esercizio UNIT2 S5/L2

consegna:

- *effettuare le seguenti scansioni sul target Metasploitable:*

● *OS fingerprint.*
● *Syn Scan.*
● *TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?*
● *Version detection.*

- *E sul target Windows:*

● *OS fingerprint.*

mostrare un report che riporti le seguenti info (dove disponibili):

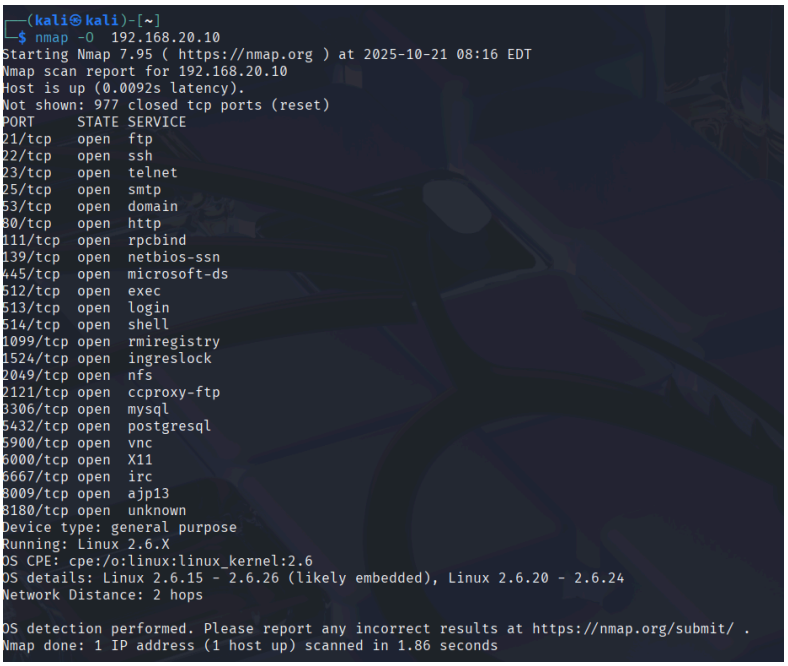
1. *IP.*
2. *Sistema Operativo.*
3. *Porte Aperte.*
4. *Servizi in ascolto con versione.*

Legenda

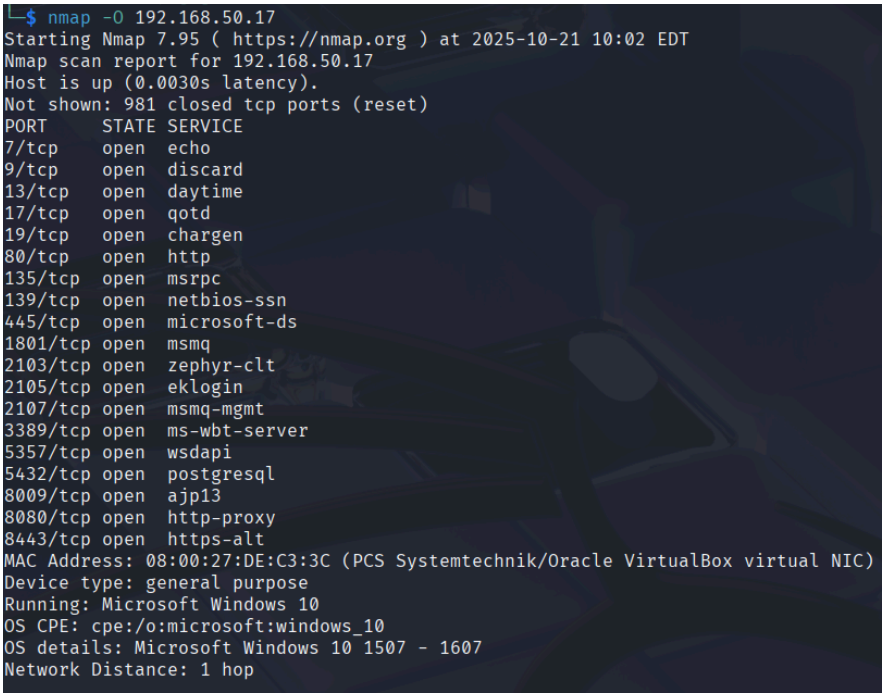
IPv4 kali: 192.168.50.10
IPv4 Metasploitable: 192.168.20.10
IPv4 Windows: 192.168.50.17

OS fingerprint:

Per la risoluzione dell'esercizio ho eseguito inizialmente tutti gli scan singolarmente per mostrare chiaramente gli output per ogni comando da terminale.
Per la ricerca dell'OS fingerprint ho eseguito il comando **nmap -O.** questo è stato l'output per l'IP della macchina Metasploitable:



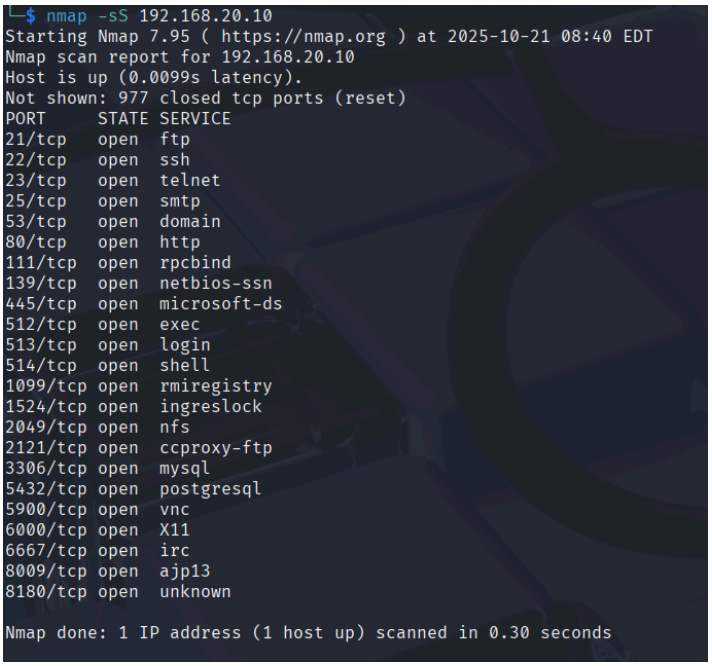
per quanto riguarda invece l'OS fingerprint della macchina Windows, utilizzando sempre lo stesso comando è possibile vedere la conferma di windows 10, mostrando in fondo al terminale



Syn Scan e TCP connect.

Per la seguente ricerca ho utilizzato i comandi **nmap -sS** per il syn scan, mentre per il TCP scan ho usato il comando **nmap -sT.**

Syn scan:



TCP scan:

```
└─$ nmap -sT 192.168.20.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 08:42 EDT
Nmap scan report for 192.168.20.10
Host is up (0.020s latency).
Not shown: 977 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

tuttavia per notare le differenze sostanziali tra i due scan ho dovuto utilizzare il programma wireshark che catturando il traffico di rete durante le scansioni mostra come nel Syn scan, essendo più leggero, la comunicazione con le porte aperte viene interrotta prima che venga data la risposta ACK del protocollo Three way handshake:

scan tramite -sS

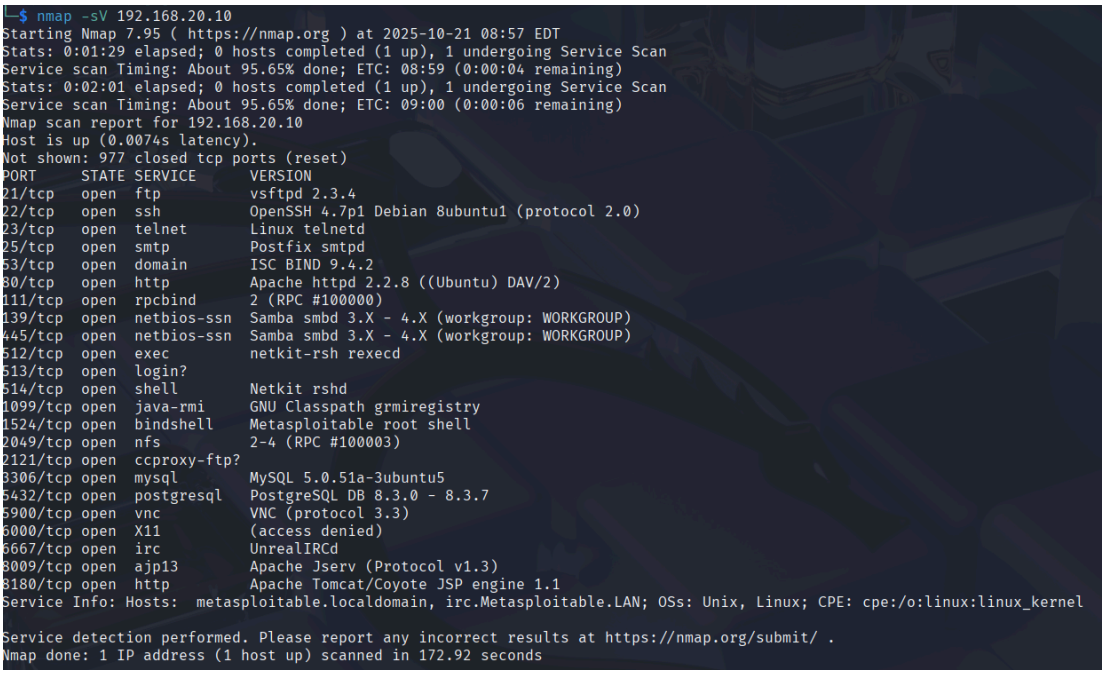
←	5	0.001149643	192.168.20.10	192.168.50.10	ICMP	60 Echo (ping) reply id=0x28e3, seq=0/0, ttl=63
	6	0.001149853	192.168.20.10	192.168.50.10	TCP	60 443 → 47896 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	7	0.001149904	192.168.20.10	192.168.50.10	ICMP	60 Timestamp reply id=0x8510, seq=0/0, ttl=63
	8	0.051633902	192.168.50.10	1.1.1.1	DNS	86 Standard query 0x4957 PTR 10.20.168.192.in-addr.a
	9	0.065031158	1.1.1.1	192.168.50.10	DNS	86 Standard query response 0x4957 No such name PTR 1
	10	0.076488190	192.168.50.10	192.168.20.10	TCP	58 48152 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	11	0.076488190	192.168.50.10	192.168.20.10	TCP	58 48152 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	12	0.076488190	192.168.50.10	192.168.20.10	TCP	58 48152 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	13	0.076488190	192.168.50.10	192.168.20.10	TCP	58 48152 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	14	0.076488190	192.168.50.10	192.168.20.10	TCP	58 48152 → 24 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	15	0.076488190	192.168.50.10	192.168.20.10	TCP	58 48152 → 20 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	16	0.087969542	192.168.20.10	192.168.50.10	TCP	60 21 → 48152 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
	17	0.087969763	192.168.20.10	192.168.50.10	TCP	60 23 → 48152 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
	18	0.087969853	192.168.20.10	192.168.50.10	TCP	60 25 → 48152 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
	19	0.087969933	192.168.20.10	192.168.50.10	TCP	60 22 → 48152 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
	20	0.087970004	192.168.20.10	192.168.50.10	TCP	60 24 → 48152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	21	0.087970074	192.168.20.10	192.168.50.10	TCP	60 20 → 48152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	22	0.088025421	192.168.50.10	192.168.20.10	TCP	54 48152 → 21 [RST] Seq=1 Win=0 Len=0
	23	0.088063435	192.168.50.10	192.168.20.10	TCP	54 48152 → 23 [RST] Seq=1 Win=0 Len=0
	24	0.088095759	192.168.50.10	192.168.20.10	TCP	54 48152 → 25 [RST] Seq=1 Win=0 Len=0
	25	0.088120383	192.168.50.10	192.168.20.10	TCP	54 48152 → 22 [RST] Seq=1 Win=0 Len=0

scan tramite -sT

→	1	0.000000000	192.168.50.10	192.168.20.10	ICMP	42 Echo (ping) request id=0xb80f, seq=0/0, ttl=56 (reply in 5)
	2	0.000266402	192.168.50.10	192.168.20.10	TCP	58 62372 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	3	0.000367654	192.168.50.10	192.168.20.10	TCP	54 62372 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
	4	0.000472440	192.168.50.10	192.168.20.10	ICMP	54 Timestamp request id=0x7e26, seq=0/0, ttl=58
←	5	0.001727070	192.168.20.10	192.168.50.10	ICMP	60 Echo (ping) reply id=0xb80f, seq=0/0, ttl=63 (request in 1)
	6	0.001727710	192.168.20.10	192.168.50.10	TCP	60 443 → 62372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	7	0.001727761	192.168.20.10	192.168.50.10	ICMP	60 Timestamp reply id=0x7e26, seq=0/0, ttl=63
	8	0.039343039	192.168.50.10	1.1.1.1	DNS	86 Standard query 0xe8d3 PTR 10.20.168.192.in-addr.arpa
	9	0.057877672	1.1.1.1	192.168.50.10	DNS	86 Standard query response 0xe8d3 No such name PTR 10.20.168.192.in-add…
	10	0.055335039	192.168.50.10	192.168.20.10	TCP	74 38132 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=9301…
	11	0.055335039	192.168.50.10	192.168.20.10	TCP	74 57508 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=9301…
	12	0.055335039	192.168.50.10	192.168.20.10	TCP	74 56986 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=9301…
	13	0.055335039	192.168.50.10	192.168.20.10	TCP	74 34520 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=9301…
	14	0.055335039	192.168.50.10	192.168.20.10	TCP	74 59866 → 24 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=9301…
	15	0.055335039	192.168.50.10	192.168.20.10	TCP	74 44488 → 20 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=9301…
	16	0.059588500	192.168.20.10	192.168.50.10	TCP	74 22 → 38132 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM …
	17	0.059588621	192.168.20.10	192.168.50.10	TCP	74 25 → 57508 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM …
	18	0.059588681	192.168.20.10	192.168.50.10	TCP	74 23 → 56986 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM …
	19	0.059588721	192.168.20.10	192.168.50.10	TCP	74 21 → 34520 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM …
	20	0.059588761	192.168.20.10	192.168.50.10	TCP	60 24 → 59866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	21	0.059588800	192.168.20.10	192.168.50.10	TCP	60 20 → 44488 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	22	0.059649465	192.168.50.10	192.168.20.10	TCP	66 38132 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=930144277 TSecr=6…
	23	0.059683132	192.168.50.10	192.168.20.10	TCP	66 57508 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=930144277 TSecr=6…
	24	0.059706285	192.168.50.10	192.168.20.10	TCP	66 56986 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=930144277 TSecr=6…
	25	0.059727314	192.168.50.10	192.168.20.10	TCP	66 34520 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=930144277 TSecr=6…
	26	0.055335039	192.168.50.10	192.168.20.10	TCP	66 38132 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=930144277 TS…
	27	0.055335039	192.168.50.10	192.168.20.10	TCP	66 57508 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=930144277 TS…
	28	0.055335039	192.168.50.10	192.168.20.10	TCP	66 56986 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=930144277 TS…
	29	0.055335039	192.168.50.10	192.168.20.10	TCP	66 34520 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=930144277 TS…

(in questo specifico caso lo scan non è stato eseguito su tutte le porte ma in un range di 20-25 per mostrare il processo.)

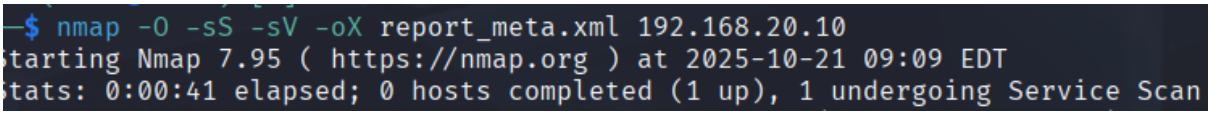
Version detection:
Con il comando **-nmap -sV** è stato possibile invece analizzare i servizi in esecuzione e le relative versioni sulle rispettiva porte.
l'output da terminale è il seguente:



```
└─$ nmap -sV 192.168.20.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 08:57 EDT
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 08:59 (0:00:04 remaining)
Stats: 0:02:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 09:00 (0:00:06 remaining)
Nmap scan report for 192.168.20.10
Host is up (0.0074s 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  ccproxy-ftp?
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 172.92 seconds
```

REPORT HTML:
A questo punto per avere un file ordinato, con tutte le info all'interno di tabelle e poter essere presentato, ho creato un file in formato xml, in cui veniva richiesta L'OS fingerprint, la version dei servizi attivi e potendo scegliere solo uno dei due scan, tra il syn scan e il tcp scan ho optato per il primo per una questione di velocità.



```
└─$ nmap -O -sS -sV -oX report_meta.xml 192.168.20.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 09:09 EDT
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
```

Una volta creato il file in formato xml, l'ho dovuto convertire in un formato leggibile, scegliendo per l'HTML

```
┌──(kali㉿kali)-[~]
└─$ xsltproc report_meta.xml -o report_meta.html
```

la versione finale, leggibile da browser alla fine è stato la seguente:

Nmap Scan Report - Scanned at Tue Oct 21 09:09:15 2025

Scan Summary | **192.168.20.10**

Scan Summary

Nmap 7.95 was initiated at Tue Oct 21 09:09:15 2025 with these arguments:
/usr/lib/nmap/nmap --privileged -O -sS -sV -oX report_meta.xml 192.168.20.10

Verbosity: 0; Debug level 0

Nmap done at Tue Oct 21 09:12:09 2025; 1 IP address (1 host up) scanned in 174.31 seconds

192.168.20.10

Address

- 192.168.20.10 (ipv4)

Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
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	ccproxy-ftp	syn-ack			
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
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		
8009	tcp	open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **41568/udp** (**closed**)
- OS match: **Linux 2.6.15 - 2.6.26 (likely embedded)** (**100%**)
- OS match: **Linux 2.6.20 - 2.6.24** (**100%**)

Misc Metrics (click to expand)

Metric	Value
Ping Results	echo-reply
System Uptime	62687 seconds (last reboot: Mon Oct 20 15:47:22 2025)
Network Distance	2 hops
TCP Sequence Prediction	Difficulty=199 (Good luck!)
IP ID Sequence Generation	All zeros

Go t
Toggle Cl

in questo report automatizzato è possibile rileggere il comando che è stato lanciato con le informazioni richieste, l'indirizzo IP della Metasploitable, le porte aperte, i servizi che operano sulle porte e loro relative versioni, e infine anche il match col sistema operativo.

Conclusioni:

Con questo esercizio è stato possibile fare l'analisi di quelli che sono potenzialmente i sistemi operativi di macchine sia presenti sulla mia stessa rete, sia di una presenta in una rete differente ma in comunicazione con la kali. Oltre a questo è stato immediato il ricevere informazioni su porte, servizi e versioni così da poter conoscere a pieno e poter in caso sfruttare potenziali vulnerabilità.