**Corvit System Multan**

***Report***

***Title: Network Scanning Fundamentals***

***Submitted By: Muhammad Adnan***

***Submitted To: Muhammad Bilal***

**Network Scanning Fundamentals**

**Definition:**

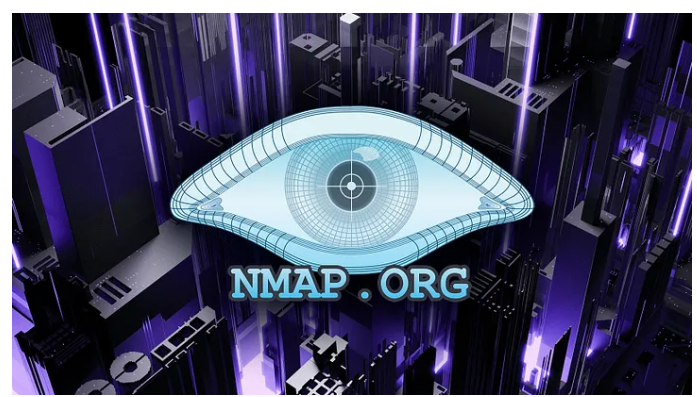
*Network scanning is the process of identifying active hosts on a network, discover open ports, and gathering information about network services and devices. It helps to identify potential vulnerabilities.*

***Techniques and Tools:***

* *Ping scanning*
* *TCP / UDP scanning*
* *Stealth scanning*

**Tools/websites:**

**Nmap***: A powerful open-source network scanner.*

**

**Types Of Network scans**

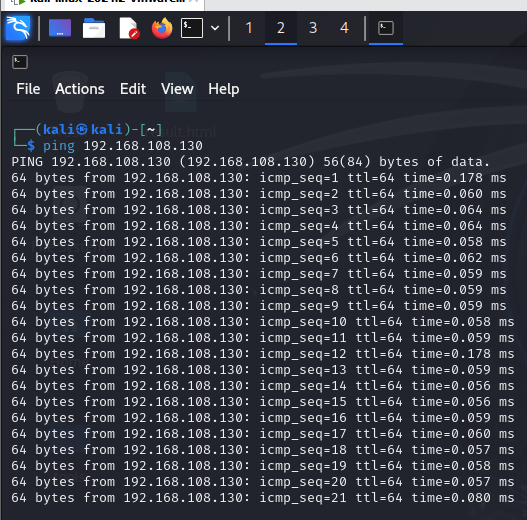
**Definition:**

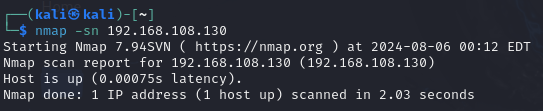
*Network Scan can be categorized based on the methods used to discover devices and services on the network.*

*Example:*

**Ping scan***:*

*A ping scan is a network scanning technique used to identify which IP addresses within a range are active or live.*





**SYN Scan:**

*A SYN scan, also known as a TCP SYN scan or half-open scan, is a popular network scanning technique used to identify open ports on a target machine. It's widely used by security professionals and network administrators because it's fast, stealthy, and effective***.**

**Techniques and Tools:**

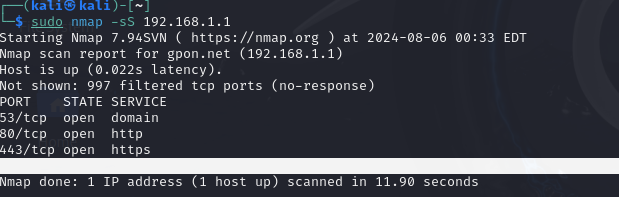
* **SYN scan**
* **ACK scan**
* **FIN scan**
* **Xmass scan**

**Tools and Websites:**

**Nmap:**

**SYN scan:**

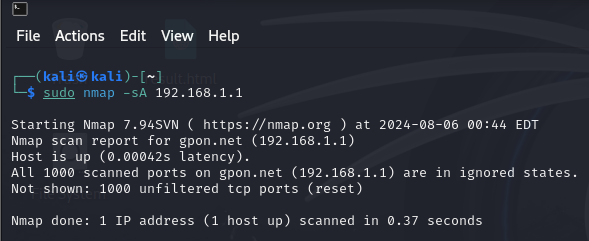
Commond: nmap -sS [target]



**ACK Scan:**

*The ACK scan is used to map out firewall rulesets, determining whether ports are filtered (by a firewall) or unfiltered.*

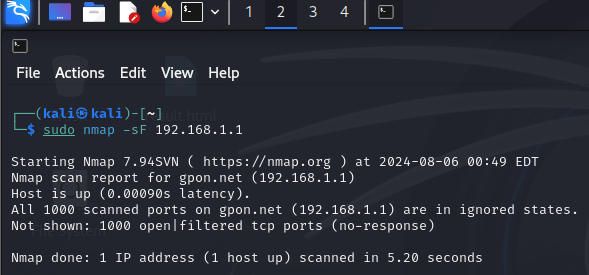
**Commond**: nmap -sA [target**]**



**FIN Scan:**

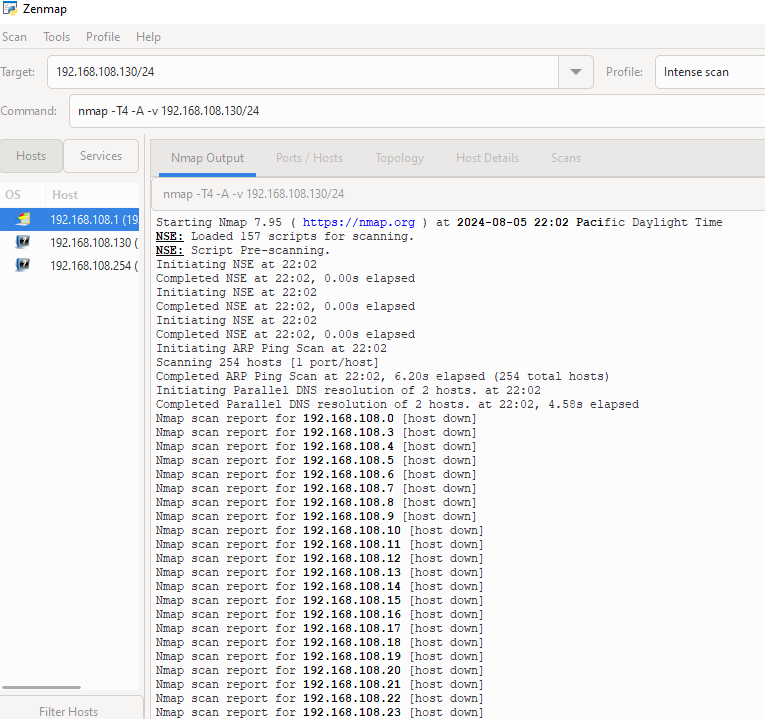
*The FIN scan is a stealthy scan that sends a TCP FIN packet to the target port. It can sometimes bypass firewalls and packet filters that drop SYN packets*.

**Command: nmap -sF [target]**



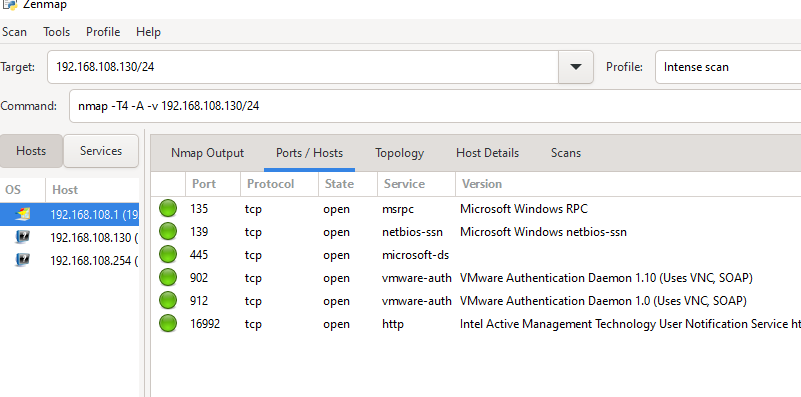
**Zenmap:**

The graphical user interface for Nmap, to perform a network scan.

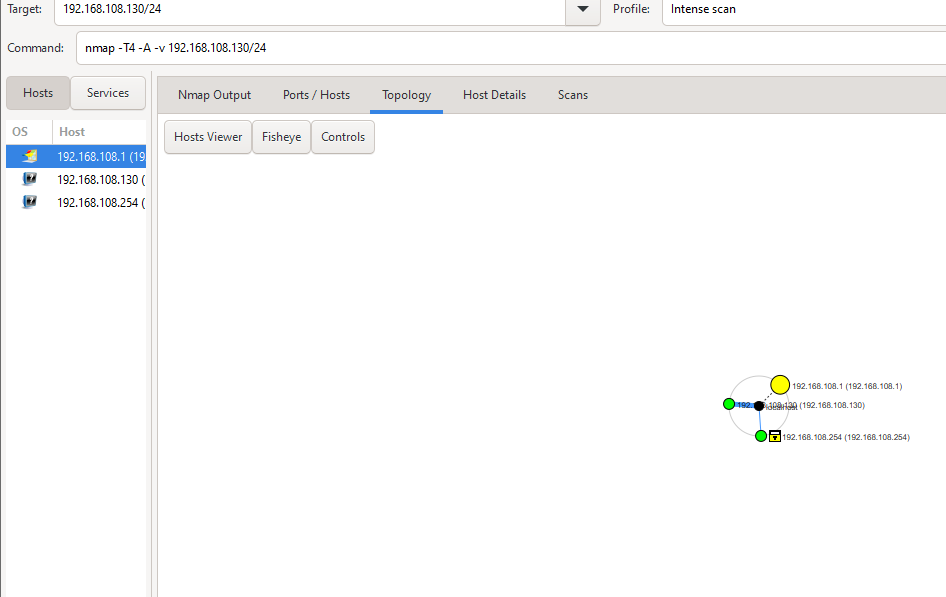


**Zenmap**

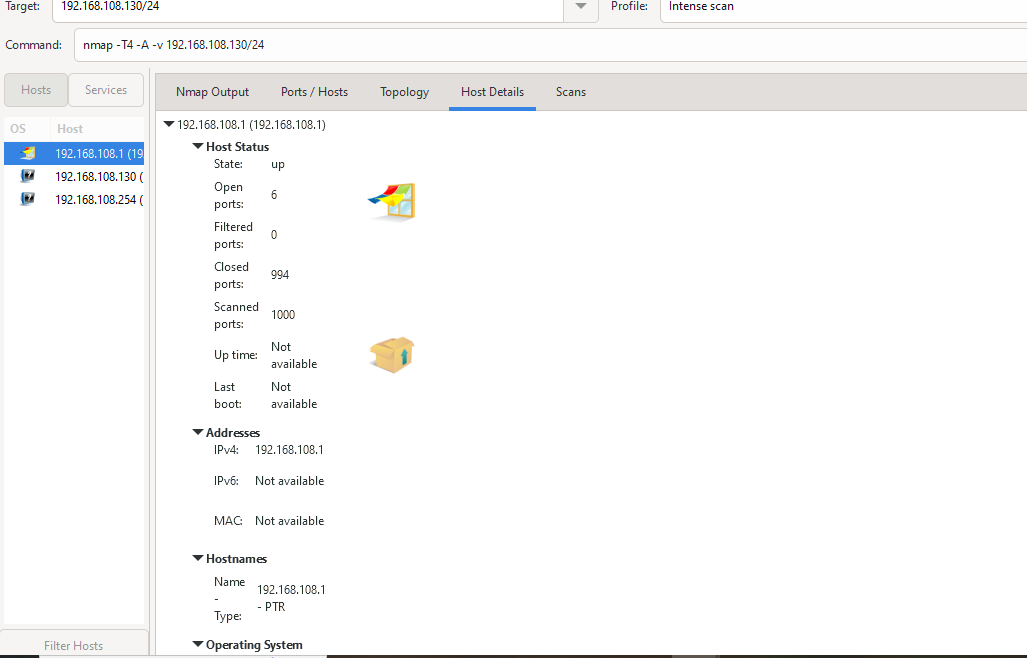
**Ports/Hosts:**



**Topology:**



**Hosts Details:**



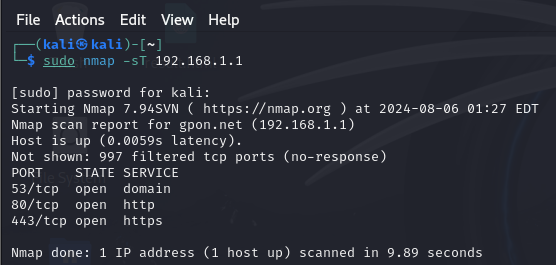


**Ports scanning techniques:**

*Port scanning is a method used in network security to determine which ports on a networked device are open and what services might be running on them****.***

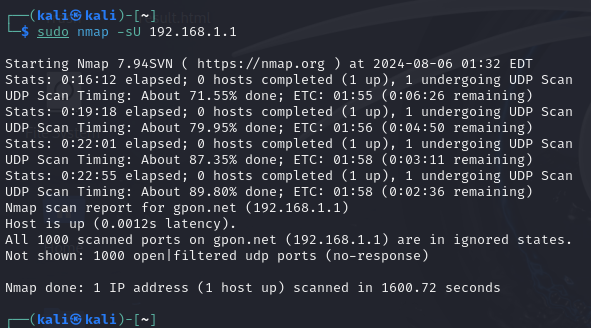
**1-TCP Connect Scan (-sT):**

*This is the simplest and most reliable scanning method. It attempts to establish a full TCP connection by completing the three-way handshake (SYN, SYN-ACK, ACK).*



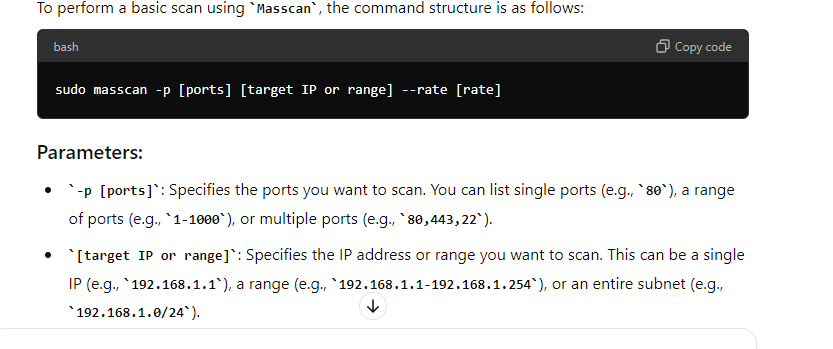
**2.** **UDP Scan (-sU):**

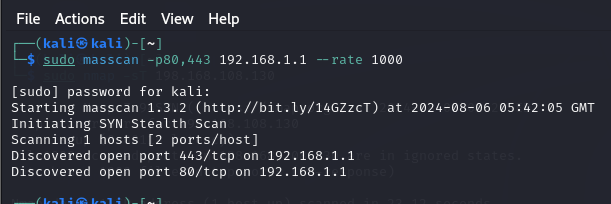
*Sends UDP packets to the target ports. Since UDP is connectionless, determining if a port is open can be tricky. If a port is closed, the target typically responds with an ICMP "Port Unreachable" message.*

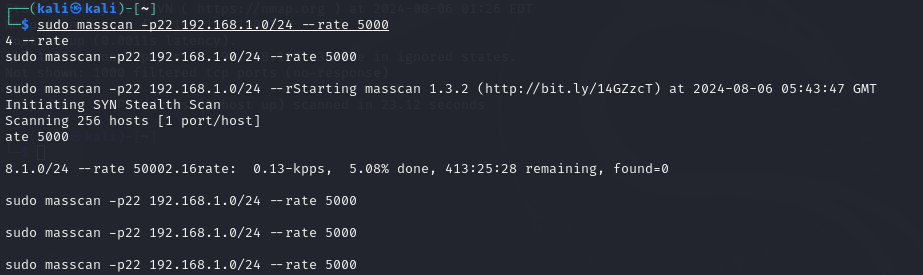


**Mass scan:**

*Masscan is a network scanning tool designed for extremely fast scanning of large networks. It is capable of scanning the entire IPv4 internet in a matter of minutes, depending on the scan configuration and the bandwidth available.*

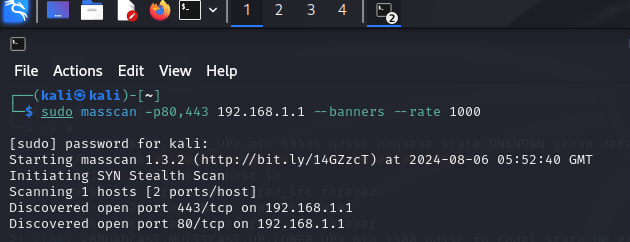






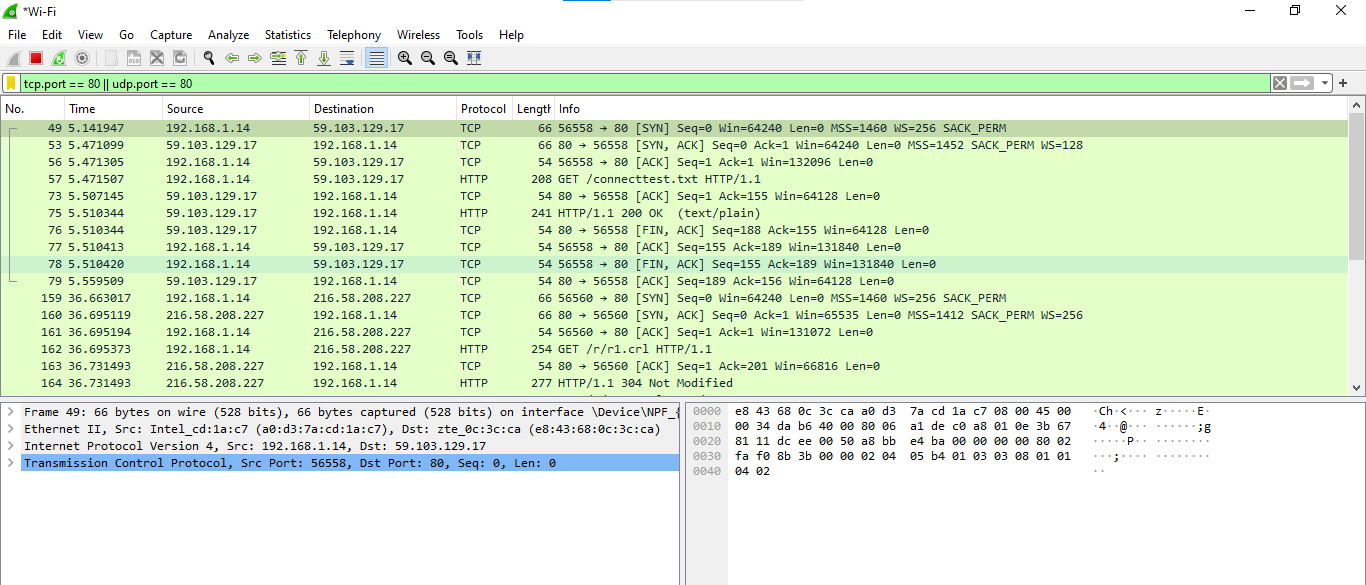
**Banner Grabbing:**

# 



**Wireshark:**

**Wireshark is a popular network protocol analyzer used to capture and analyze network traffic in real time. It allows you to inspect the data traveling over a network, which can be useful for troubleshooting network issues, analyzing network performance, and debugging network applications.**

****