

Network Security Essentials: A Guide to Nmap and Zenmap

Aseel Abujaber

Jan,08-2025

Contents

1. Introduction to Nmap	3
2. Accessing the Nmap Reference Guide:.....	3
3. Scanning a Subnet for Active Hosts:.....	4
4. Identifying Active Devices Without Service Details:	5
5. Detailed service Scan with Skipped Host Discovery:	5
6. SYN Scan for Open Ports Across Subnet	6
7. Comprehensive Port Scan Across All Devices	7
8. Faster Scanning with Timing Templates.....	8
9. Exhaustive TCP Port Scanning on a Single Host:.....	10
10. Introduction to Zenmap: Nmap's GUI	11
11. Installing Zenmap on Kali Linux.....	11
12. Using Zenmap for Visualized Network Scans	11
13. Visualizing Your Network with Zenmap's Topology View	11
Conclusion:.....	14

1. Introduction to Nmap

Nmap (Network Mapper) is a powerful tool used for network discovery and security auditing. It allows you to scan IP addresses or entire subnets to identify open ports, running services, and potential vulnerabilities in a network.

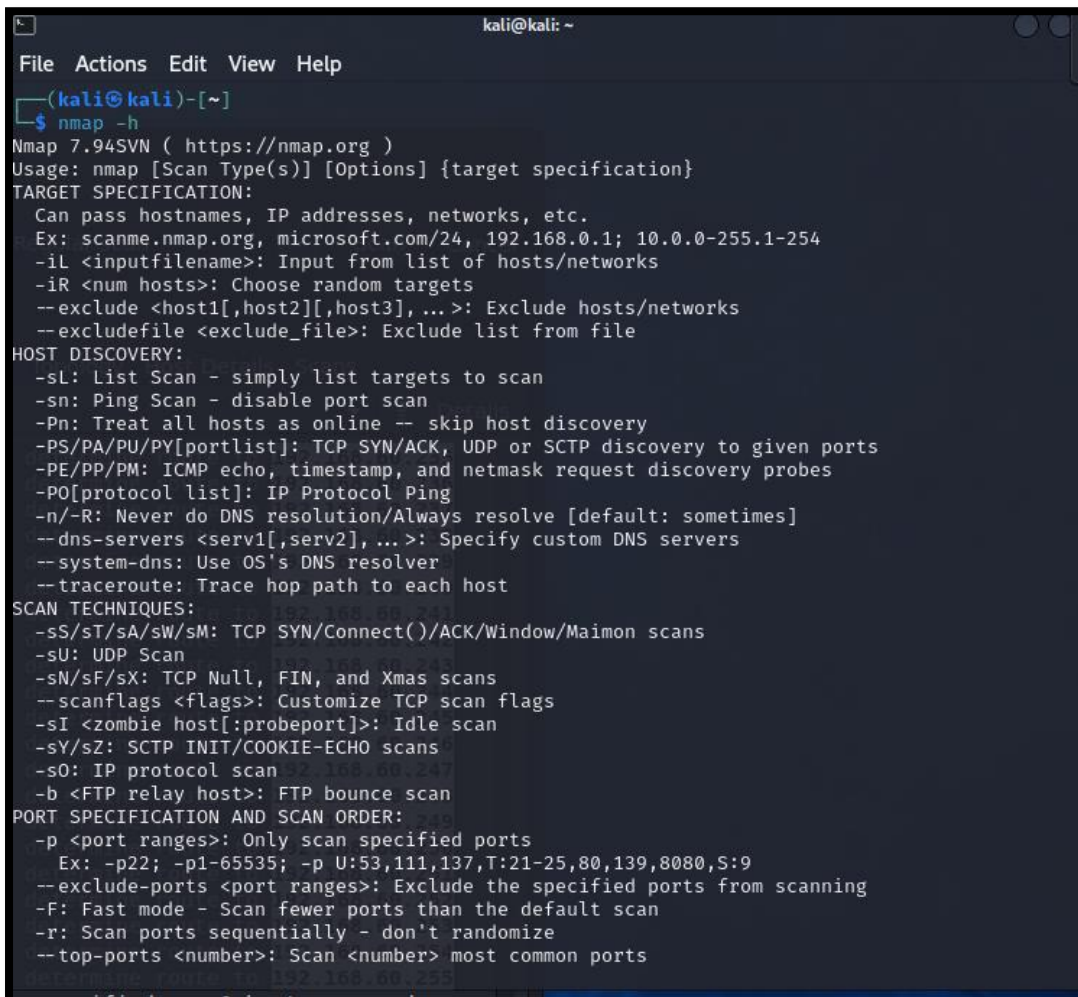
You can run this command to reach out for Nmap Reference Guide using this command.



```
(kali@kali)-[~]  
$ man nmap
```

2. Accessing the Nmap Reference Guide:

Use the [nmap -h] command to show a helpful guide on how to use Nmap. When you run it, Nmap will display a list of options and commands, along with brief descriptions of what each one does. This is a great way to get familiar with the different features and settings Nmap offers, like how to choose specific targets, scan types, or adjust the scan's speed. It's perfect if you're unsure about a particular command or need a quick reminder of how to use Nmap for different tasks.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -h  
Nmap 7.94SVN ( https://nmap.org )  
Usage: nmap [Scan Type(s)] [Options] {target specification}  
TARGET SPECIFICATION:  
  Can pass hostnames, IP addresses, networks, etc.  
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254  
  -iL <inputfilename>: Input from list of hosts/networks  
  -iR <num hosts>: Choose random targets  
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks  
  --excludefile <exclude_file>: Exclude list from file  
HOST DISCOVERY:  
  -sL: List Scan - simply list targets to scan  
  -sn: Ping Scan - disable port scan  
  -Pn: Treat all hosts as online -- skip host discovery  
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports  
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes  
  -PO[portlist]: IP Protocol Ping  
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]  
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers  
  --system-dns: Use OS's DNS resolver  
  --traceroute: Trace hop path to each host  
SCAN TECHNIQUES:  
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans  
  -sU: UDP Scan  
  -sN/sF/sX: TCP Null, FIN, and Xmas scans  
  --scanflags <flags>: Customize TCP scan flags  
  -sI <zombie host[:probeport]>: Idle scan  
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans  
  -sO: IP protocol scan  
  -b <FTP relay host>: FTP bounce scan  
PORT SPECIFICATION AND SCAN ORDER:  
  -p <port ranges>: Only scan specified ports  
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9  
  --exclude-ports <port ranges>: Exclude the specified ports from scanning  
  -F: Fast mode - Scan fewer ports than the default scan  
  -r: Scan ports sequentially - don't randomize  
  --top-ports <number>: Scan <number> most common ports
```

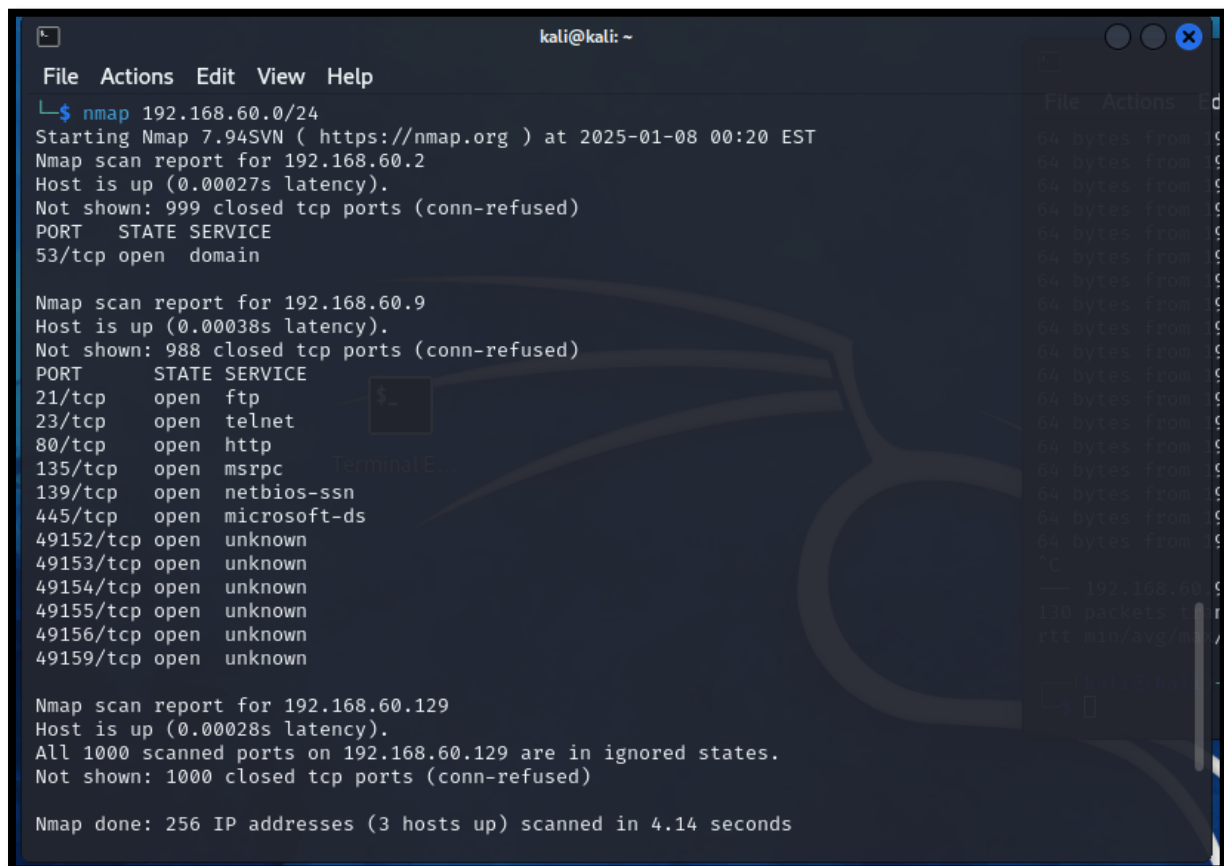
3. Scanning a Subnet for Active Hosts:

In the following example, the command `nmap 192.168.60.0/24` is used to scan the entire subnet (from 192.168.60.0 to 192.168.60.255), checking all the devices connected to the network.

The scan results identified three active hosts within the network:

1. **192.168.60.2** – This device is running a DNS service on port 53.
2. **192.168.60.9** – A Windows 7 machine with multiple open services, including FTP, Telnet, HTTP, and SMB. These open ports indicate potential exposure to security risks.
3. **192.168.60.129** – This host has no open ports, which could be attributed to a firewall or the absence of active services.

This scan provides a comprehensive overview of the services running on devices in the network. By identifying open ports and active services, it enables you to pinpoint potential vulnerabilities and address security concerns effectively.



```
kali@kali: ~  
File Actions Edit View Help  
$ nmap 192.168.60.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 00:20 EST  
Nmap scan report for 192.168.60.2  
Host is up (0.00027s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
53/tcp    open  domain  
  
Nmap scan report for 192.168.60.9  
Host is up (0.00038s latency).  
Not shown: 988 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
23/tcp    open  telnet  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49159/tcp open  unknown  
  
Nmap scan report for 192.168.60.129  
Host is up (0.00028s latency).  
All 1000 scanned ports on 192.168.60.129 are in ignored states.  
Not shown: 1000 closed tcp ports (conn-refused)  
  
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.14 seconds
```

4. Identifying Active Devices Without Service Details:

The results of the `sudo nmap -sn 192.168.60.0/24` scan revealed five active devices on the network:

1. **192.168.60.1, 192.168.60.2, 192.168.60.9, and 192.168.60.254** – These devices exhibit low latencies and are associated with VMware, indicating they are virtual machines operating within the network.
2. **192.168.60.129** – This device is online but does not provide a MAC address, suggesting it could be a physical device or one configured to hide its MAC address.

This scan is particularly useful for quickly identifying connected devices in the network. While it does not provide information about open ports or active services, it offers a foundational understanding of the devices present and their basic characteristics.

```
(kali@kali)-[~]
$ sudo nmap -sn 192.168.60.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 00:26 EST
Nmap scan report for 192.168.60.1
Host is up (0.00019s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.60.2
Host is up (0.00012s latency).
MAC Address: 00:50:56:F9:00:9A (VMware)
Nmap scan report for 192.168.60.9
Host is up (0.00023s latency).
MAC Address: 00:0C:29:8D:B6:A1 (VMware)
Nmap scan report for 192.168.60.254
Host is up (0.00020s latency).
MAC Address: 00:50:56:EF:EF:8D (VMware)
Nmap scan report for 192.168.60.129
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.08 seconds
```

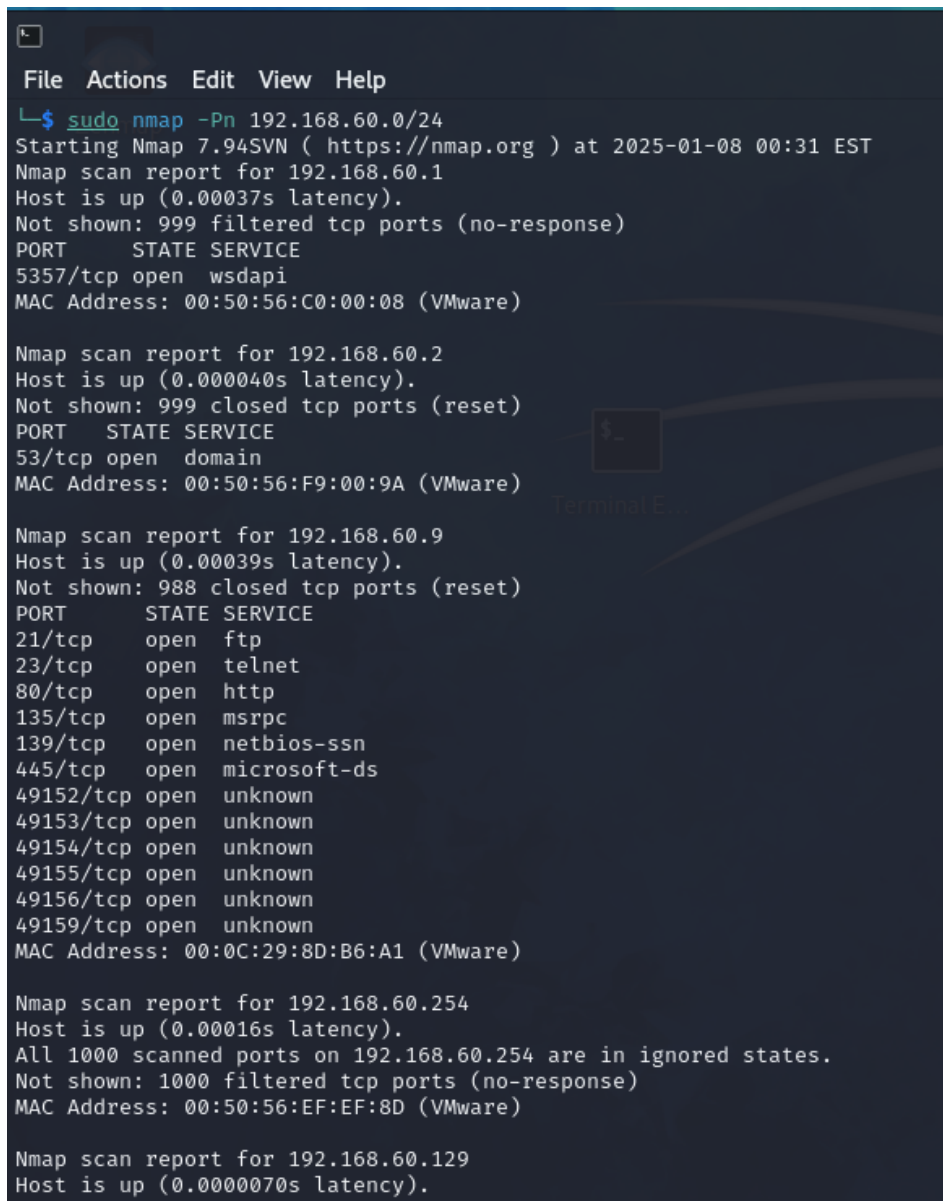
5. Detailed service Scan with Skipped Host Discovery:

The results of the `sudo nmap -Pn 192.168.60.0/24` scan identified five active hosts on the network:

1. **192.168.60.1** – This host is running **WSDAPI** (Port 5357), likely used for device communication, and is a VMware virtual machine.
2. **192.168.60.2** – This device is hosting a **DNS service** (Port 53) and is also a VMware virtual machine.
3. **192.168.60.9** – A Windows 7 machine with several open services, including **FTP** (Port 21), **Telnet** (Port 23), and **HTTP** (Port 80). These open ports present potential security risks and indicate that the device is a VMware virtual machine.

4. **192.168.60.254** and **192.168.60.129** – Both devices show no open ports or services. However, **192.168.60.254** has filtered ports, while **192.168.60.129** is configured to ignore all scanned ports.

This scan provides valuable insight into the services and configurations of devices within the network. By identifying open ports and the presence of active services, it helps in assessing potential security vulnerabilities and strengthening network defences.



```
File Actions Edit View Help
└─$ sudo nmap -Pn 192.168.60.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 00:31 EST
Nmap scan report for 192.168.60.1
Host is up (0.00037s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
5357/tcp  open  wsddapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.60.2
Host is up (0.000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F9:00:9A (VMware)

Nmap scan report for 192.168.60.9
Host is up (0.00039s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:0C:29:8D:B6:A1 (VMware)

Nmap scan report for 192.168.60.254
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.60.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EF:EF:8D (VMware)

Nmap scan report for 192.168.60.129
Host is up (0.0000070s latency).
```

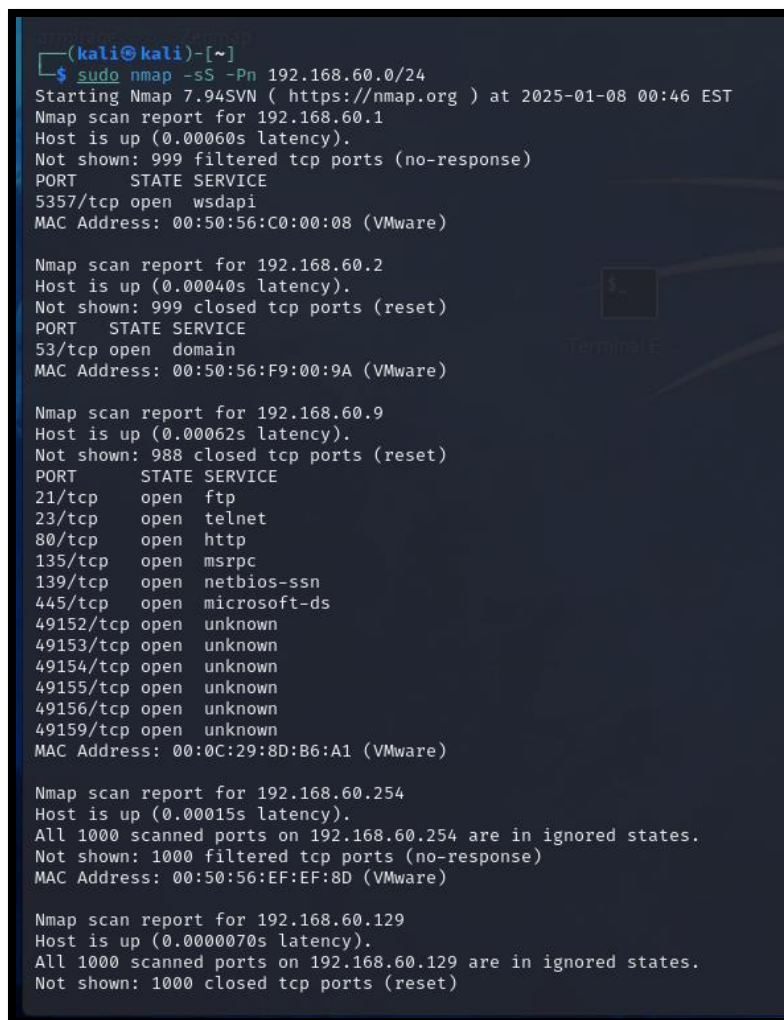
6. SYN Scan for Open Ports Across Subnet

Using `sudo nmap -sS -Pn 192.168.60.0/24` scan was performed to identify open ports across the entire subnet, bypassing the host discovery phase and assuming all devices are online. The results showed the following:

1. **192.168.60.1** – Running a **WSDAPI service** on port 5357, this device is a VMware virtual machine.

2. **192.168.60.2** – Hosting a **DNS service** on port 53 and is also a VMware virtual machine.
3. **192.168.60.9** – A Windows machine with multiple open ports, including **FTP** (Port 21), **Telnet** (Port 23), and **HTTP** (Port 80), suggesting several active services that may present security risks.
4. **192.168.60.254** and **192.168.60.129** – Both devices showed no open ports, with all scanned ports marked as filtered or ignored, likely due to security configurations or lack of open services.

The SYN scan used in this test is less intrusive than a full TCP connect scan, identifying open ports without completing the full handshake, making it a more discrete method of port discovery.



```
(kali㉿kali)-[~]
$ sudo nmap -sS -Pn 192.168.60.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 00:46 EST
Nmap scan report for 192.168.60.1
Host is up (0.00060s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
5357/tcp  open  wsddapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.60.2
Host is up (0.00040s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F9:00:9A (VMware)

Nmap scan report for 192.168.60.9
Host is up (0.00062s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:0C:29:8D:B6:A1 (VMware)

Nmap scan report for 192.168.60.254
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.60.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EF:EF:8D (VMware)

Nmap scan report for 192.168.60.129
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.60.129 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

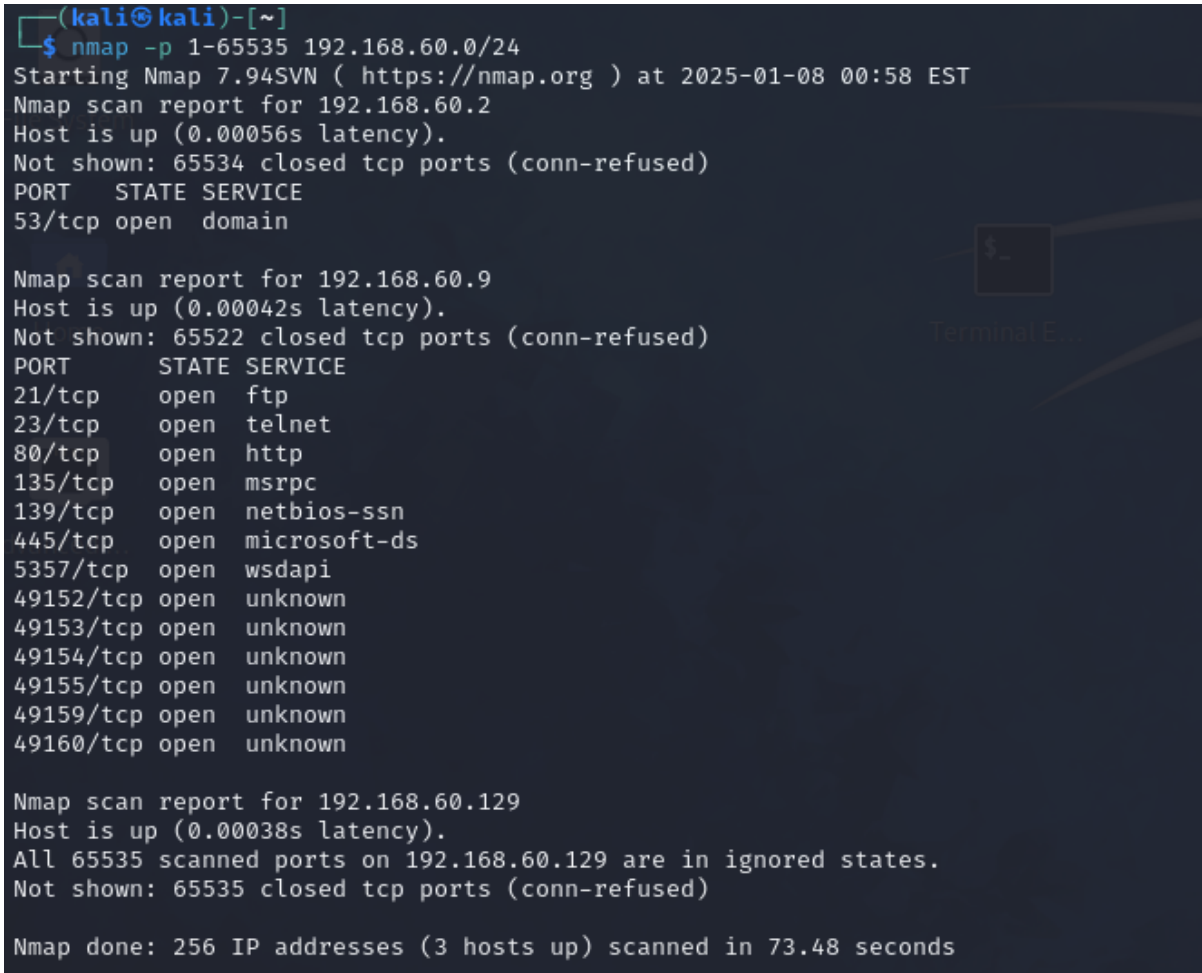
7. Comprehensive Port Scan Across All Devices

The `nmap -p 1-65535 192.168.60.0/24` command scans all 65,535 TCP ports across the subnet to identify open services. The scan results showed the following:

1. **192.168.60.2** – Running a **DNS service** on port 53, with all other ports closed.

2. **192.168.60.9** – A Windows machine with several open ports, including **FTP** (Port 21), **Telnet** (Port 23), **HTTP** (Port 80), **MSRPC** (Port 135), and a range of unknown ports (**49152-49160**), which could suggest additional services or applications running on the device.
3. **192.168.60.129** – This device has all ports closed, likely due to firewall restrictions or the absence of any open services.

This comprehensive scan provides a detailed view of the open services and potential security vulnerabilities on the devices within the network, aiding in the identification and assessment of security risks.

A terminal window with a dark background and light blue text. The prompt is '(kali@kali)-[~]'. The user enters '\$ nmap -p 1-65535 192.168.60.0/24'. The output shows the Nmap version (7.94SVN), the start time (2025-01-08 00:58 EST), and the scan report for 192.168.60.2. For 192.168.60.2, it shows port 53/tcp is open (domain) and all other ports are closed. Then it shows the scan report for 192.168.60.9, listing multiple open ports: 21/tcp (ftp), 23/tcp (telnet), 80/tcp (http), 135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 5357/tcp (wsdapi), and a range of unknown ports from 49152 to 49160. Finally, it shows the scan report for 192.168.60.129, stating that all 65535 scanned ports are in ignored states. The scan is done in 73.48 seconds.

```
(kali@kali)-[~]
$ nmap -p 1-65535 192.168.60.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 00:58 EST
Nmap scan report for 192.168.60.2
Host is up (0.00056s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 192.168.60.9
Host is up (0.00042s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown

Nmap scan report for 192.168.60.129
Host is up (0.00038s latency).
All 65535 scanned ports on 192.168.60.129 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (3 hosts up) scanned in 73.48 seconds
```

8. Faster Scanning with Timing Templates

The `nmap -T4 192.168.60.0/24` command performs a subnet scan for open services using a faster timing template. The results revealed the following:

1. **192.168.60.2** – This device is active with port 53 (**DNS**) open, and all other ports are closed.
2. **192.168.60.9** – A Windows machine with multiple open ports, including **FTP** (Port 21), **Telnet** (Port 23), **HTTP** (Port 80), **MSRPC** (Port 135), **NetBIOS-SSN** (Port 139), **Microsoft-DS** (Port 445), **WSDAPI** (Port 5357), and a range of

unknown ports (**49152-49160**). This suggests that several services or applications are running, which could present potential security risks.

3. **192.168.60.129** – This device is online, but all 1000 scanned ports were marked as ignored, likely due to firewall restrictions.

This scan provides a rapid overview of open services across network devices, allowing for a quick assessment of potential security concerns.

```
(kali㉿kali)-[~]
$ nmap -T4 192.168.60.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 01:08 EST
Nmap scan report for 192.168.60.2
Host is up (0.00030s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 192.168.60.9
Host is up (0.00052s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown

Nmap scan report for 192.168.60.129
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.60.129 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (3 hosts up) scanned in 6.67 seconds
```

```
(kali㉿kali)-[~]
$ nmap -p- 192.168.60.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 01:07 EST
Nmap scan report for 192.168.60.9
Host is up (0.0011s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49159/tcp  open  unknown
49160/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 73.20 seconds
```

9. Exhaustive TCP Port Scanning on a Single Host:

The `nmap -p- 192.168.60.9` command performs a scan of all 65,535 TCP ports on the host **192.168.60.9**. The scan results indicate that the host is active, with a latency of **0.0011 seconds**. Of the total ports, **65,522** are closed, but several ports are open, including:

- **FTP** (Port 21)
- **Telnet** (Port 23)
- **HTTP** (Port 80)
- **MSRPC** (Port 135)
- **NetBIOS-SSN** (Port 139)
- **Microsoft-DS** (Port 445)
- **WSDAPI** (Port 5357)
- A range of unknown ports (**49152-49160**)

This scan provides a comprehensive view of the open services on the host, offering valuable insight into potential security vulnerabilities that could be addressed to enhance the device's security posture.

10. Introduction to Zenmap: Nmap's GUI

Zenmap Network Scanning Report

Introduction: Zenmap is the official graphical user interface (GUI) for Nmap, a powerful tool used for network discovery and security auditing. Zenmap makes Nmap easier to use by providing a user-friendly interface that allows you to perform network scans, save scan results, and compare them over time. It's perfect for those who prefer a visual approach to network scanning and analysis.

11. Installing Zenmap on Kali Linux

Step by step instructions to get Zenmap up and running on Kali Linux:

1. **Update your system:** Open a terminal and run the following commands to ensure your system is up-to-date: `sudo apt-get update`
2. `sudo apt-get upgrade`
3. **Install Zenmap:** Once your system is updated, install Zenmap using the following command:

```
sudo apt-get install zenmap
```

12. Using Zenmap for Visualized Network Scans

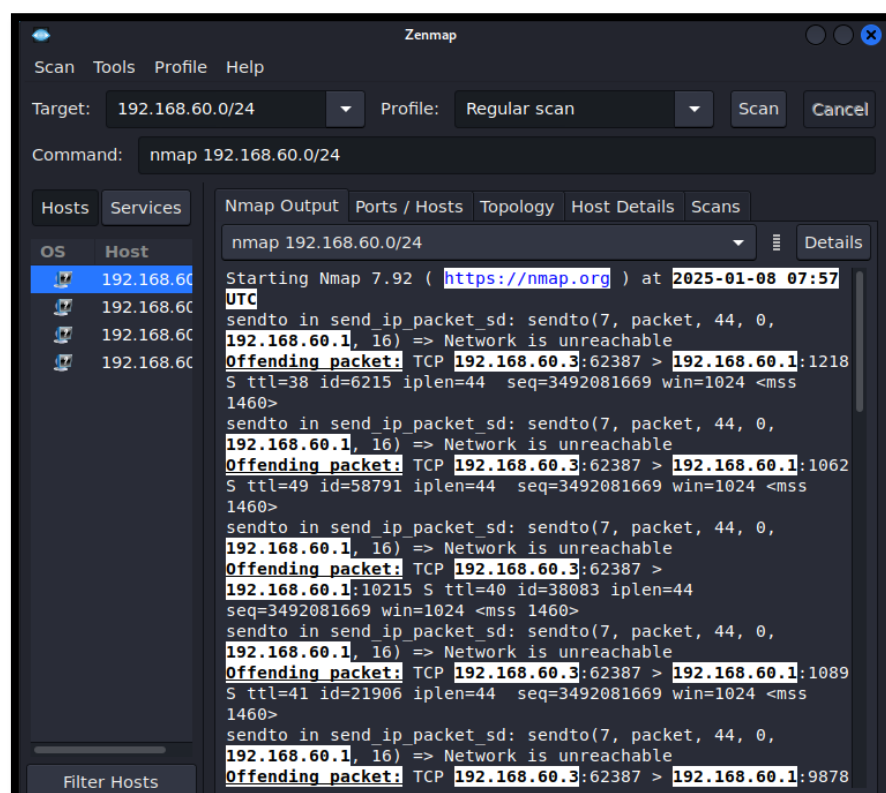
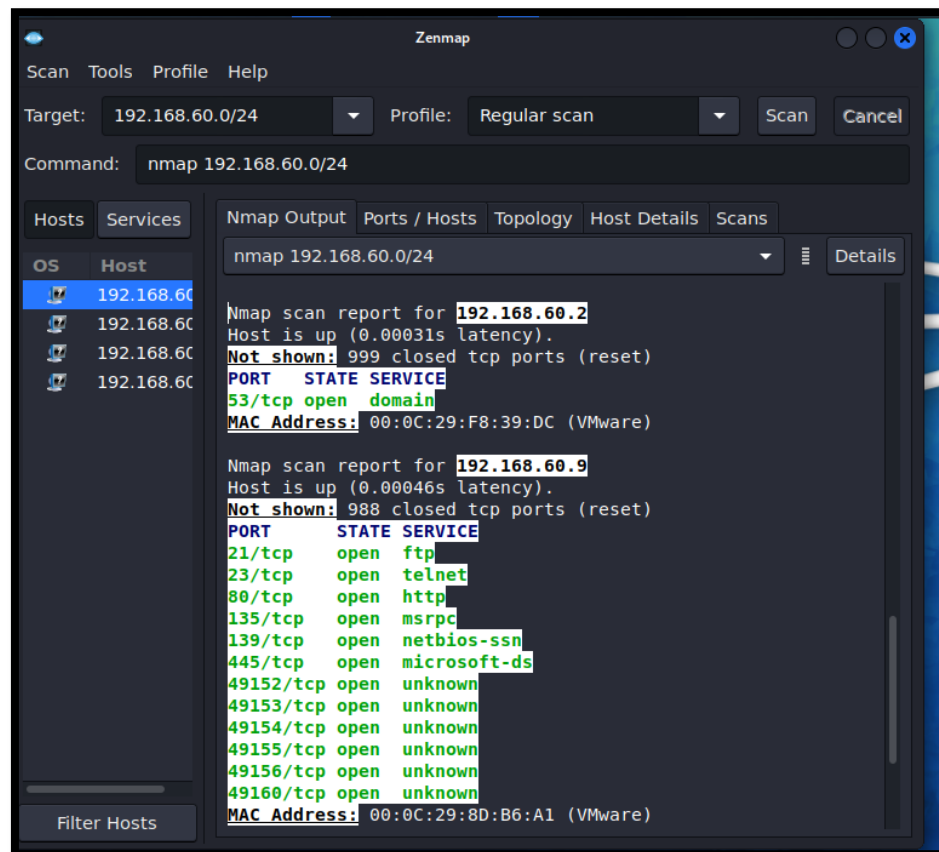
Using **Zenmap**, the graphical user interface (GUI) for **Nmap**, allows for a more visual and user-friendly way to conduct network scans. It simplifies the process of running Nmap commands by providing options to customize scan types, ranges, and outputs through an easy-to-use interface.

In this example, using Zenmap to scan the IP range resulted in the same details as the Nmap command-line output:

1. **192.168.60.2** has **Port 53 (DNS)** open, and all other ports are closed, suggesting that it is primarily a DNS server.
2. **192.168.60.9** (your Windows machine) has several open ports, such as **FTP (Port 21)**, **Telnet (Port 23)**, **HTTP (Port 80)**, and others, which could indicate the machine is running multiple services. These open ports can be valuable for identifying potential vulnerabilities if not properly secured.

13. Visualizing Your Network with Zenmap's Topology View

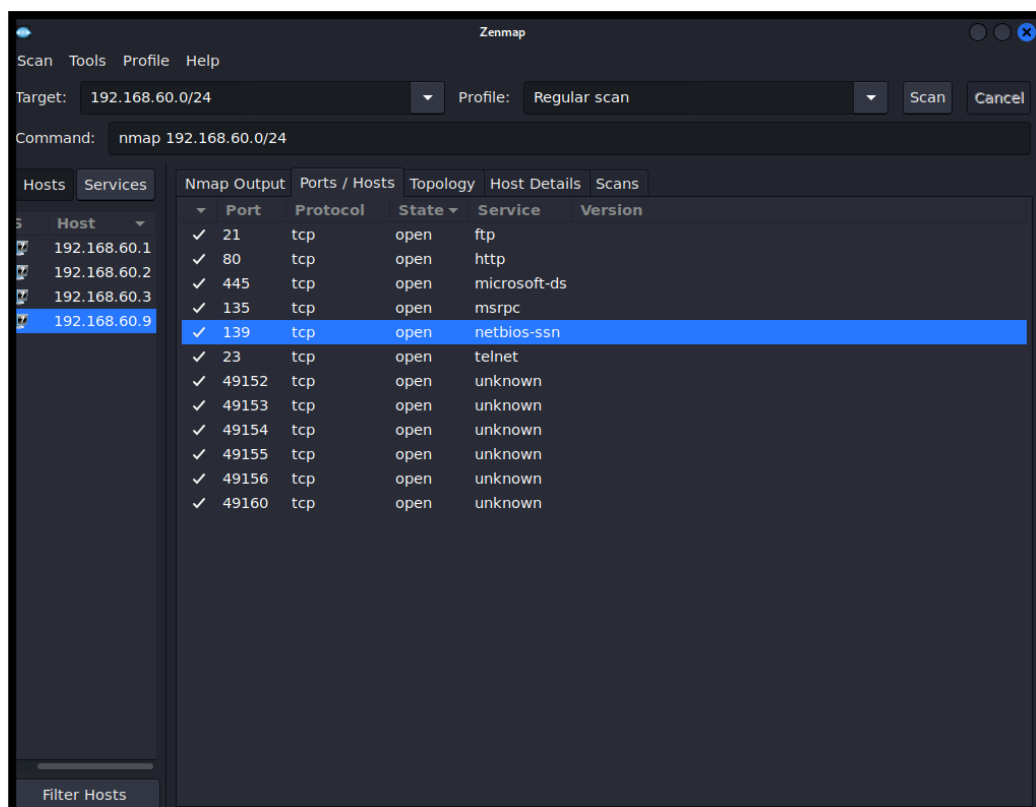
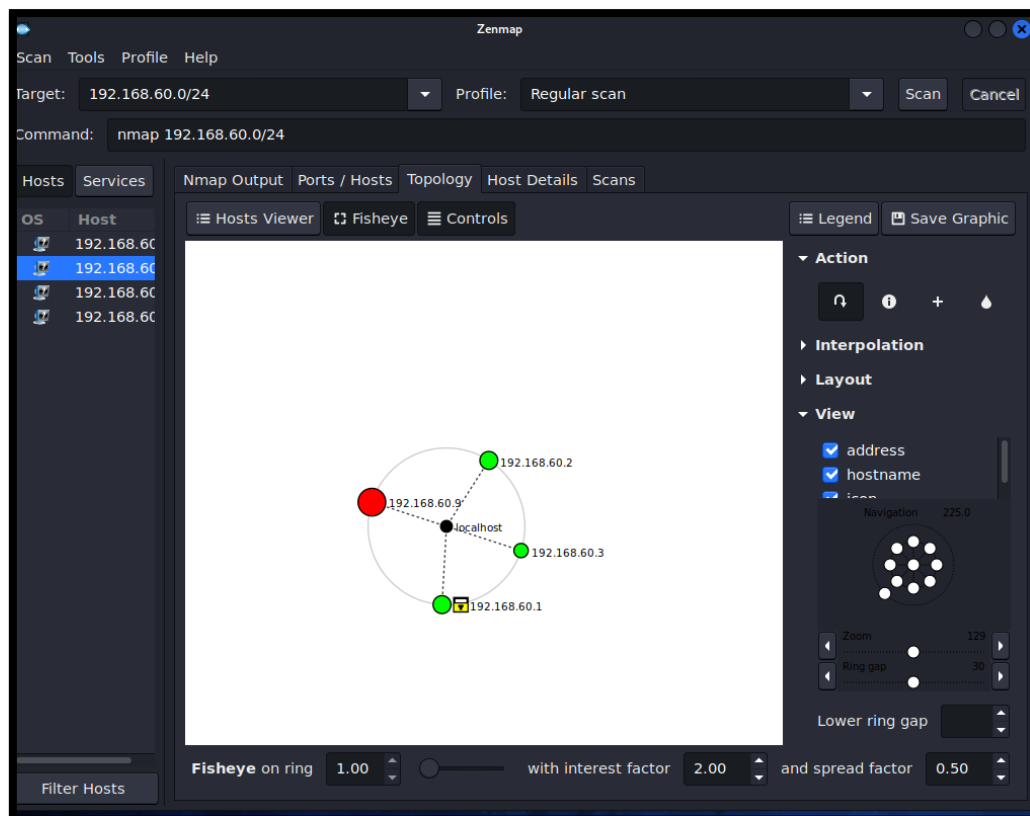
Zenmap provides a more visual representation of these scan results, allowing you to see the details in a more organized manner, like port status and service information. You can also save or export these results for later analysis or reporting.



Zenmap's **Topology View** provides a simple visual layout of your network. It shows devices as points (nodes) and connects them with lines (edges) to indicate how they're linked. Each device typically displays its IP address and sometimes its MAC address or

Network Security Essentials: A Guide to Nmap and Zenmap

open ports. This view helps you quickly spot active devices, see how they're connected, and identify services running on them, making it easier to understand the structure of your network and potential security risks.



Conclusion:

This guide provided a comprehensive overview of Nmap and Zenmap, two powerful tools used for network discovery and security auditing. Through various scanning techniques, including subnet scans, detailed service scans, SYN scans, and exhaustive port scans, we explored how to identify active devices, open ports, and services running within a network. These tools help detect potential vulnerabilities and security risks, offering a critical foundation for network security assessments.

The use of Nmap's command-line interface and Zenmap's graphical user interface (GUI) allows for flexibility and ease in scanning and analyzing networks. Zenmap, in particular, enhances the user experience by providing visual representations of network topologies, making it simpler to visualize device connections and pinpoint security concerns.

By mastering these scanning techniques, network administrators and security professionals can gain valuable insights into their network infrastructure, assess risks, and take appropriate measures to strengthen network defenses. Ultimately, regular network scanning is essential for identifying and addressing vulnerabilities to ensure a secure network environment.