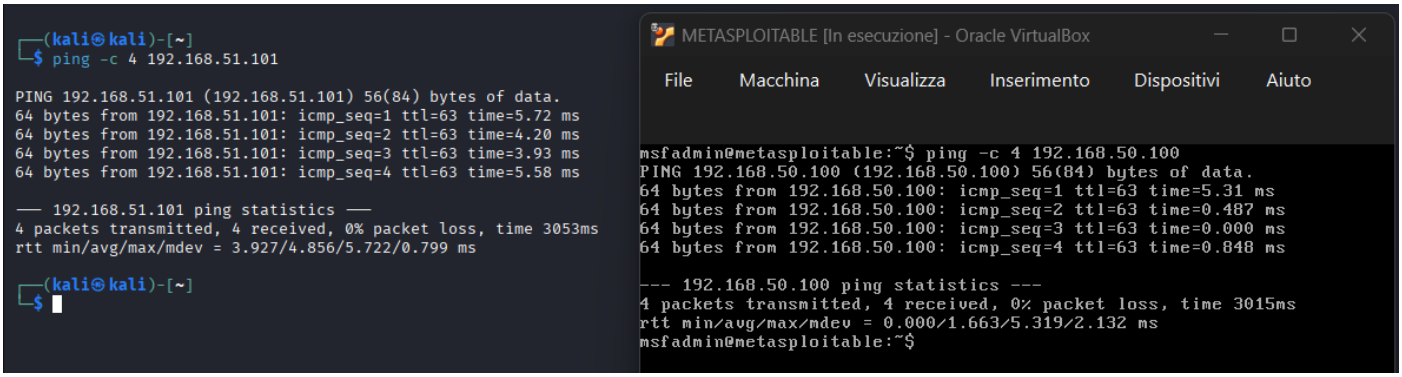
# INDICE

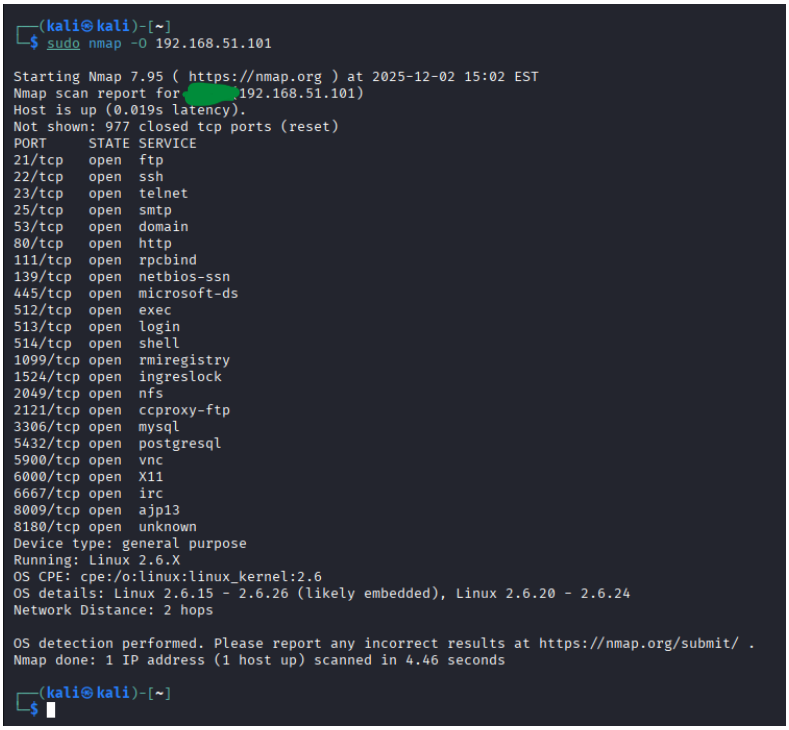
# INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: l'analisi condotta si è focalizzata sull'osservazione del comportamento di un host collocato all'interno di una rete opportunamente segmentata, con l'obiettivo di comprendere in che modo un sistema distribuito su una sottorete dedicata risponda a differenti tecniche di enumerazione applicate da un nodo situato in un dominio di rete distinto.
L'infrastruttura è stata predisposta per replicare uno scenario organizzativo in cui gli apparati sono distribuiti su più segmenti, instradati tramite un punto di transito centralizzato; questo assetto consente di valutare con precisione quali servizi risultino effettivamente raggiungibili al di là della segmentazione e come tali servizi rispondano quando osservati attraverso diverse modalità di ricognizione.

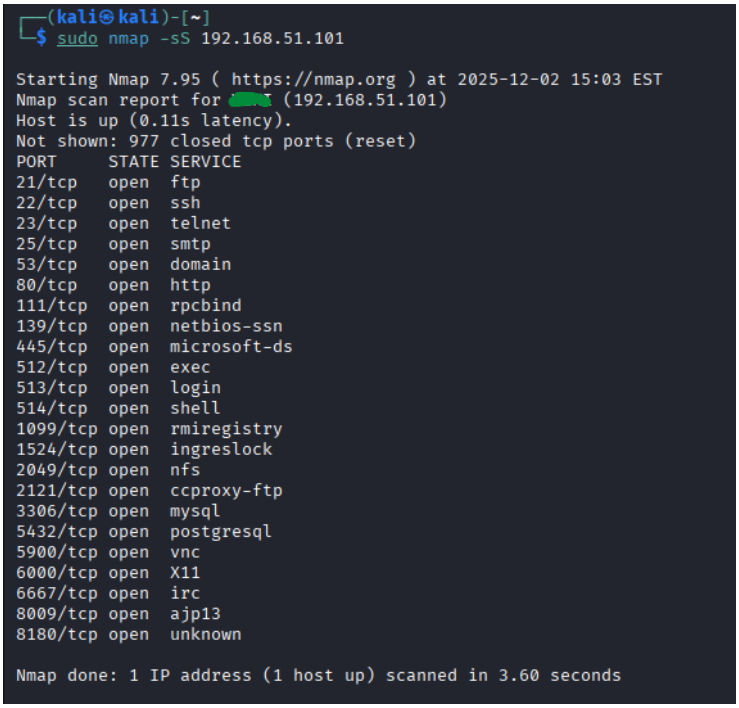
OBIETTIVO: identificare il sistema operativo, la superficie esposta tramite porte e servizi, le relative versioni applicative e il comportamento dell'host rispetto a differenti tipologie di scansione, valutando il livello di esposizione e la precisione delle risposte fornite dagli strumenti di analisi.




L'interazione iniziale tra i due sistemi è stata verificata attraverso un test di raggiungibilità reciproca.
Ciascun host ha inviato una serie di pacchetti ICMP verso l'altro, ottenendo in risposta valori di latenza stabili e l'assenza totale di perdita dei pacchetti ; il risultato complessivo dimostra quindi una connettività pienamente operativa e idonea a procedere con le analisi successive.

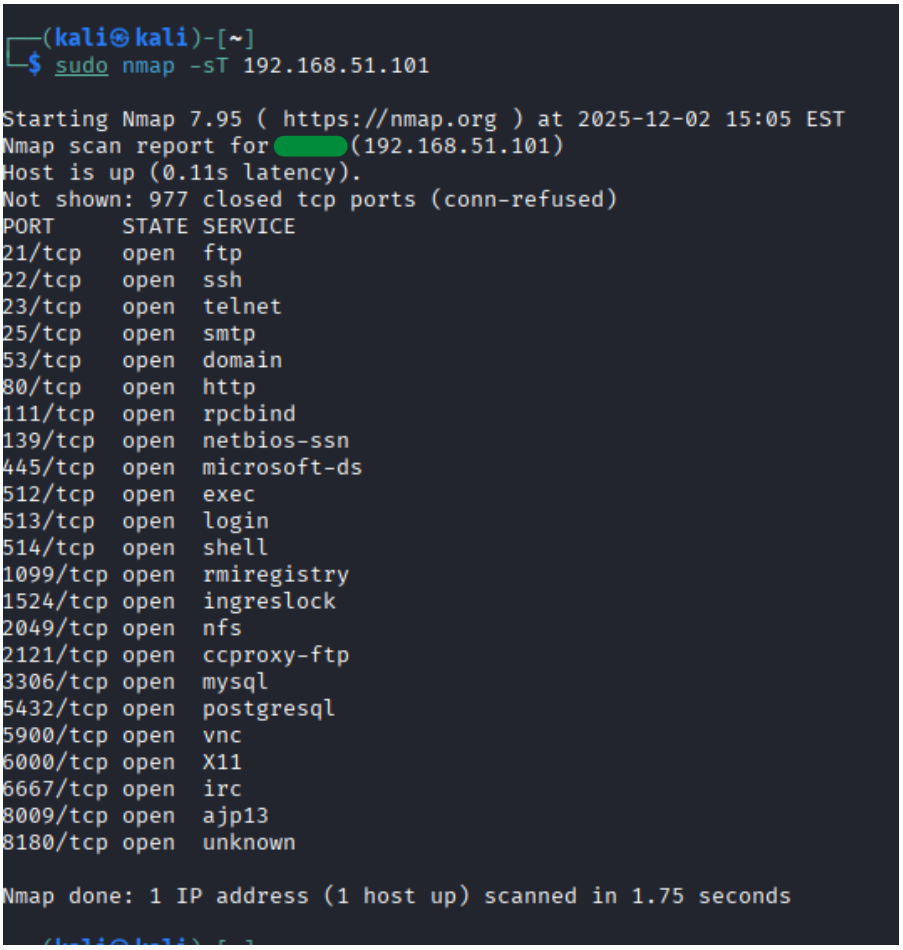



sudo nmap -O 192.168.51.101 : utilizzato per identificare le caratteristiche del sistema operativo di un host remoto tramite analisi passiva e attiva dei pacchetti di risposta. L'operazione restituisce un quadro completo dei servizi effettivamente raggiungibili, evidenziando numerose porte TCP in stato "open" associate a servizi di rete differenti.
L'host risulta pienamente operativo, raggiungibile con tempi di risposta contenuti, e presenta un profilo riconducibile a un sistema Linux della serie 2.6.x.




sudo nmap -sS 192.168.51.101 Il comando ha impiegato la modalità SYN scan tramite l'opzione -sS, una tecnica che consente di identificare le porte TCP in ascolto senza instaurare una connessione completa.

L'operazione ha restituito un elenco coerente di servizi attivi sulla destinazione, confermando la presenza di numerose porte aperte e un ampio profilo di esposizione applicativa; l'esito complessivo ha fornito una visione chiara delle porte effettivamente raggiungibili e delle funzionalità rese disponibili dal sistema analizzato, consolidando la comprensione della sua superficie di servizio.




sudo nmap -sT 192.168.51.101 : È stata eseguita una rilevazione basata su connessioni TCP, finalizzata a verificare quali servizi risultassero raggiungibili attraverso l'apertura di sessioni standard verso l'host analizzato.

Il comando utilizzato ha permesso di instaurare una connessione completa su ciascuna porta interrogata, ottenendo quindi un riscontro preciso sui servizi effettivamente disponibili e correttamente rispondenti.

L'analisi ha confermato la presenza di numerosi punti di accesso attivi, distribuiti su differenti ambiti funzionali – dai servizi di comunicazione remota ai protocolli applicativi più diffusi – indicando che l'host espone un'ampia superficie di servizio e risponde regolarmente alle richieste provenienti dalla rete.

Il completamento del test ha inoltre evidenziato tempi di risposta contenuti e un comportamento coerente con sistemi operativi appartenenti alla famiglia Linux, confermando la stabilità del percorso di rete e la corretta gestione delle connessioni in ingresso.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV  192.168.51.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 15:11 EST
Nmap scan report for [redacted](192.168.51.101)
Host is up (0.061s 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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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
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 13.80 seconds
```

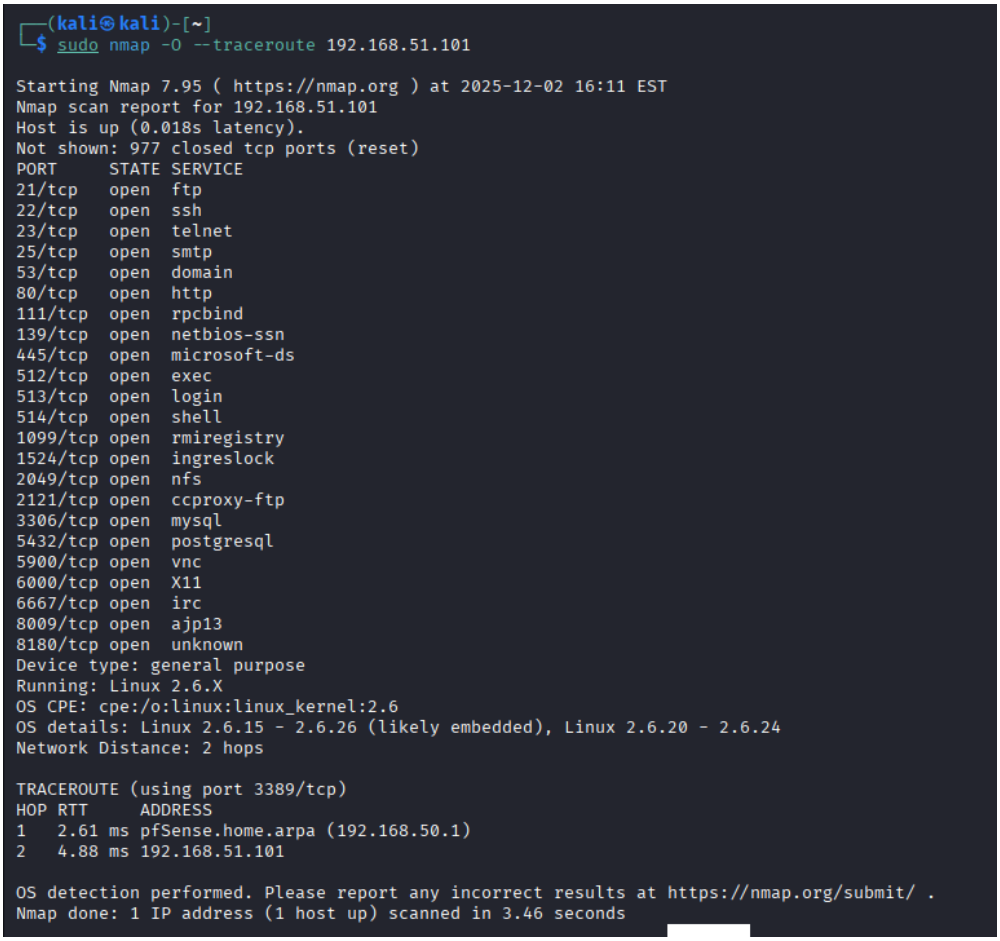
sudo nmap -sV 192.168.51.101: l'operazione ha previsto l'impiego di una scansione orientata all'identificazione puntuale dei servizi attivi sull'host di destinazione, con particolare attenzione alla rilevazione delle versioni dei software in ascolto.

Questo approccio ha consentito di ottenere una mappatura accurata delle applicazioni esposte, evidenziando sia i protocolli abilitati sia le relative implementazioni.

L'esito della procedura ha mostrato la presenza di numerosi servizi raggiungibili tramite connessioni TCP, tra cui componenti per la gestione remota, piattaforme applicative, servizi di rete e database.

Per ognuno di essi sono state identificate non solo la porta e il protocollo, ma anche la versione specifica del software, elemento che ha permesso di delineare in maniera chiara il profilo operativo dell'host.

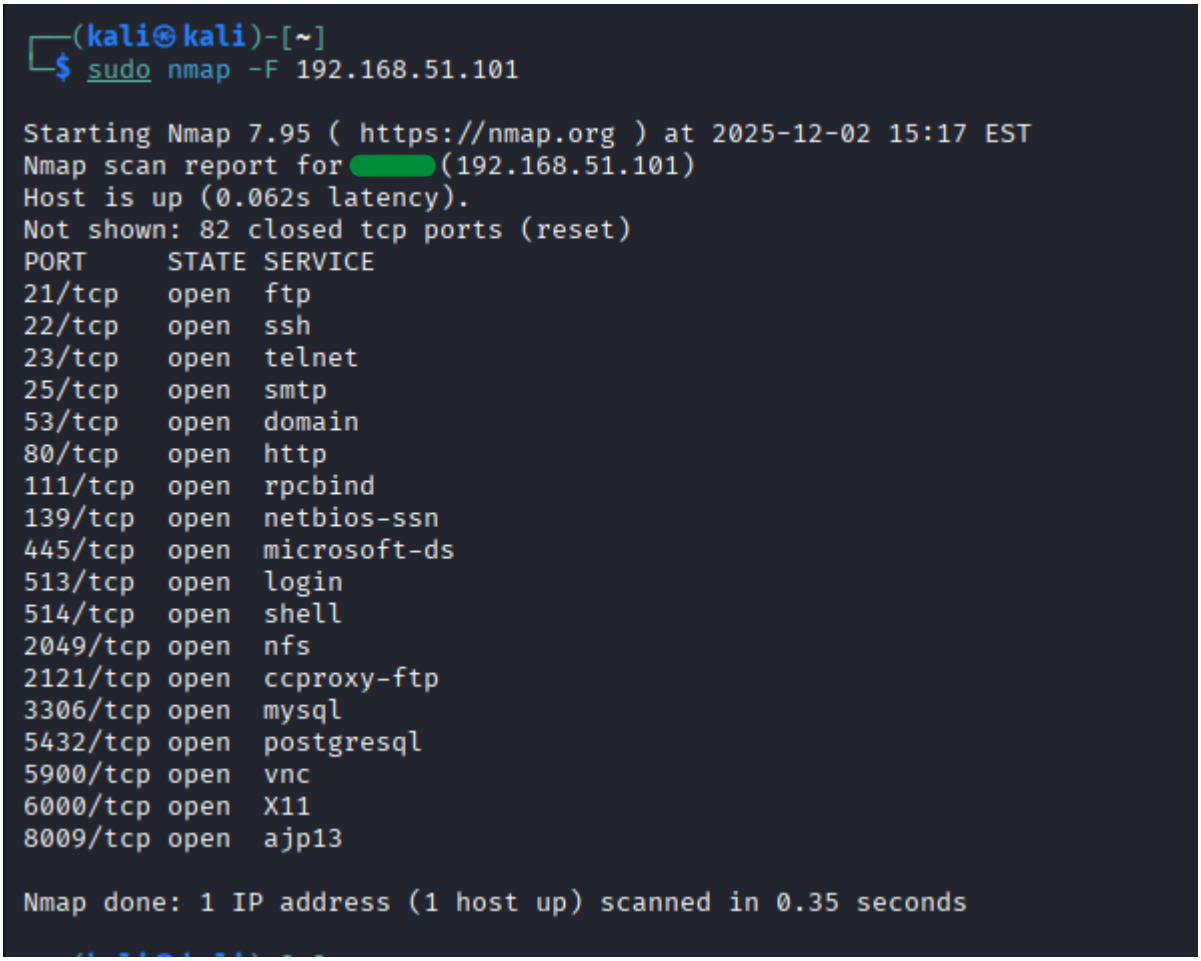
L'analisi ha inoltre confermato che il sistema risponde attraverso un numero significativo di servizi applicativi, presentando un comportamento coerente con quello di un ambiente articolato e ricco di funzionalità lato server.




sudo nmap -O --traceroute 192.168.51.101 : l'operazione ha previsto l'utilizzo di una procedura orientata al riconoscimento delle caratteristiche strutturali dell'host, con l'obiettivo di determinarne la configurazione di sistema e il percorso di rete attraverso cui viene raggiunto.

La modalità impiegata ha permesso di ottenere sia un'analisi dei servizi esposti sia una valutazione del sistema operativo identificato, mettendo in evidenza gli elementi fondamentali che definiscono il comportamento dell'apparato.

Parallelamente, è stato possibile osservare in modo dettagliato il tracciato seguito dal traffico nel suo percorso verso la destinazione; questo ha consentito di misurare la distanza di rete tra il punto di origine e l'host analizzato evidenziando la presenza di un nodo intermedio e confermando la struttura segmentata dell'ambiente.




sudo nmap -F 192.168.51.101 : l'operazione ha previsto l'utilizzo di una scansione rapida orientata all'individuazione esclusiva delle porte più comunemente utilizzate nelle comunicazioni di rete, con l'obiettivo di ottenere una fotografia sintetica ma immediatamente significativa dei servizi effettivamente accessibili sull'host analizzato.
L'esecuzione ha evidenziato un insieme mirato di servizi attivi, comprendente componenti per la gestione remota, funzioni applicative e piattaforme di supporto tipicamente impiegate in contesti server strutturati.
Le porte rilevate risultano tutte operative, confermando la presenza di un sistema che espone un numero significativo di funzionalità essenziali distribuite su protocolli differenziati.
La scansione ha inoltre certificato la piena raggiungibilità dell'host e la capacità del sistema di rispondere con continuità ai tentativi di interrogazione, fornendo così un quadro chiaro e immediato del suo comportamento di rete.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 80 192.168.51.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 06:28 EST
Nmap scan report for 192.168.51.101
Host is up (0.0067s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Sudo nmap -p 80 192.168.51.101: questa operazione è stata utilizzata per verificare in modo puntuale la disponibilità del servizio associato alla porta specificata, senza coinvolgere ulteriori componenti o procedure di rilevazione estese.
L'approccio consente di concentrarsi esclusivamente su un servizio ben definito, riducendo i tempi di analisi e offrendo una risposta immediata in merito alla sua effettiva raggiungibilità.
L'esito della verifica ha confermato la presenza del servizio in ascolto sulla porta indicata, che risulta attivo e correttamente accessibile dal nodo richiedente; ciò indica che l'host mette a disposizione un servizio web standard e lo espone regolarmente sulla rete di competenza, rispondendo in modo coerente ai protocolli previsti per la comunicazione su tale porta.

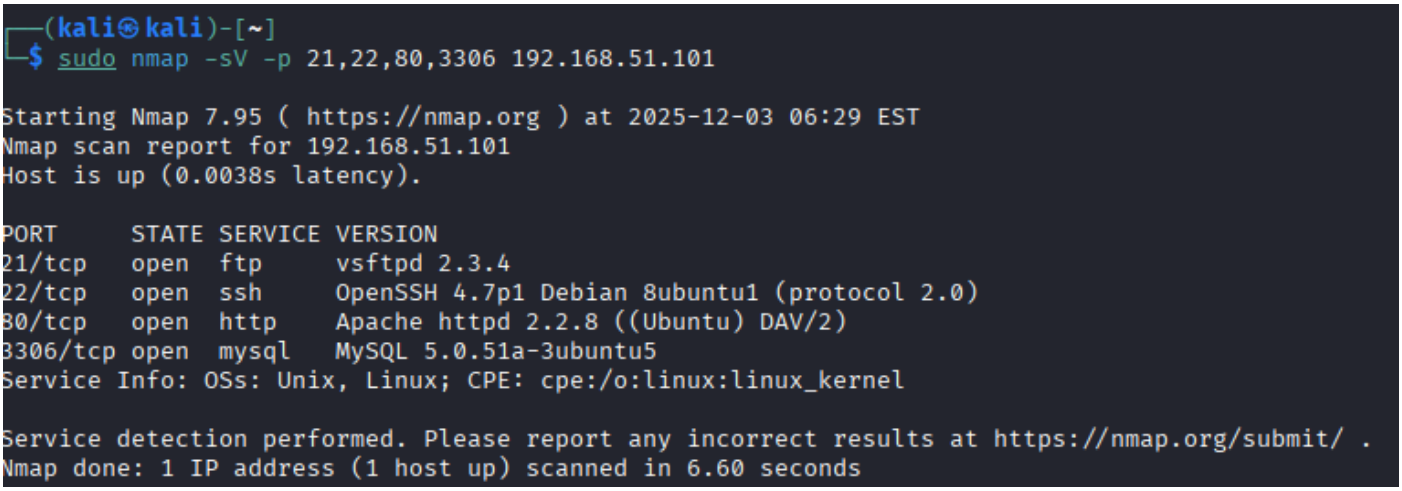
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 21,22,80,3306 192.168.51.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 06:29 EST
Nmap scan report for 192.168.51.101
Host is up (0.0046s latency).

PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

L'attività ha previsto l'esecuzione di una scansione mirata su un insieme specifico di porte, selezionate per verificare in modo puntuale la presenza e la disponibilità di determinati servizi sull'host di destinazione; questa modalità focalizzata consente di concentrare l'attenzione esclusivamente su componenti di particolare rilevanza operativa, riducendo i tempi di esecuzione e fornendo un riscontro immediato in merito allo stato delle risorse individuate.
L'esito della procedura ha confermato che tutte le porte esaminate risultano attive e operative, restituendo un quadro chiaro della presenza dei servizi associati alle funzionalità di trasferimento file, gestione remota, erogazione di contenuti web e gestione di database.
Il risultato complessivo evidenzia una corretta disponibilità dei servizi selezionati, delineando una configurazione che appare coerente con un ambiente server dotato di componenti essenziali per l'erogazione di funzionalità applicative e di rete.




sudo nmap -sV -p 21,22,80,3306 192.168.51.101: l'operazione ha previsto l'esecuzione di una rilevazione mirata su un insieme selezionato di porte.
L'approccio selettivo adottato permette di concentrare l'attenzione esclusivamente su componenti specifici, ottimizzando i tempi di esecuzione e fornendo un quadro chiaro e immediato sul comportamento dell'host.
Dalla rilevazione sono emersi servizi pienamente operativi, riconducibili alle funzioni di trasferimento file, gestione remota, pubblicazione web e gestione di database.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -T4 -sV 192.168.51.101

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 07:41 EST
Nmap scan report for 192.168.51.101
Host is up (0.29s 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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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
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 14.82 seconds
```

sudo nmap -T4 -sV 192.168.51.101 : è stata eseguita una scansione completa dei servizi presenti sull'host, integrando l'identificazione delle versioni con l'opzione di intensificazione dei tempi di rilevamento.

L'operazione ha restituito una panoramica esaustiva dell'infrastruttura, evidenziando un elevato numero di servizi attivi, per ciascun servizio sono state identificate in modo puntuale sia le porte di ascolto sia le versioni specifiche dei software, permettendo di delineare un profilo tecnico particolarmente dettagliato del sistema.

L'esito complessivo mostra un host caratterizzato da una presenza significativa di funzionalità lato server, con un insieme strutturato di componenti che operano in maniera coerente e rispondono in modo regolare anche alle richieste più approfondite.

La qualità e la varietà delle risposte ottenute confermano un comportamento stabile dell'infrastruttura, coerente con un ambiente predisposto per supportare numerosi servizi contemporaneamente.

# CONCLUSIONE

L’analisi condotta ha permesso di ottenere una visione chiara e strutturata del comportamento dell’host esaminato all’interno della rete segmentata.
Le diverse verifiche svolte hanno evidenziato una configurazione coerente, caratterizzata da un’elevata disponibilità dei servizi e da una risposta stabile alle richieste provenienti dai diversi metodi di interrogazione adottati.
La mappatura risultante conferma la presenza di un sistema dotato di componenti applicative eterogenee e pienamente operative, capaci di supportare funzionalità di gestione remota, trasferimento dati, servizi applicativi e comunicazioni interne. L’insieme delle rilevazioni evidenzia inoltre una struttura di rete ordinata e instradata correttamente, nella quale il traffico segue percorsi definiti e prevedibili.
Nel complesso, l’esito delle attività fornisce un quadro affidabile dello stato dell’host e della sua operatività all’interno dell’infrastruttura, offrendo una base solida per eventuali valutazioni future legate alla gestione, all’ottimizzazione o all’evoluzione dell’ambiente analizzato.