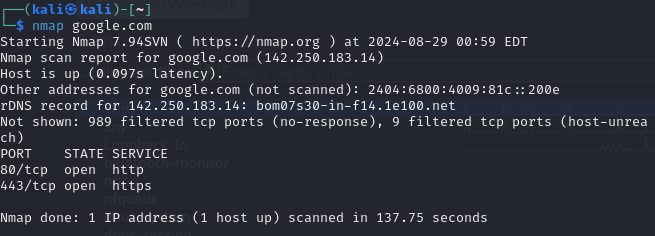
Day 16 – Learning Nmap

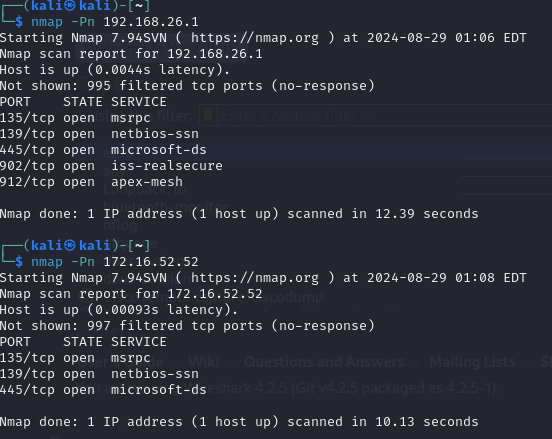
I used Nmap to perform network scanning and discovery tasks. Nmap is a powerful tool that allows me to identify hosts, services, and open ports on a network, providing essential information for network security assessments. By specifying different options, I can perform tasks such as ping sweeps, OS detection, and service version detection. The tool is highly efficient, with the ability to scan large networks quickly, and it provides detailed output, making it invaluable for both network administrators and security professionals. My experience with Nmap was smooth, and it delivered accurate and actionable insights.

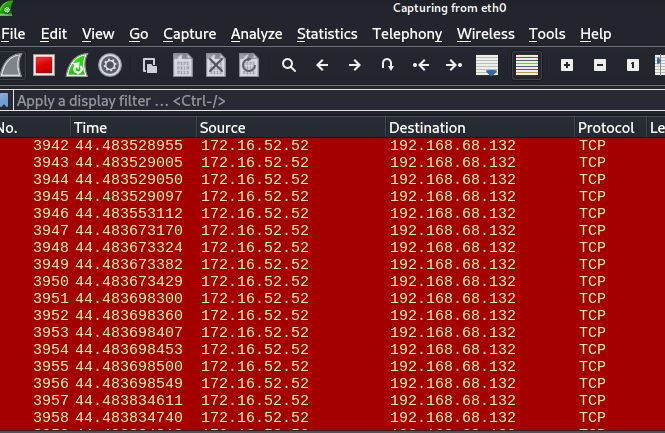
**Overview of Nmap Commands**

1. **Basic Scan**
   * **Command**: nmap [target]
   * **Description**: Performs a basic scan to identify open ports on the target.
   * **Example**: nmap 192.168.1.1
   * **Explanation**: This command scans the target IP address (192.168.1.1) and lists the open ports.

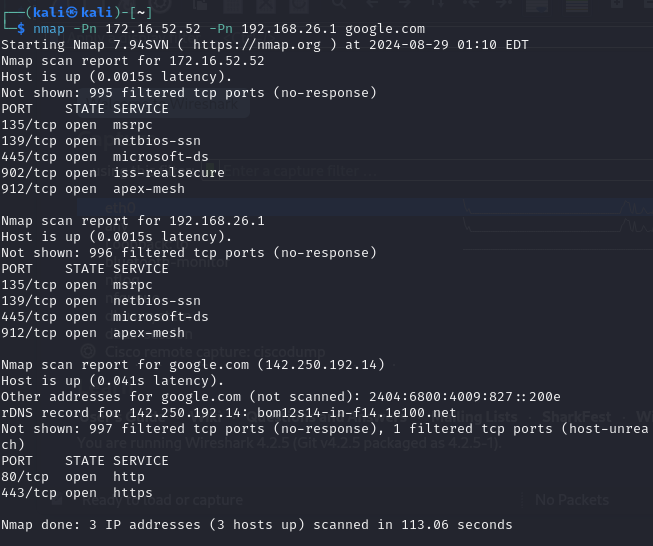


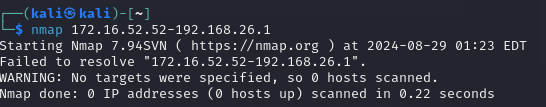
1. **Scan Multiple Targets**
   * **Command**: nmap [target1] [target2] ...
   * **Description**: Scans multiple IP addresses or hostnames.
   * **Example**: nmap 192.168.1.1 192.168.1.2
   * **Explanation**: This command scans both IP addresses (192.168.1.1 and 192.168.1.2) for open ports.



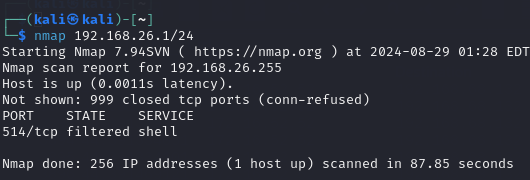


1. **Scan a Range of IPs**
   * **Command**: nmap [startIP-endIP]
   * **Description**: Scans a range of IP addresses.
   * **Example**: nmap 192.168.1.1-20
   * **Explanation**: This scans all IP addresses from 192.168.1.1 to 192.168.1.20.

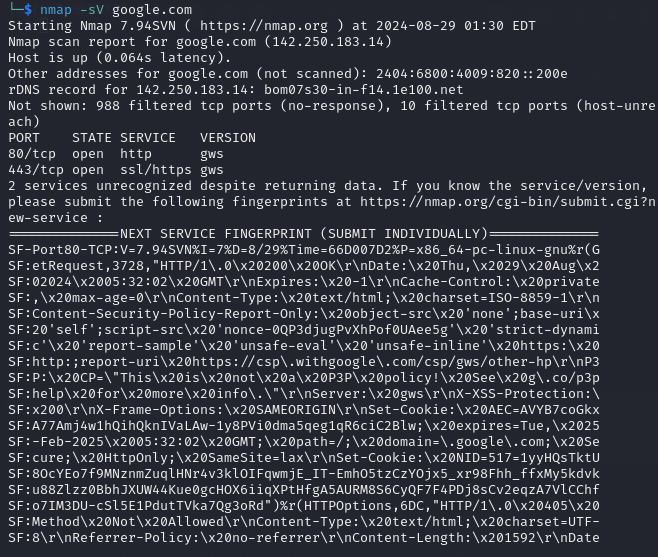




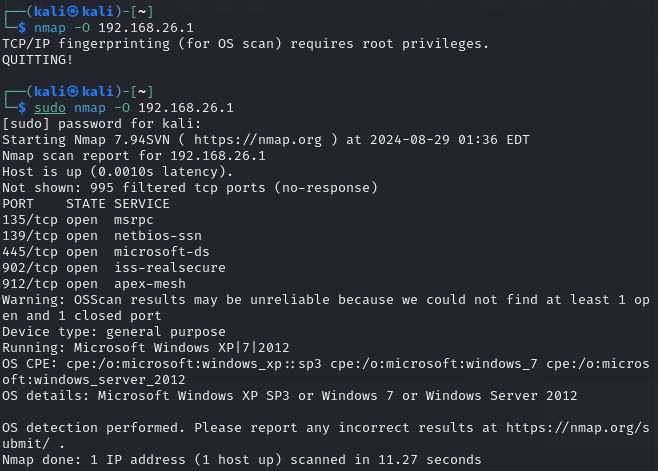
1. **Scan an Entire Subnet**
   * **Command**: nmap [network]/[CIDR]
   * **Description**: Scans all devices in a subnet.
   * **Example**: nmap 192.168.1.0/24
   * **Explanation**: This scans all IP addresses within the 192.168.1.0 subnet with a subnet mask of 255.255.255.0.



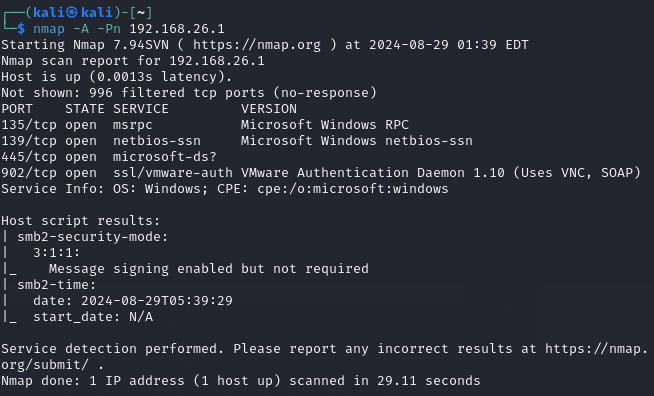
1. **Service Version Detection**
   * **Command**: nmap -sV [target]
   * **Description**: Detects versions of services running on open ports.
   * **Example**: nmap -sV 192.168.1.1
   * **Explanation**: This command not only identifies open ports but also determines the versions of the services running on those ports.



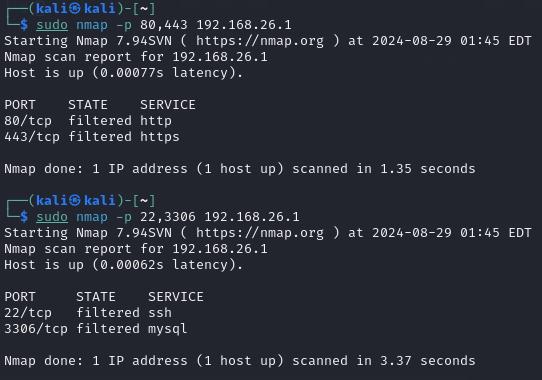
1. **Operating System Detection**
   * **Command**: nmap -O [target]
   * **Description**: Attempts to determine the operating system of the target.
   * **Example**: nmap -O 192.168.1.1
   * **Explanation**: This scans the target and tries to guess the operating system based on network responses.

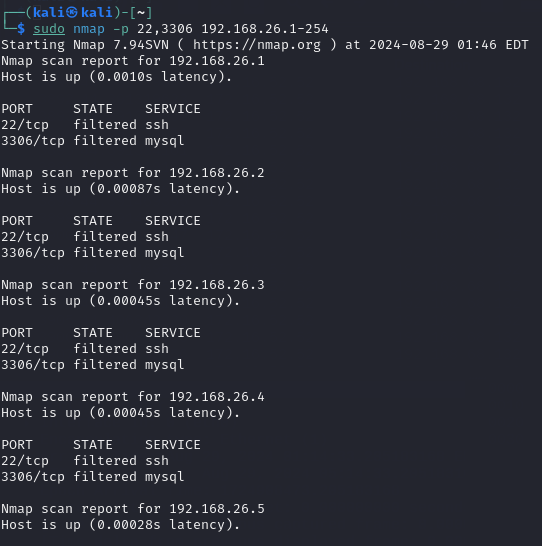


1. **Aggressive Scan**
   * **Command**: nmap -A [target]
   * **Description**: Performs a more comprehensive scan, including OS detection, version detection, script scanning, and traceroute.
   * **Example**: nmap -A 192.168.1.1
   * **Explanation**: This command provides detailed information about the target, including open ports, service versions, OS, and potential vulnerabilities.



1. **Scan with Specific Port**
   * **Command**: nmap -p [port] [target]
   * **Description**: Scans a specific port or a range of ports.
   * **Example**: nmap -p 80,443 192.168.1.1
   * **Explanation**: This scans only ports 80 and 443 on the target IP address.





1. **Stealth Scan**
   * **Command**: nmap -sS [target]
   * **Description**: Performs a SYN scan, which is less likely to be detected by firewalls and intrusion detection systems.
   * **Example**: nmap -sS 192.168.1.1
   * **Explanation**: This command sends SYN packets to the target’s ports to determine if they are open, without completing the TCP handshake.

