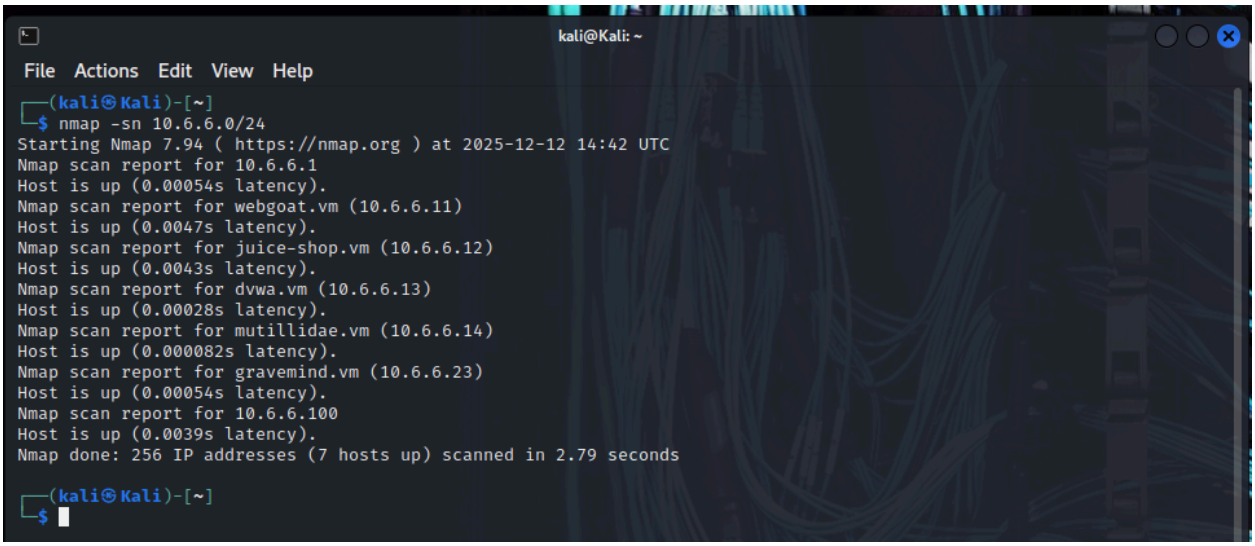
Network traffic analysis and manipulation techniques.

Odebode Seun

1. Identifying Network Hosts

```
nmap  -sn 10.6.6.6.0/24
```



7 host was found in the network.

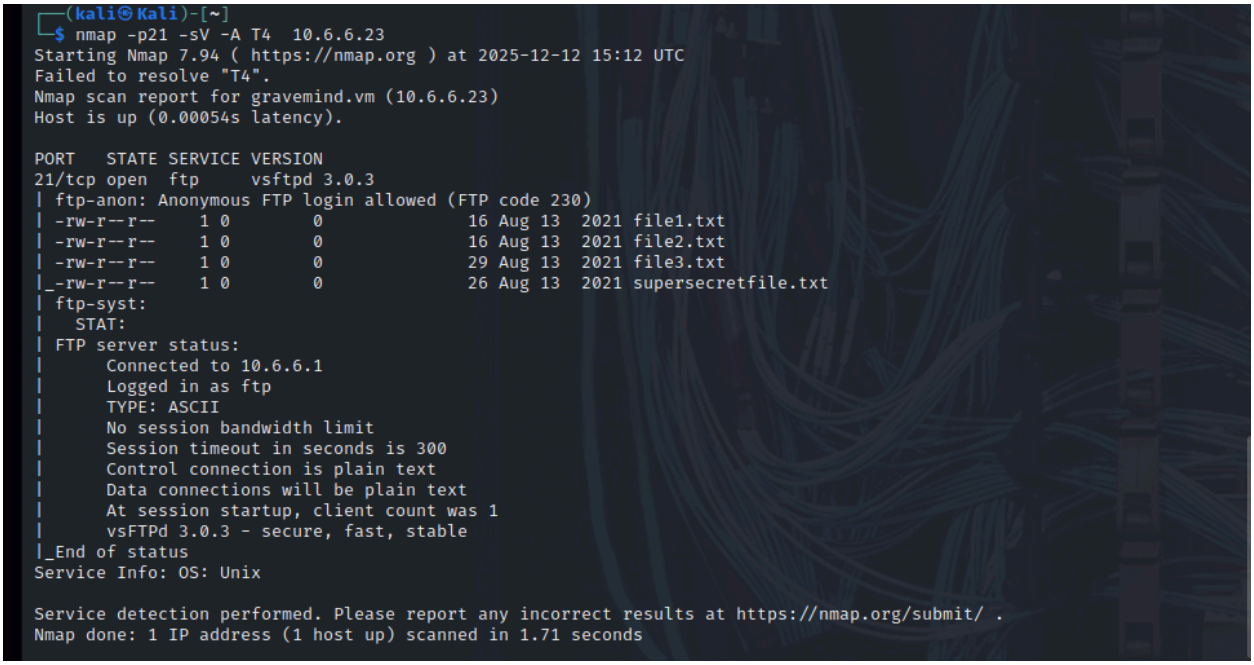
Finding an Operating System

```
sudo nmap -O 10.6.6.23
```

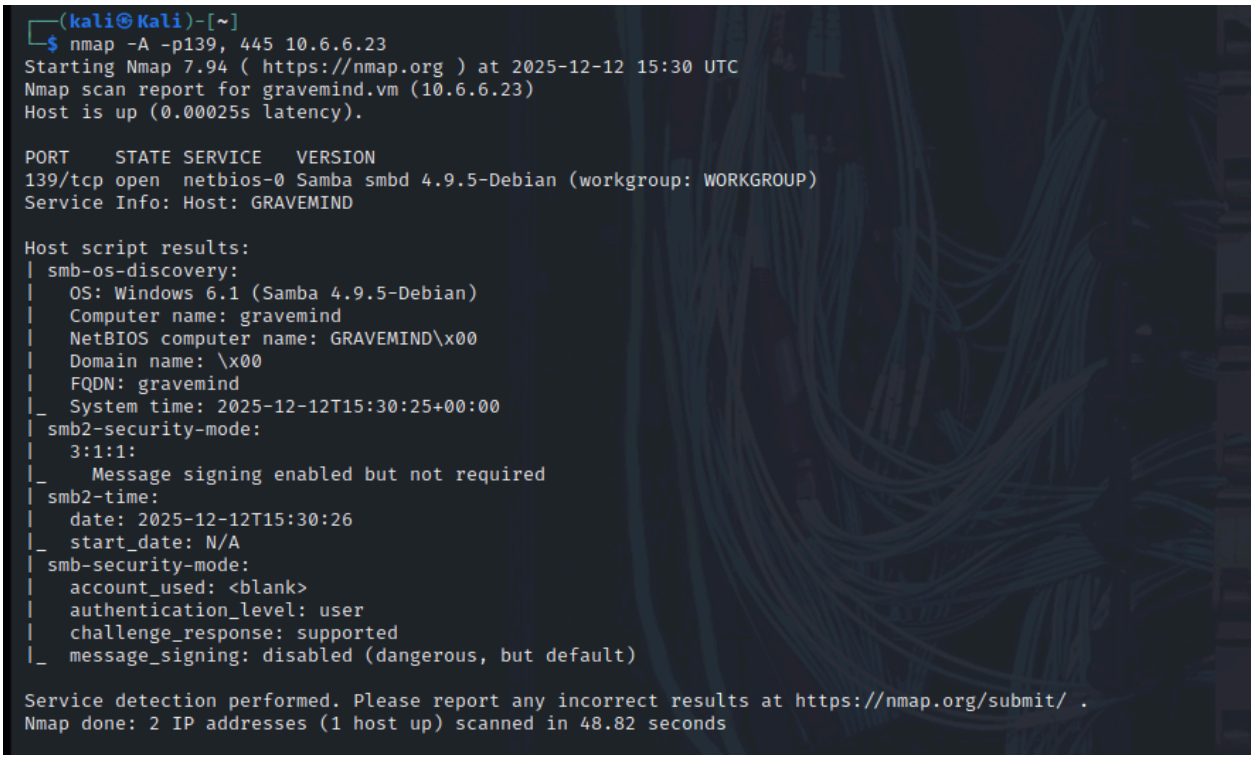
Linux 4.15 -5.8 is running on this host

Aggressive Scanning

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

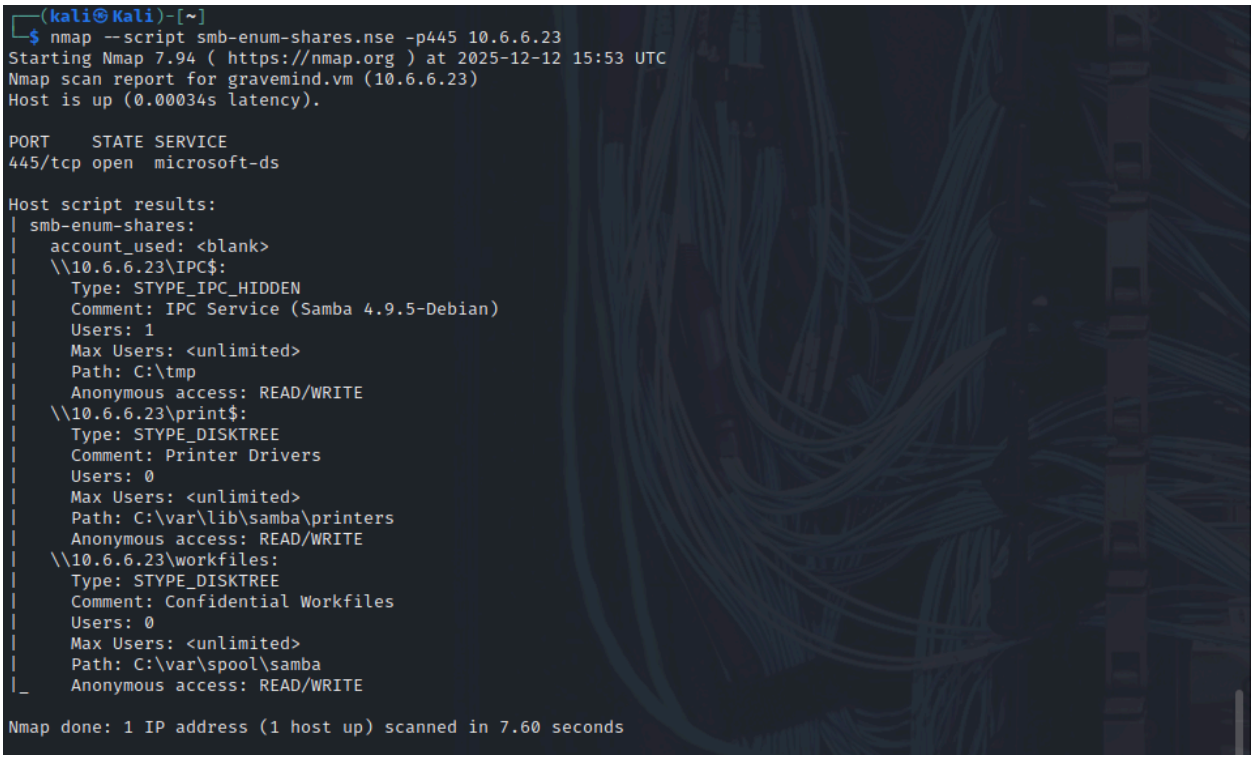


nmap -A -p139, 445 10.6.6.23
-A ---- Agressive
-p ---- port 139 and 445 -



SMB Enumeration Techniques

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

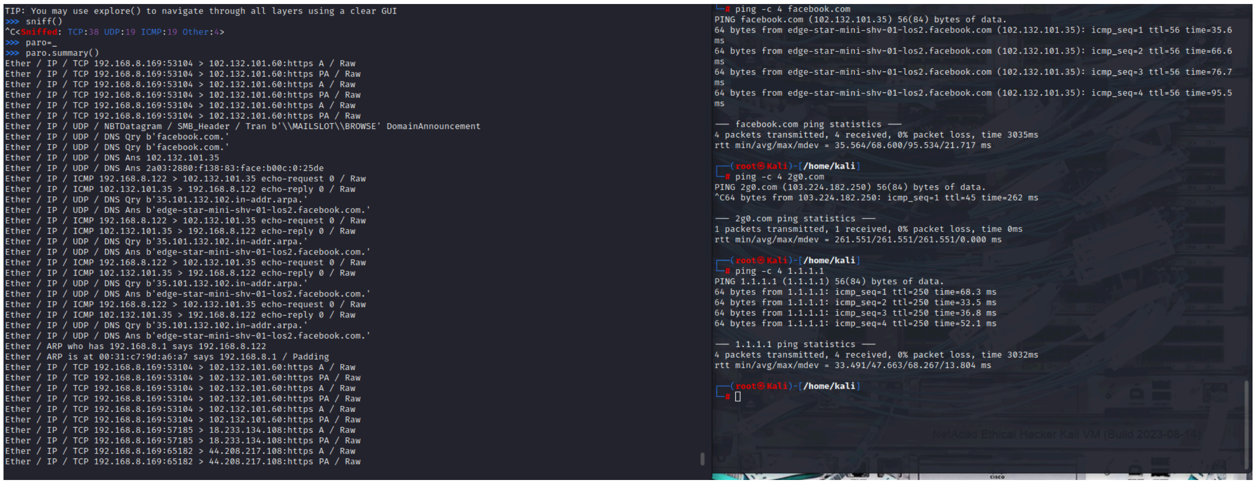


SCAPY

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
```