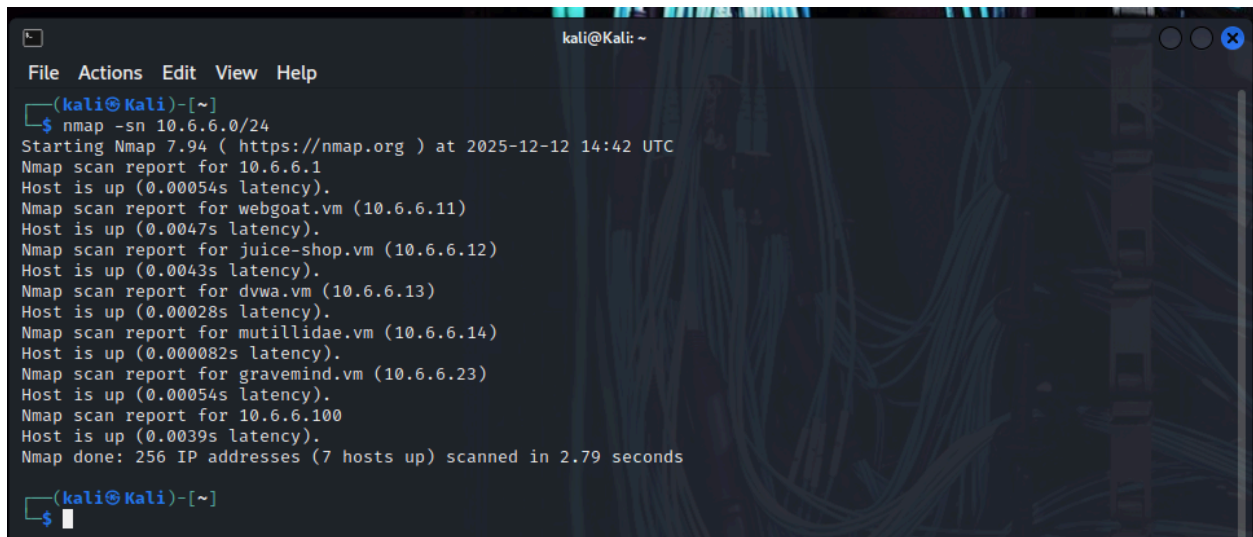


Network traffic analysis and manipulation techniques.

Odecode Seun

1. Identifying Network Hosts

```
nmap -sn 10.6.6.0/24
```



```
(kali㉿kali)-[~]  
$ nmap -sn 10.6.6.0/24  
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 14:42 UTC  
Nmap scan report for 10.6.6.1  
Host is up (0.00054s latency).  
Nmap scan report for webgoat.vm (10.6.6.11)  
Host is up (0.0047s latency).  
Nmap scan report for juice-shop.vm (10.6.6.12)  
Host is up (0.0043s latency).  
Nmap scan report for dvwa.vm (10.6.6.13)  
Host is up (0.00028s latency).  
Nmap scan report for mutillidae.vm (10.6.6.14)  
Host is up (0.000082s latency).  
Nmap scan report for gravemind.vm (10.6.6.23)  
Host is up (0.00054s latency).  
Nmap scan report for 10.6.6.100  
Host is up (0.0039s latency).  
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.79 seconds  
  
(kali㉿kali)-[~]  
$
```

7 host was found in the network.

Finding an Operating System

```
sudo nmap -O 10.6.6.23
```

```
(kali@kali)-[~]
$ sudo nmap -O 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 15:00 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00016s 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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds
```

Linux 4.15 -5.8 is running on this host

Aggressive Scanning

```
sudo -p21 -sV -A T4 10.6.6.23
# -p ---- port 21
# -sV ----- Version
# -A ----- Aggressive scan
# T4 ----- scanning Time
```

```

(kali㉿kali)-[~]
$ nmap -p21 -sV -A T4 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 15:12 UTC
Failed to resolve "T4".
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00054s 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 1
|     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 1.71 seconds

```

```

nmap -A -p139, 445 10.6.6.23
# -A ---- Aggressive
# -p ---- port 139 and 445 -

```

```

(kali㉿kali)-[~]
$ nmap -A -p139, 445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 15:30 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00025s latency).

PORT      STATE SERVICE  VERSION
139/tcp    open  netbios-0 Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
Service Info: Host: GRAVEMIND

Host script results:
| 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: 2025-12-12T15:30:25+00:00
| smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required
| smb2-time:
|   date: 2025-12-12T15:30:26
|_  start_date: N/A
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (1 host up) scanned in 48.82 seconds

```

SMB Enumeration Techniques

```
nmap --script smb-enum-shares.nse -p445 10.6.6.23
```

```

(kali㉿kali)-[~]
$ nmap --script smb-enum-shares.nse -p445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 15:53 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00034s 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 7.60 seconds

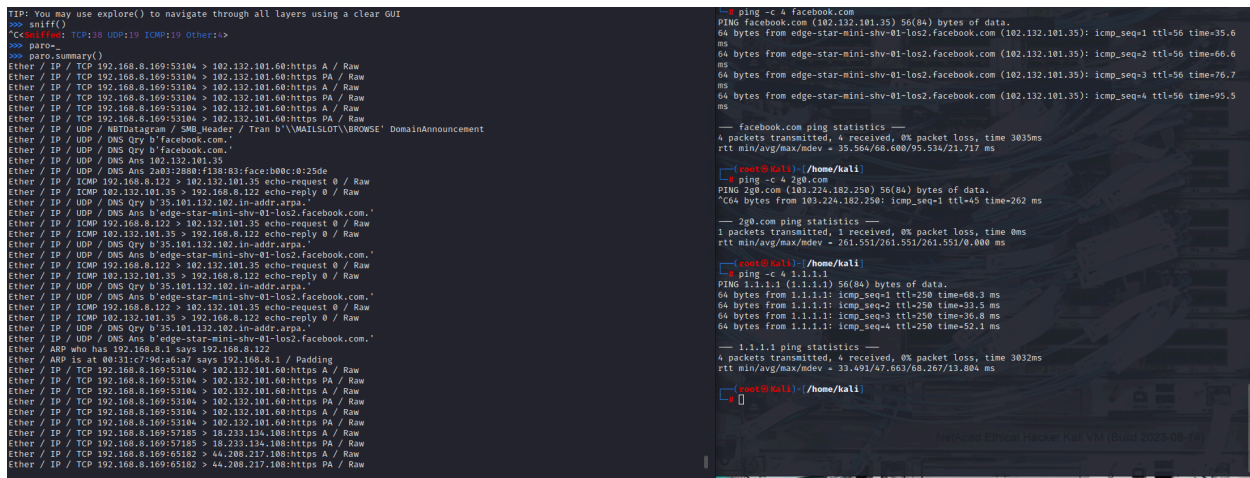
```

SCAPY

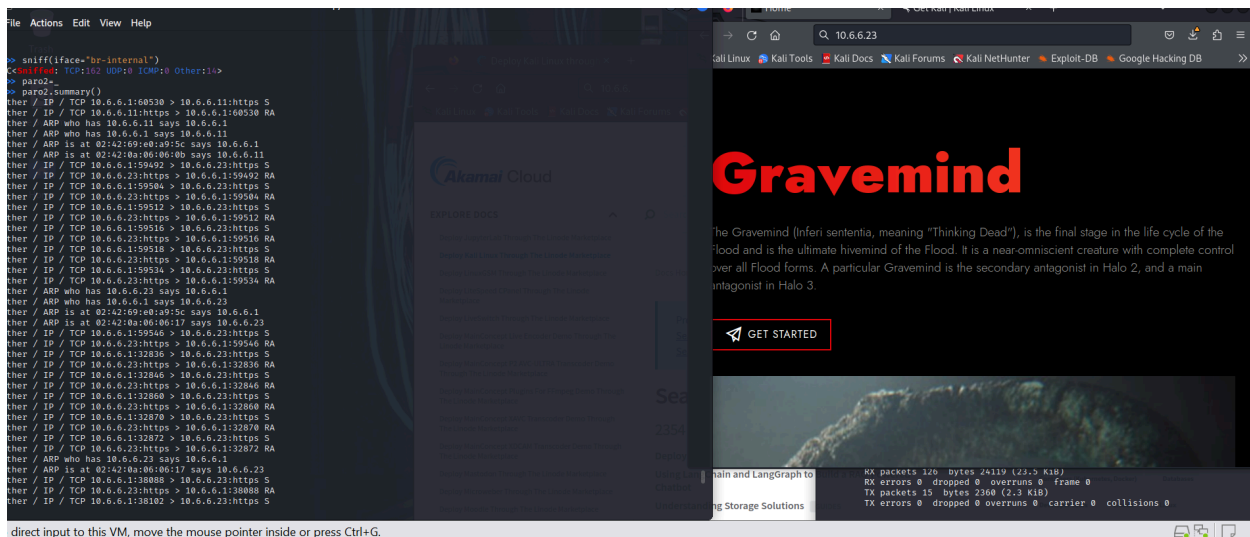
Packet Sniffng

Sniff ()

note:_ (underscore) is automatically used to store the last returned value from many functions — including the packets captured by sniff()).



sniff(iface="br-internal")
iface-----Interface to listen on



direct input to this VM, move the mouse pointer inside or press Ctrl+G.