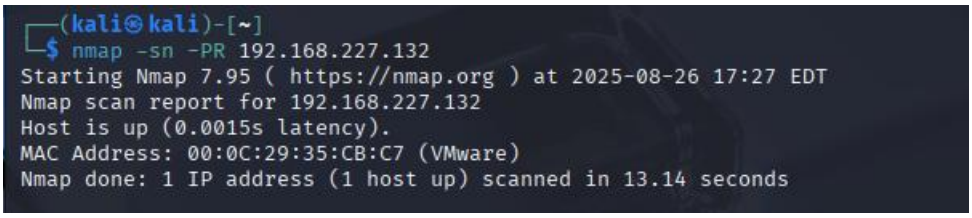
Module 3:

Lab 1:

Tool:nmap

-sn: to check host is alive

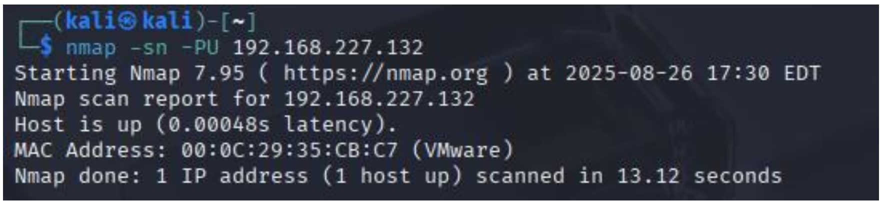
-PR: ARP ping scan



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PR 192.168.227.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 17:27 EDT
Nmap scan report for 192.168.227.132
Host is up (0.0015s latency).
MAC Address: 00:0C:29:35:CB:C7 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

Figure 1:ARP Scan

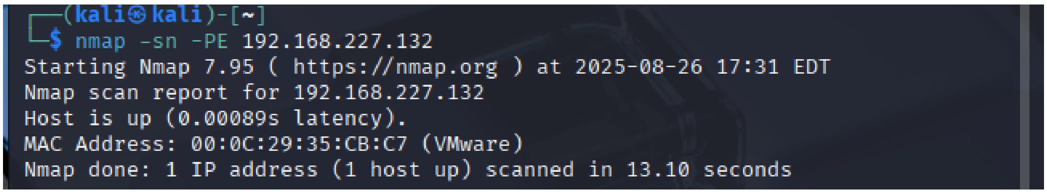
-PU:UDP ping scan



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PU 192.168.227.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 17:30 EDT
Nmap scan report for 192.168.227.132
Host is up (0.00048s latency).
MAC Address: 00:0C:29:35:CB:C7 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

Figure 2:UDP Scan

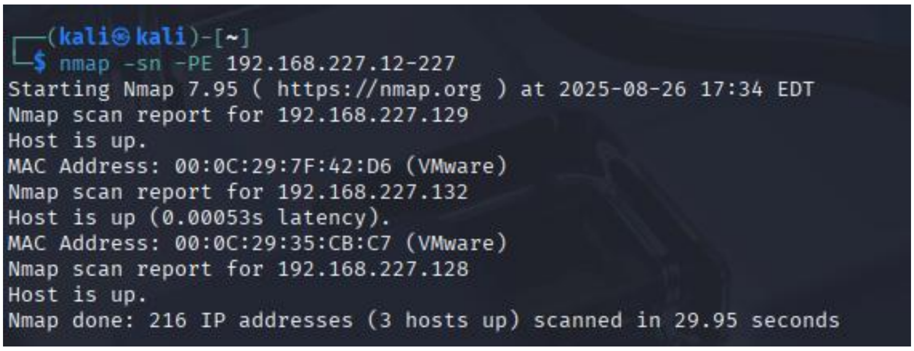
-PE:ICMP Echo ping scan



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.227.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 17:31 EDT
Nmap scan report for 192.168.227.132
Host is up (0.00089s latency).
MAC Address: 00:0C:29:35:CB:C7 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
```

Figure 3:ICMP Echo ping scan

Range of IP Scan



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.227.12-227
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 17:34 EDT
Nmap scan report for 192.168.227.129
Host is up.
MAC Address: 00:0C:29:7F:42:D6 (VMware)
Nmap scan report for 192.168.227.132
Host is up (0.00053s latency).
MAC Address: 00:0C:29:35:CB:C7 (VMware)
Nmap scan report for 192.168.227.128
Host is up.
Nmap done: 216 IP addresses (3 hosts up) scanned in 29.95 seconds
```

Figure 4:Range

-PM:Mask Ping scan

-PS: Syn ping scan

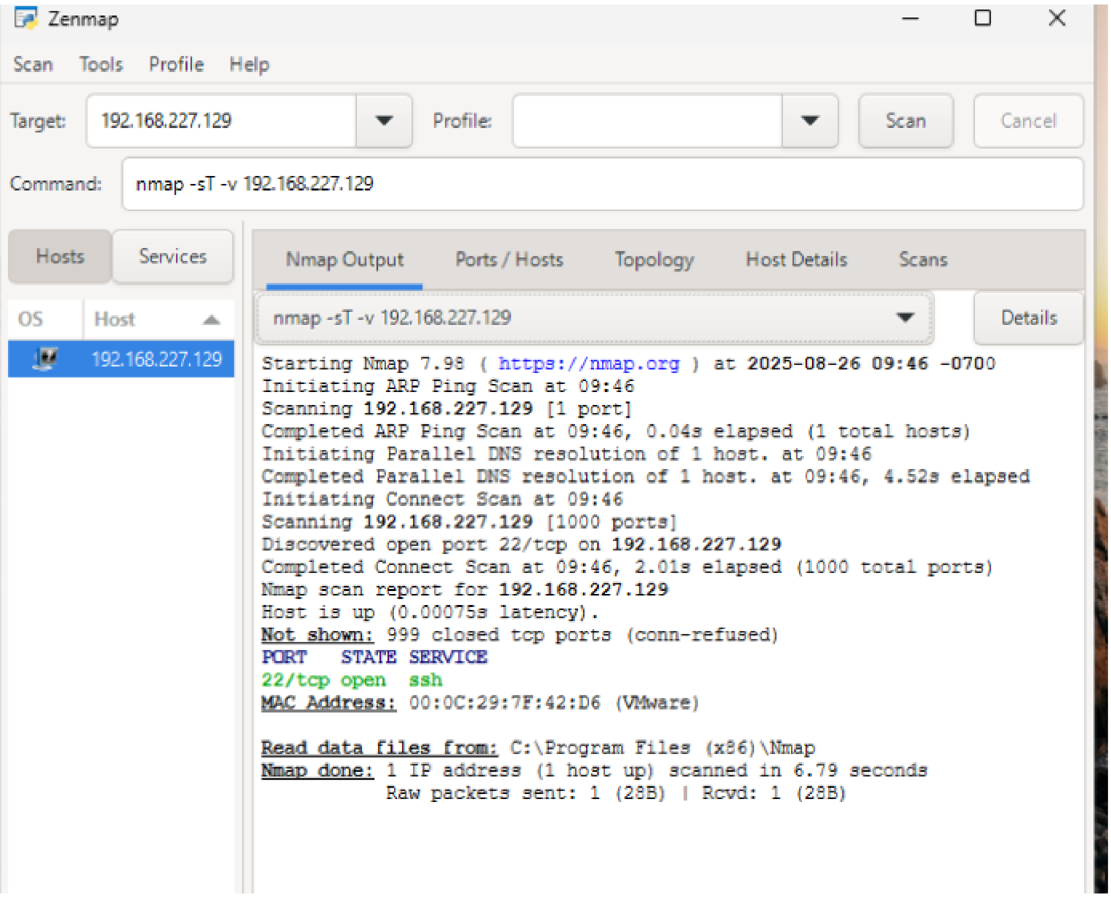
-PA:Ack Ping scan

-PO: Protocol Ping scan

Lab 2:

Tools: Zenmap

1)Full TCP scan: 3 way handshake



Target: 192.168.227.129

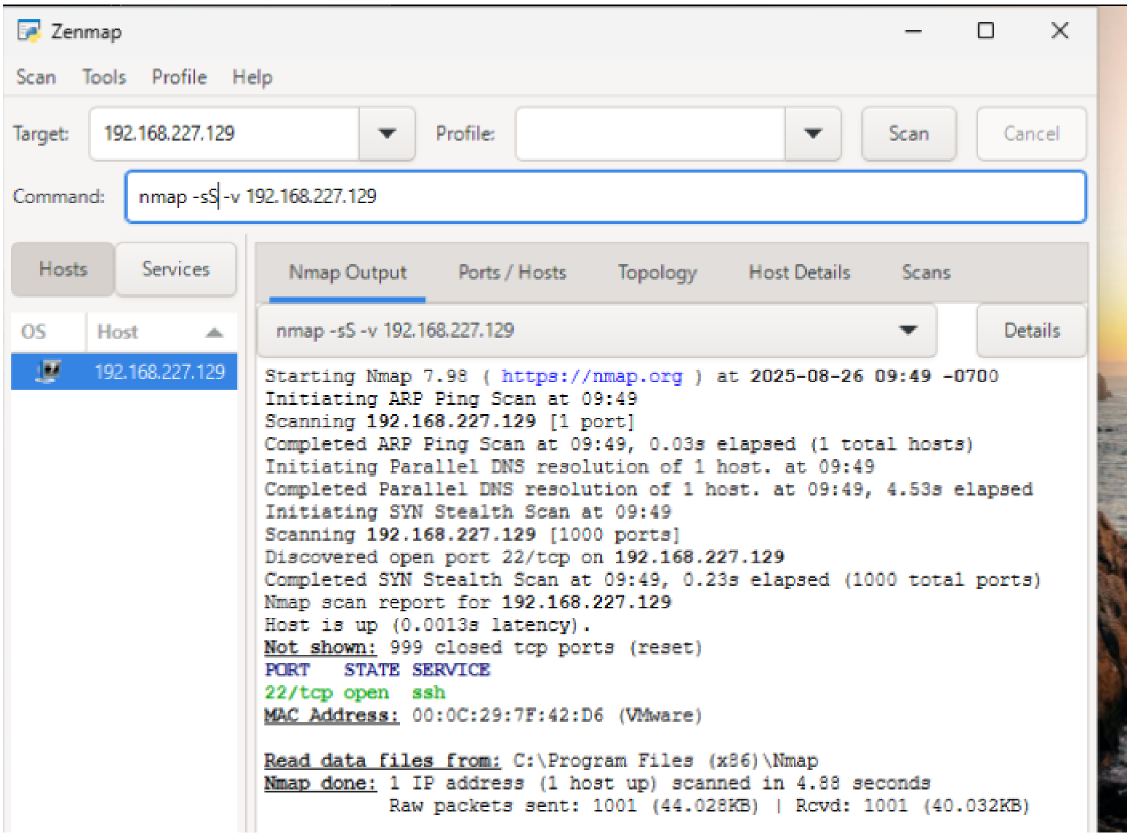
Command: nmap -sT -v 192.168.227.129

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-08-26 09:46 -0700
Initiating ARP Ping Scan at 09:46
Scanning 192.168.227.129 [1 port]
Completed ARP Ping Scan at 09:46, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:46
Completed Parallel DNS resolution of 1 host. at 09:46, 4.52s elapsed
Initiating Connect Scan at 09:46
Scanning 192.168.227.129 [1000 ports]
Discovered open port 22/tcp on 192.168.227.129
Completed Connect Scan at 09:46, 2.01s elapsed (1000 total ports)
Nmap scan report for 192.168.227.129
Host is up (0.00075s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:7F:42:D6 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

Figure 5: Full TCP Scan

2:TCP Stealth scan/Half open scan:

Connection between the client and the host resets before completing the 3 way hand shake so FW rules can be by passed



Target: 192.168.227.129

Profile:

Command: nmap -sS -v 192.168.227.129

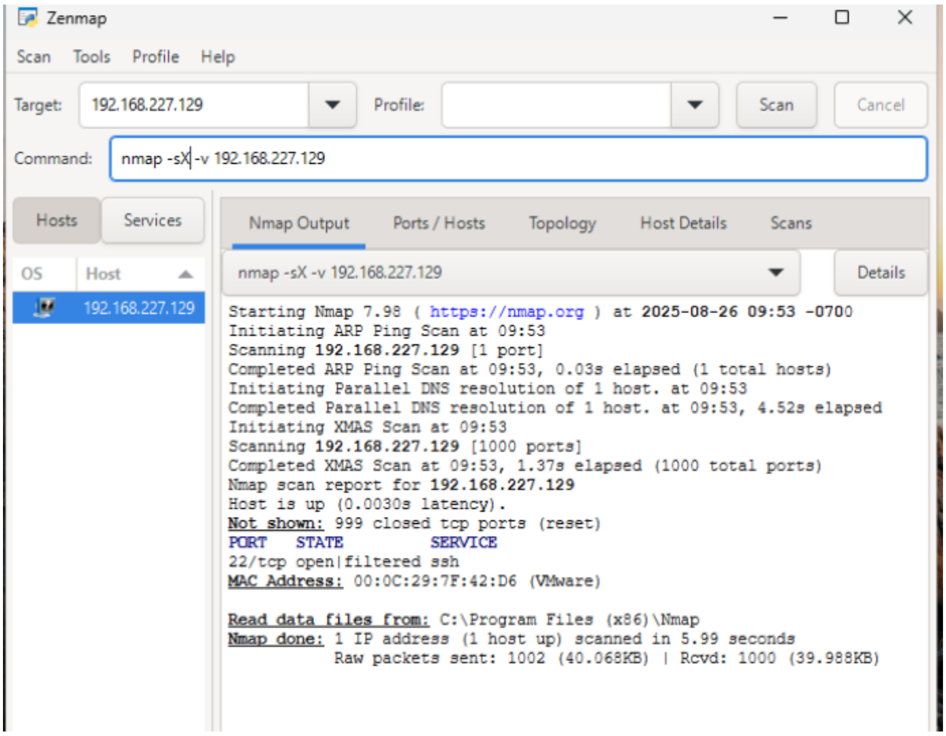
192.168.227.129

nmap -sS -v 192.168.227.129

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-08-26 09:49 -0700
Initiating ARP Ping Scan at 09:49
Scanning 192.168.227.129 [1 port]
Completed ARP Ping Scan at 09:49, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:49
Completed Parallel DNS resolution of 1 host. at 09:49, 4.53s elapsed
Initiating SYN Stealth Scan at 09:49
Scanning 192.168.227.129 [1000 ports]
Discovered open port 22/tcp on 192.168.227.129
Completed SYN Stealth Scan at 09:49, 0.23s elapsed (1000 total ports)
Nmap scan report for 192.168.227.129
Host is up (0.0013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:7F:42:D6 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 4.88 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.032KB)
```

Figure 6:Stealth Scan

Xmas scan: Sends TCP frames of FIN,URG and PUSH Flags. If target has opened the port you will receive no response while if ports are closed you will receive RST response



Target: 192.168.227.129

Profile:

Command: nmap -sX -v 192.168.227.129

192.168.227.129

nmap -sX -v 192.168.227.129

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-08-26 09:53 -0700
Initiating ARP Ping Scan at 09:53
Scanning 192.168.227.129 [1 port]
Completed ARP Ping Scan at 09:53, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:53
Completed Parallel DNS resolution of 1 host. at 09:53, 4.52s elapsed
Initiating XMAS Scan at 09:53
Scanning 192.168.227.129 [1000 ports]
Completed XMAS Scan at 09:53, 1.37s elapsed (1000 total ports)
Nmap scan report for 192.168.227.129
Host is up (0.0030s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 00:0C:29:7F:42:D6 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.99 seconds
           Raw packets sent: 1002 (40.068KB) | Rcvd: 1000 (39.988KB)
```

Figure 7:XMas Scan

Maimon Scan: -sM, FIN/ACK is sent to target. If no response mean port is open if RST response mean port is closed

SCTP Protocol: The Stream Control Transmission Protocol (SCTP) is a reliable, connection-oriented transport layer protocol for internet communication, designed by the IETF SIGTRAN group to carry telecommunication signaling over IP networks. It combines aspects of both TCP (reliability, connection-orientation) and UDP (message-orientation), offering features like ordered and unordered data delivery, multihoming for fault tolerance, and enhanced security.

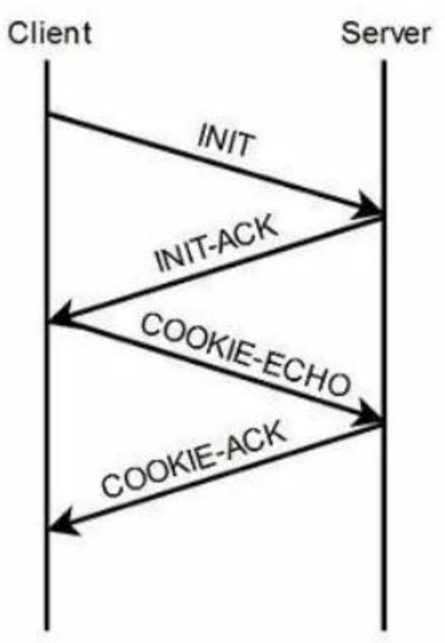


Figure 8:SCTP Protocol

SCTP Cookie ECHO scan: -sZ

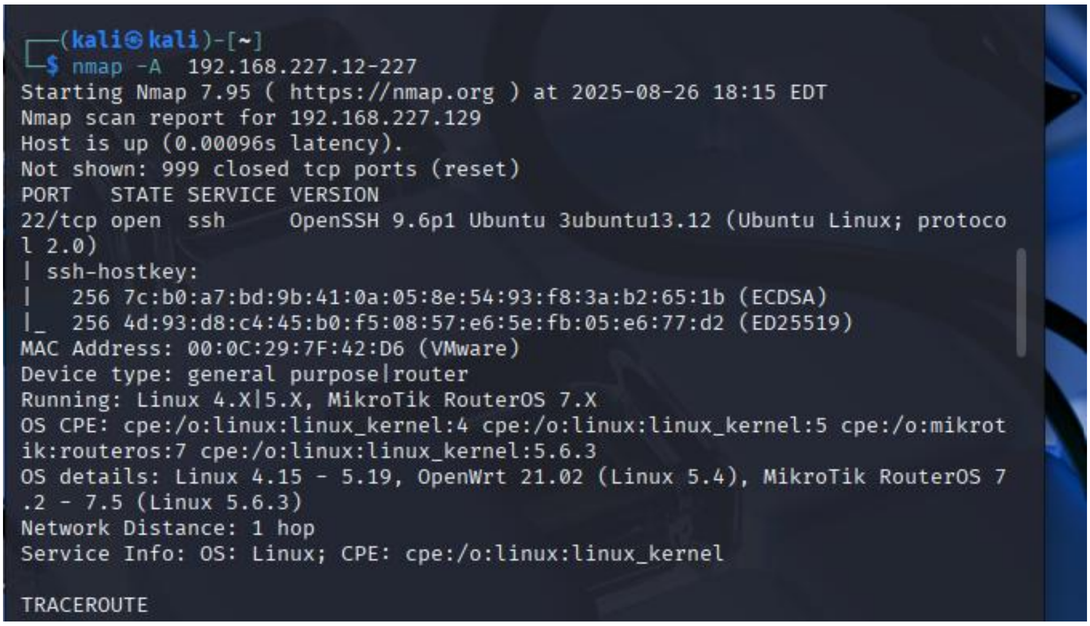
SCTP INIT Scan: -sY

Version Scan:-sV

Lab 3:

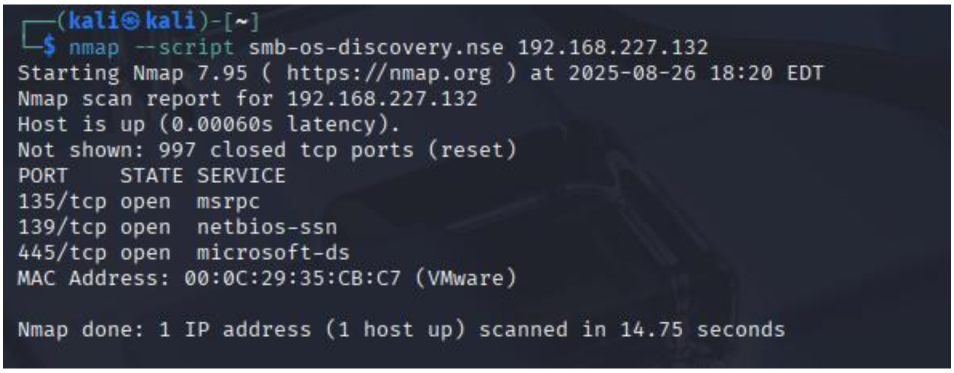
Tools:Nmap

Aggressive Scan: -A



```
┌──(kali㉿kali)-[~]
└─$ nmap -A  192.168.227.12-227
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 18:15 EDT
Nmap scan report for 192.168.227.129
Host is up (0.00096s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.12 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   256 7c:b0:a7:bd:9b:41:0a:05:8e:54:93:f8:3a:b2:65:1b (ECDSA)
|_  256 4d:93:d8:c4:45:b0:f5:08:57:e6:5e:fb:05:e6:77:d2 (ED25519)
MAC Address: 00:0C:29:7F:42:D6 (VMware)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrot
ik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7
.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
```

Figure 9:Aggressive Scan



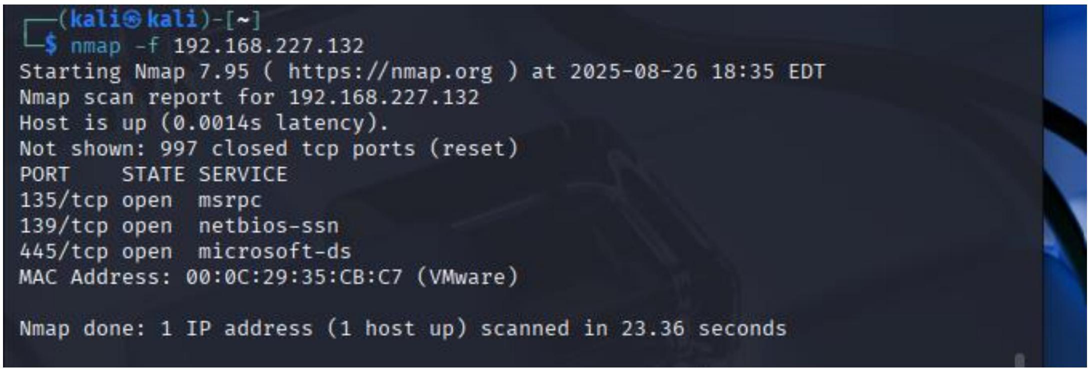
```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-os-discovery.nse 192.168.227.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 18:20 EDT
Nmap scan report for 192.168.227.132
Host is up (0.00060s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:35:CB:C7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.75 seconds
```

Figure 10:Script using nmap

Lab 4:

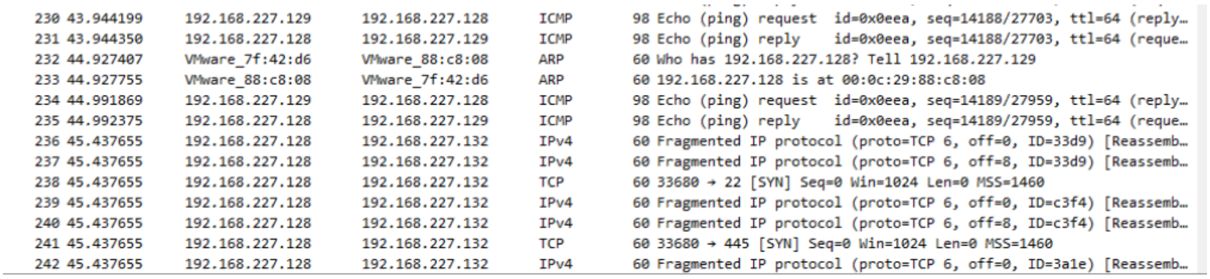
Tool: Nmap

Fragmentation attack: -f Packet



```
┌──(kali㉿kali)-[~]
└─$ nmap -f 192.168.227.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 18:35 EDT
Nmap scan report for 192.168.227.132
Host is up (0.0014s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:35:CB:C7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.36 seconds
```

Figure 11: Fragment Attack



```
230 43.944199   192.168.227.129   192.168.227.128   ICMP   98 Echo (ping) request  id=0x0eea, seq=14188/27703, ttl=64 (reply…
231 43.944350   192.168.227.128   192.168.227.129   ICMP   98 Echo (ping) reply    id=0x0eea, seq=14188/27703, ttl=64 (reque…
232 44.927407   VMware_7f:42:d6   VMware_88:c8:08   ARP    60 Who has 192.168.227.128? Tell 192.168.227.129
233 44.927755   VMware_88:c8:08   VMware_7f:42:d6   ARP    60 192.168.227.128 is at 00:0c:29:88:c8:08
234 44.991869   192.168.227.129   192.168.227.128   ICMP   98 Echo (ping) request  id=0x0eea, seq=14189/27959, ttl=64 (reply…
235 44.992375   192.168.227.128   192.168.227.129   ICMP   98 Echo (ping) reply    id=0x0eea, seq=14189/27959, ttl=64 (reque…
236 45.437655   192.168.227.128   192.168.227.132   IPv4   60 Fragmented IP protocol (proto=TCP 6, off=0, ID=33d9) [Reassemb…
237 45.437655   192.168.227.128   192.168.227.132   IPv4   60 Fragmented IP protocol (proto=TCP 6, off=8, ID=33d9) [Reassemb…
238 45.437655   192.168.227.128   192.168.227.132   TCP    60 33680 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
239 45.437655   192.168.227.128   192.168.227.132   IPv4   60 Fragmented IP protocol (proto=TCP 6, off=0, ID=c3f4) [Reassemb…
240 45.437655   192.168.227.128   192.168.227.132   IPv4   60 Fragmented IP protocol (proto=TCP 6, off=8, ID=c3f4) [Reassemb…
241 45.437655   192.168.227.128   192.168.227.132   TCP    60 33680 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
242 45.437655   192.168.227.128   192.168.227.132   IPv4   60 Fragmented IP protocol (proto=TCP 6, off=0, ID=3a1e) [Reassemb…
```

Figure 12: Wireshark output

Few Additional Commands:

Nmap -g 80 IP: Against a specific port

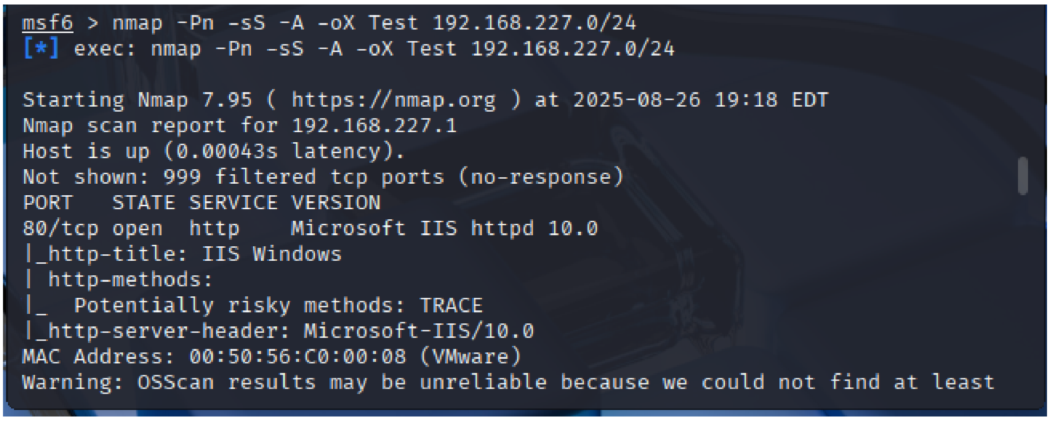
Nmap -mtu 8 IP: MTU is maximum transmission unit and size of packet is 8 Byte

Nmap -D RND:10 IP: Decoy scan against 10 non reserved IP

Nmap -St -Pn –spoof-mac 0 IP: Random MAC address , Full TCP Scan and skip host Discovery

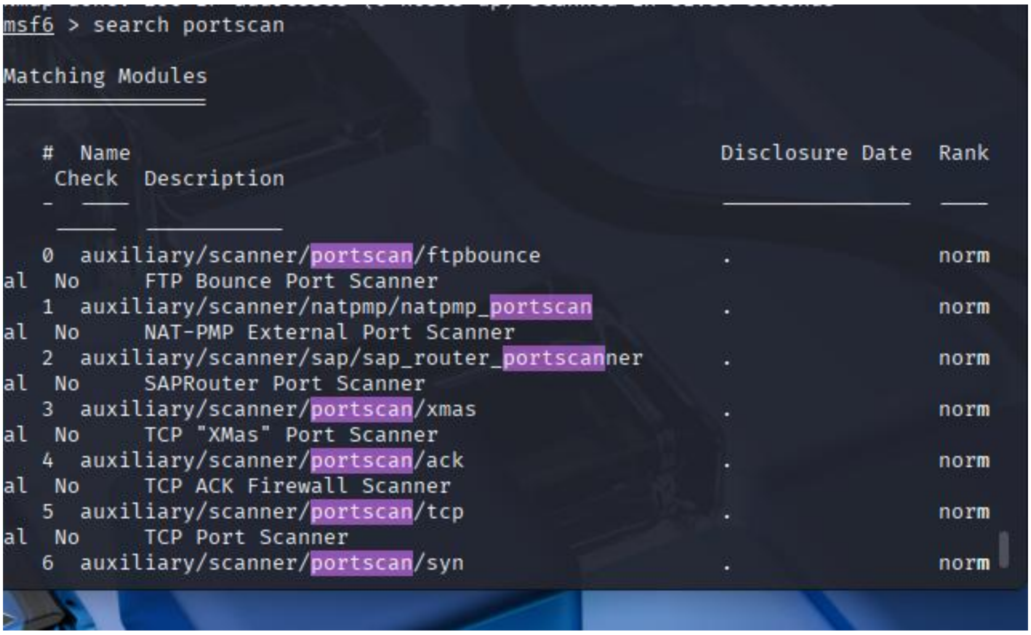
Lab 5:

Tool:Metasploite



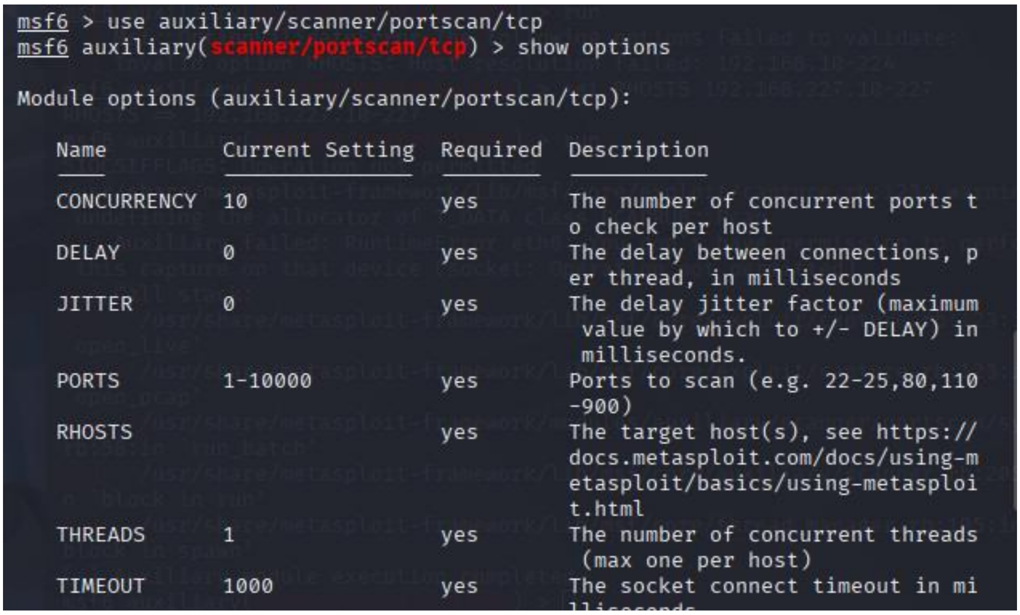
```
msf6 > nmap -Pn -sS -A -oX Test 192.168.227.0/24
[*] exec: nmap -Pn -sS -A -oX Test 192.168.227.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 19:18 EDT
Nmap scan report for 192.168.227.1
Host is up (0.00043s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
```

Figure 13: Using nmap via Metasploite



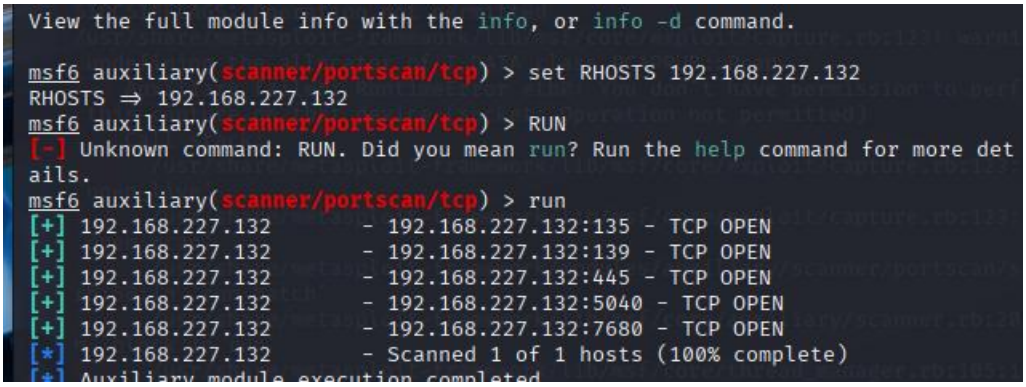
```
msf6 > search portscan

Matching Modules
================

   #  Name                                               Disclosure Date  Rank
    Check  Description
   -  ----                                               ---------------  ----
    -----  -----------
   0  auxiliary/scanner/portscan/ftpbounce                .                norm
al  No     FTP Bounce Port Scanner
   1  auxiliary/scanner/natpmp/natpmp_portscan            .                norm
al  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/sap/sap_router_portscanner        .                norm
al  No     SAPRouter Port Scanner
   3  auxiliary/scanner/portscan/xmas                     .                norm
al  No     TCP "XMas" Port Scanner
   4  auxiliary/scanner/portscan/ack                      .                norm
al  No     TCP ACK Firewall Scanner
   5  auxiliary/scanner/portscan/tcp                      .                norm
al  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/syn                      .                norm
```

Figure 14: Search Portscan



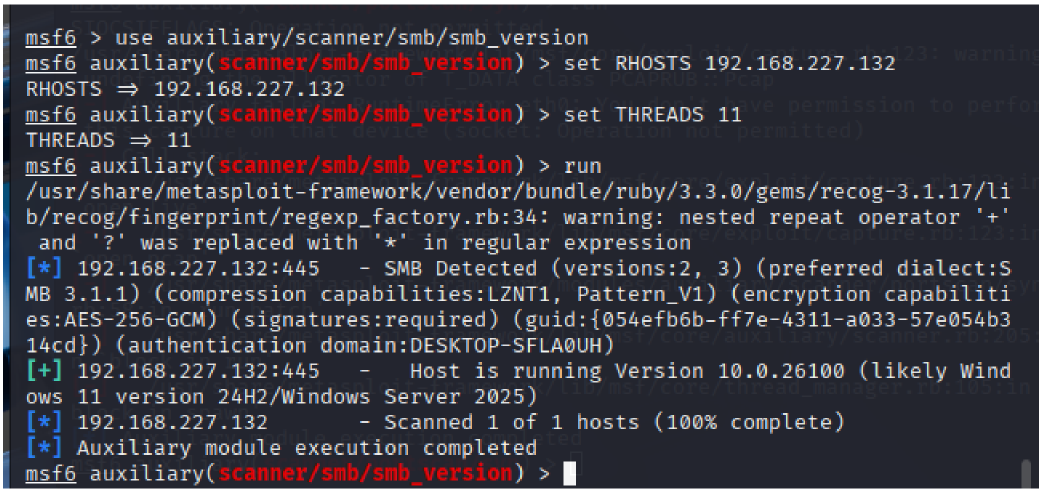
```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports t
                                           o check per host
   DELAY        0                yes       The delay between connections, p
                                           er thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum
                                            value by which to +/- DELAY) in
                                            milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110
                                           -900)
   RHOSTS                        yes       The target host(s), see https://
                                           docs.metasploit.com/docs/using-m
                                           etasploit/basics/using-metasploi
                                           t.html
   THREADS      1                yes       The number of concurrent threads
                                            (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in mi
                                           lliseconds
```

Figure 15:using TCP module



```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.227.132
RHOSTS ⇒ 192.168.227.132
msf6 auxiliary(scanner/portscan/tcp) > RUN
[-] Unknown command: RUN. Did you mean run? Run the help command for more det
ails.
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 192.168.227.132       - 192.168.227.132:135 - TCP OPEN
[+] 192.168.227.132       - 192.168.227.132:139 - TCP OPEN
[+] 192.168.227.132       - 192.168.227.132:445 - TCP OPEN
[+] 192.168.227.132       - 192.168.227.132:5040 - TCP OPEN
[+] 192.168.227.132       - 192.168.227.132:7680 - TCP OPEN
[*] 192.168.227.132       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 16:Set RHost



```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.227.132
RHOSTS ⇒ 192.168.227.132
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS ⇒ 11
msf6 auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/li
b/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'
 and '?' was replaced with '*' in regular expression
[*] 192.168.227.132:445   - SMB Detected (versions:2, 3) (preferred dialect:S
MB 3.1.1) (compression capabilities:LZNT1, Pattern_V1) (encryption capabiliti
es:AES-256-GCM) (signatures:required) (guid:{054efb6b-ff7e-4311-a033-57e054b3
14cd}) (authentication domain:DESKTOP-SFLA0UH)
[+] 192.168.227.132:445   -   Host is running Version 10.0.26100 (likely Wind
ows 11 version 24H2/Windows Server 2025)
[*] 192.168.227.132       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > 
```

Figure 17:Using SMB