**Practical: 02**

**Aim:** Document Nmap commands, execute DoS attack, analyse with Wireshark, and suggest countermeasures for network security.

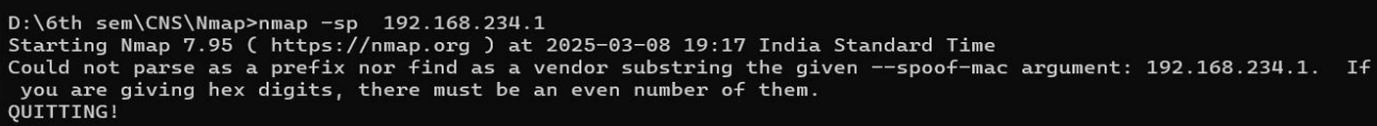
**Introduction to Nmap**

Nmap (Network Mapper) is an open-source tool for network discovery and security auditing. It is used to scan networks and identify open ports, running services, and vulnerabilities.

**N-map Commands with Output & Description:**

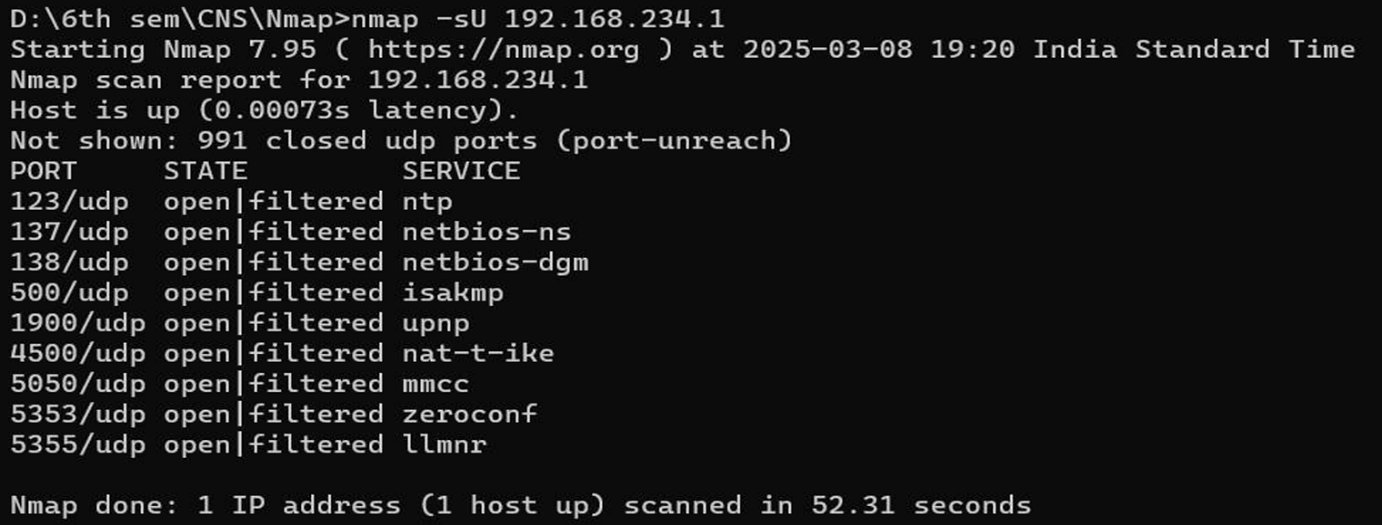
1. **Ping Scan:**

cmd- nmap -sP <target ip>

****des-Performs a simple ping scan to check live hosts.

1. **UDP Scan:**

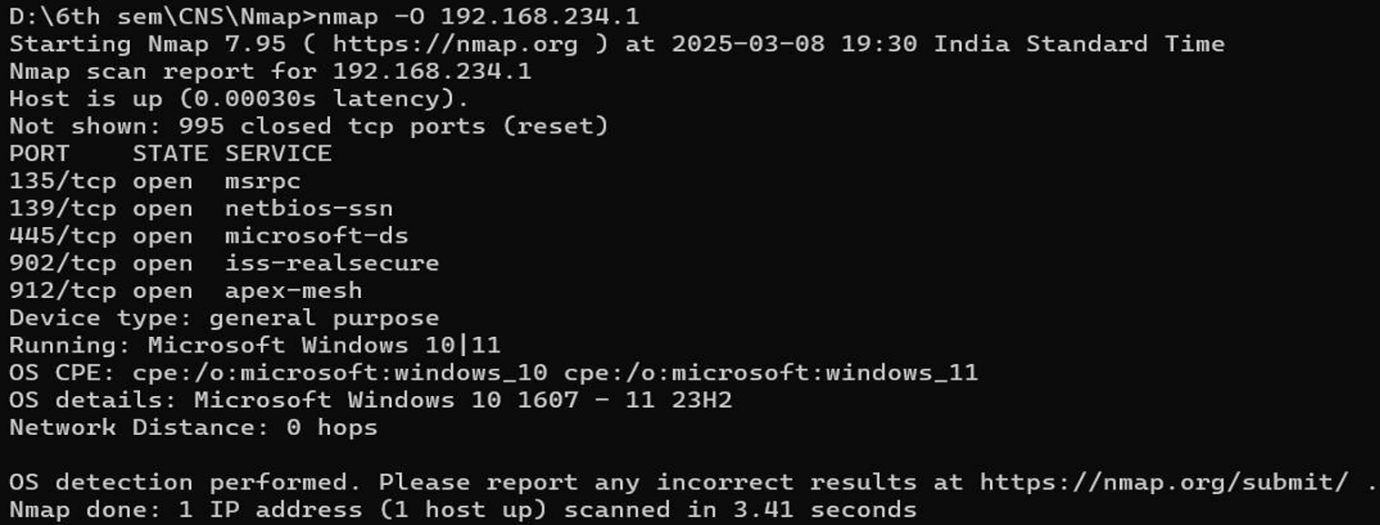
cmd- nmap -sU <target ip>

****des- Scans for open UDP ports.

1. **OS Detection:**

cmd- nmap -O <target ip>

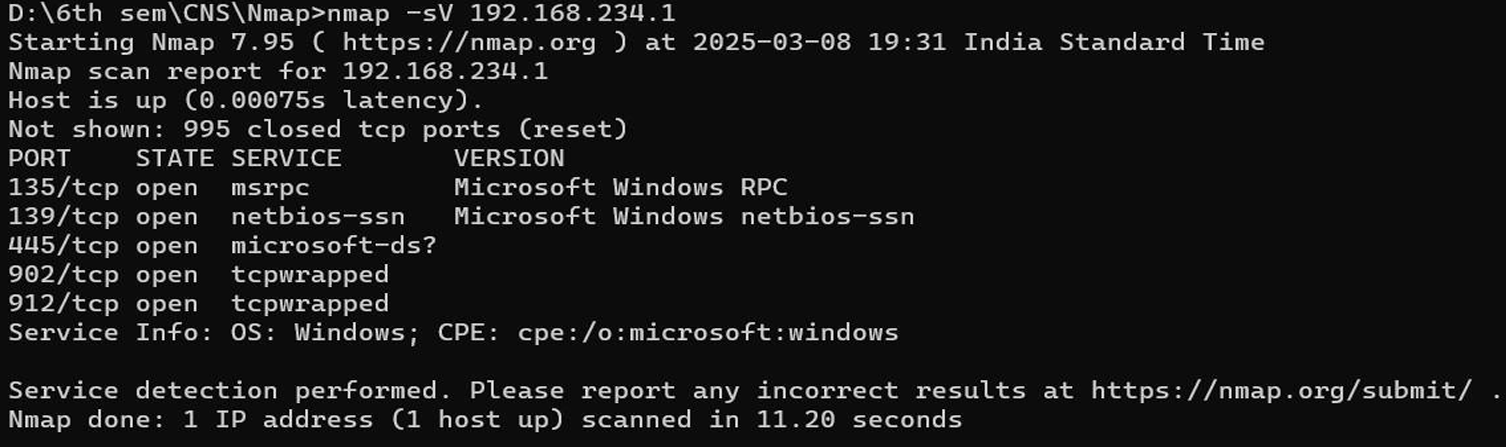
des- Detects the operating system of the target.

****

1. **Service Version Detection:**

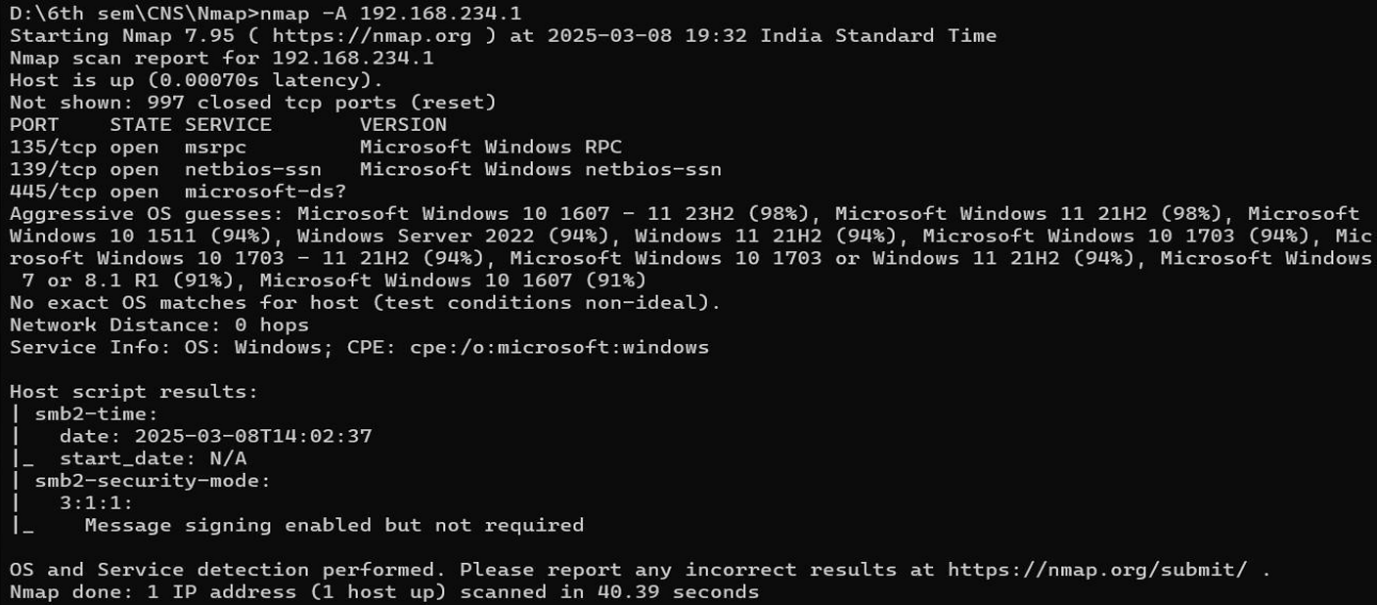
cmd- nmap -sV <target ip>

des- Identifies versions of running services.

****

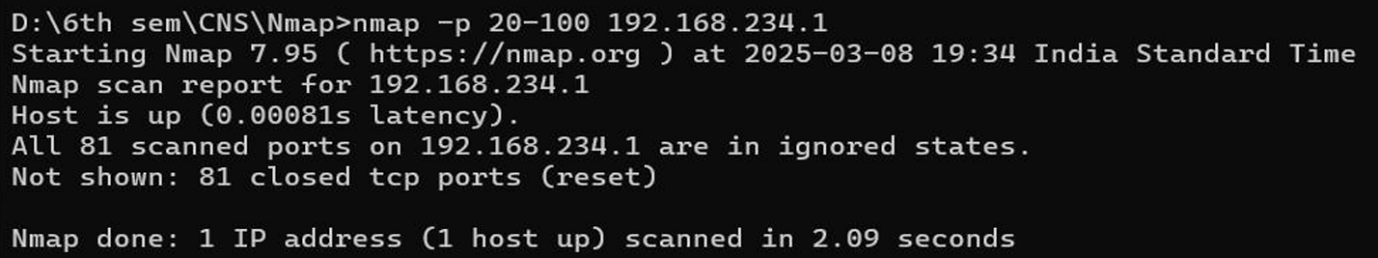
1. **Aggressive Scan:**

cmd- nmap -A <target\_ip>

****des- Performs OS detection, version detection, script scanning, and traceroute.

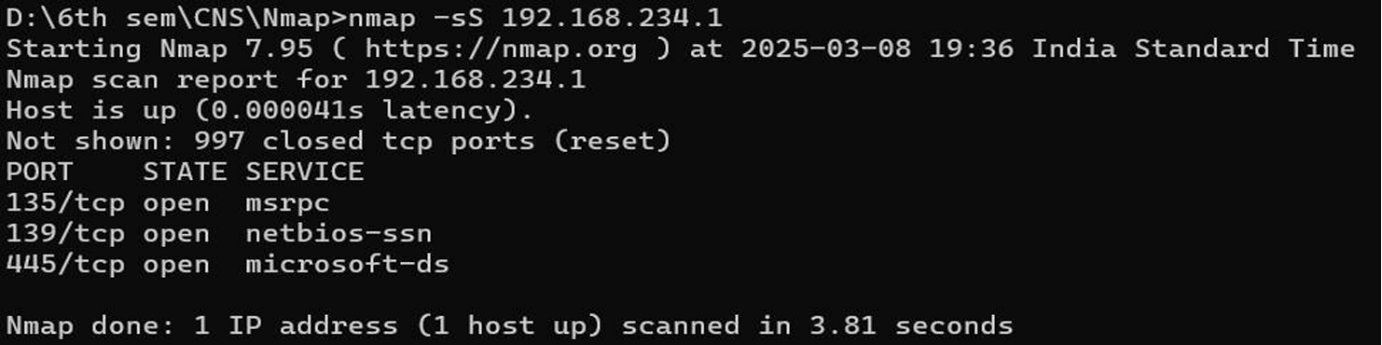
1. **Port Range Scan:**

cmd- nmap -p 20-100 <target\_ip>

****des- Scans ports 20 to 100 for open services.

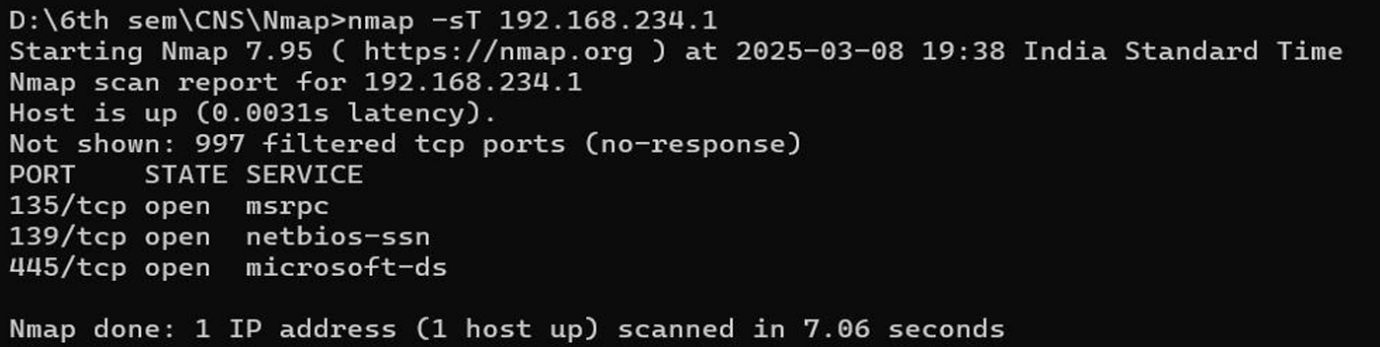
1. **TCP SYN Scan:**

cmd- nmap -sS <target\_ip>

****des- Performs a stealthy SYN scan to detect open ports without establishing full connections.

1. **TCP Connect Scan:**

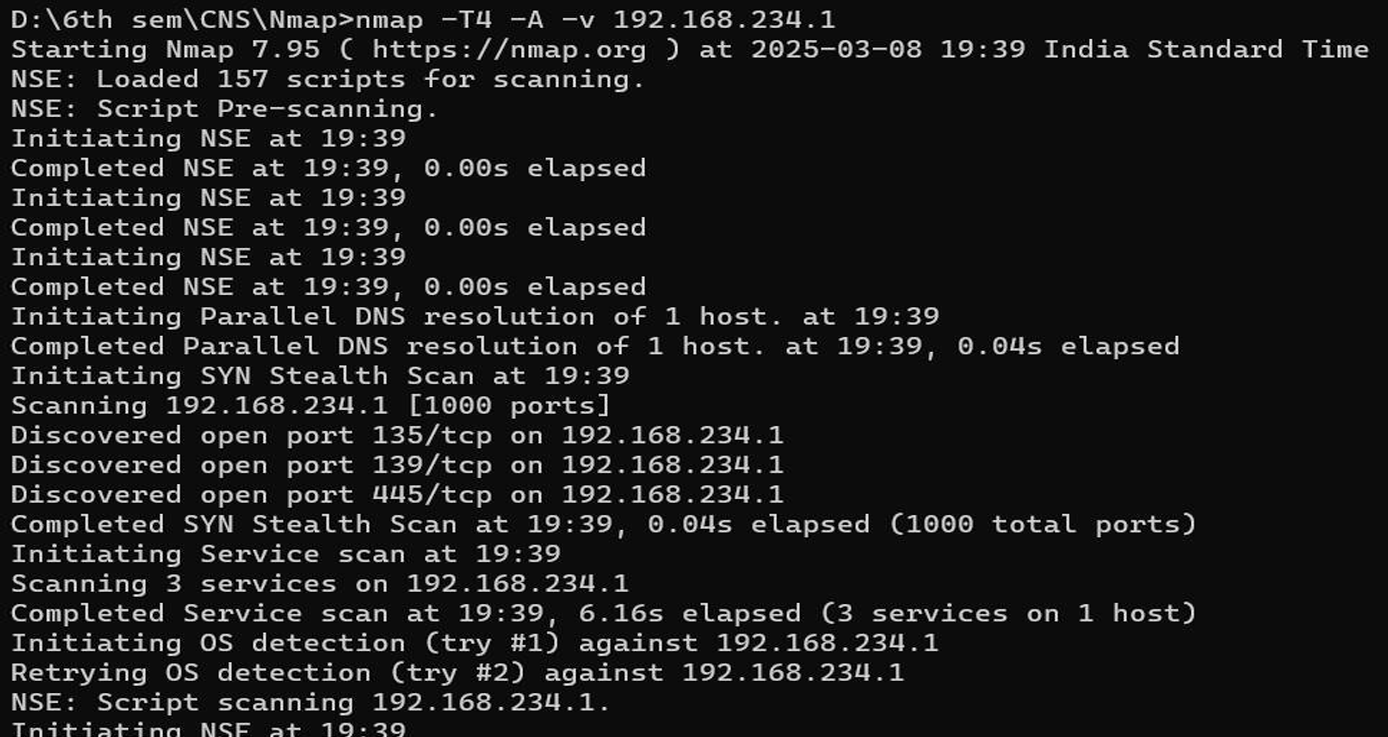
cmd- nmap -sT <target\_ip>

****des- Establishes a full TCP connection to detect open ports.

1. **Comprehensive Scan:**

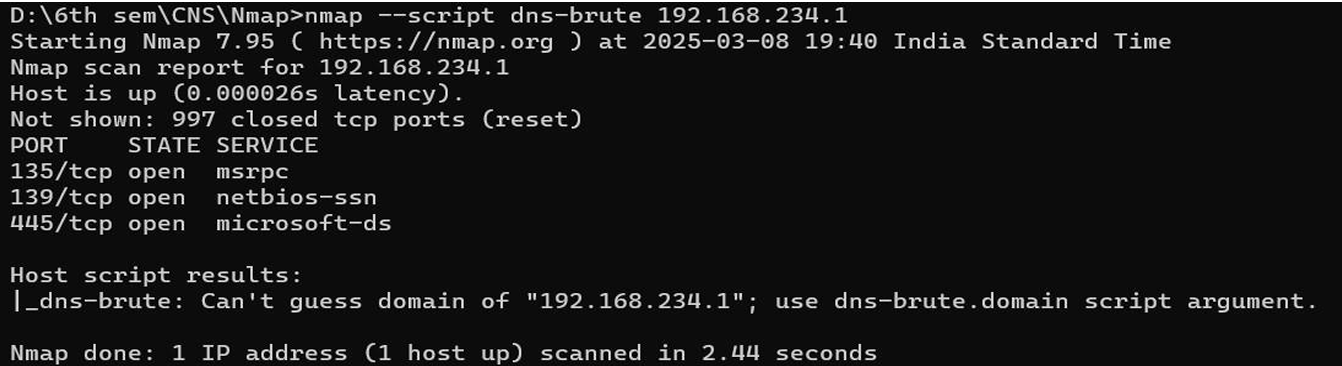
cmd- nmap -T4 -A -v <target ip>

des- Performs a detailed scan with aggressive timing and verbosity.

****

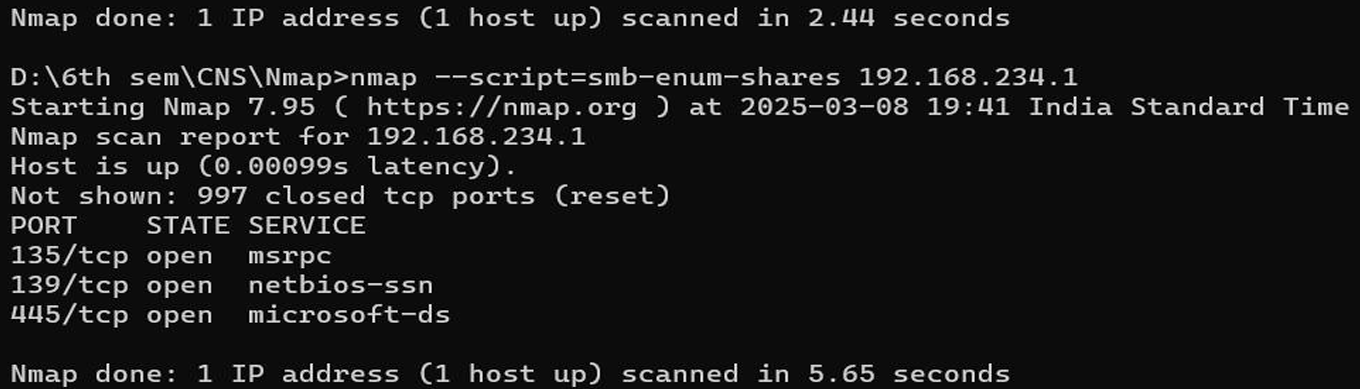
1. **DNS Brute Force Scan:**

cmd- nmap --script dns-brute <target\_ip>

****des- Attempts to enumerate subdomains using DNS brute force.

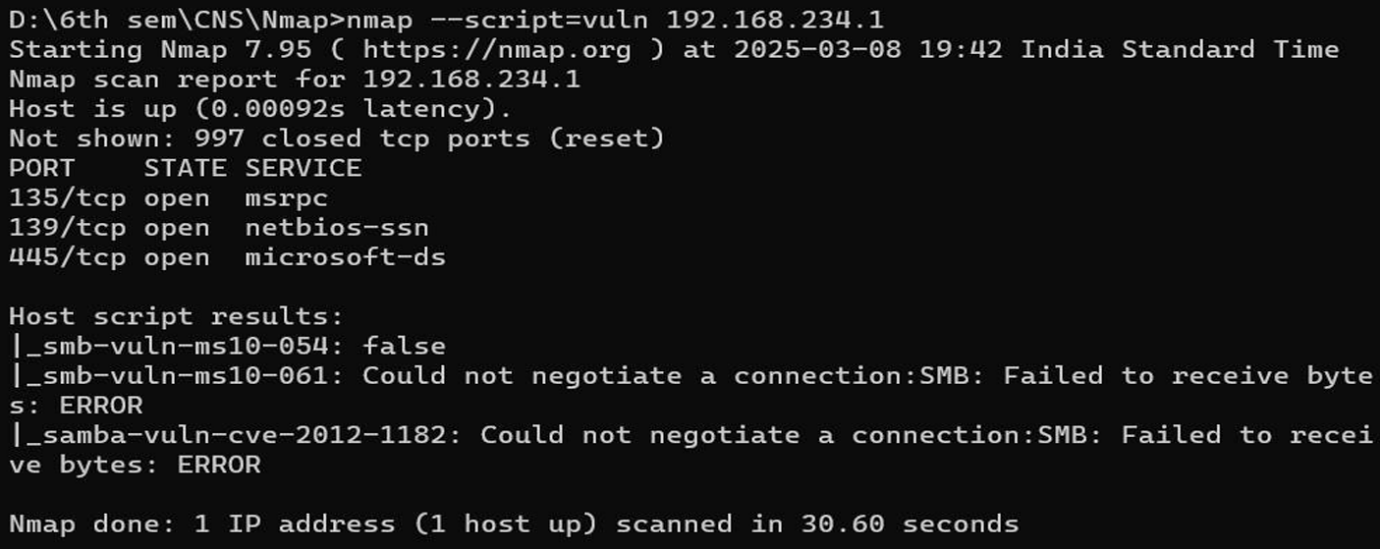
1. **SMB Enumeration:**

cmd- nmap --script=smb-enum-shares <target\_ip>

****des- Identifies shared folders on an SMB server.

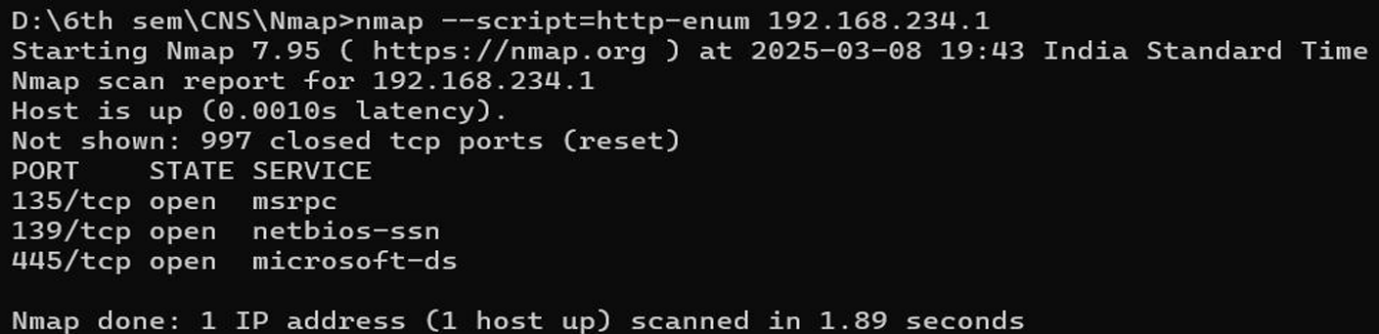
1. **Vulnerability Scan:**

cmd- nmap --script=vuln <target ip>

****des- Scans for known vulnerabilities on the target.

1. **HTTP Enumeration:**

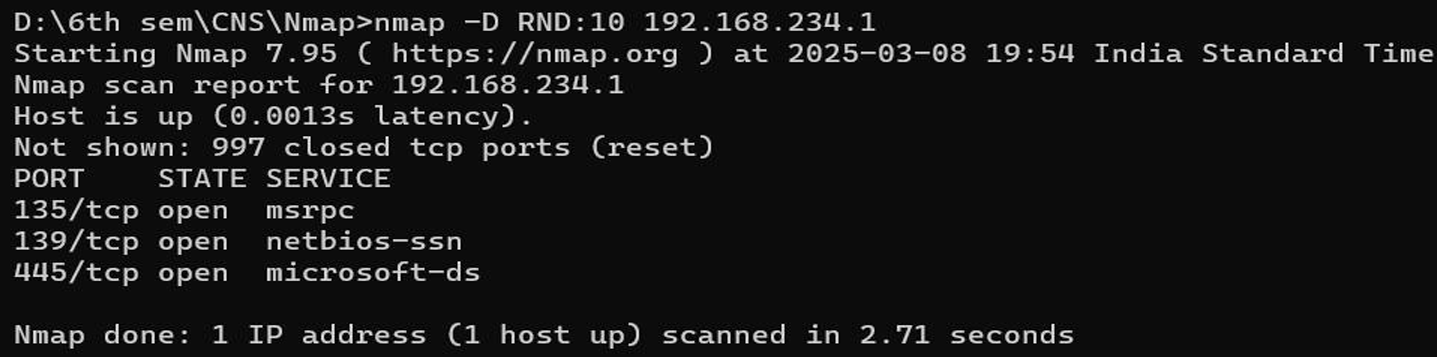
cmd- nmap --script=http-enum <target\_ip>

****des- Enumerates directories and files hosted on a web server.

1. **Decoy Scan:**

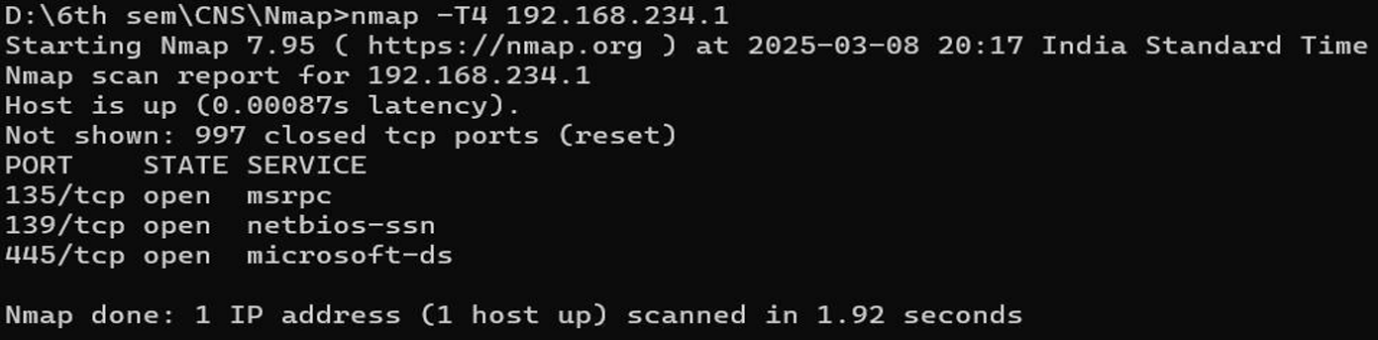
cmd- nmap -D RND:10 <target\_ip>

des- Uses random decoys to obscure the true scanning source.

****

1. **Fast Scanning:**

cmd- nmap -T4 <target\_ip>

****des- Uses a faster scanning method.

1. **Counter measures to Prevent DoS Attacks**
2. Deploy Firewalls & Apply Rate Limiting o Configure iptables or similar firewall rules

to restrict excessive connection requests.

1. Utilize DDoS Protection Services o Implement cloud-based security solutions like

Cloudflare, AWS Shield, or Akamai to mitigate large-scale attacks.

1. Enable SYN Flood Protection o Activate SYN cookies to prevent attackers from

exhausting server resources through SYN flood attacks.

1. Set Up Intrusion Detection & Prevention Systems (IDS/IPS) o Use tools such as

Snort, Suricata, or Fail2ban to monitor network traffic and block suspicious activities.

1. Manage Access with IP Filtering o Identify and block malicious IP addresses while

whitelisting trusted sources to ensure secure access.

1. **Wireshark Traffic Analysis**

Monitor Regular Network Traffic

• Launch Wireshark and apply a filter to capture routine communication:

ip.src == <your\_ip> && ip.dst == <target\_ip>

Detect DoS Attack Traffic

• While executing the attack, track an unusual surge of SYN packets by using:

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