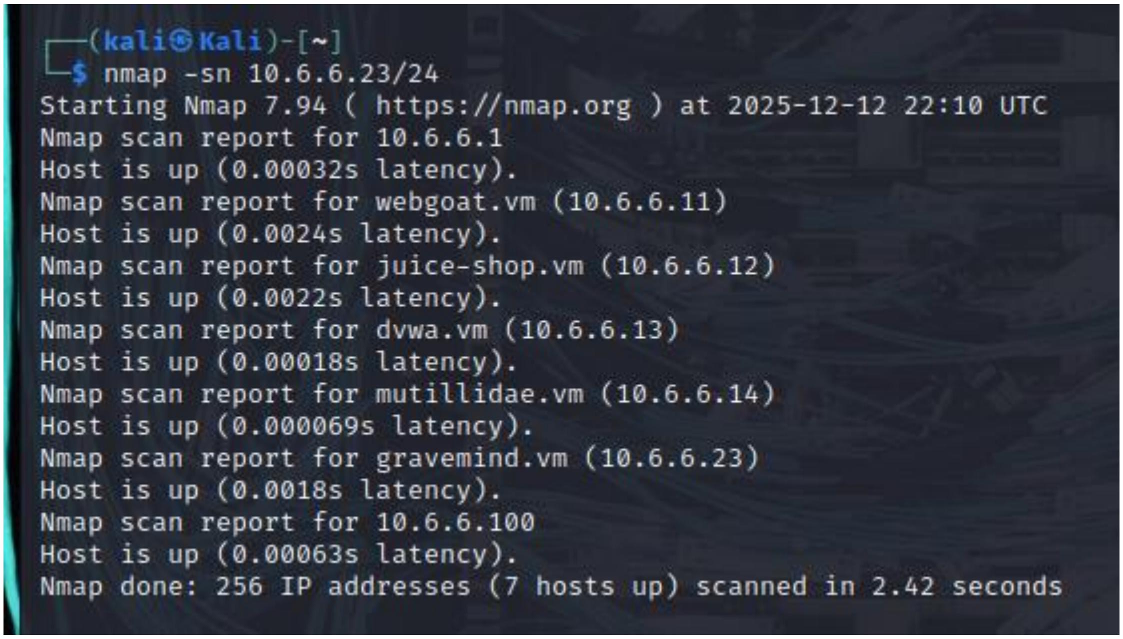
Host Discovery

Network Scan – to determine which Host Ip are Up.

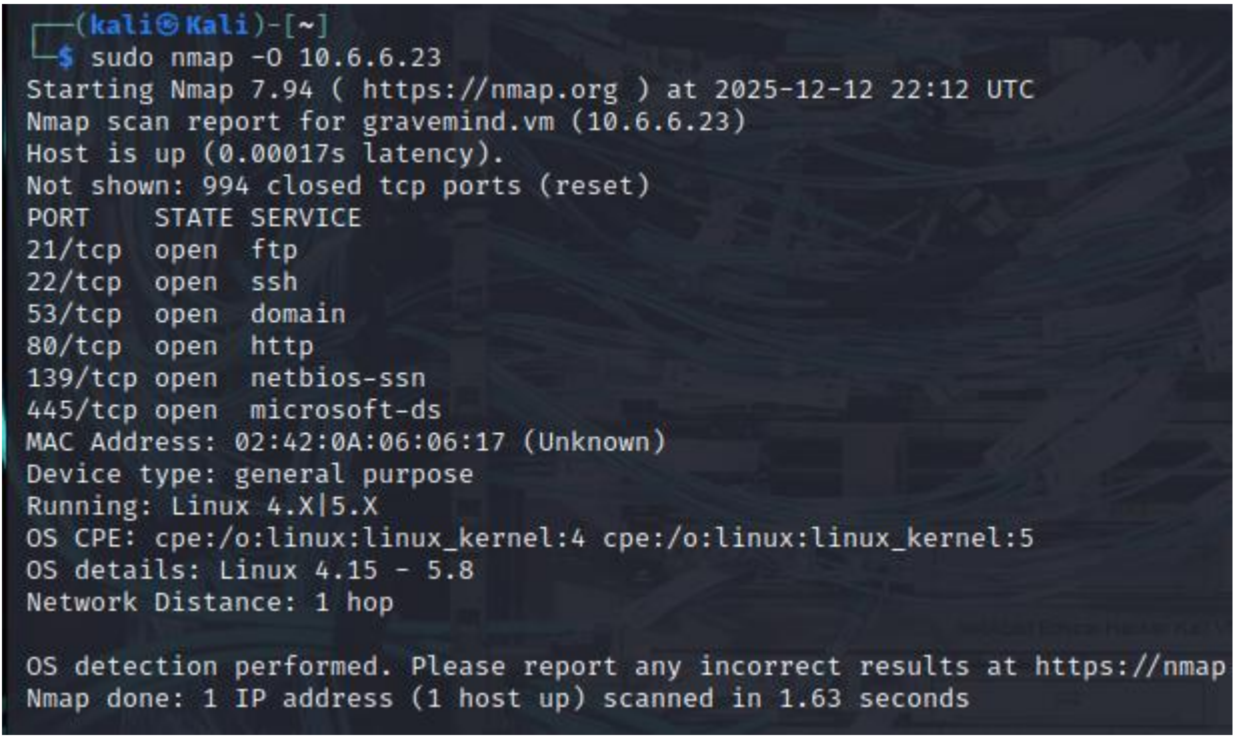
Performs a ping sweep to identify active hosts on the subnet



```
┌──(kali㉿Kali)-[~]
└─$ nmap -sn 10.6.6.23/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 22:10 UTC
Nmap scan report for 10.6.6.1
Host is up (0.00032s latency).
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.0024s latency).
Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.0022s latency).
Nmap scan report for dvwa.vm (10.6.6.13)
Host is up (0.00018s latency).
Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.000069s latency).
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0018s latency).
Nmap scan report for 10.6.6.100
Host is up (0.00063s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.42 seconds
```

Operating System Detection

Attempts OS fingerprinting using Nmap's OS detection engine.

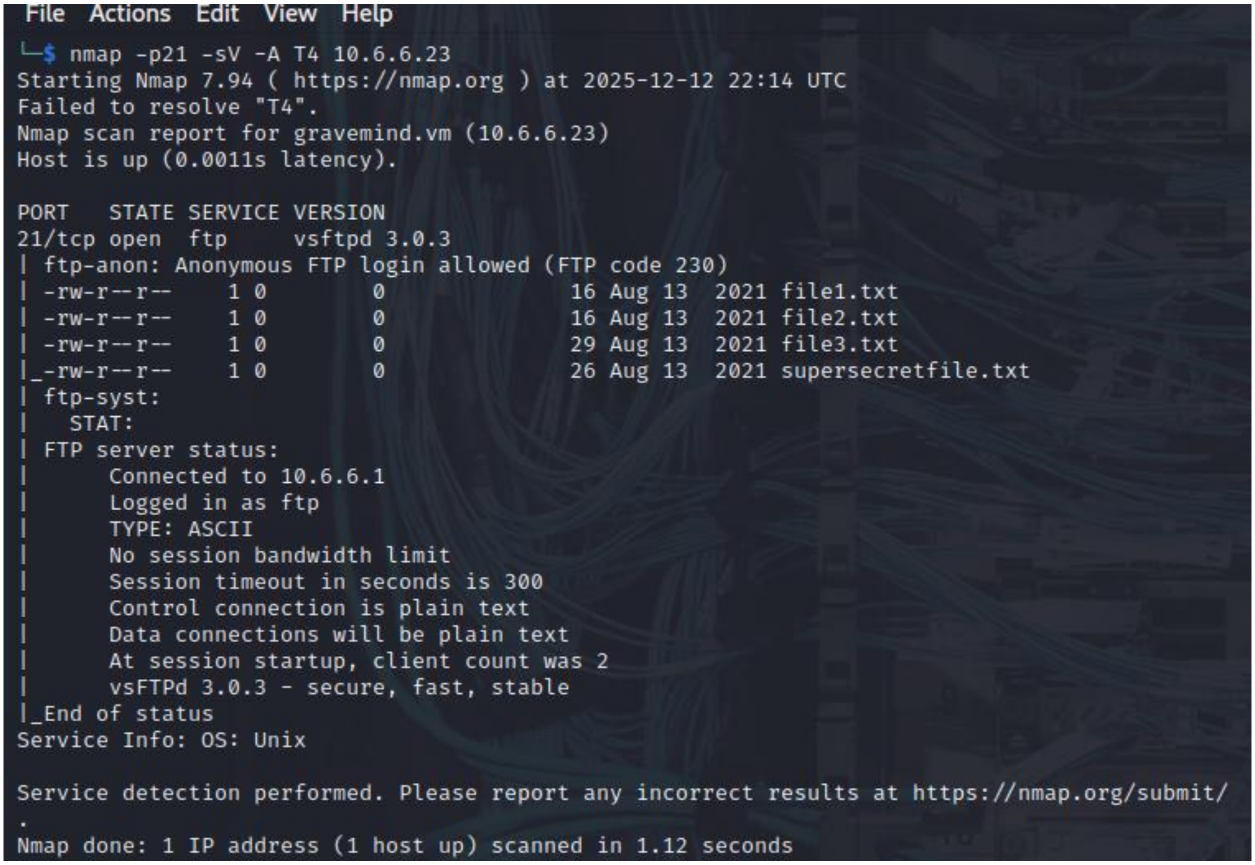


```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -O 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 22:12 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00017s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 02:42:0A:06:06:17 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

.

Port 21 Aggressive Service Scan

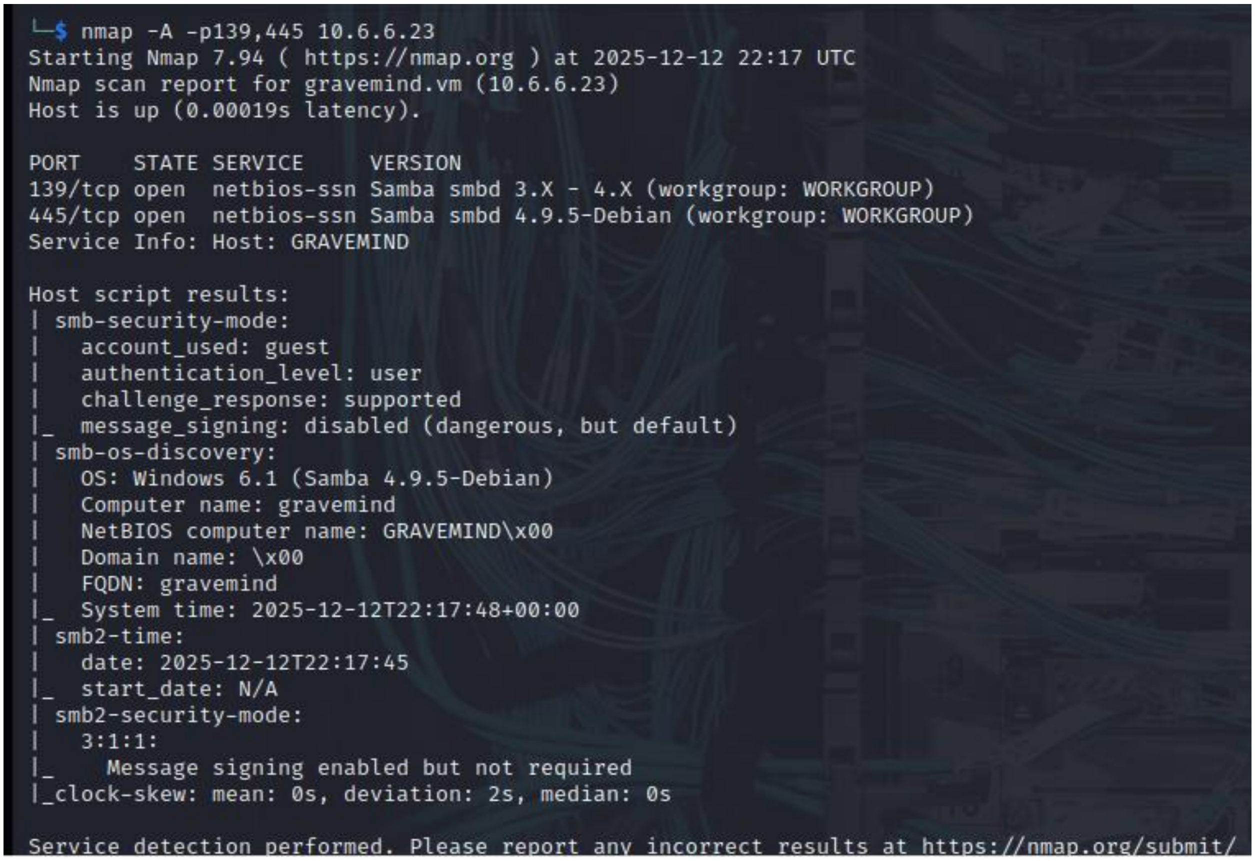
Identifies the service running on port 21, detects version information, and performs aggressive scanning.



```
└─$ nmap -p21 -sV -A T4 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 22:14 UTC
Failed to resolve "T4".
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0011s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              16 Aug 13  2021 file1.txt
| -rw-r--r--    1 0        0              16 Aug 13  2021 file2.txt
| -rw-r--r--    1 0        0              29 Aug 13  2021 file3.txt
|_-rw-r--r--    1 0        0              26 Aug 13  2021 supersecretfile.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.6.6.1
|      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
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
```

SMB Ports Scan (139 and 445)

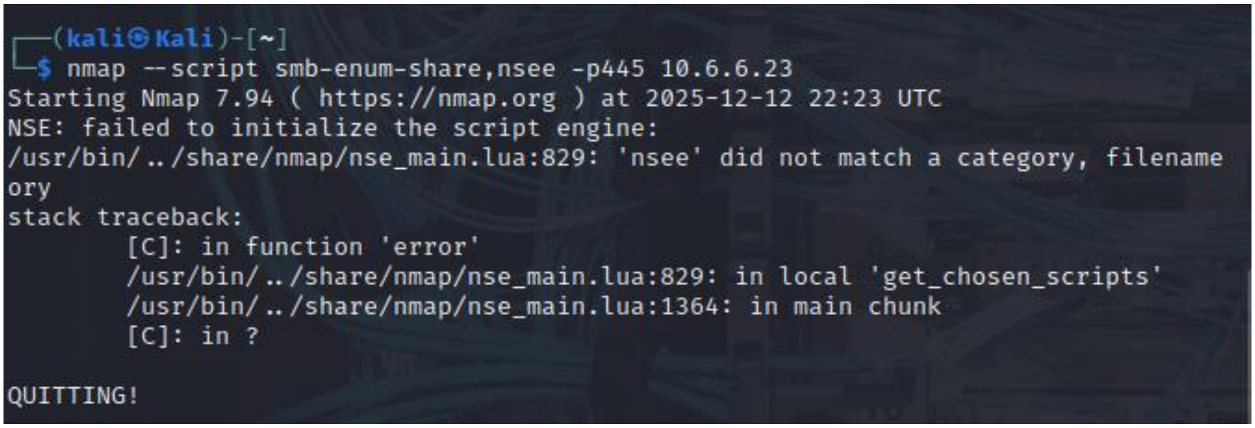
Enumerates SMB services and gathers additional OS and network information



```
└─$ nmap -A -p139,445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 22:17 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00019s latency).

PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
Service Info: Host: GRAVEMIND

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: gravemind
|   NetBIOS computer name: GRAVEMIND\x00
|   Domain name: \x00
|   FQDN: gravemind
|_  System time: 2025-12-12T22:17:48+00:00
| smb2-time:
|   date: 2025-12-12T22:17:45
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 0s, deviation: 2s, median: 0s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
```

SMB Share Enumeration with NSE Script

Used to manually verify SMB access and inspect the discovered share.



```
┌──(kali㉿Kali)-[~]
└─$ nmap --script smb-enum-share,nsee -p445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 22:23 UTC
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:829: 'nsee' did not match a category, filename
ory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1364: in main chunk
        [C]: in ?

QUITTING!
```

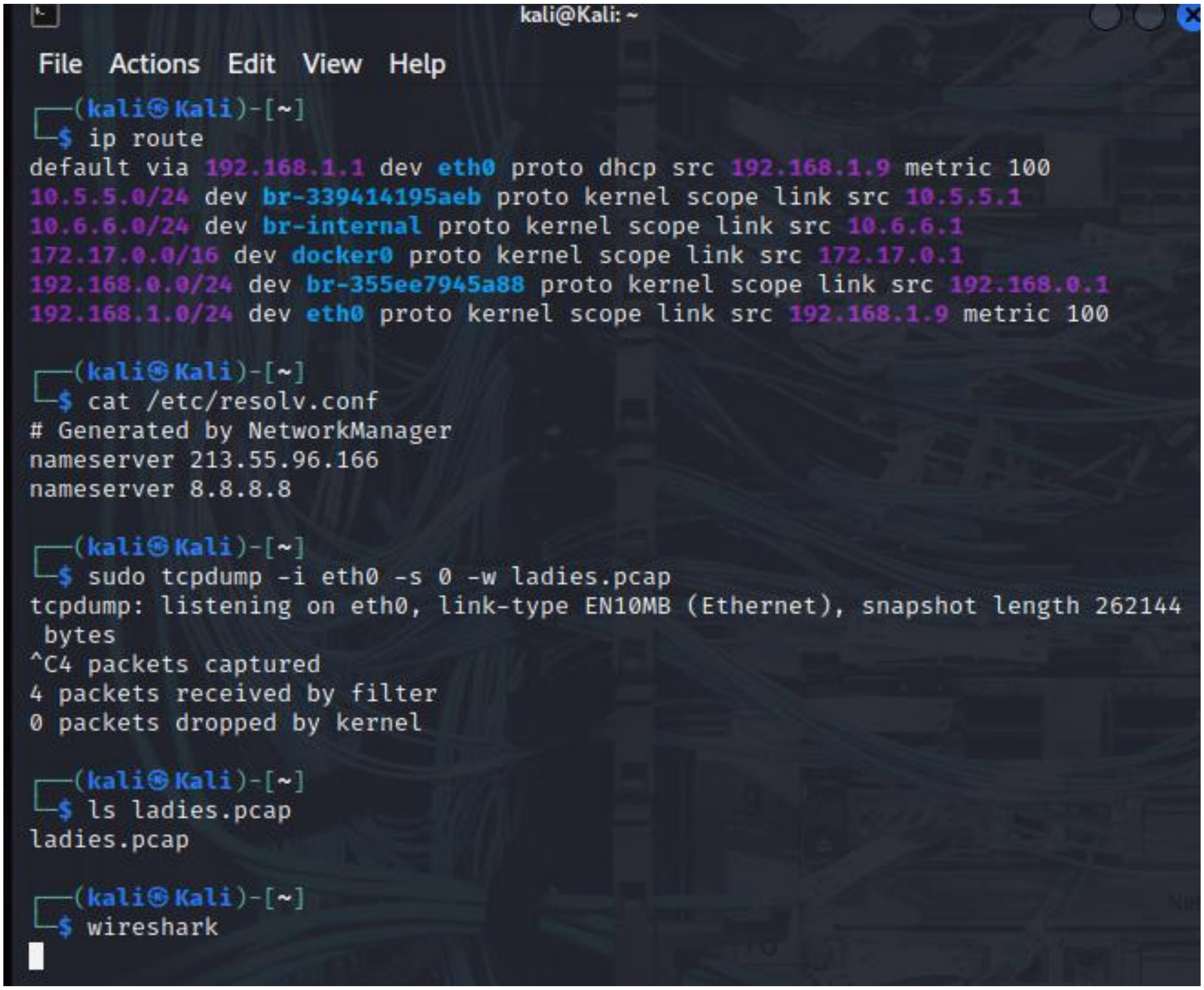
Supporting Network Context Commands

Displays interface information, route paths, and DNS resolver configuration.

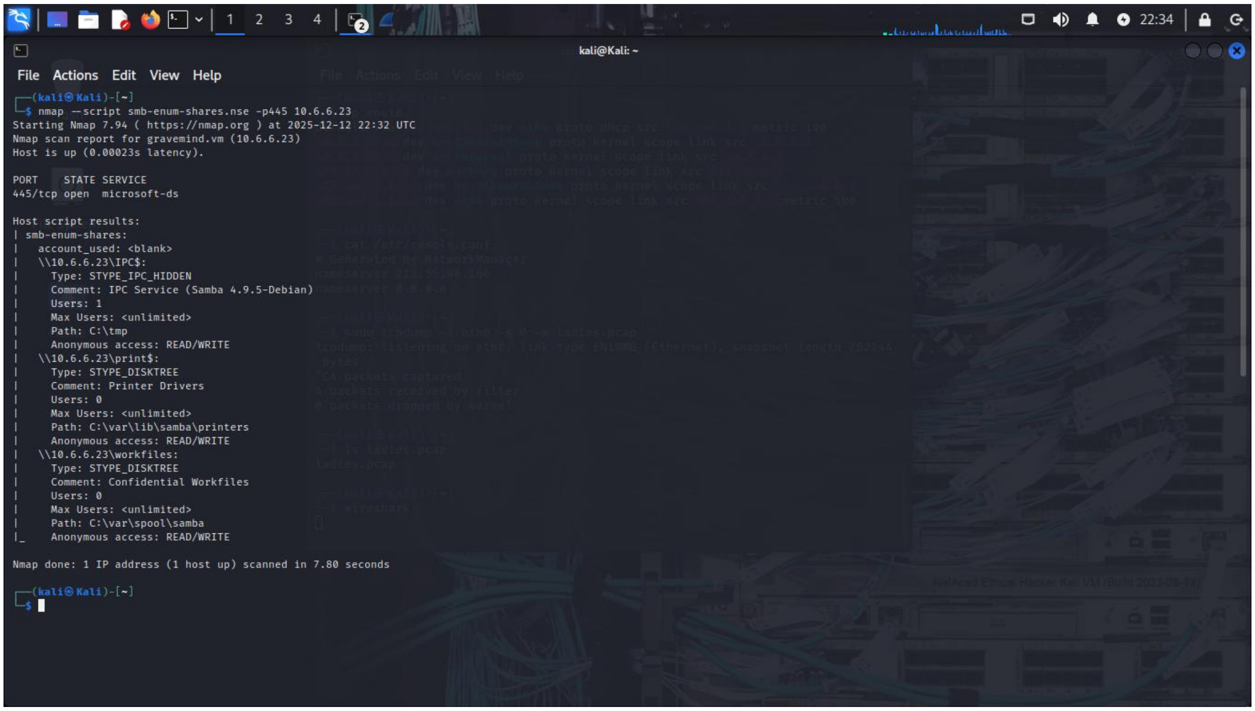
Packet Capture with tcpdump

Captures all packets passing through the interface during the scans.

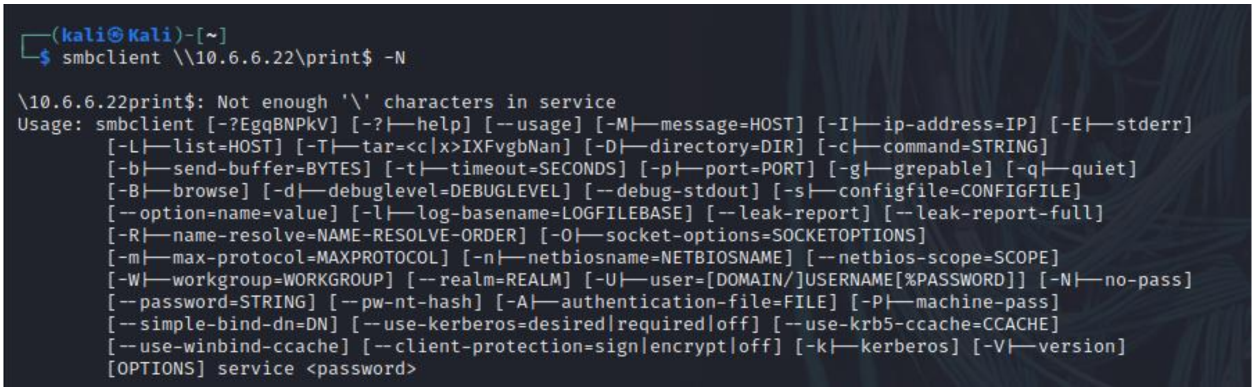
To stop capture: Press Ctrl + C. and Verify file.



```
┌──(kali㉿Kali)-[~]
└─$ ip route
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.9 metric 100
10.5.5.0/24 dev br-339414195aeb proto kernel scope link src 10.5.5.1
10.6.6.0/24 dev br-internal proto kernel scope link src 10.6.6.1
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1
192.168.0.0/24 dev br-355ee7945a88 proto kernel scope link src 192.168.0.1
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.9 metric 100

┌──(kali㉿Kali)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 213.55.96.166
nameserver 8.8.8.8

┌──(kali㉿Kali)-[~]
└─$ sudo tcpdump -i eth0 -s 0 -w ladies.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144
 bytes
^C4 packets captured
4 packets received by filter
0 packets dropped by kernel

┌──(kali㉿Kali)-[~]
└─$ ls ladies.pcap
ladies.pcap

┌──(kali㉿Kali)-[~]
└─$ wireshark
█
```



```
┌──(kali㉿Kali)-[~]
└─$ nmap --script smb-enum-shares.nse -p445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 22:32 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00023s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\10.6.6.23\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba 4.9.5-Debian)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\workfiles:
|     Type: STYPE_DISKTREE
|     Comment: Confidential Workfiles
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\spool\samba
|_    Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 7.80 seconds

┌──(kali㉿Kali)-[~]
└─$ 
```



```
┌──(kali㉿Kali)-[~]
└─$ smbclient \\10.6.6.22\print$ -N

\10.6.6.22print$: Not enough '\' characters in service
Usage: smbclient [-?EgqBNPkV] [-?|--help] [--usage] [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr]
        [-L|--list=HOST] [-T|--tar=<c|x>IXFvgbNan] [-D|--directory=DIR] [-c|--command=STRING]
        [-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT] [-g|--grepable] [-q|--quiet]
        [-B|--browse] [-d|--debuglevel=DEBUGLEVEL] [--debug-stdout] [-s|--configfile=CONFIGFILE]
        [--option=name=value] [-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full]
        [-R|--name-resolve=NAME-RESOLVE-ORDER] [-O|--socket-options=SOCKETOPTIONS]
        [-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE]
        [-W|--workgroup=WORKGROUP] [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass]
        [--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE] [-P|--machine-pass]
        [--simple-bind-dn=DN] [--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE]
        [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k|--kerberos] [-V|--version]
        [OPTIONS] service <password>
```