FASE 1

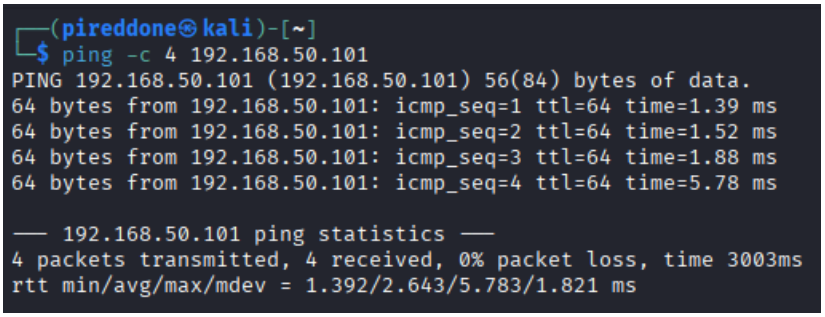
In questa prima fase dell'esercitazione ho effettuato una serie di analisi sulla macchina Metasploitable 2 utilizzando Nmap, con lo scopo di identificare le porte aperte, i servizi attivi e raccogliere quante più informazioni possibili prima di eventuali fasi di attacco controllato.

- **1. Verifica della raggiungibilità (Ping)**

Per prima cosa ho verificato che Kali Linux e Metasploitable comunicassero correttamente all'interno della rete interna.
Ho eseguito un semplice ping verso l'indirizzo della macchina target:

ping -c 4 192.168.50.101

La macchina ha risposto senza problemi, con una latenza bassa e stabile. Questo mi ha confermato che potevo procedere con le scansioni.



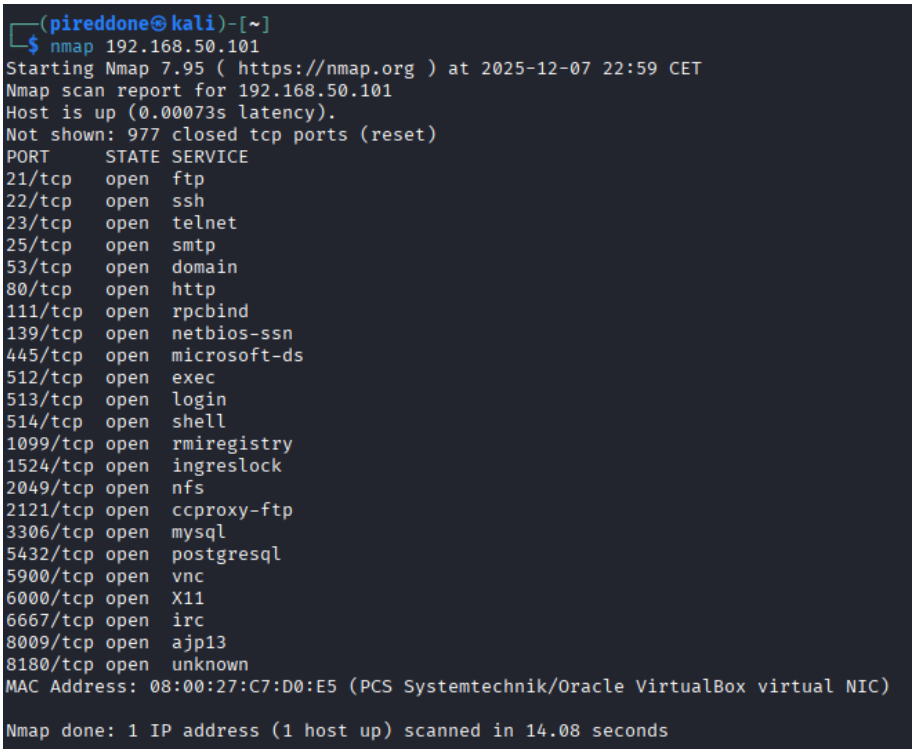
🔹 2. Scansione Nmap Standard

Come primo passo ho eseguito una scansione base con Nmap:

nmap 192.168.50.101

Questa scansione ha subito mostrato una superficie d'attacco enorme: Metasploitable espone un numero impressionante di porte aperte, molte delle quali sono note per essere vulnerabili o comunque non dovrebbero mai essere accessibili su un sistema reale.

Le porte principali trovate includono FTP, SSH, Telnet, SMTP, HTTP, SMB, RPC, MySQL, PostgreSQL, VNC e molte altre.



🔹 3. Scansione con rilevamento delle versioni (-sV)

Per ottenere maggiori informazioni sui servizi attivi, ho eseguito una scansione più approfondita con l'opzione -sV:

nmap -sV 192.168.50.101

Questa scansione è stata molto utile perché ha mostrato con precisione quale versione di ciascun servizio è in esecuzione.
Tra i risultati più significativi:

- **vsftpd 2.3.4** (FTP) – versione vulnerabile a una backdoor nota
- **OpenSSH 4.7p1** – obsoleta
- **Apache 2.2.8** – anche questa molto vecchia

- **Samba 3.x** – vulnerabile a SambaCry
- **MySQL 5.0.51a** – anch'esso obsoleto
- **PostgreSQL 8.3.x**
- **VNC 3.3** – connessione non cifrata

Tutti questi dati confermano il livello estremamente insicuro della macchina.

```
┌──(pireddone㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 23:00 CET
Nmap scan report for 192.168.50.101
Host is up (0.00068s 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:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
ux_kernel
```

🔹 4. Scansione Aggressiva (-A)

Successivamente ho lanciato una scansione aggressiva:

nmap -A 192.168.50.101

Questa opzione combina più funzionalità (OS detection, version detection, script NSE, traceroute) e fornisce una quantità enorme di informazioni.

Tra le cose più importanti trovate:

- Conferma dei banner FTP e SSH
- Identificazione del sistema operativo (Linux 2.6.x)
- Banner HTTP con Apache 2.2.8
- Informazioni SMB dettagliate (utente guest attivo, dominio WORKGROUP)
- Identificazione dei database attivi (MySQL e PostgreSQL)
- Presenza di un servizio VNC esposto sulla porta 5900

- Porte RPC e Java RMI aperte, tipicamente usate in exploit remoti
- Hostname: metasploitable.localdomain

Questa scansione è quella che conferma in modo più completo quanto Metasploitable sia progettata per essere sfruttabile.

```
┌──(pireddone㉿kali)-[~]
└─$ nmap -A 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 23:02 CET
Nmap scan report for 192.168.50.101
Host is up (0.0014s 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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
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      49256/udp   mountd
|   100005  1,2,3      58935/tcp   mountd
|   100021  1,3,4      35228/udp   nlockmgr
|   100021  1,3,4      56159/tcp   nlockmgr
|   100024  1          35744/udp   status
|_  100024  1          44219/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
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, Support41Auth, LongColumnFlag, SupportsTransactions, SupportsCompress
ion, SwitchToSSLAfterHandshake, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: y/{Aq6X;Y/}MG[sQz6<f
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no
 such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-12-07T22:04:50+00:00; +1s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
ux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
```

```
|   FQDN: metasploitable.localdomain
|_  System time: 2025-12-07T17:03:27-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h40m00s, deviation: 2h53m13s, median: 0s

TRACEROUTE
HOP RTT     ADDRESS
1   1.40 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 143.02 seconds
```

🔹 5. Scansione delle porte più comuni (-F)

Ho poi fatto una scansione veloce sulle porte più comuni:

nmap -F 192.168.50.101

Anche in questo caso, sono comparse moltissime porte aperte, a conferma che anche una scansione superficiale su Metasploitable restituisce già un quadro molto critico.

```
┌──(pireddone㉿kali)-[~]
└─$ nmap -F 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 23:09 CET
Nmap scan report for 192.168.50.101
Host is up (0.00073s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
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
8009/tcp open  ajp13
MAC Address: 08:00:27:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

🔹 6. Scansione completa di tutte le porte (-p-)

Infine, ho eseguito una scansione completa di tutte le porte TCP:

nmap -p- 192.168.50.101

Questa scansione ha rivelato ulteriori porte aperte, soprattutto su range molto alti, dove spesso si trovano:

- servizi sperimentali
- processi custom
- componenti vulnerabili di test

La quantità di porte aperte è anomala per qualsiasi macchina reale e conferma che Metasploitable è un ambiente creato per essere sfruttato a scopo didattico.

```
┌──(pireddone㉿kali)-[~]
└─$ nmap -p- 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 23:10 CET
Nmap scan report for 192.168.50.101
Host is up (0.00081s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
44219/tcp open  unknown
56159/tcp open  unknown
58935/tcp open  unknown
59899/tcp open  unknown
MAC Address: 08:00:27:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 68.14 seconds
```

🔹 **Riepilogo finale della fase Nmap**

Dalla scansione emerge che:

- La macchina espone **tantissimi servizi vulnerabili**, molti dei quali in versioni ormai abbandonate.
- I servizi FTP, SSH, HTTP, SMB, SQL, VNC e RPC sono tutti accessibili direttamente.
- Molti dei servizi identificati hanno vulnerabilità documentate e sfruttabili.
- L'OS detection conferma la natura obsoleta del sistema (Linux 2.6).
- La superficie d'attacco è estremamente ampia e offre molti spunti per le prossime fasi del penetration testing.

In sintesi: la fase di ricognizione con Nmap ha fornito tutte le informazioni necessarie per passare alla fase successiva dell'esercitazione, che prevede l'uso di strumenti aggiuntivi come hping3, netcat e altri comandi di host-scanning.

FASE 2

In questa seconda fase dell'esercitazione ho utilizzato una serie di strumenti di host scanning e banner grabbing (netcat, hping3, telnet e alcuni tool DNS) per ottenere informazioni aggiuntive sui servizi attivi su Metasploitable. Questi strumenti servono a confermare e approfondire ciò che avevo già individuato nella fase precedente con Nmap.

1) **Banner Grabbing con Netcat (nc)**

Ho iniziato utilizzando **netcat**, uno strumento molto utile per connettersi direttamente alle porte dei servizi e leggere i banner restituiti dai vari servizi.

✓ FTP (porta 21)

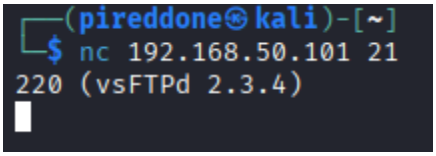
Il comando:

nc 192.168.50.101 21

mi ha subito restituito il banner:

220 (vsFTPd 2.3.4)

Questa versione di vsFTPd è famosissima perché contiene una backdoor inserita in una versione compromessa del software.



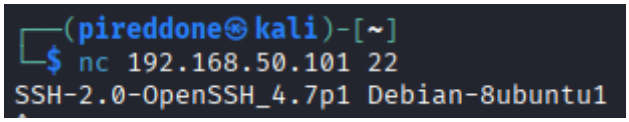
✓ SSH (porta 22)

nc 192.168.50.101 22

Output:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

Una versione molto datata di OpenSSH, anch'essa presente per scopi didattici.



✓ **HTTP (porta 80)**

Per il servizio web mi sono collegato alla porta 80 e ho inviato una richiesta HEAD manuale:

nc 192.168.50.101 80

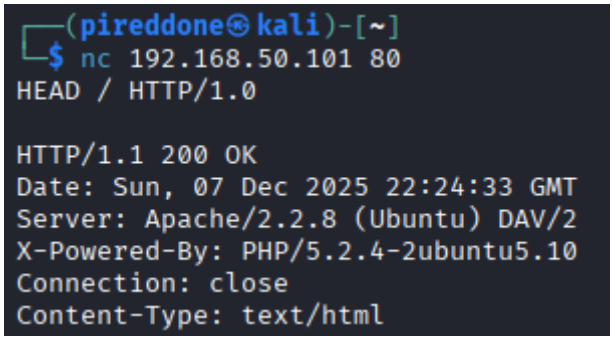
HEAD / HTTP/1.0

Il server mi ha risposto con:

Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4

Anche qui abbiamo versioni estremamente vecchie di Apache e PHP.



2) **Analisi delle porte con Hping3**

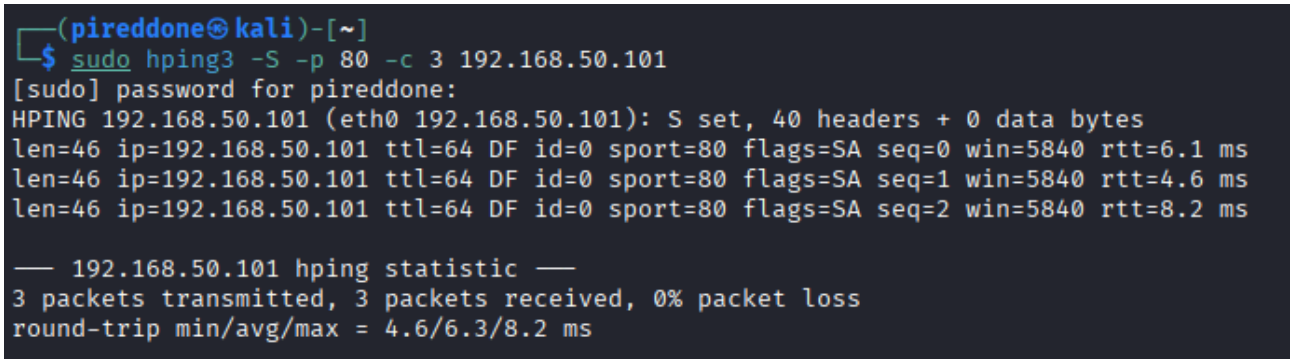
Poi ho utilizzato **hping3**, che permette di inviare pacchetti TCP e ICMP personalizzati per vedere come risponde la macchina.

✓ **Ping TCP sulla porta 80 (SYN scan manuale)**

sudo hping3 -S -p 80 -c 3 192.168.50.101

Risultato:

- Risposte **SYN/ACK**, che indicano chiaramente che la porta 80 è **open**.
- RTT molto bassi.



✓ Ping TCP su porta 22 (SSH)

sudo hping3 -S -p 22 -c 3 192.168.50.101

Anche in questo caso ho ricevuto SYN/ACK, cioè conferma che la porta SSH è aperta e risponde correttamente.

```
┌──(pireddone㉿kali)-[~]
└─$ sudo hping3 -S -p 22 -c 3 192.168.50.101
HPING 192.168.50.101 (eth0 192.168.50.101): S set, 40 headers + 0 data bytes
len=46 ip=192.168.50.101 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=5840 rtt=4.0 ms
len=46 ip=192.168.50.101 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=5840 rtt=9.2 ms
len=46 ip=192.168.50.101 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=5840 rtt=2.7 ms

── 192.168.50.101 hping statistic ──
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.7/5.3/9.2 ms
```

✓ Ping ICMP (alternativa al ping standard)

sudo hping3 -1 -c 3 192.168.50.101

Il sistema risponde normalmente ai pacchetti ICMP.

```
┌──(pireddone㉿kali)-[~]
└─$ sudo hping3 -1 -c 3 192.168.50.101
HPING 192.168.50.101 (eth0 192.168.50.101): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.50.101 ttl=64 id=49991 icmp_seq=0 rtt=2.9 ms
len=46 ip=192.168.50.101 ttl=64 id=49992 icmp_seq=1 rtt=10.0 ms
len=46 ip=192.168.50.101 ttl=64 id=49993 icmp_seq=2 rtt=6.0 ms

── 192.168.50.101 hping statistic ──
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.9/6.3/10.0 ms
```

3) Telnet su Porta SMTP (25)

Con telnet ho verificato il banner del server SMTP:

telnet 192.168.50.101 25

Risposta:

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

Anche questo servizio è molto vecchio e volutamente insicuro.

```
┌──(pireddone㉿kali)-[~]
└─$ telnet 192.168.50.101 25
Trying 192.168.50.101 ...
Connected to 192.168.50.101.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

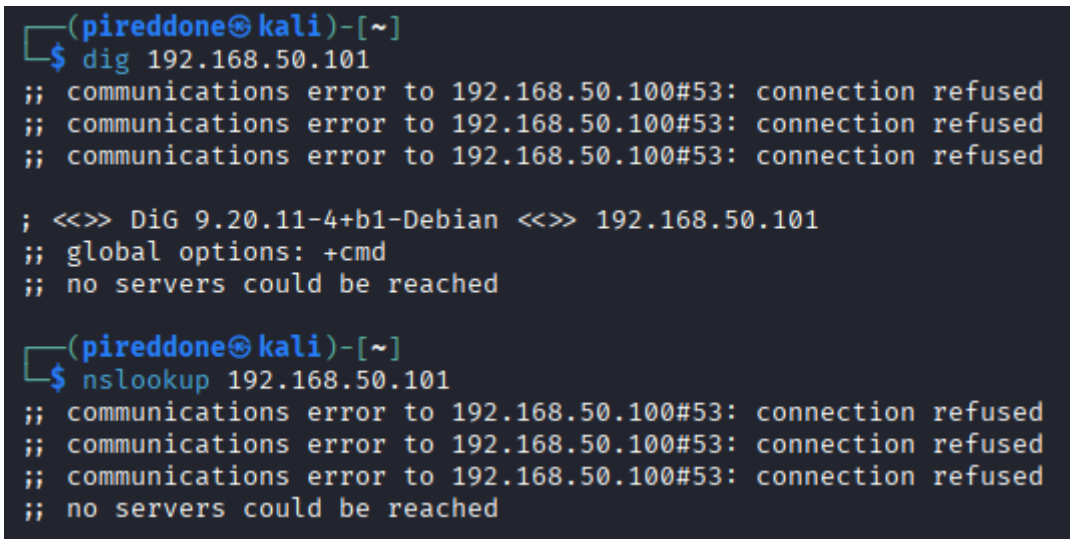
4) DIG e NSLOOKUP (DNS Queries)

Come ultimo test ho provato a ottenere informazioni DNS:

dig 192.168.50.101

nslookup 192.168.50.101

Entrambi gli strumenti riportano **connection refused**, il che significa che **Metasploitable non esegue alcun DNS server**, esattamente come prevedibile.



Conclusione della Fase 2

Gli strumenti utilizzati in questa fase hanno confermato e approfondito ciò che era emerso dalle scansioni Nmap:

- molti servizi espongono banner completi e facilmente leggibili
- le versioni dei servizi sono tutte obsolete e vulnerabili
- i protocolli non sono protetti (FTP anonimo, Telnet aperto, SMTP aperto)
- hping3 conferma l'apertura delle porte tramite SYN/ACK
- nessun DNS server in ascolto

L'insieme di questi dati dimostra quanto Metasploitable sia una macchina espressamente progettata per essere analizzata nelle esercitazioni di penetration testing e quanto sia semplice raccogliere informazioni sensibili sui servizi.