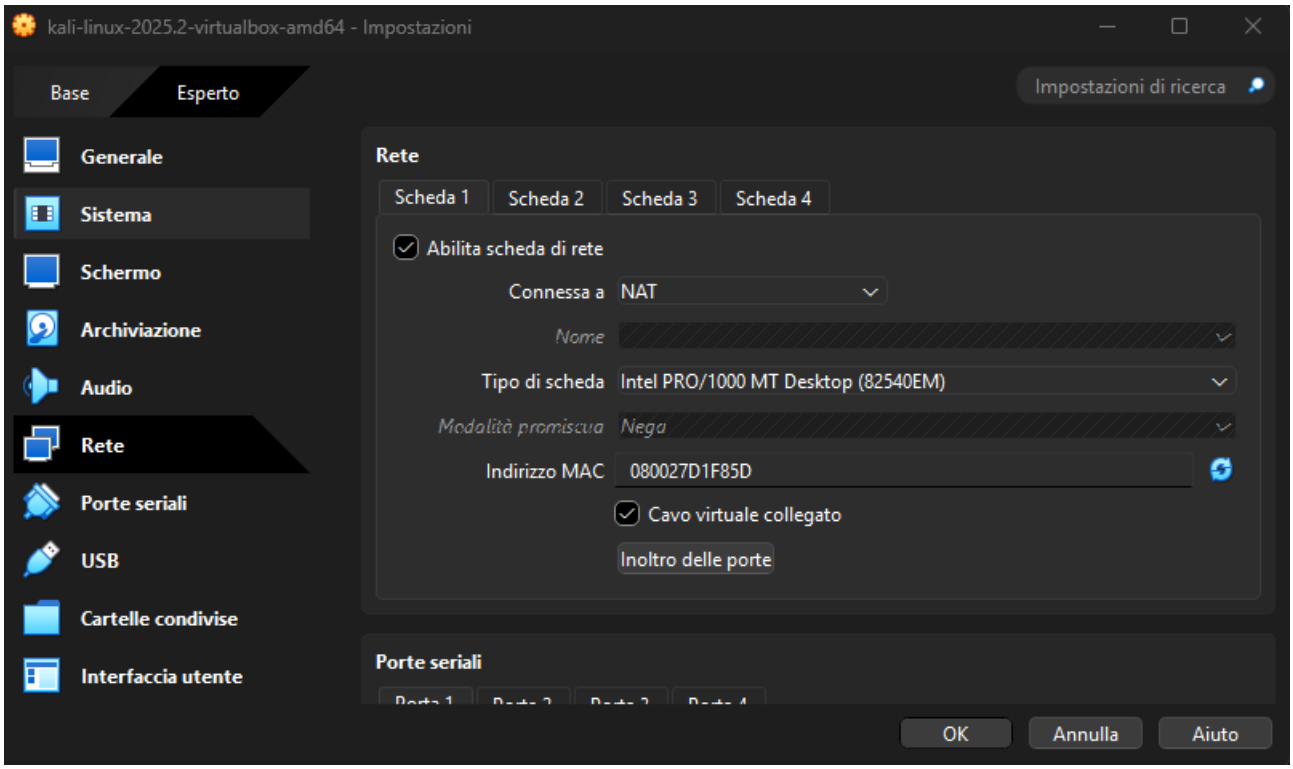
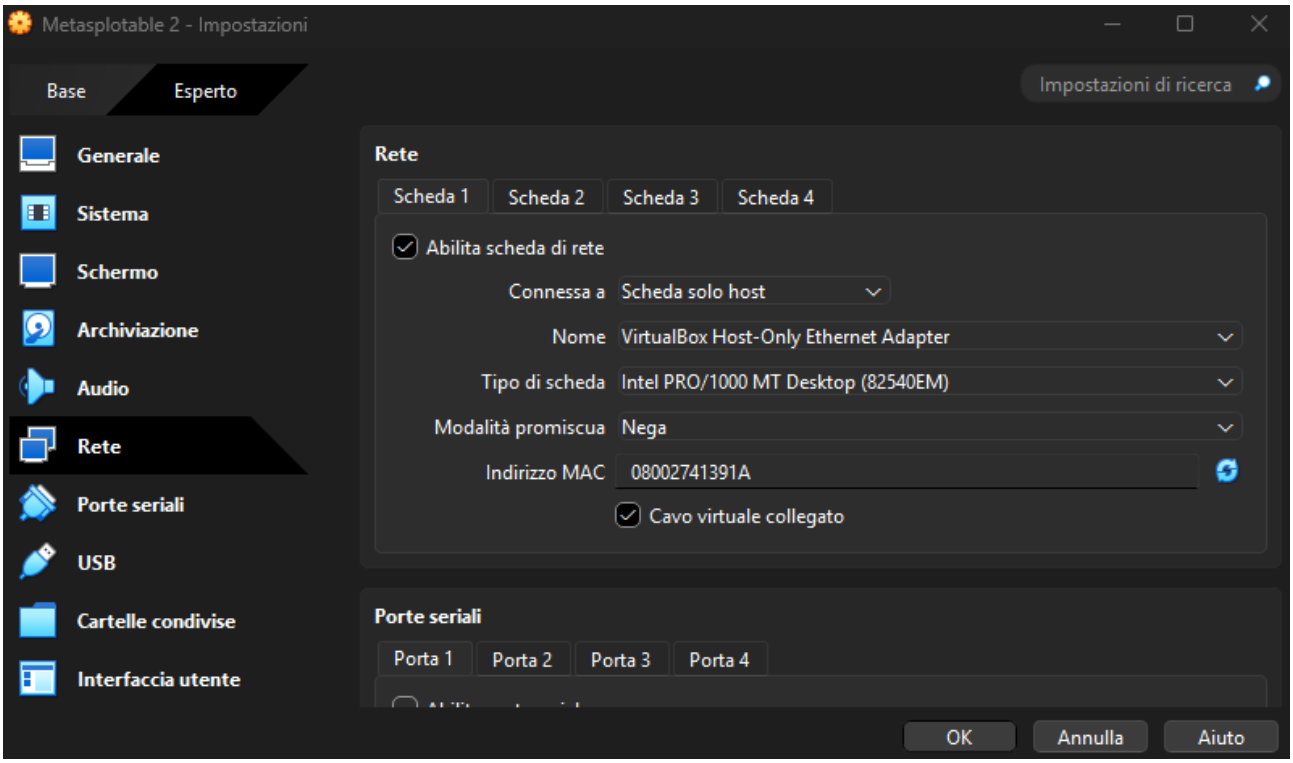
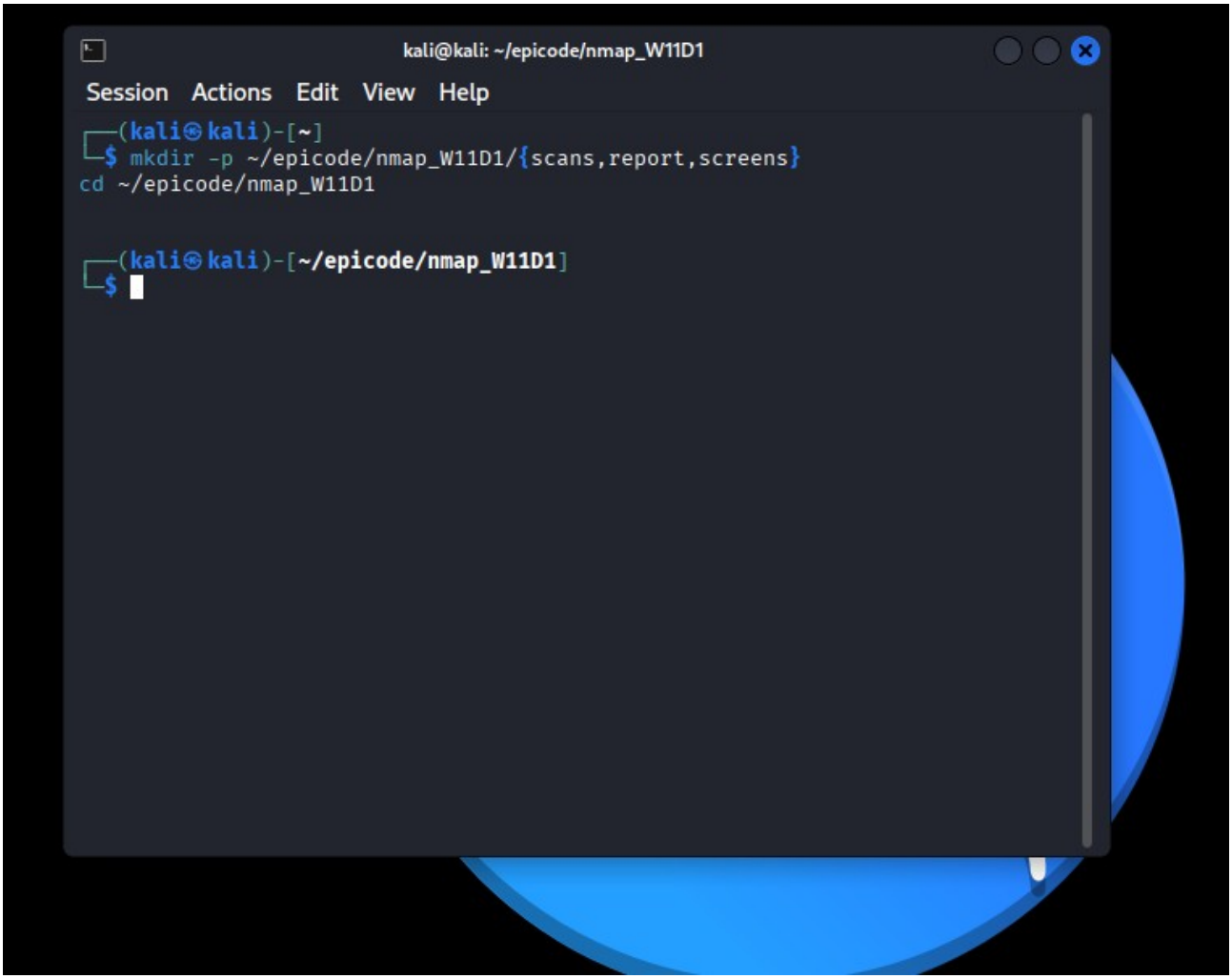
W11D1 – FRANCESCO MONTALTO

INTRO: Innanzitutto ho impostato le due VM su due reti diverse, come richiesto dall'esercizio. Nel mio caso, Kali su NAT e Metasploitable su Host-Only.

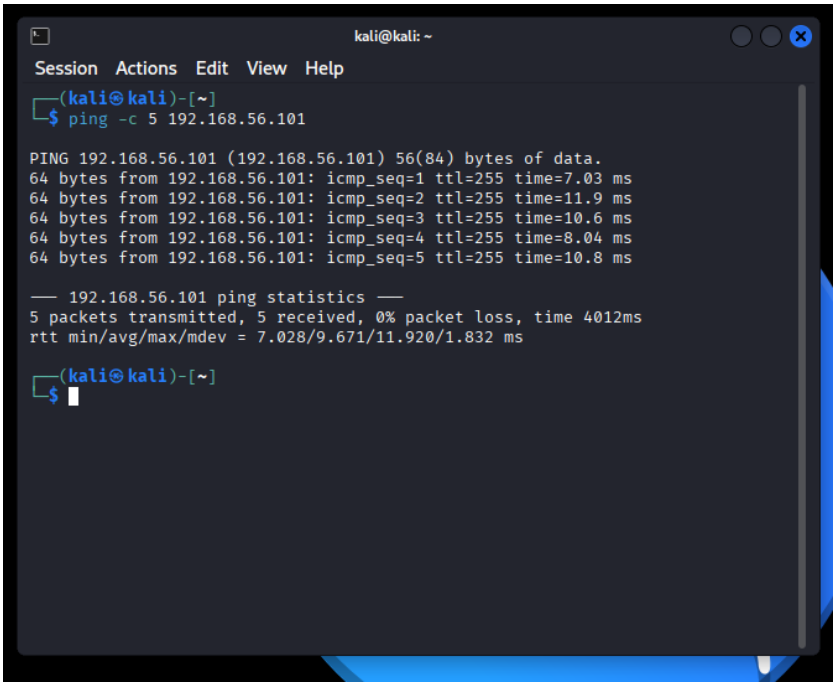




Ho poi creato un percorso ordinato per tenere sotto controllo gli output che poi andremo ad esaminare.



Dal momento che il ping funzionerà solo se esiste routing tra le nostre due reti e se il target non ha un firewall specifico a bloccare, se vogliamo dimostrare con sicurezza la connettività, facciamo prima i controlli basilari. In questo caso, la connettività verso il target è ok.



1. SCANSIONI

OS FINGERPRINT

```
kali@kali: ~/epicode/nmap_W11D1
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/epicode/nmap_W11D1]
└─$ sudo nmap -O --osscan-guess --osscan-limit --reason -oA scans/os_fingerprint 192.168.56.101

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 07:57 EDT
Nmap scan report for 192.168.56.101
Host is up, received reset ttl 255 (0.0023s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 64
22/tcp   open  ssh          syn-ack ttl 64
23/tcp   open  telnet       syn-ack ttl 64
25/tcp   open  smtp         syn-ack ttl 64
53/tcp   open  domain       syn-ack ttl 64
80/tcp   open  http         syn-ack ttl 64
111/tcp  open  rpcbind      syn-ack ttl 64
139/tcp  open  netbios-ssn  syn-ack ttl 64
445/tcp  open  microsoft-ds syn-ack ttl 64
512/tcp  open  exec         syn-ack ttl 64
513/tcp  open  login        syn-ack ttl 64
514/tcp  open  shell        syn-ack ttl 64
1099/tcp open  rmiregistry  syn-ack ttl 64
1524/tcp open  ingreslock   syn-ack ttl 64
2049/tcp open  nfs          syn-ack ttl 64
2121/tcp open  ccproxy-ftp  syn-ack ttl 64
3306/tcp open  mysql        syn-ack ttl 64
5432/tcp open  postgresql   syn-ack ttl 64
5900/tcp open  vnc          syn-ack ttl 64
6000/tcp open  X11          syn-ack ttl 64
6667/tcp open  irc          syn-ack ttl 64
8009/tcp open  ajp13        syn-ack ttl 64
8180/tcp open  unknown      syn-ack ttl 64

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

Per conoscere la specifica versione dell'OS del target: informazioni utili per correlare servizi a vulnerabilità note e per comprendere l'ambiente target.

Come ho strutturato il comando:

nmap
Lo scanner.

-O
Attiva l'OS detection tramite analisi del TCP/IP stack.

--osscan-guess
Se Nmap non è sicuro al 100% fornisce la migliore ipotesi comunque utile al report.

--osscan-limit
Limita i test di OS detection agli host che sembrano avere porte aperte; riduce rumore e tempi inutili.

--reason
Mostra la motivazione dietro lo stato di ogni porta (per es.: perché Nmap ha classificato una porta come open/filtered).

-oA scans/os_fingerprint
Salva i risultati in tre formati (.nmap, .xml, .gnmap) nella directory scans/ con prefisso os_fingerprint.

SYN SCAN

```
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/epicode/nmap_W11D1]
└─$ sudo nmap -sS -p- -T4 --min-rate 500 -sV -sC --reason -oA scans/syn_scan 192.168.56.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 08:05 EDT
Stats: 0:02:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 08:07 (0:00:02 remaining)
Stats: 0:02:32 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 08:07 (0:00:02 remaining)
Stats: 0:02:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 08:08 (0:00:02 remaining)
Stats: 0:03:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 08:08 (0:00:03 remaining)
Nmap scan report for 192.168.56.101
Host is up, received reset ttl 255 (0.013s latency).
Not shown: 65505 filtered tcp ports (no-response)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.1
|      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         syn-ack ttl 64 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      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2025-09-25T12:09:30+00:00; -1s from scanner time.
| 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
```

Per mappare l'intera superficie TCP (porte 0–65535) in modo rapido e meno rilevabile.

Come ho strutturato il comando:

-sS
SYN scan, invia SYN e, se riceve SYN/ACK, invia RST invece di completare handshake. Meno tracciabile.

-p-
Scansiona tutte le porte (0–65535).

-T4
Timing: aggressivo, velocizza la scansione su reti locali. Bilanciato per non generare troppi falsi negativi.

--min-rate 500
Impone una velocità minima di pacchetti/sec (utile in LAN).

-sV
Service/version detection: chiede banner ai servizi per identificare versione.

-sC
Esegue gli script NSE di default (info aggiuntive, banner grab, checks base).

--reason
Giustifica lo stato delle porte.

-oA scans/syn_scan
Salvataggio completo in tre formati.

TCP CONNECT SCAN

```
┌──(kali㉿kali)-[~/epicode/nmap_W11D1]
└─$ nmap -sT -p- -T3 -sV --reason -oA scans/tcp_connect 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 08:10 EDT
Nmap scan report for 192.168.56.101
Host is up, received reset ttl 255 (0.015s latency).
Not shown: 65505 filtered tcp ports (no-response)
PORT      STATE SERVICE     REASON  VERSION
21/tcp    open  ftp         syn-ack vsftpd 2.3.4
22/tcp    open  ssh         syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack Linux telnetd
25/tcp    open  smtp        syn-ack Postfix smtpd
53/tcp    open  domain      syn-ack ISC BIND 9.4.2
80/tcp    open  http        syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack netkit-rsh rexecd
513/tcp   open  login?      syn-ack
514/tcp   open  shell       syn-ack Netkit rshd
1099/tcp  open  java-rmi    syn-ack GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack Metasploitable root shell
2049/tcp  open  nfs         syn-ack 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack (access denied)
6667/tcp  open  irc         syn-ack UnrealIRCd
6697/tcp  open  tcpwrapped  syn-ack
8009/tcp  open  ajp13       syn-ack Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35436/tcp open  nlockmgr    syn-ack 1-4 (RPC #100021)
38608/tcp open  java-rmi    syn-ack GNU Classpath grmiregistry
45132/tcp open  status      syn-ack 1 (RPC #100024)
48309/tcp open  mountd      syn-ack 1-3 (RPC #100005)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ke
rnel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 231.17 seconds
```

Per confrontare comportamento e risultati rispetto al SYN scan: -sT completa il 3-way handshake (connect()), quindi simula connessioni reali e può far emergere differenze dovute a firewall/IDS/rules basate sullo stato della connessione.

Come ho strutturato il comando:

nmap
(sudo non è necessario, perché -sT usa la libc connect())

-sT
TCP connect scan: completa handshake. Più “rumoroso” e registrato sui log del target.

-p-
Scansiona tutte le porte.

-T3
Timing medio (più stabile per connect scan).

-sV
Version detection.

--reason
Motivazione dello stato.

-oA scans/tcp_connect
Salvataggio output.

2. ESTRAZIONE DELLE PORTE APERTE TROVATE DAL SYN SCAN

```
┌──(kali㉿kali)-[~/epicode/nmap_W11D1]
└─$ grep -E '/tcp.*open' scans/syn_scan.nmap > scans/syn_open_ports.txt
less scans/syn_open_ports.txt
```

Come ho strutturato il comando:

1) grep -E '/tcp.*open' scans/syn_scan.nmap filtra tutte le righe in cui Nmap segnala porte TCP aperte. Uso l'-E per regex estesa e ".*" in modo da poter coinvolgere qualsiasi carattere tra "/tcp" e "open".

2) scans/syn_open_ports.txt per redirigervi l'output, in modo da avere un file verificabile e allegabile.

3) less per permettere una lettura a schermo.

```
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  shell       syn-ack ttl 64 Netkit rshd
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35436/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
38608/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
45132/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
48309/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
scans/syn_open_ports.txt (END)
```

3. VISIONARE LA LISTA PORTE SEPARATA DALLE VIRGOLE (PER VERSION DETECTION)

```
┌──(kali㉿kali)-[~/epicode/nmap_W11D1]
└─$ grep -E '/tcp.*open' scans/syn_scan.nmap | awk '{print $1}' | sed 's#/tcp##' | paste -sd, - > scans/open_ports_list.txt
echo "Porte: $(cat scans/open_ports_list.txt)"

Porte: 21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,3632,5432,5900,6000,6667,6697,8009,8180,8787,35436,38608,45132,48309

┌──(kali㉿kali)-[~/epicode/nmap_W11D1]
└─$
```

Come ho strutturato il comando:

1) grep prende le righe con open.

2) awk '{print $1}' estrae la prima colonna (22/tcp).

3) sed 's#/tcp##' rimuove la parte /tcp, restando solo il numero di porta.

4) paste -sd, - concatena tutte le righe in una singola riga separata da virgole: formato ideale per -p di nmap.

5) Salvato su scans/open_ports_list.txt per riutilizzo e controllo.

4. VERSION DETECTION DELLE PORTE TROVATE

```
┌──(kali㉿kali)-[~/epicode/nmap_W11D1]
└─$ PORTS=$(cat scans/open_ports_list.txt)
sudo nmap -sV --version-intensity 5 --version-all -p $PORTS -oA scans/version_detection 192.168.56.101 --stats-every 15s

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 10:22 EDT
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 10:22 (0:00:01 remaining)
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 10:23 (0:00:01 remaining)
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 10:23 (0:00:02 remaining)
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 10:23 (0:00:02 remaining)
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 10:23 (0:00:03 remaining)
Stats: 0:01:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 10:24 (0:00:03 remaining)
Stats: 0:01:46 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 10:24 (0:00:04 remaining)
Stats: 0:02:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 10:24 (0:00:04 remaining)
Stats: 0:02:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 10:25 (0:00:05 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```

Come ho strutturato il comando:

PORTS=$(cat scans/open_ports_list.txt): salva la lista di porte nella variabile bash $PORTS per chiarezza e riuso.

sudo: classico per i permessi

-sV: esegue la Version Detection (application-layer probes). È il cuore per ottenere la versione del servizio.

--version-intensity 5: intensità intermedia di probe. Scala 0..9. Ho scelto 5 perché è bilanciato tra accuratezza e tempo.

--version-all: prova tutti i test disponibili nella libreria di probe di nmap

-p $PORTS: istruisce nmap a sondare solo quelle porte (evita le 65k porte).

-oA scans/version_detection: salva output in .nmap, .xml, .gnmap.

--stats-every 15s: mostra progresso periodico.

5. REPORT E ANALISI

1) DATI GENERICI

Target IP: 192.168.56.101

Host up: sì (latency ~1–15 ms nei vari run)

Metodologia:

OS fingerprint: nmap -O

SYN scan full-port + version + NSE: nmap -sS -p- -sV -sC

TCP connect full-port + version: nmap -sT -p- -sV

Version detection mirata su porte open: nmap -sV --version-all -p <lista porte>

2) SISTEMA OPERATIVO:

Evidenze rilevate:
Service Info e script SMB indicano Unix/Linux; smb-os-discovery riporta “Unix (Samba 3.0.20-Debian)”.

Conclusione:
Linux

3. PORTE APERTE E SERVIZI (VERSION DETECTION MIRATA)

Porta	Servizio	Versione
21	ftp	vsftpd 2.3.4
22	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	telnet	Linux telnetd
25	smtp	Postfix smtpd
53	domain	ISC BIND 9.4.2
80	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	rpcbind	2 (RPC #100000)
139	netbios-ssn	Samba smbd 3.X–4.X (WORKGROUP)
445	netbios-ssn	Samba smbd 3.X–4.X (WORKGROUP)
512	exec	netkit-rsh rexecd
513	login	login?
514	shell	Netkit rshd
1099	java-rmi	GNU Classpath grmiregistry
1524	bindshell	Metasploitable root shell
2049	nfs	2–4 (RPC #100003)
2121	ftp	ProFTPD 1.3.1
3306	mysql	MySQL 5.0.51a-3ubuntu5
3632	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432	postgresql	PostgreSQL DB 8.3.0–8.3.7
5900	vnc	VNC (protocol 3.3)
6000	X11	(access denied)
6667	irc	UnrealIRCd
6697	irc	UnrealIRCd
8009	ajp13	Apache Jserv (Protocol v1.3)
8180	http	Apache Tomcat/Coyote JSP engine 1.1
8787	drb	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35436	nlockmgr	1–4 (RPC #100021)
38608	java-rmi	GNU Classpath grmiregistry
45132	status	1 (RPC #100024)
48309	mountd	1–3 (RPC #100005)

4. DESCRIZIONE DEI SERVIZI
Ho proceduto a informarmi sull'efficienza ed i rischi principali (a grandi linee) di ogni porta.

1.FTP vsftpd 2.3.4 (21): versione storicamente vulnerabile; anonymous enabled = rischio esfiltrazione/upload non autorizzato.

2. SSH OpenSSH 4.7p1 (22): release datata; raccomandati hardening e aggiornamento (disabilitare root login, ciphers moderni).

3. Telnet (23): protocolli in chiaro = credenziali intercettabili; da dismettere.

4. SMTP Postfix (25): supporto SSLv2 e cifrari deboli = rischio crittografico; aggiornare e limitare comandi come VRFY.

5. DNS BIND 9.4.2 (53): branch obsoleto con CVE storiche; restringere recursion, aggiornare.

6. HTTP Apache 2.2.8 (80) / Tomcat 5.5 (8180) / AJP13 (8009): stack web legacy con vulnerabilità note; aggiornare o filtrare.

7. SMB 139/445: condivisioni potenzialmente enumerabili; hardening e filtro perimetrale.

8. rsh/rexec/rlogin (512/513/514): protocolli legacy non cifrati; da rimuovere.

9. Java RMI (1099/38608) & Ruby DRb (8787): superfici RMI/deserializzazione; restringere bind, autenticare.

10. Bindshell (1524): backdoor dimostrativa; da rimuovere in contesti reali.

11. NFS & RPC (2049, nlockmgr, mountd, status): possibili export permissivi; verificare /etc/exports e limitare per IP.

12. DBMS MySQL 5.0.51a (3306) / PostgreSQL 8.3.x (5432): versioni EOL; rafforzare autenticazione e cifratura, aggiornare.

13. VNC 3.3 (5900): autenticazione debole, traffico non cifrato.

14. X11 (6000): porta esposta anche se "access denied"; filtrare.

15. IRC UnrealIRCd (6667/6697): demo/lab; 6697 solitamente TLS.

5. DIFFERENZE REPERITE TRA SYN E TCP

Porta	**Stato (SYN)**	**Servizio (SYN)**	**Stato (TCP)**	**Servizio (TCP)**	**Considerazioni finali**
445	open	Samba smbd 3.0.20-Debian	open	Samba smbd 3.X–4.X	Probe diversi hanno estratto banner con granularità differente; il servizio è lo stesso.
6697	open	irc UnrealIRCd	open	tcpwrapped	Con handshake completo il servizio chiude subito o è dietro wrapper; metà delle suite IRC su 6697 richiedono TLS specifico.
altre porte	open	coerente	open	coerente	Nessuna differenza

Come visibile, differiscono alcune stringhe di identificazione servizio per via dei diversi probe/handshake.