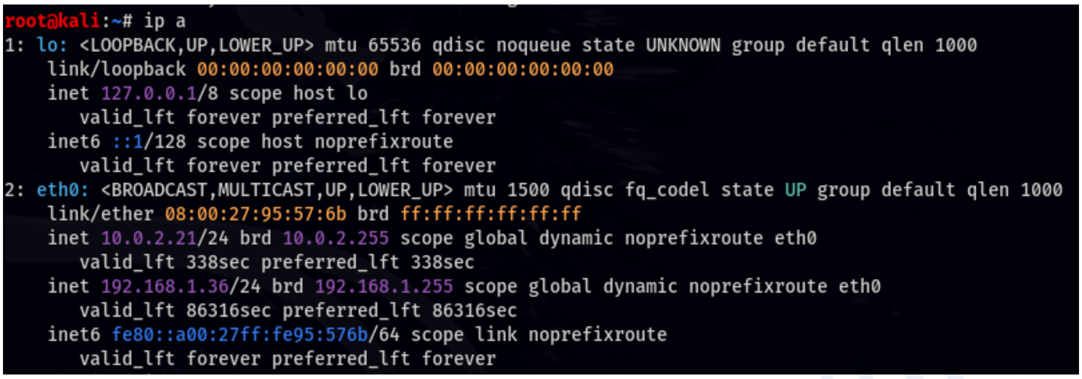
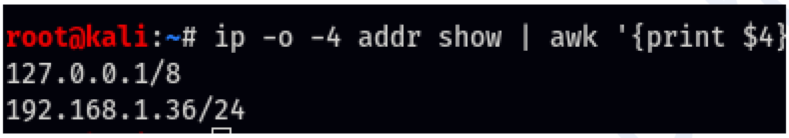
Task 1: Scan Your Local Network for Open Ports

1.Install Nmap from official website.



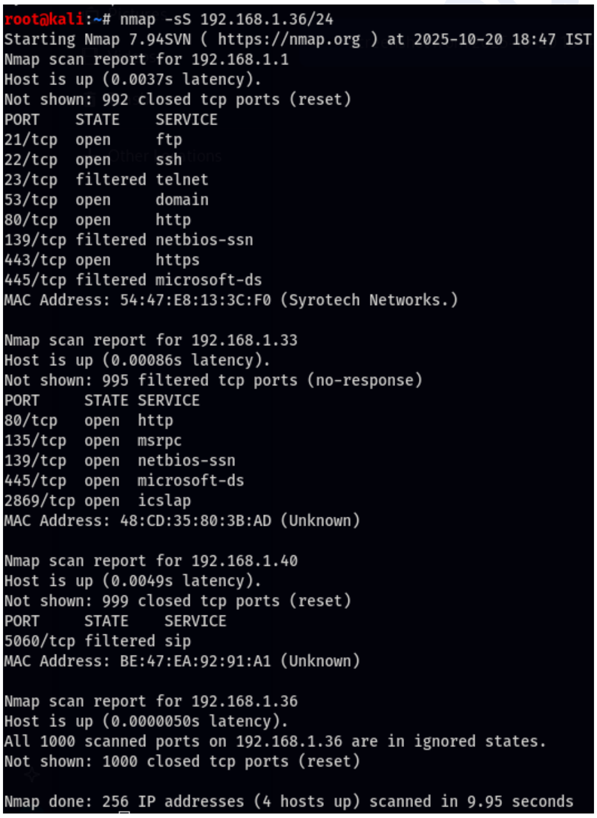
```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:95:57:6b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.21/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 338sec preferred_lft 338sec
    inet 192.168.1.36/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 86316sec preferred_lft 86316sec
    inet6 fe80::a00:27ff:fe95:576b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

2.Find your local IP range



```
root@kali:~# ip -o -4 addr show | awk '{print $4}
127.0.0.1/8
192.168.1.36/24
```

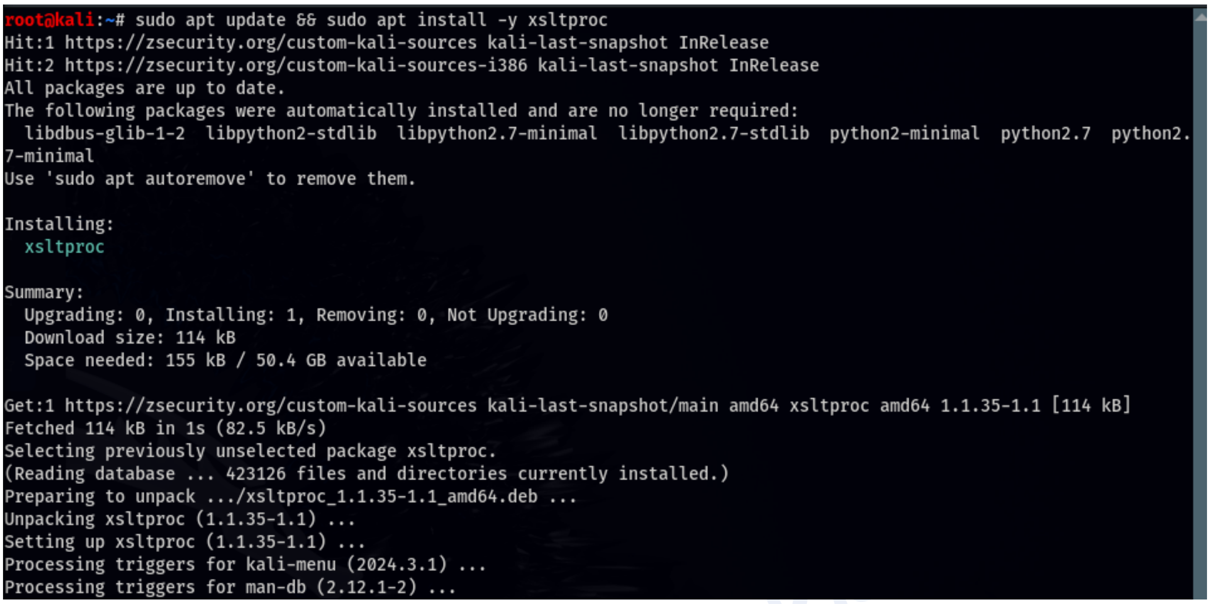
3.Perform TCP SYN scan



```
root@kali:~# nmap -sS 192.168.1.36/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-20 18:47 IST
Nmap scan report for 192.168.1.1
Host is up (0.0037s latency).
Not shown: 992 closed tcp ports (reset)
PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  open     ssh
23/tcp  filtered telnet
53/tcp  open     domain
80/tcp  open     http
139/tcp filtered netbios-ssn
443/tcp open     https
445/tcp filtered microsoft-ds
MAC Address: 54:47:E8:13:3C:F0 (Syrotech Networks.)

Nmap scan report for 192.168.1.33
Host is up (0.00086s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 48:CD:35:80:3B:AD (Unknown)

Nmap scan report for 192.168.1.40
Host is up (0.0049s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE    SERVICE
5060/tcp filtered sip
MAC Address: BE:47:EA:92:91:A1 (Unknown)

Nmap scan report for 192.168.1.36
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.1.36 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 9.95 seconds
```

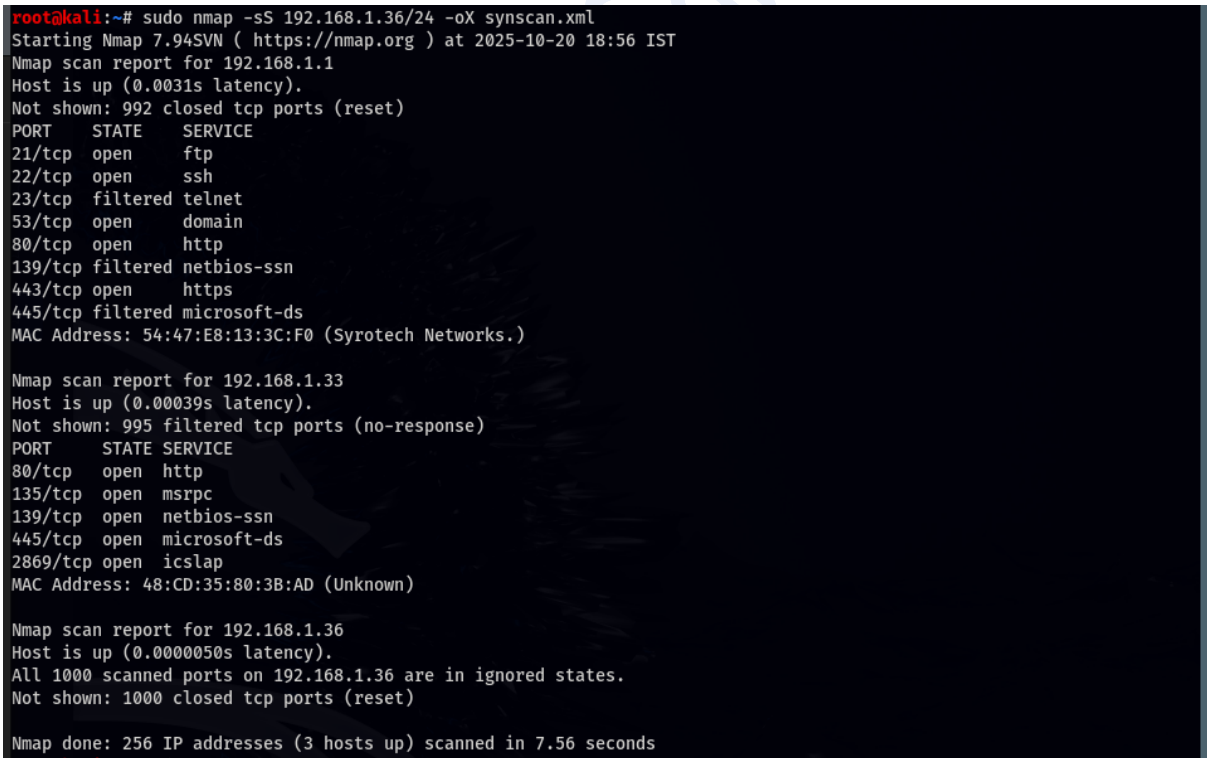
Capturing packets for wireshark:

Transform that XML to HTML with xsltproc using Nmap’s XSL stylesheet.



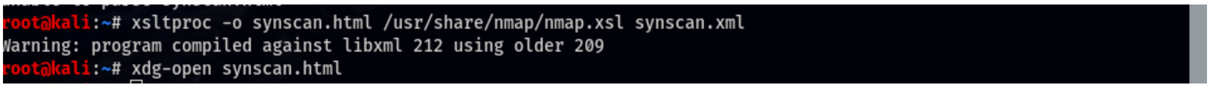
```
root@kali:~# sudo apt update && sudo apt install -y xsltproc
Hit:1 https://zsecurity.org/custom-kali-sources kali-last-snapshot InRelease
Hit:2 https://zsecurity.org/custom-kali-sources-i386 kali-last-snapshot InRelease
All packages are up to date.
The following packages were automatically installed and are no longer required:
  libdbus-glib-1-2  libpython2-stdlib  libpython2.7-minimal  libpython2.7-stdlib  python2-minimal  python2.7  python2.
7-minimal
Use 'sudo apt autoremove' to remove them.

Installing:
  xsltproc

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 114 kB
  Space needed: 155 kB / 50.4 GB available

Get:1 https://zsecurity.org/custom-kali-sources kali-last-snapshot/main amd64 xsltproc amd64 1.1.35-1.1 [114 kB]
Fetched 114 kB in 1s (82.5 kB/s)
Selecting previously unselected package xsltproc.
(Reading database ... 423126 files and directories currently installed.)
Preparing to unpack .../xsltproc_1.1.35-1.1_amd64.deb ...
Unpacking xsltproc (1.1.35-1.1) ...
Setting up xsltproc (1.1.35-1.1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for man-db (2.12.1-2) ...
```

Save the syn scan as xml file



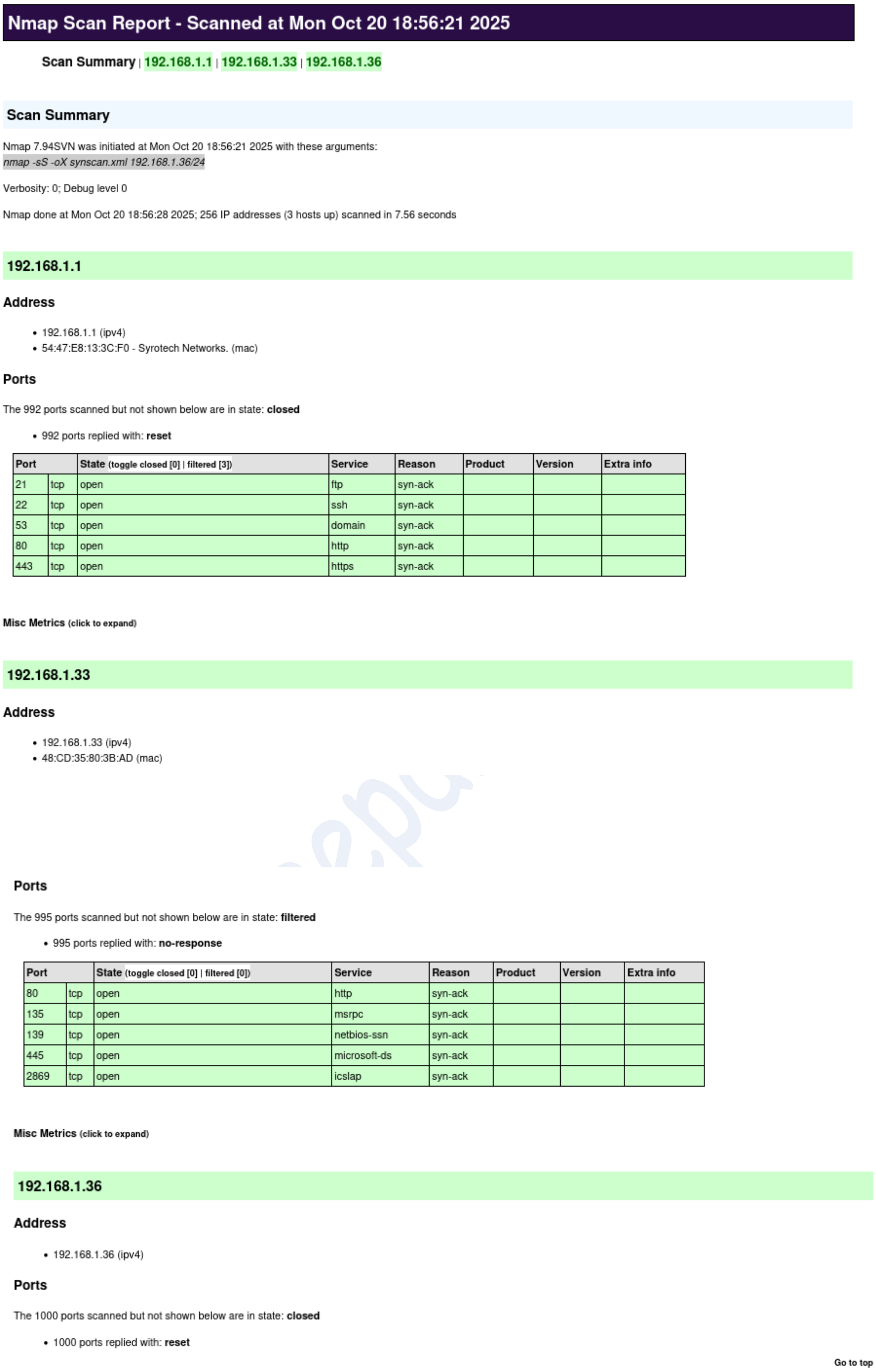
```
root@kali:~# sudo nmap -sS 192.168.1.36/24 -oX synscan.xml
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-20 18:56 IST
Nmap scan report for 192.168.1.1
Host is up (0.0031s latency).
Not shown: 992 closed tcp ports (reset)
PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  open     ssh
23/tcp  filtered telnet
53/tcp  open     domain
80/tcp  open     http
139/tcp filtered netbios-ssn
443/tcp open     https
445/tcp filtered microsoft-ds
MAC Address: 54:47:E8:13:3C:F0 (Syrotech Networks.)

Nmap scan report for 192.168.1.33
Host is up (0.00039s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 48:CD:35:80:3B:AD (Unknown)

Nmap scan report for 192.168.1.36
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.1.36 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 7.56 seconds
```

Converting xml to html



```
root@kali:~# xsltproc -o synscan.html /usr/share/nmap/nmap.xsl synscan.xml
Warning: program compiled against libxml 212 using older 209
root@kali:~# xdg-open synscan.html
```

TCP Syn scan report as html:



Nmap Scan Report - Scanned at Mon Oct 20 18:56:21 2025

Scan Summary | 192.168.1.1 | 192.168.1.33 | 192.168.1.36

Scan Summary

Nmap 7.94SVN was initiated at Mon Oct 20 18:56:21 2025 with these arguments:
nmap -sS -oX synscan.xml 192.168.1.36/24

Verbosity: 0; Debug level 0

Nmap done at Mon Oct 20 18:56:28 2025; 256 IP addresses (3 hosts up) scanned in 7.56 seconds

192.168.1.1

Address

- 192.168.1.1 (ipv4)
- 54:47:E8:13:3C:F0 - Syrotech Networks. (mac)

Ports

The 992 ports scanned but not shown below are in state: **closed**

- 992 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [3])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack			
22	tcp	open	ssh	syn-ack			
53	tcp	open	domain	syn-ack			
80	tcp	open	http	syn-ack			
443	tcp	open	https	syn-ack			

Misc Metrics (click to expand)

192.168.1.33

Address

- 192.168.1.33 (ipv4)
- 48:CD:35:80:3B:AD (mac)

Ports

The 995 ports scanned but not shown below are in state: **filtered**

- 995 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack			
135	tcp	open	msrpc	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
2869	tcp	open	icslap	syn-ack			

Misc Metrics (click to expand)

192.168.1.36

Address

- 192.168.1.36 (ipv4)

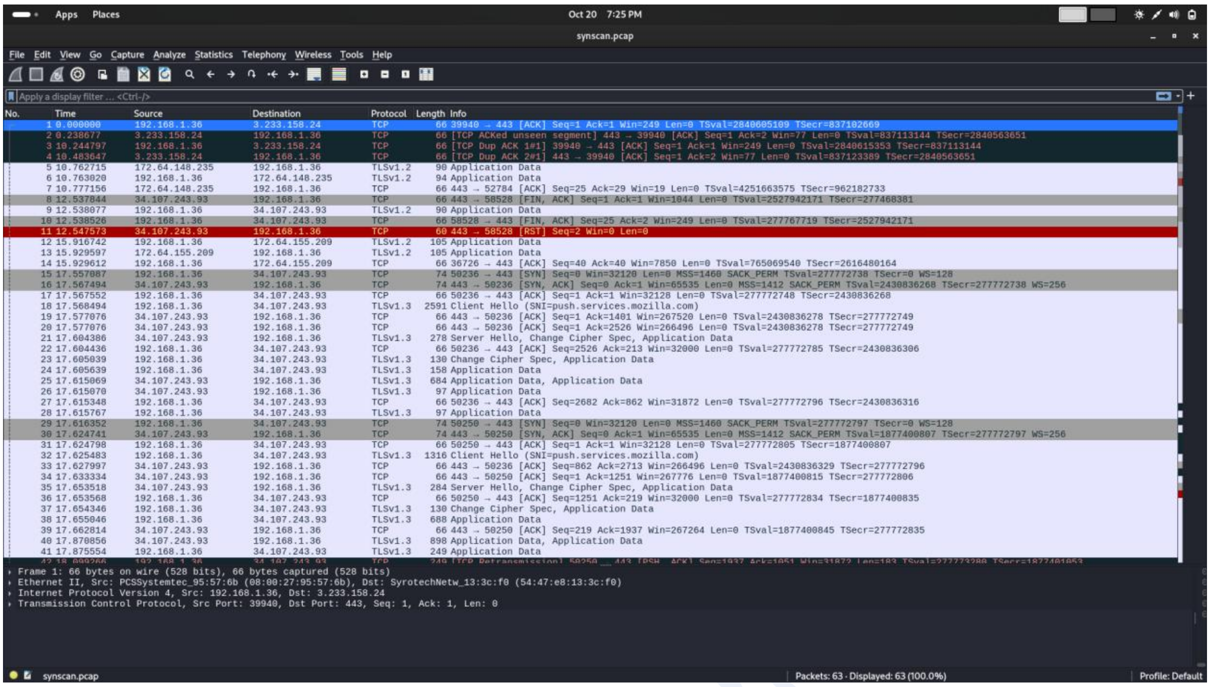
Ports

The 1000 ports scanned but not shown below are in state: **closed**

- 1000 ports replied with: **reset**

Go to top

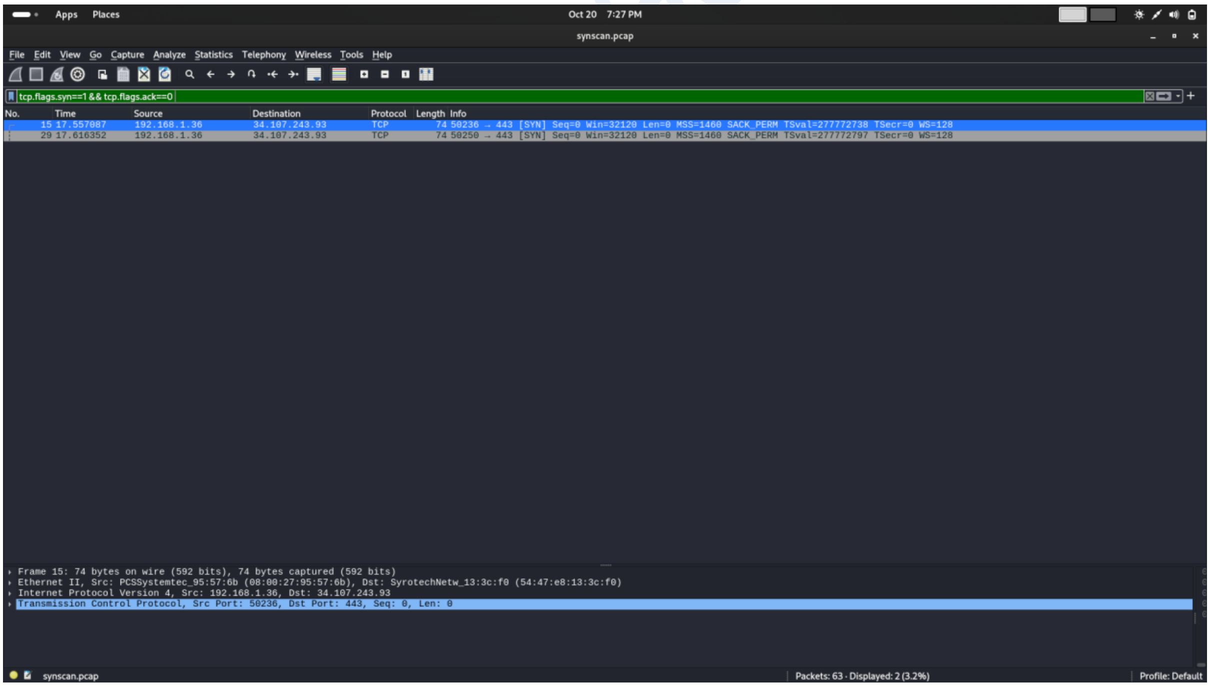
Wireshark scan:


Apps
Places
Oct 20 7:25 PM
synscan.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
synscan.pcap
Packets: 63 · Displayed: 63 (100.0%)
Profile: Default

```
No.  Time       Source          Destination     Protocol Length Info
  1 0.000000    192.168.1.36    3.233.158.24    TCP        66 39940 → 443 [ACK] Seq=1 Ack=1 Win=249 Len=0 TSval=2840605109 TSecr=837102669
  2 0.238677    3.233.158.24    192.168.1.36    TCP        66 [TCP ACKed unseen segment] 443 → 39940 [ACK] Seq=1 Ack=2 Win=77 Len=0 TSval=837113144 TSecr=2840563651
  3 10.244797   192.168.1.36    3.233.158.24    TCP        66 [TCP Dup ACK 1#1] 39940 → 443 [ACK] Seq=1 Ack=1 Win=249 Len=0 TSval=2840615353 TSecr=837113144
  4 10.483647   3.233.158.24    192.168.1.36    TCP        66 [TCP Dup ACK 2#1] 443 → 39940 [ACK] Seq=1 Ack=2 Win=77 Len=0 TSval=837123389 TSecr=2840563651
  5 10.762715   172.64.148.235  192.168.1.36    TLSv1.2    90 Application Data
  6 10.763020   192.168.1.36    172.64.148.235  TLSv1.2    94 Application Data
  7 10.777156   172.64.148.235  192.168.1.36    TCP        66 443 → 52784 [ACK] Seq=25 Ack=29 Win=19 Len=0 TSval=4251663575 TSecr=962182733
  8 12.537844   34.107.243.93   192.168.1.36    TCP        66 443 → 58528 [FIN, ACK] Seq=1 Ack=1 Win=1044 Len=0 TSval=2527942171 TSecr=277468381
  9 12.538077   192.168.1.36    34.107.243.93   TLSv1.2    90 Application Data
 10 12.538526   192.168.1.36    34.107.243.93   TCP        66 58528 → 443 [FIN, ACK] Seq=25 Ack=2 Win=249 Len=0 TSval=277767719 TSecr=2527942171
 11 12.547573   34.107.243.93   192.168.1.36    TCP        60 443 → 58528 [RST] Seq=2 Win=0 Len=0
 12 15.916742   192.168.1.36    172.64.155.209  TLSv1.2   105 Application Data
 13 15.929597   172.64.155.209  192.168.1.36    TLSv1.2   105 Application Data
 14 15.929612   192.168.1.36    172.64.155.209  TCP        66 36726 → 443 [ACK] Seq=40 Ack=40 Win=7850 Len=0 TSval=765069540 TSecr=2616480164
 15 17.557087   192.168.1.36    34.107.243.93   TCP        74 50236 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=277772738 TSecr=0 WS=128
 16 17.567494   34.107.243.93   192.168.1.36    TCP        74 443 → 50236 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=2430836268 TSecr=277772738 WS=256
 17 17.567552   192.168.1.36    34.107.243.93   TCP        66 50236 → 443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=277772748 TSecr=2430836268
 18 17.568494   192.168.1.36    34.107.243.93   TLSv1.3  2591 Client Hello (SNI=push.services.mozilla.com)
 19 17.577076   34.107.243.93   192.168.1.36    TCP        66 443 → 50236 [ACK] Seq=1 Ack=1401 Win=267520 Len=0 TSval=2430836278 TSecr=277772749
 20 17.577076   34.107.243.93   192.168.1.36    TCP        66 443 → 50236 [ACK] Seq=1 Ack=2526 Win=266496 Len=0 TSval=2430836278 TSecr=277772749
 21 17.604386   34.107.243.93   192.168.1.36    TLSv1.3   278 Server Hello, Change Cipher Spec, Application Data
 22 17.604436   192.168.1.36    34.107.243.93   TCP        66 50236 → 443 [ACK] Seq=2526 Ack=213 Win=32000 Len=0 TSval=277772785 TSecr=2430836306
 23 17.605039   192.168.1.36    34.107.243.93   TLSv1.3   130 Change Cipher Spec, Application Data
 24 17.605639   192.168.1.36    34.107.243.93   TLSv1.3   158 Application Data
 25 17.615069   34.107.243.93   192.168.1.36    TLSv1.3   684 Application Data, Application Data
 26 17.615070   34.107.243.93   192.168.1.36    TLSv1.3    97 Application Data
 27 17.615348   192.168.1.36    34.107.243.93   TCP        66 50236 → 443 [ACK] Seq=2682 Ack=862 Win=31872 Len=0 TSval=277772796 TSecr=2430836316
 28 17.615767   192.168.1.36    34.107.243.93   TLSv1.3    97 Application Data
 29 17.616352   192.168.1.36    34.107.243.93   TCP        74 50250 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=277772797 TSecr=0 WS=128
 30 17.624741   34.107.243.93   192.168.1.36    TCP        74 443 → 50250 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=1877400807 TSecr=277772797 WS=256
 31 17.624798   192.168.1.36    34.107.243.93   TCP        66 50250 → 443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=277772805 TSecr=1877400807
 32 17.625483   192.168.1.36    34.107.243.93   TLSv1.3  1316 Client Hello (SNI=push.services.mozilla.com)
 33 17.627997   34.107.243.93   192.168.1.36    TCP        66 443 → 50236 [ACK] Seq=862 Ack=2713 Win=266496 Len=0 TSval=2430836329 TSecr=277772796
 34 17.633334   34.107.243.93   192.168.1.36    TCP        66 443 → 50250 [ACK] Seq=1 Ack=1251 Win=267776 Len=0 TSval=1877400815 TSecr=277772806
 35 17.653518   34.107.243.93   192.168.1.36    TLSv1.3   284 Server Hello, Change Cipher Spec, Application Data
 36 17.653568   192.168.1.36    34.107.243.93   TCP        66 50250 → 443 [ACK] Seq=1251 Ack=219 Win=32000 Len=0 TSval=277772834 TSecr=1877400835
 37 17.654346   192.168.1.36    34.107.243.93   TLSv1.3   130 Change Cipher Spec, Application Data
 38 17.655046   192.168.1.36    34.107.243.93   TLSv1.3   688 Application Data
 39 17.662814   34.107.243.93   192.168.1.36    TCP        66 443 → 50250 [ACK] Seq=219 Ack=1937 Win=267264 Len=0 TSval=1877400845 TSecr=277772835
 40 17.870856   34.107.243.93   192.168.1.36    TLSv1.3   898 Application Data, Application Data
 41 17.875554   192.168.1.36    34.107.243.93   TLSv1.3   249 Application Data
 42 18.099266   192.168.1.36    34.107.243.93   TCP       249 [TCP Retransmission] 50250 → 443 [PSH, ACK] Seq=1937 Ack=1051 Win=31872 Len=183 TSval=277773280 TSecr=1877401053
```

```
› Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
› Ethernet II, Src: PCSSystemtec_95:57:6b (08:00:27:95:57:6b), Dst: SyrotechNetw_13:3c:f0 (54:47:e8:13:3c:f0)
› Internet Protocol Version 4, Src: 192.168.1.36, Dst: 3.233.158.24
› Transmission Control Protocol, Src Port: 39940, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

TCP Syn scan:

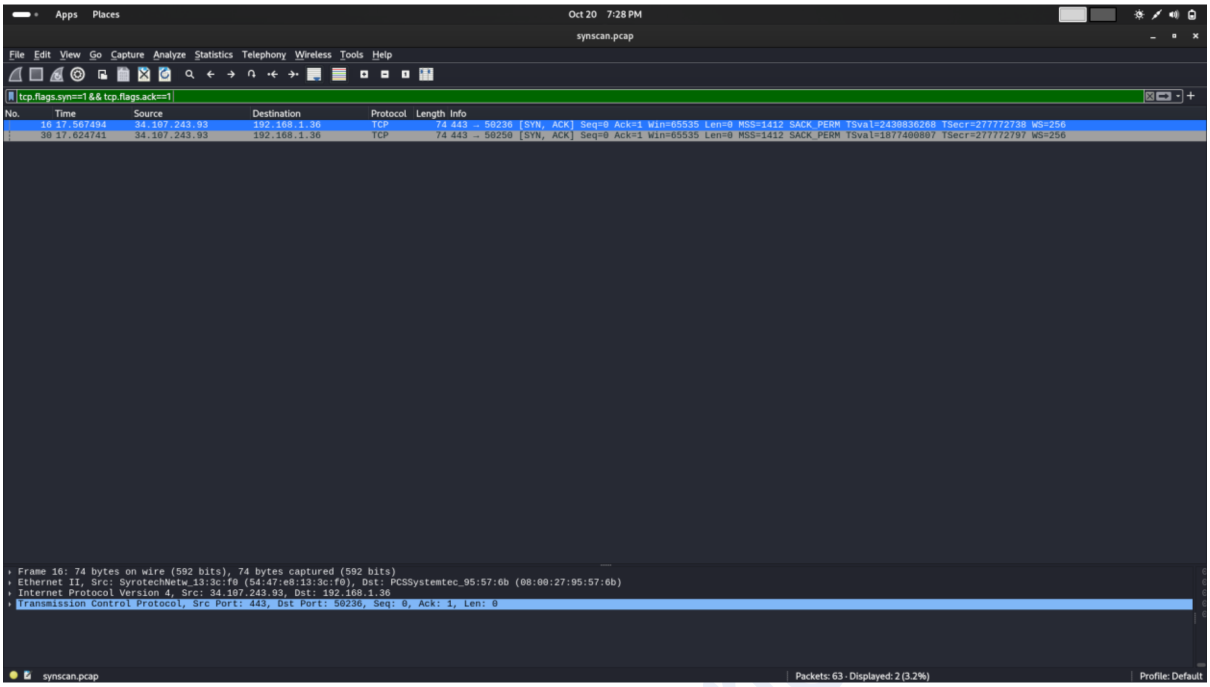

Apps
Places
Oct 20 7:27 PM
synscan.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
synscan.pcap
Packets: 63 · Displayed: 2 (3.2%)
Profile: Default

```
tcp.flags.syn==1 && tcp.flags.ack==0
```

```
No.  Time       Source          Destination     Protocol Length Info
 15 17.557087   192.168.1.36    34.107.243.93   TCP        74 50236 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=277772738 TSecr=0 WS=128
 29 17.616352   192.168.1.36    34.107.243.93   TCP        74 50250 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=277772797 TSecr=0 WS=128
```

```
› Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
› Ethernet II, Src: PCSSystemtec_95:57:6b (08:00:27:95:57:6b), Dst: SyrotechNetw_13:3c:f0 (54:47:e8:13:3c:f0)
› Internet Protocol Version 4, Src: 192.168.1.36, Dst: 34.107.243.93
› Transmission Control Protocol, Src Port: 50236, Dst Port: 443, Seq: 0, Len: 0
```

TCP SYN ACK scan:


Apps
Places
Oct 20 7:28 PM
synscan.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

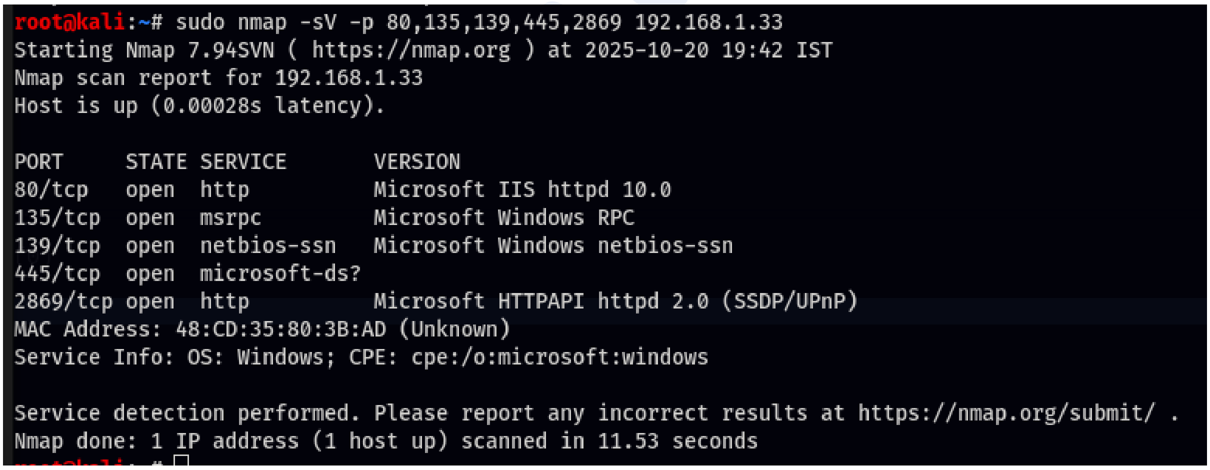
tcp.flags.syn==1 && tcp.flags.ack==1

```
No.   Time       Source         Destination   Protocol Length Info
   16 17.567494  34.107.243.93  192.168.1.36  TCP        74 443 → 50236 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=2430836268 TSecr=277772738 WS=256
   30 17.624741  34.107.243.93  192.168.1.36  TCP        74 443 → 50250 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=1877400807 TSecr=277772797 WS=256
```

```
▸ Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: SyrotechNetw_13:3c:f0 (54:47:e8:13:3c:f0), Dst: PCSSystemtec_95:57:6b (08:00:27:95:57:6b)
▸ Internet Protocol Version 4, Src: 34.107.243.93, Dst: 192.168.1.36
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 50236, Seq: 0, Ack: 1, Len: 0
```

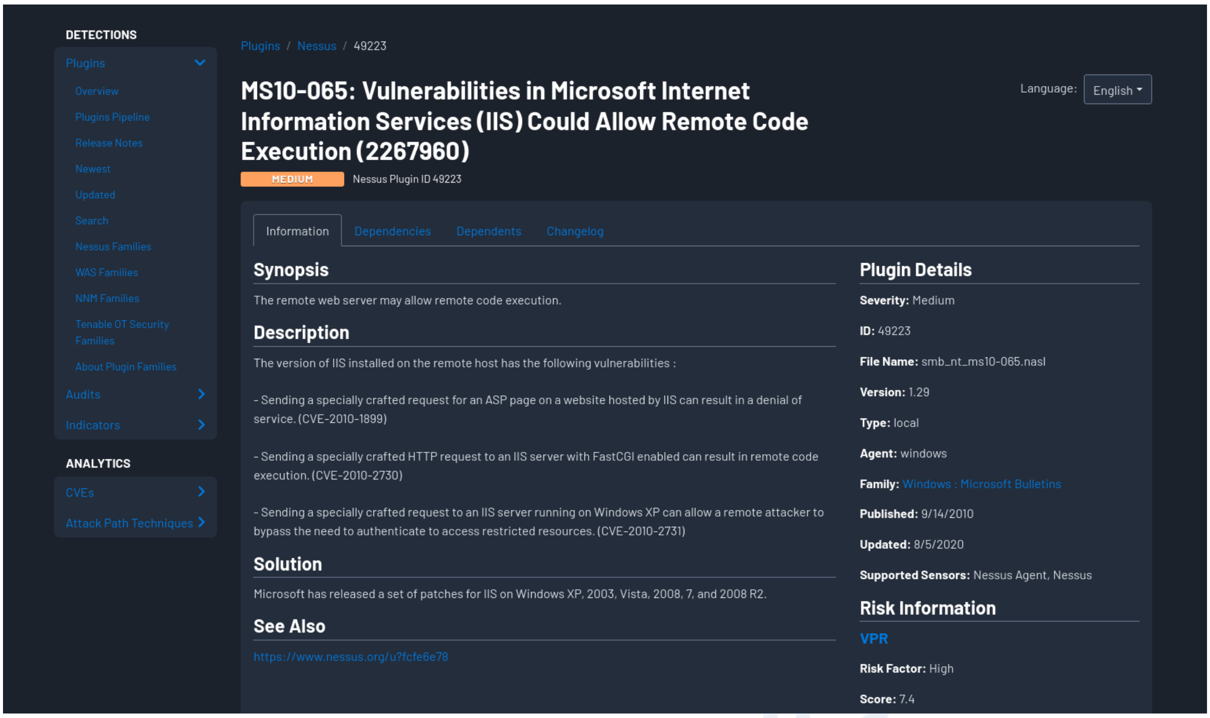
synscan.pcap | Packets: 63 · Displayed: 2 (3.2%) | Profile: Default

Doing Version Scan to find out the open ports to find if they are vulnerable or not:



```
root@kali:~# sudo nmap -sV -p 80,135,139,445,2869 192.168.1.33
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-20 19:42 IST
Nmap scan report for 192.168.1.33
Host is up (0.00028s latency).

PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2869/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 48:CD:35:80:3B:AD (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.53 seconds
root@kali:~#
```

Here Microsoft IIS httpd 10.0 seems to be vulnerable so searching for the exploits in that



MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960)

MEDIUM Nessus Plugin ID 49223

Synopsis

The remote web server may allow remote code execution.

Description

The version of IIS installed on the remote host has the following vulnerabilities :

- Sending a specially crafted request for an ASP page on a website hosted by IIS can result in a denial of service. (CVE-2010-1899)

- Sending a specially crafted HTTP request to an IIS server with FastCGI enabled can result in remote code execution. (CVE-2010-2730)

- Sending a specially crafted request to an IIS server running on Windows XP can allow a remote attacker to bypass the need to authenticate to access restricted resources. (CVE-2010-2731)

Solution

Microsoft has released a set of patches for IIS on Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

See Also

https://www.nessus.org/u?fcfe6e78

Plugin Details

Severity: Medium

ID: 49223

File Name: smb_nt_ms10-065.nasl

Version: 1.29

Type: local

Agent: windows

Family: Windows : Microsoft Bulletins

Published: 9/14/2010

Updated: 8/5/2020

Supported Sensors: Nessus Agent, Nessus

Risk Information

VPR

Risk Factor: High

Score: 7.4