REPORT ON SCANNING NETWORK

-TANMAY KHEDEKAR

Table of Content:

INTRODUCTION

In today’s digital landscape, where organizations increasingly rely on interconnected systems and online services, cybersecurity has become a critical concern. One of the foundational steps in securing a network or application is conducting a comprehensive **security scan**. Scanning is a proactive approach used to identify potential vulnerabilities, misconfigurations, and exposure points in a system before they can be exploited by malicious actors.

The scanning phase is typically performed during the early stages of a vulnerability assessment or penetration test. It involves the systematic discovery of live hosts, open ports, running services, and software versions, followed by the detection of known vulnerabilities associated with them. Tools such as **Nmap**, **Nessus**, **Nikto**, and **OWASP ZAP** are commonly used to perform different types of scans, including port scanning, vulnerability scanning, web application scanning, and network discovery.

The objective of scanning is not only to detect weaknesses but also to understand the system's current security posture and guide remediation efforts effectively. By identifying and categorizing vulnerabilities based on severity, organizations can prioritize fixes, reduce attack surfaces, and strengthen their overall defense mechanisms.

This report presents the findings from a scanning exercise conducted on <<target environment>>, with the goal of identifying potential security risks. The results will assist stakeholders in understanding existing threats, assessing risk levels, and implementing appropriate countermeasures to protect critical assets.

TYPES OF SCANNING-

1. Port Scanning

- Identifies open, closed, or filtered ports on a system.
- Helps determine what services are running (HTTP, FTP, SSH, etc.).
- Tools: **Nmap, Angry IP Scanner**.
- Types of port scans:
  - **TCP connect scan**
  - **SYN (Half-open) scan**
  - **UDP scan**
  - **FIN, Xmas, NULL scans** (used for stealth scanning)

2. Network Scanning

- Discovers **live hosts**, devices, and network topology.
- Identifies IP addresses, MAC addresses, OS, and running services.
- Tools: **Nmap, Advanced IP Scanner, Wireshark**.

3. Vulnerability Scanning

- Scans systems and applications for **known vulnerabilities** (misconfigurations, outdated software, missing patches).
- Uses vulnerability databases (CVE, NVD).
- Tools: **Nessus, OpenVAS, Qualys**.

OBJECTIVE

The main objective of scanning in cyber security is to identify potential weaknesses, open doors, and risks in a computer system, network, or application before attackers can misuse them. Scanning acts like a **security check-up** that provides detailed information about the target environment.

First, scanning helps to **detect active devices and services** in a network. This allows security teams to understand what systems are running, what ports are open, and which applications are accessible. If attackers can find this information, they might exploit it, so ethical hackers and administrators scan first to stay one step ahead.

Second, scanning aims to **find vulnerabilities and misconfigurations**. Outdated software, weak passwords, or unpatched systems are common entry points for cybercriminals. By identifying these issues early, organizations can fix them quickly.

Third, scanning supports **risk management and compliance**. Many industries require regular security checks to meet standards and protect sensitive data.

Finally, scanning helps to **reduce the attack surface** by showing which unnecessary services should be closed or removed. This makes the system stronger and harder to break into.

In short, the objective of scanning is not only to discover weaknesses but also to provide the knowledge needed to secure systems, prevent attacks, and maintain trust in digital environments.

LAB 1- HOST DISCOVERY

Host discovery is the process of identifying active devices or systems within a network. It is the first step in network scanning, where the goal is to find which IP addresses are live and responding. This helps security professionals understand the network's size, structure, and potential targets. Host discovery is often done using techniques like ICMP echo requests (ping), TCP SYN/ACK probes, or ARP requests. Once active hosts are identified, further scanning can be performed to check open ports, services, and vulnerabilities. In short, host discovery acts like a map to locate all available systems in a network.

OBJECTIVE OF LAB –

Perform host discovery using Nmap

TASK 1- HOST DISCOVERY USING NMAP

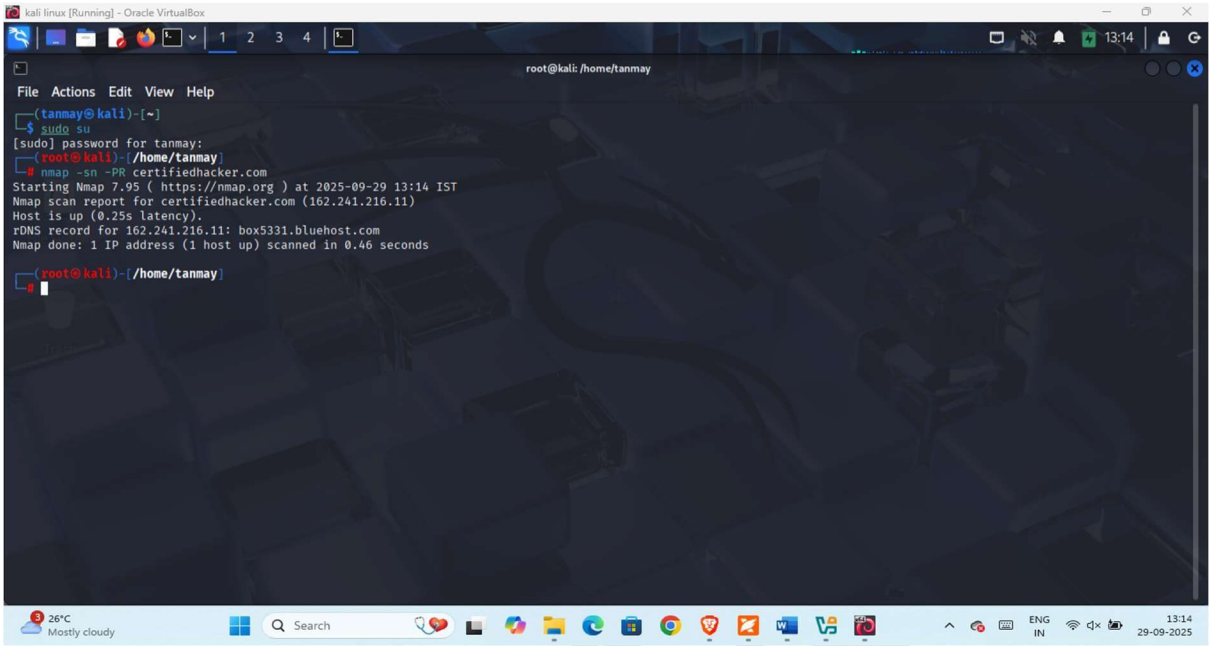
WHAT IS NMAP?

Nmap (Network Mapper) is a free, open-source tool used to discover hosts and services on a computer network. Security professionals and system admins use it for network inventory, port scanning, service/version detection, and basic vulnerability reconnaissance. It works by sending specially crafted packets to targets and analysing responses to learn which devices are alive, which ports are open, what services run there, and sometimes which operating system the host uses.

Key features

- Host discovery and port scanning (-p for ports).
- Service/version detection (-sV).
- OS detection (-O).
- Aggressive scan mode combining several checks (-A).
- Powerful scripting engine (NSE) for automated checks and exploits.

1} ARP PING SCANNING

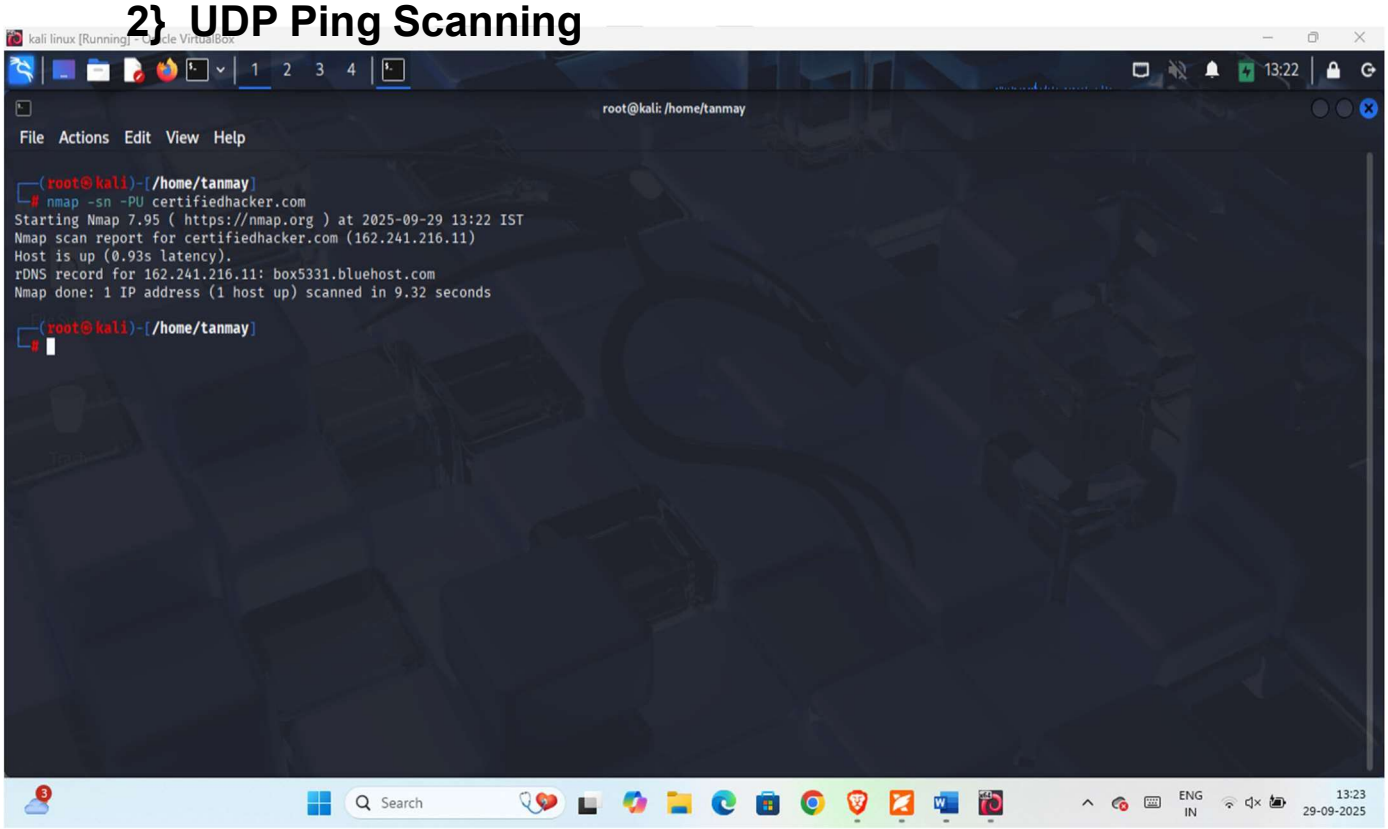


COMMAND - nmap -sn -PR (TARGET IP)

NOTE: sn- Disable port scan

PR- Performs APR ping Scanning

2} UDP Ping Scanning

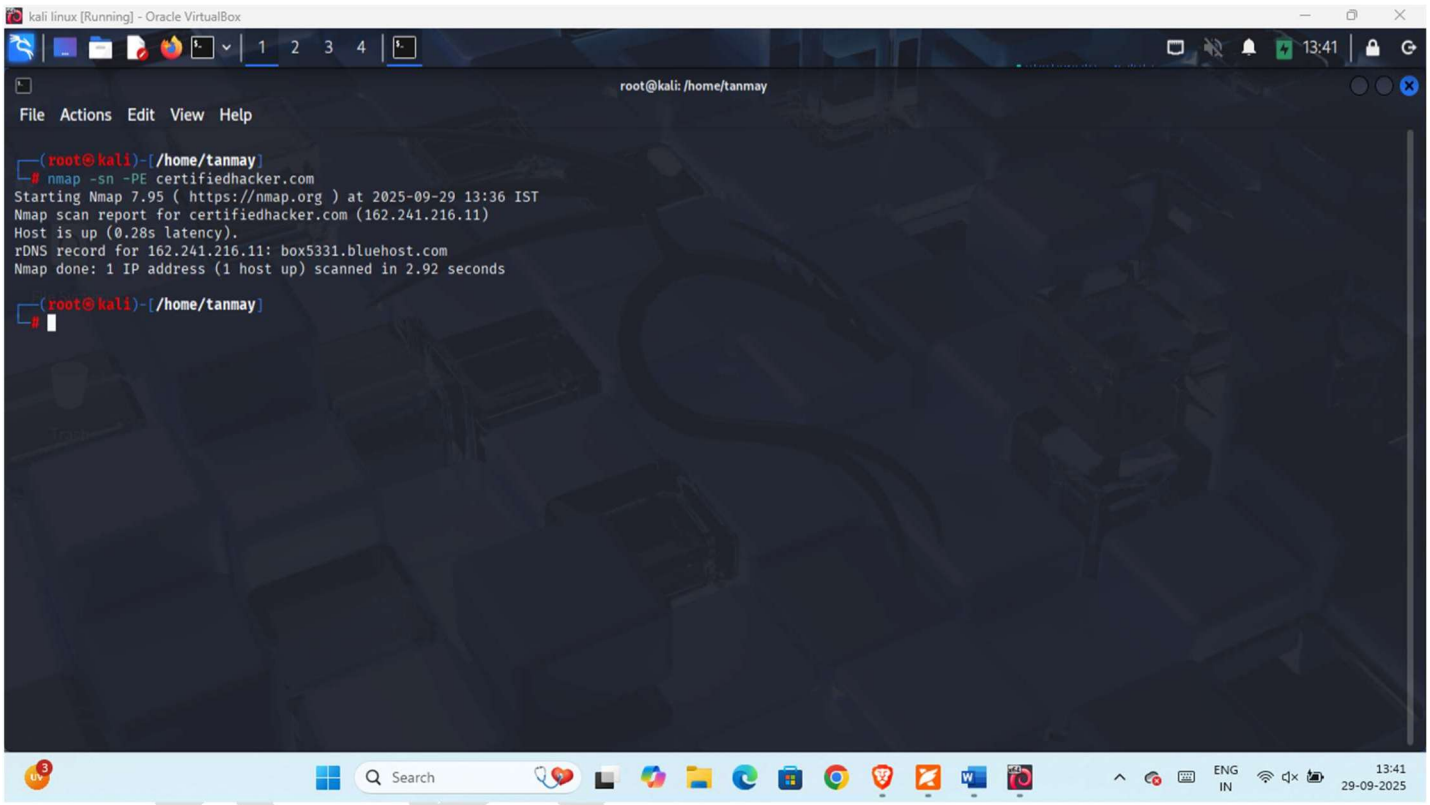


COMMAND - nmap -sn -PU (TARGET IP)

NOTE: sn- Disable port scan

PR- Performs UDP ping Scanning

3} ICMP ping Scanning

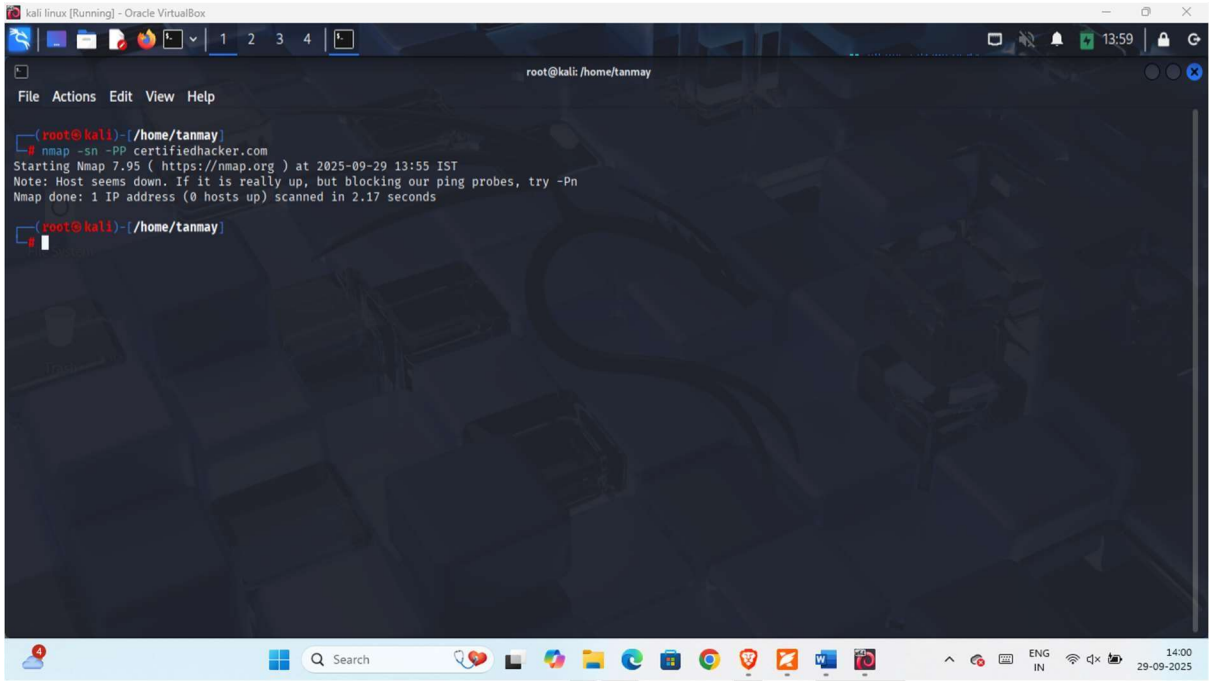


COMMAND - nmap -sn -PE (TARGET IP)

NOTE: sn- Disable port scan

PE- Performs ICMP ECHO ping Scanning

4. ICMP Timestamp ping Scanning

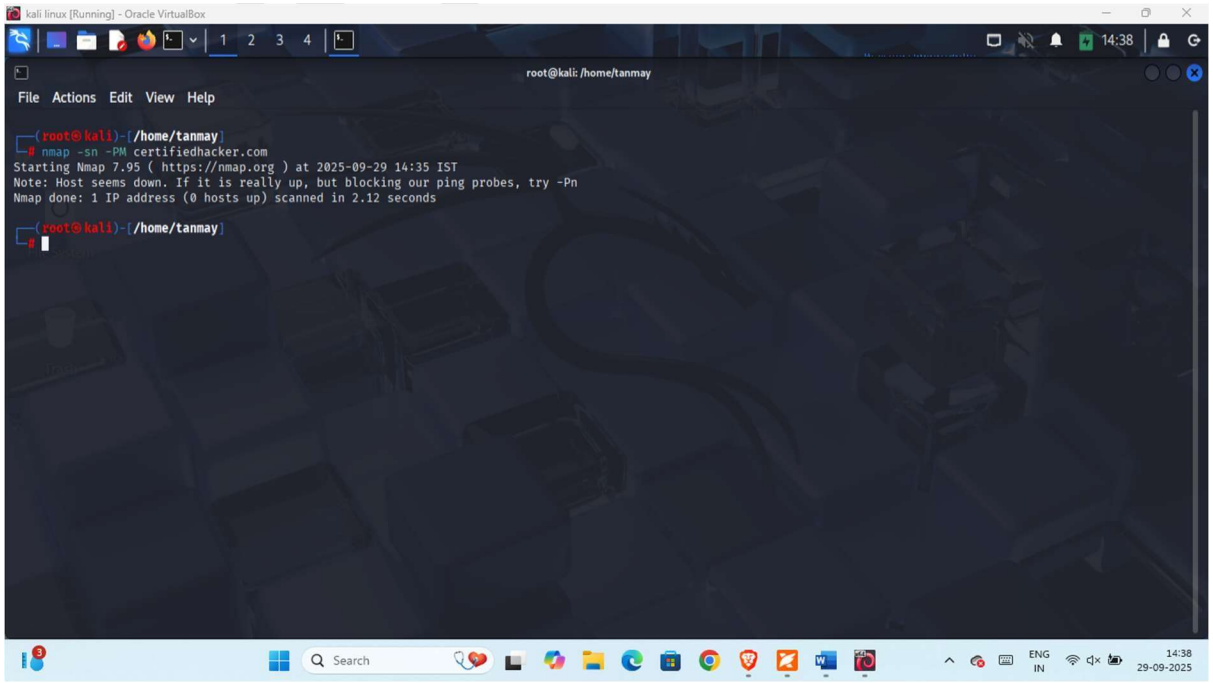


COMMAND - nmap -sn -PP (TARGET IP)

NOTE: sn- Disable port scan

PP- Performs ICMP timestamp ping Scanning

5. ICMP Address mac Ping Scanning



LAB 2- Perform Port and Services Discovery

Port and services discovery is the process of finding which network ports are open on a system and identifying the services running on them. It is an important step in scanning because open ports often act as entry points for attackers.

- Ports are virtual communication endpoints. Each service (like HTTP, FTP, SSH) runs on a specific port. For example, port 80 is used for HTTP, 443 for HTTPS, and 22 for SSH.
- Port discovery helps detect whether these ports are open, closed, or filtered (blocked by a firewall).
- Service discovery goes one step further. It checks what application or service is running on an open port and sometimes even its version. For example, port 80 may be running Apache HTTP Server version 2.4.49.

Techniques used:

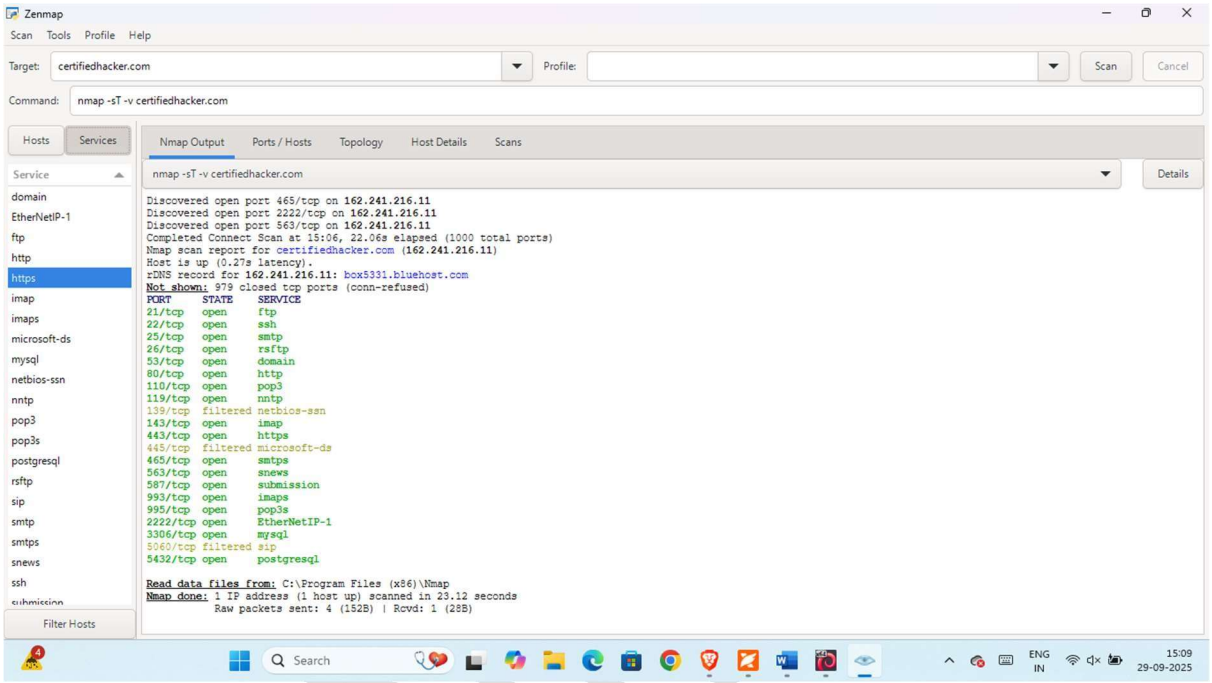
- TCP connect scan and SYN scan for finding open ports.
- UDP scan for identifying UDP-based services.
- Service/version detection (nmap -sV) to get detailed information.

LAB OBJECTIVE-

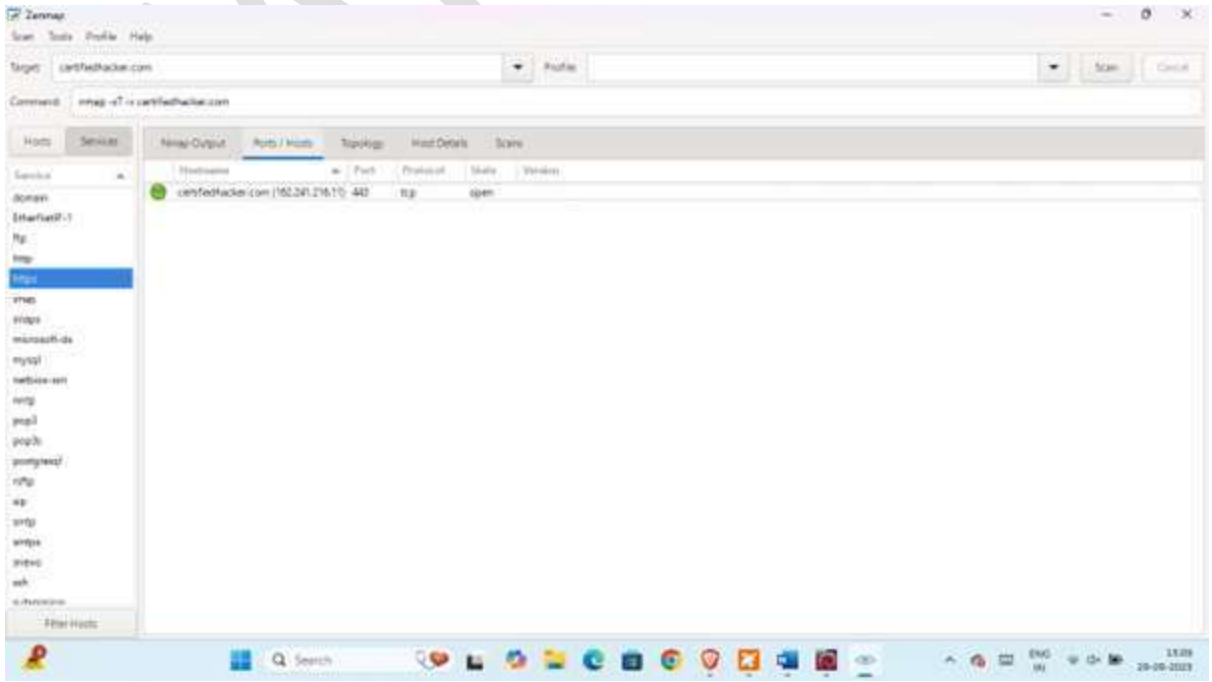
Explore Various networks scanning techniques using namp

Task 1- Explore Various Network Scanning Techniques using Nmap Tool.

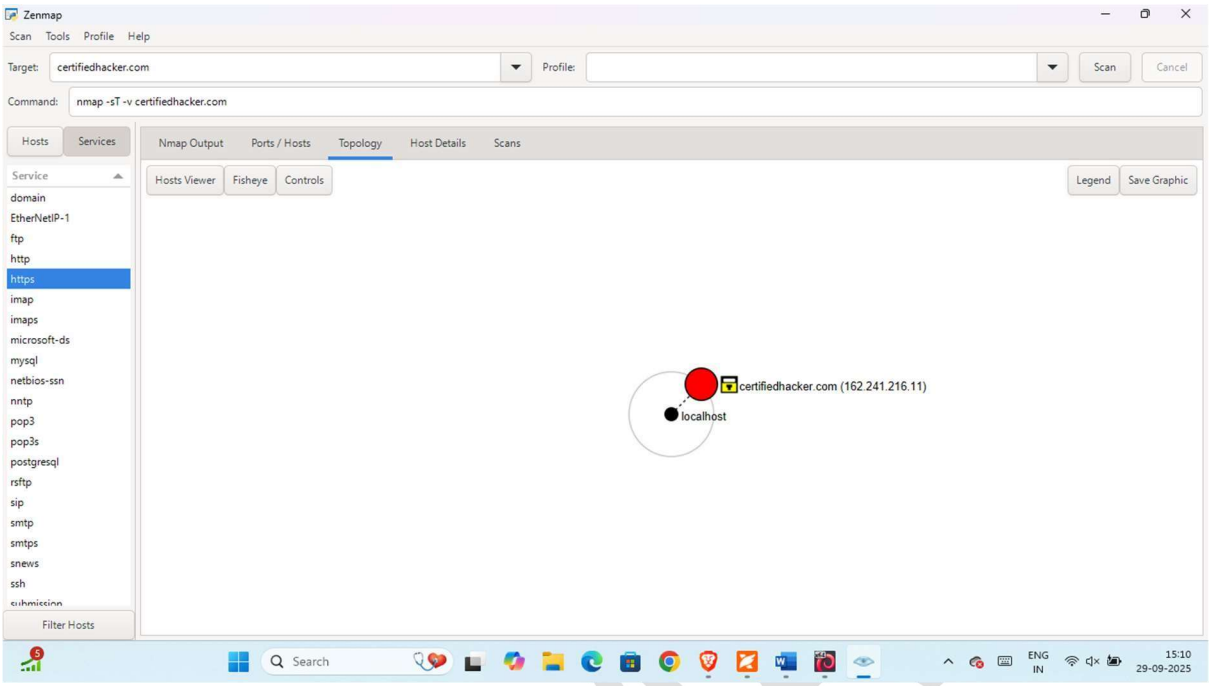
The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.



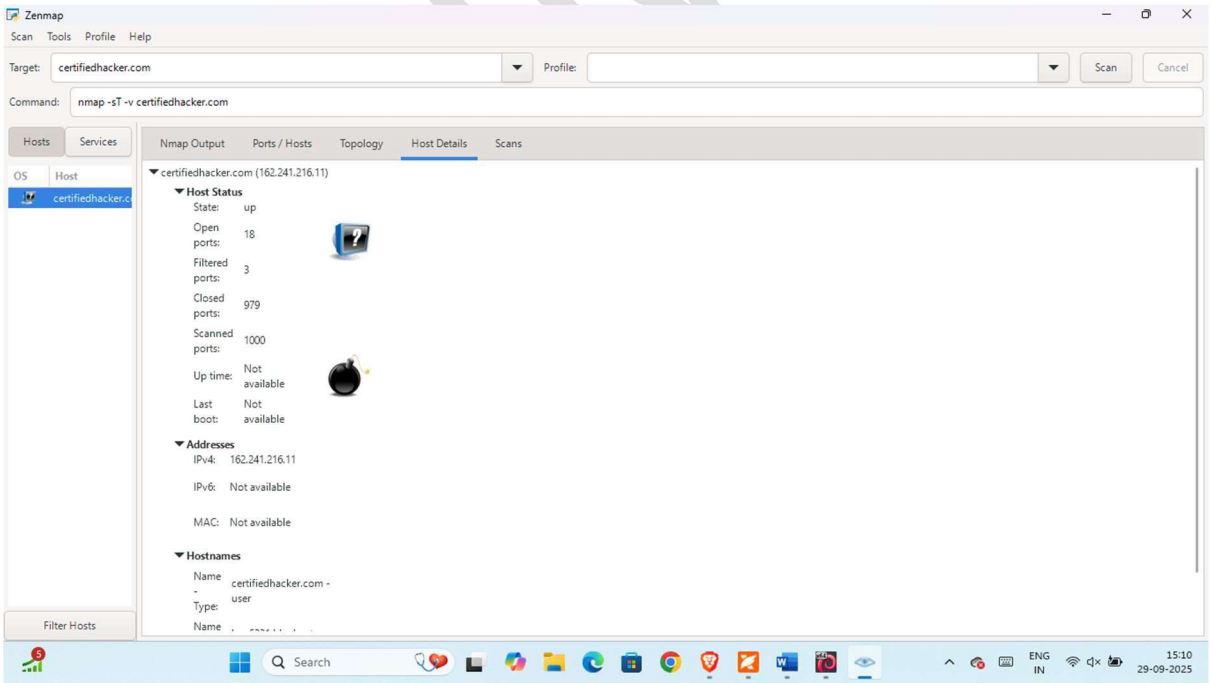
Clicking on the Ports/Hosts tab to gather more information on the scan results.



Clicking the Topology tab to view the topology of the target network that contain the provided IP address.



In the same way after clicking on the Host Details it shows the details of the TCP connect scan.

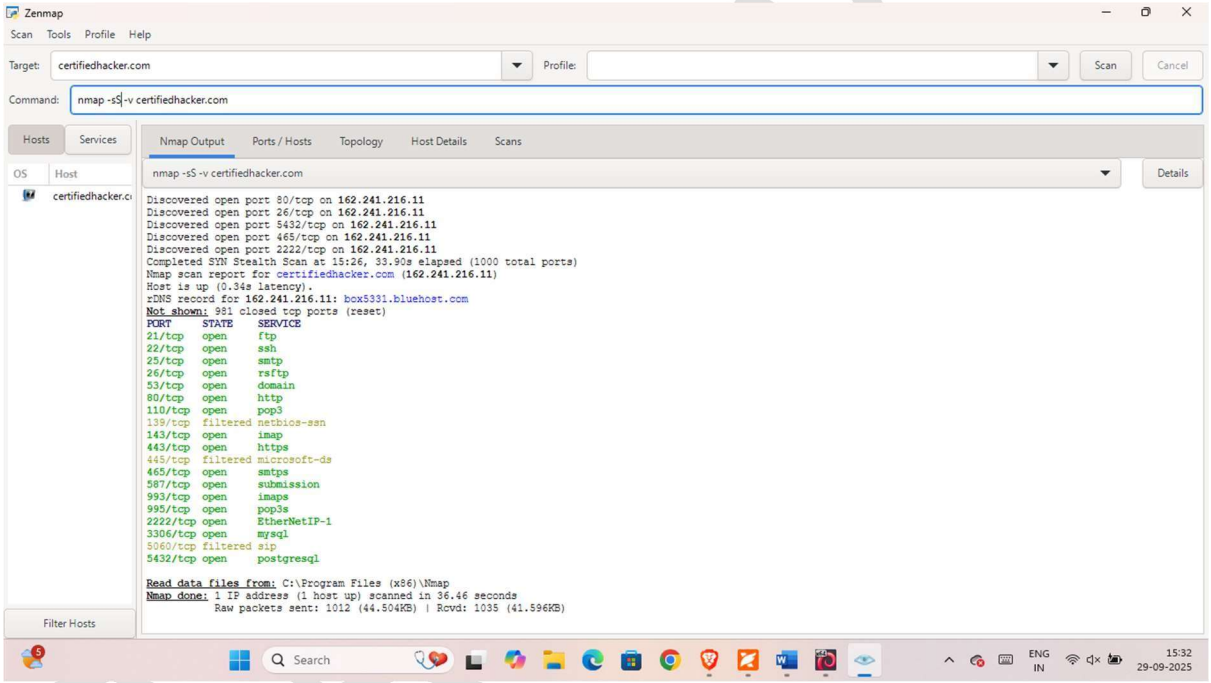


In this this scenario we perform the stealth scan, Xmas scan, TCP Maimon scan and ACK Flag probe on a firewall-enabled machine.

Stealth scan/TCP half-open scan:

In this the scan Result Appear, display all the TCP ports and services running on the target machine, as shown in the screenshot. **(Target-Certifiedhacker.com)**

Note: The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.



Command: - nmap -sS -v cetifedhacker.com

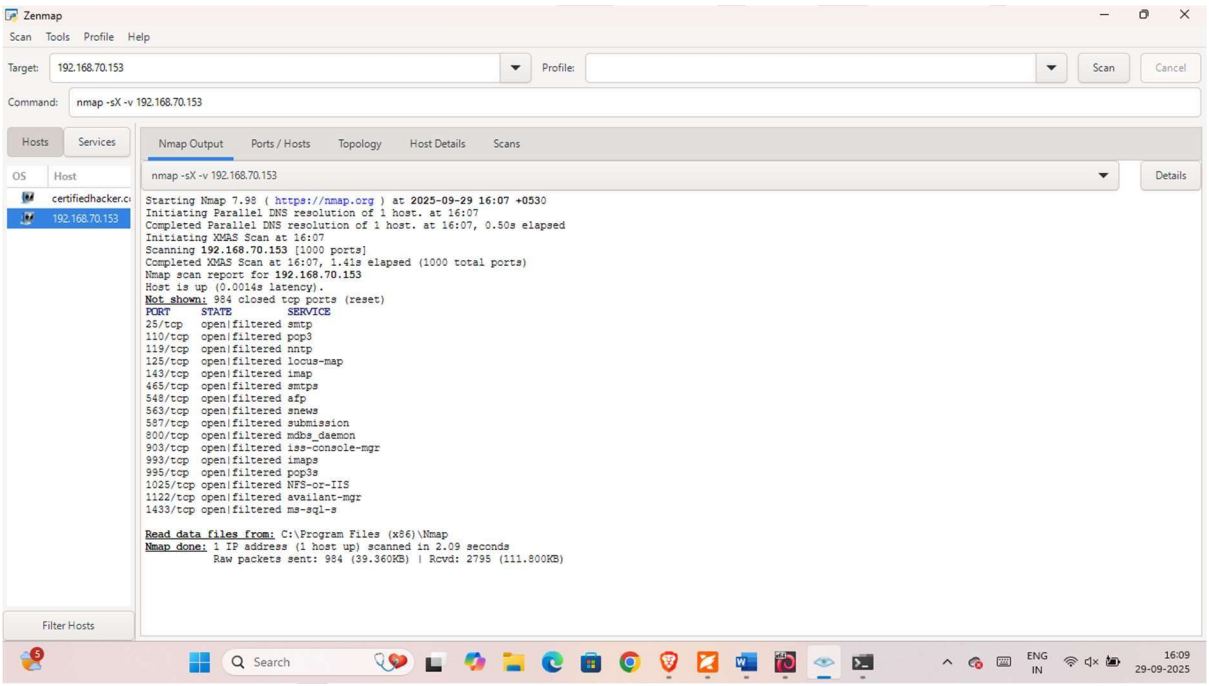
Note: -sS : perform the stealth scan/TCP half-open scan

-v: enable the verbose output

Xmas Scan:

The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.

Note: Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.



Command: - nmap -sX -v 192.168.70.153

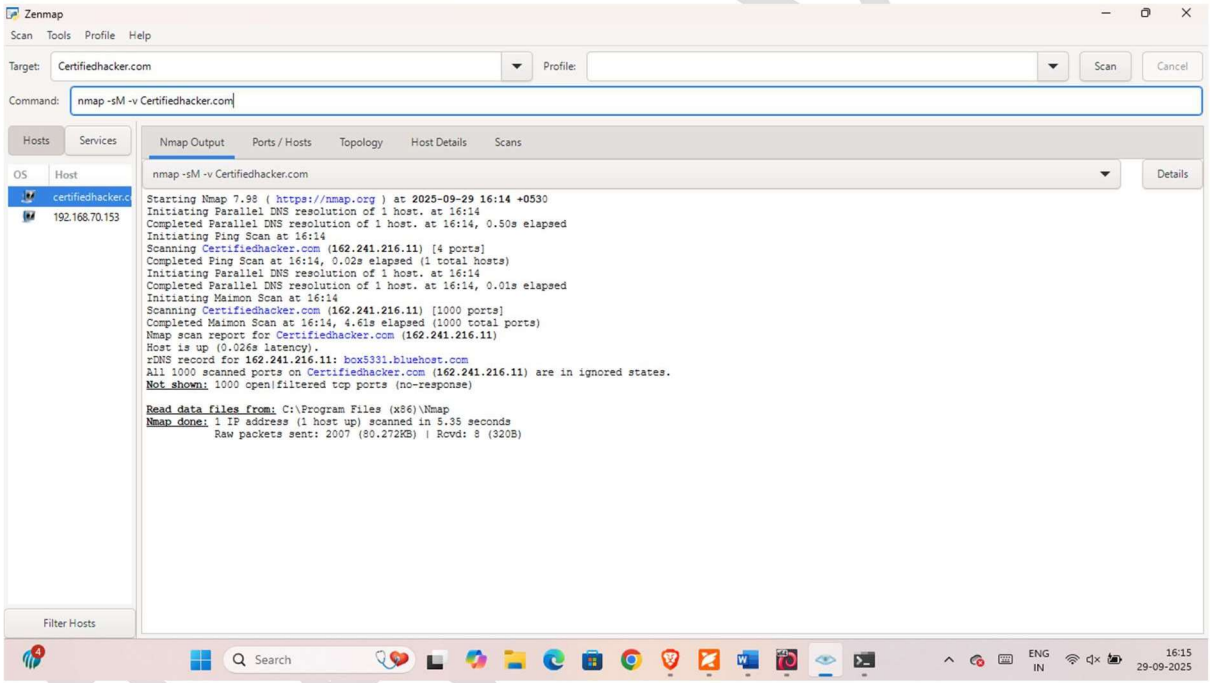
Note: -sX : perform the Xmas scan

-v: enable the verbose output

TCP Maimon scan:

The scan results appear, displaying either the ports are open/filtered on the target machine, which means a firewall has been configured on the target machine.

Note: In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open | Filtered, but if the RST packet is sent as a response, then the port is closed.



Command: - nmap -sM -v 192.168.70.153

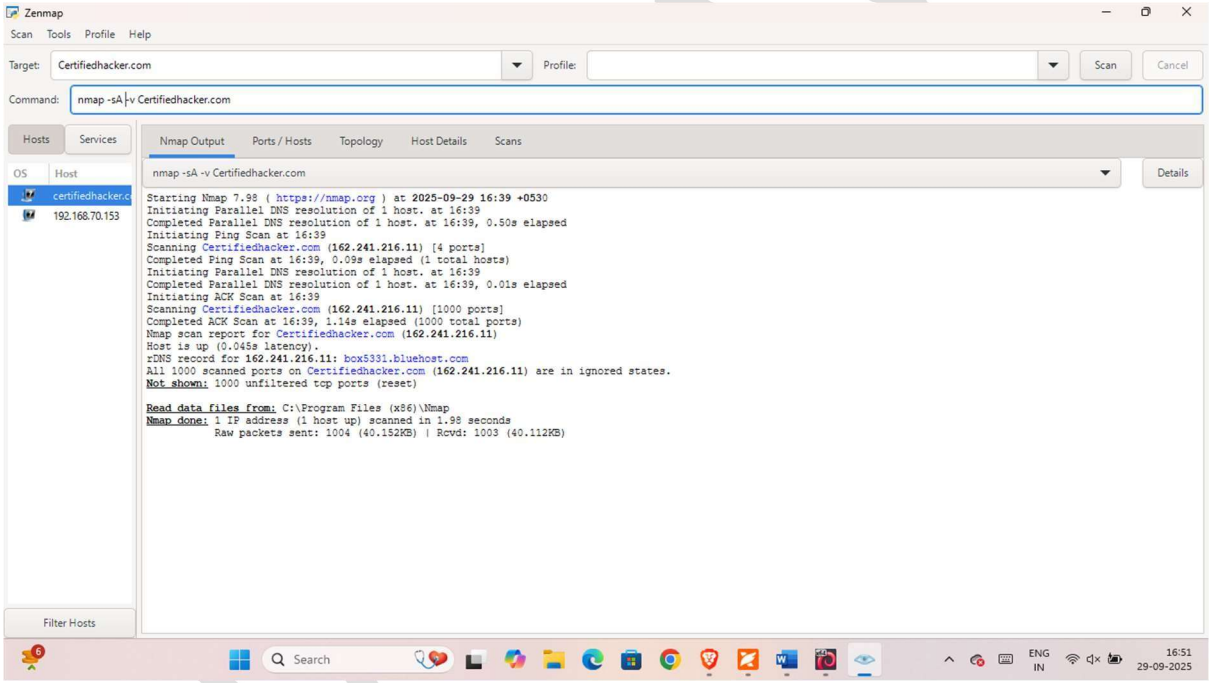
Note: -sM : perform the TCP Maimon scan

-v: enable the verbose output

ACK Flag probe scan:

The scan results appear, displaying that the ports are filtered on the target machine, as shown in the screenshot.

Note: The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered.



Command: - nmap -sA -v 192.168.70.153

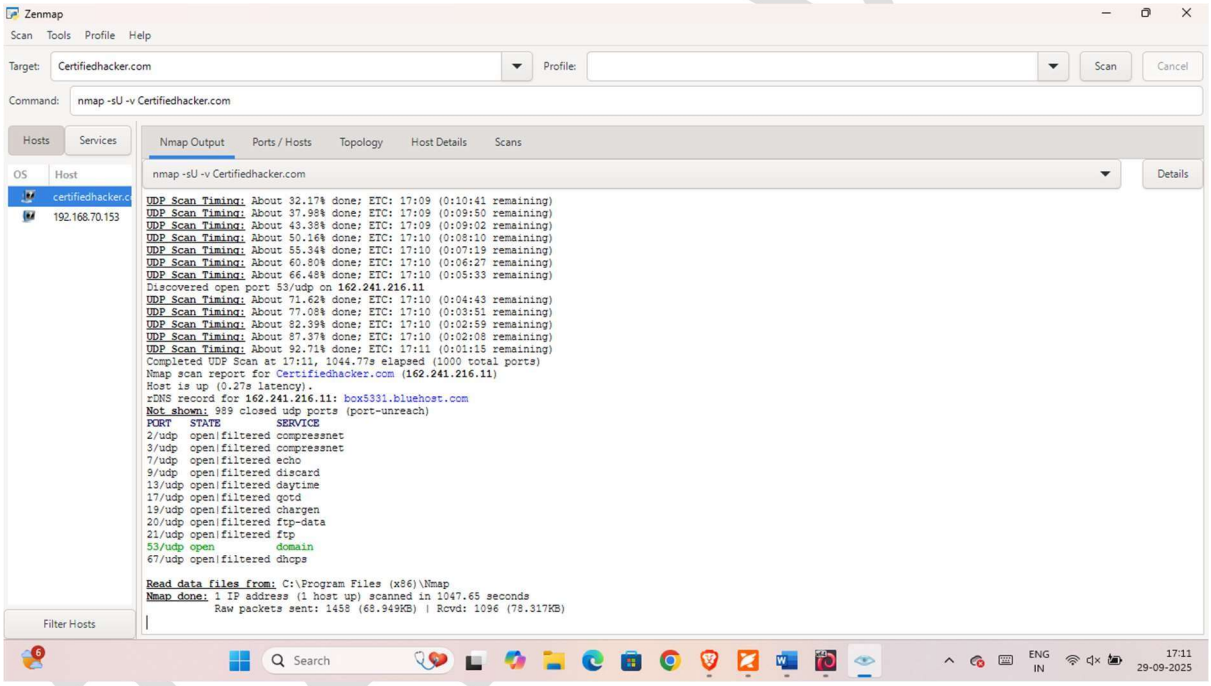
Note: -sA : performs the ACK flag probe scan

-v: enable the verbose output

UDP scan:

The scan results appear, displaying all open UDP ports and services running on the target machine, as shown in the screenshot.

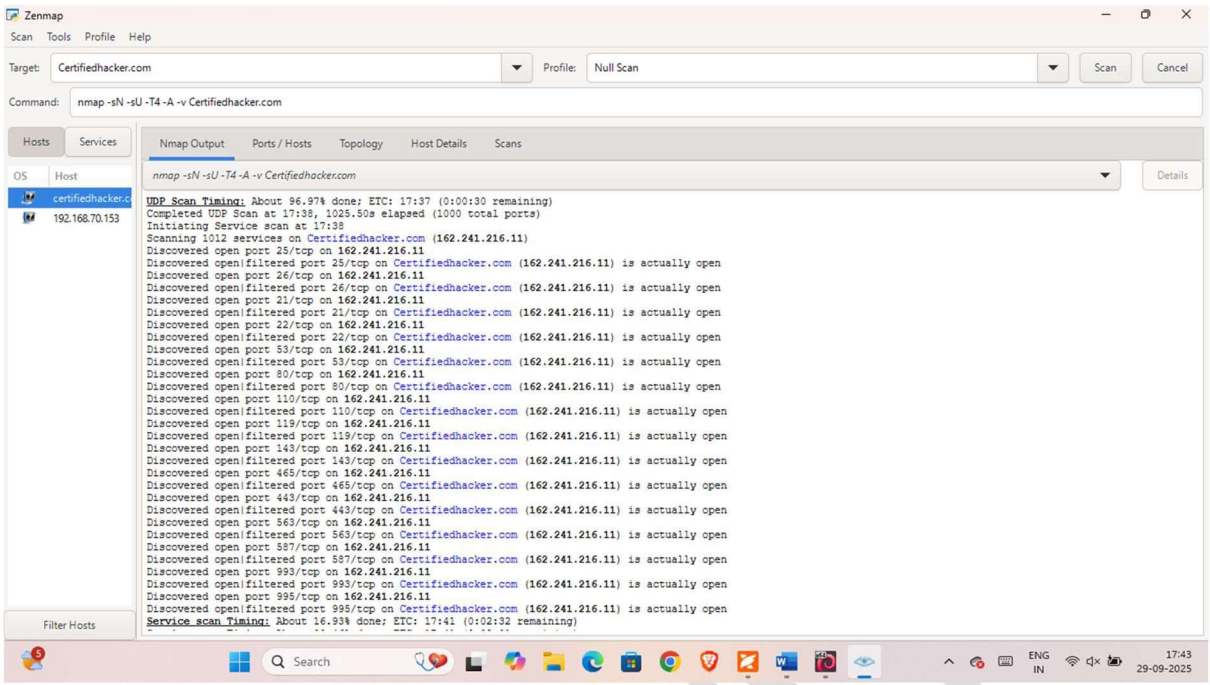
Note: The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received.



Command: - nmap -sU -v certifiedhacker.com

Note: -sU : performs the UDP scan

-v: enable the verbose output



Command- nmap -sN -sU -T4 -A -v certifiedhacker.com

Note: -sN: TCP null scan

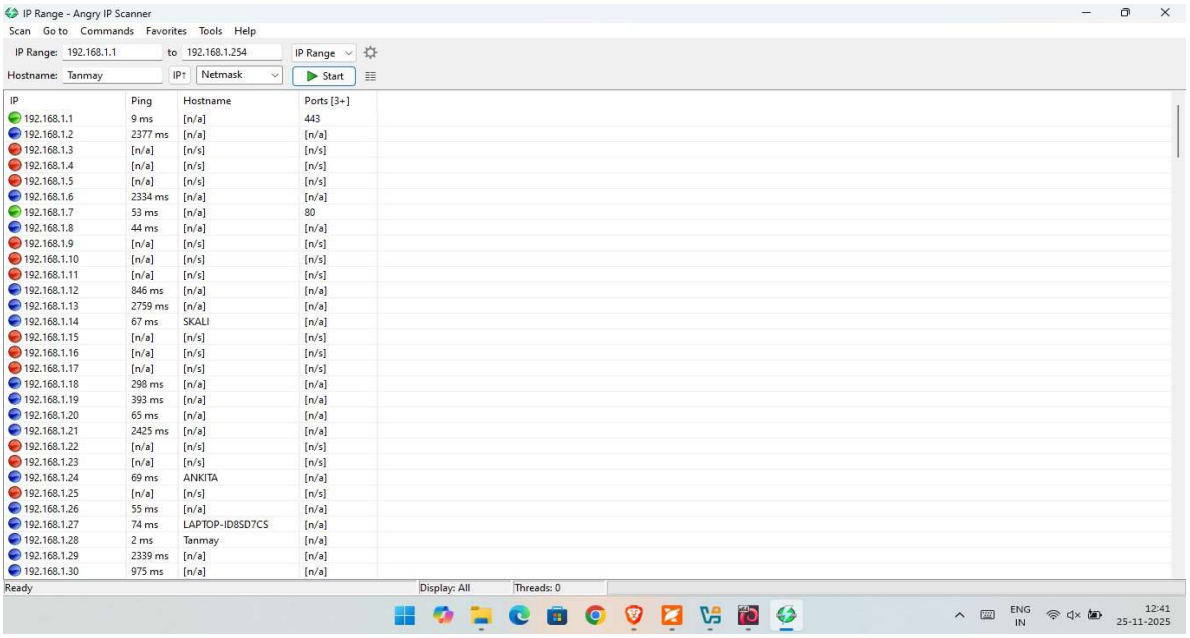
-sU: UDP scan

-T4: Aggressive scan

-A: Enable all advance aggressive scan

-v: enable the verbose output

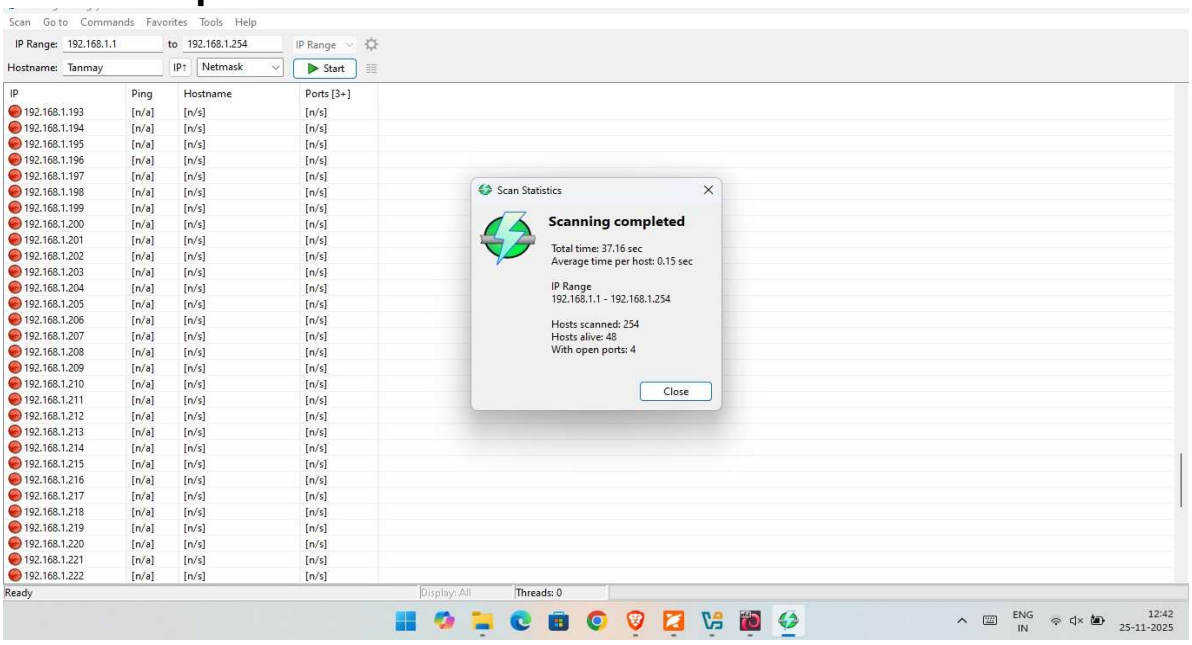
Host Discovery — Angry IP Scanner (Main Results)



Command / Tool used: Angry IP Scanner GUI — IP range 192.168.1.1 to 192.168.1.254

Detailed Explanation: This screenshot shows the list of scanned IPs in the subnet including IP, ping latency, discovered hostname and a basic open-ports indicator. Angry IP Scanner probes hosts using ICMP/TCP pings and simple port checks to determine if a host is alive. Hostnames discovered (e.g., Tanmay, LAPTOP-...) indicate devices that respond to NetBIOS/MDNS/Reverse DNS lookups.

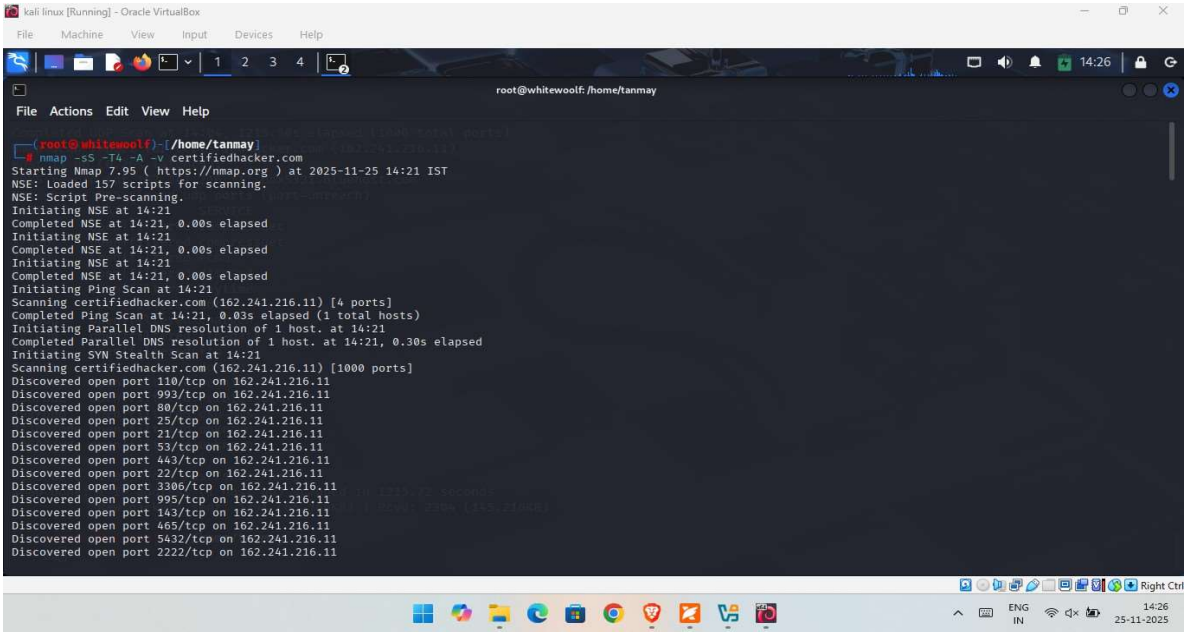
Scan Completion Statistics



Command / Tool used: Angry IP Scanner summary dialog (scan finished)

Detailed Explanation: This small dialog lists total scan time, average time per host, IP range scanned, hosts scanned count, hosts alive count and number of hosts with open ports. It verifies scan coverage and quick performance metrics.

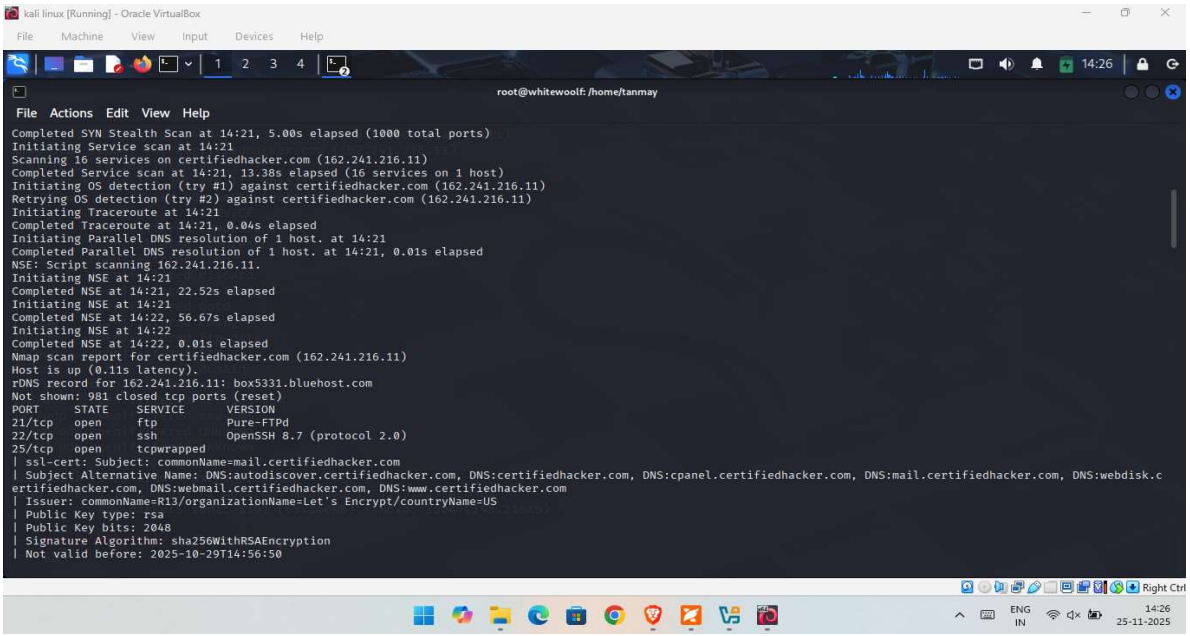
Nmap SYN Scan — Open Ports Overview



Command / Tool used: nmap -sS -T4 -v (SYN stealth scan, verbose)

Detailed Explanation: This Nmap output shows a SYN (half-open) scan where Nmap sends SYN packets and analyses responses (SYN/ACK, RST). It's faster and stealthier than a full connect scan. The output lists discovered open ports and notes on NSE scripts execution and DNS resolution.

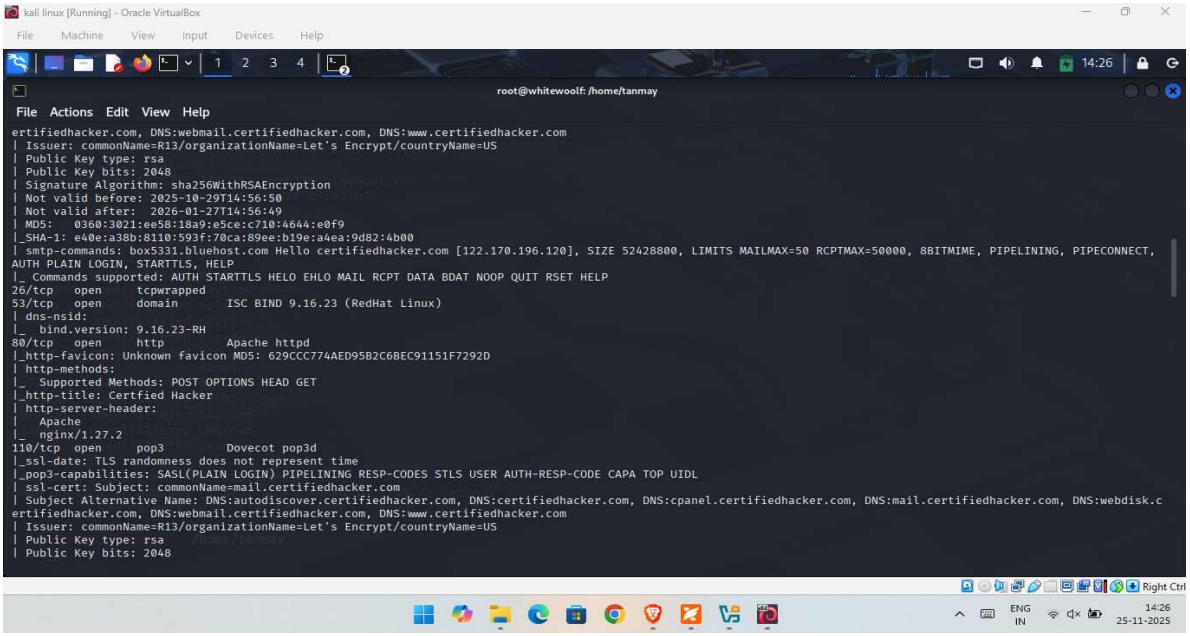
Nmap Service & Version Detection — Detailed Output



Command / Tool used: nmap -sV -A (service/version detection, OS detection, scripts)

Detailed Explanation: This screenshot contains verbose service/version detection output: open ports, service names, versions and SSL certificate details (issuer, subject alternative names). Nmap uses banner grabbing, probes and NSE scripts to gain additional context about running services.

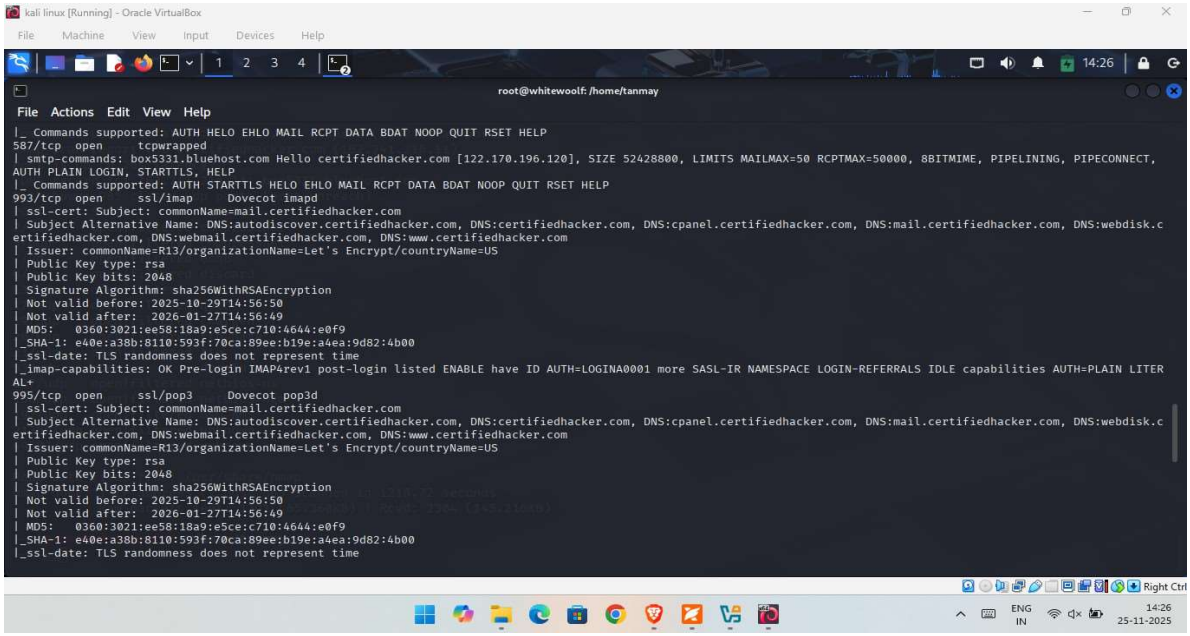
Nmap Service Detection — Additional Details



Command / Tool used: nmap -sV -A (continued)

Detailed Explanation: Continuation of the service detection output showing more ports and their service fingerprints. It may include product/versions and SMTP/IMAP capabilities. This level of detail helps prioritize vulnerability research for specific services.

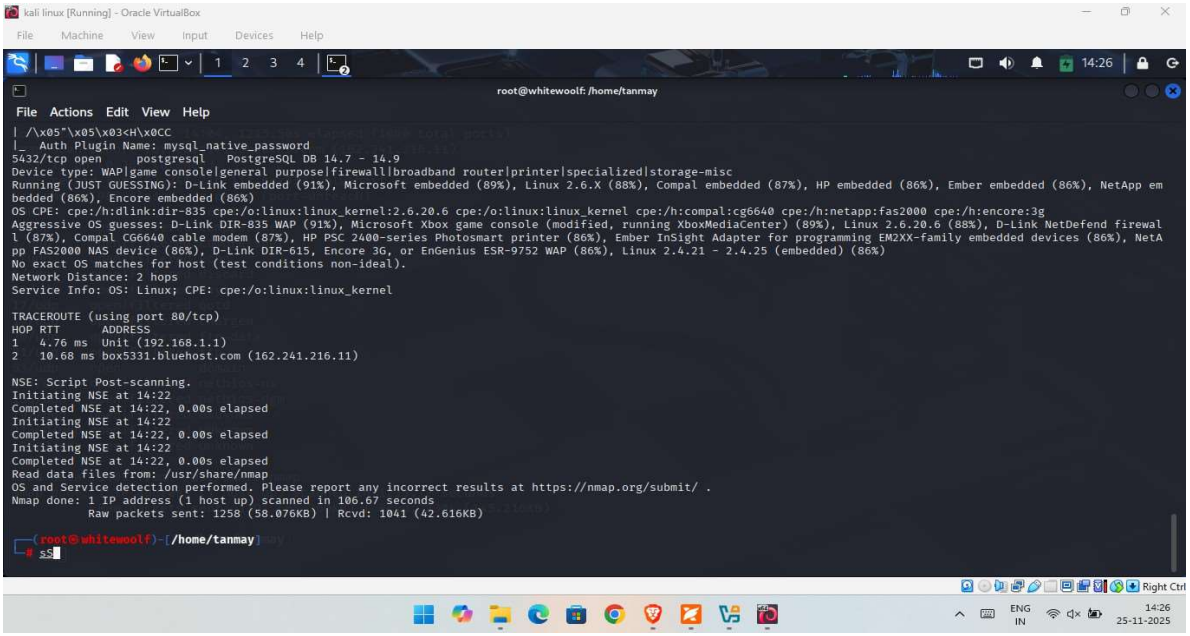
Nmap SSL & Certificate Details



Command / Tool used: nmap -sV --script ssl-cert (extract TLS certificate details)

Detailed Explanation: This output shows TLS certificate metadata discovered by Nmap: common name, SANs, issuer (Let's Encrypt), validity and public key details. Certificates expose hostnames and domains configured on the server.

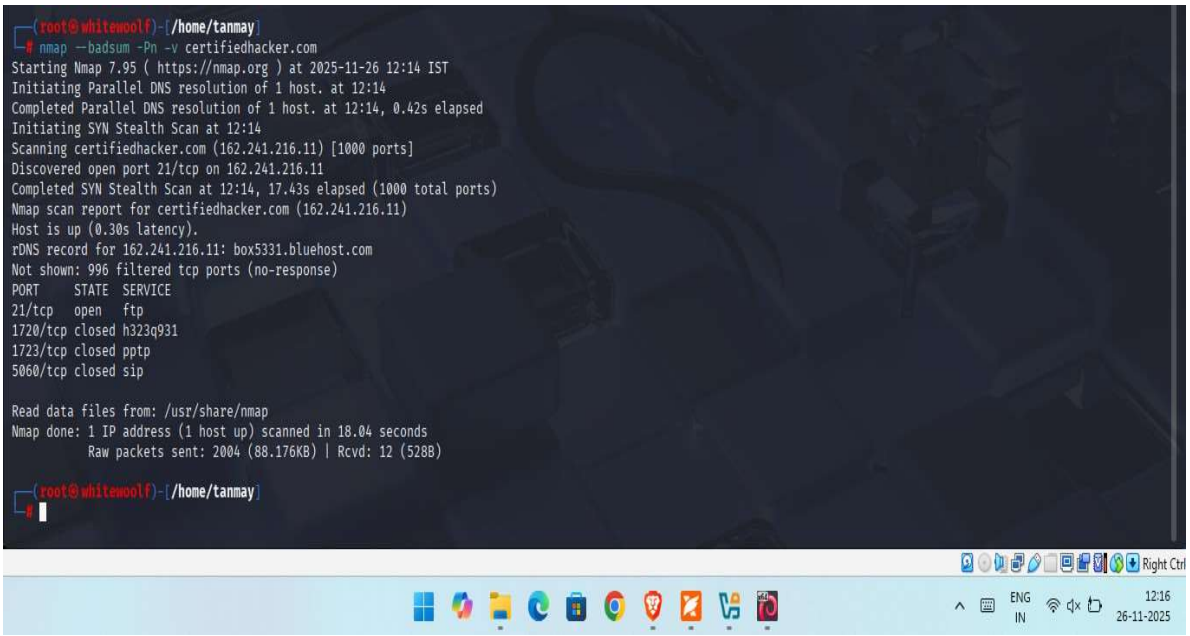
Nmap OS Detection & Aggressive Guesses



Command / Tool used: nmap -O -A (OS detection with aggressive heuristics)

Detailed Explanation: This screenshot shows Nmap's OS detection output including 'aggressive guesses' when a precise match isn't found. It lists probable device types and CPEs, and includes traceroute hops discovered during the scan.

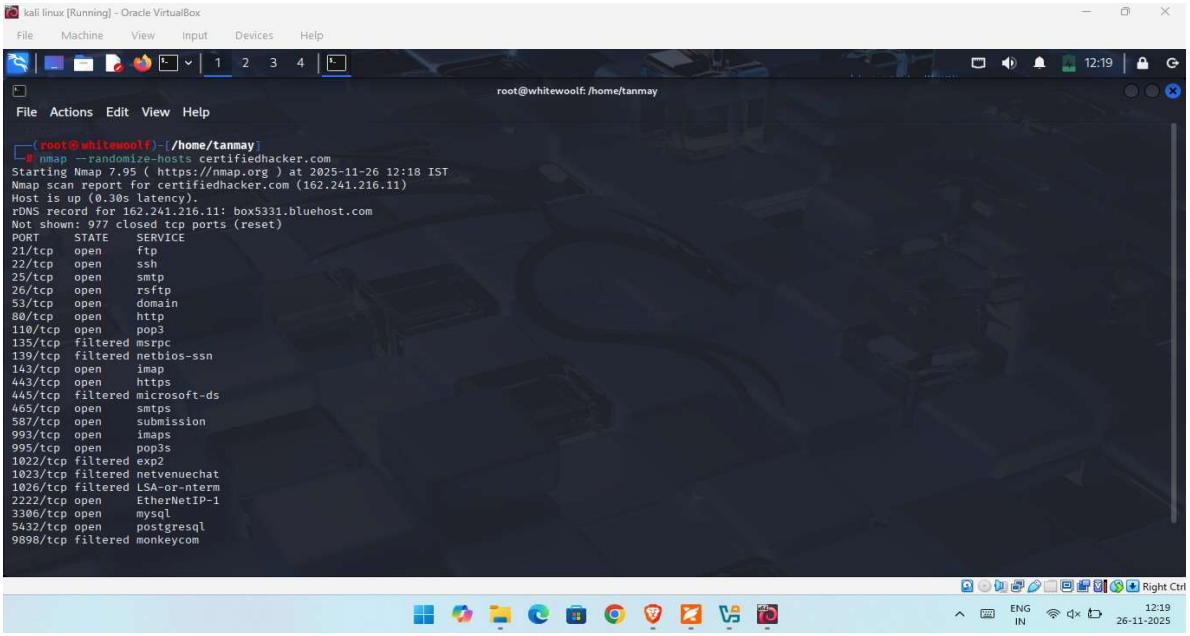
Nmap --badsum Scan (Checksum manipulation detection)



Command / Tool used: nmap --badsum -Pn -v (send packets with bad checksum)

Detailed Explanation: The --badsum option crafts packets with intentionally incorrect checksums. Legitimate hosts typically drop or ignore such packets, but some firewalls or middleboxes may incorrectly accept or respond. This test helps detect buggy IDS/IPS or filtering devices that mishandle invalid checksums.

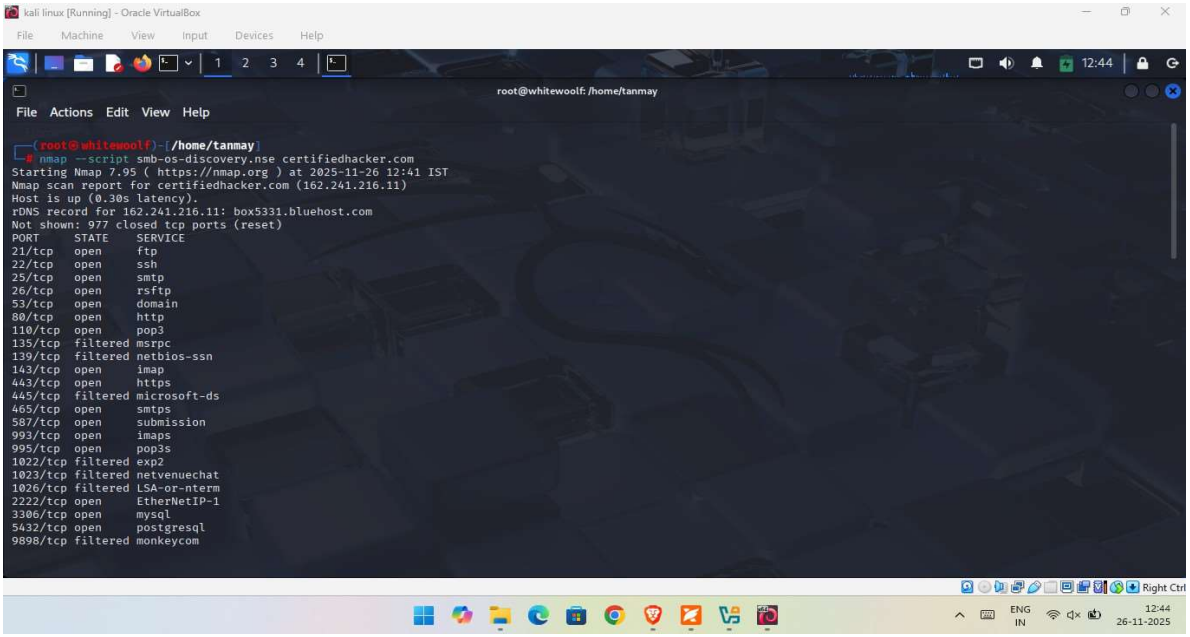
Nmap --randomize-hosts (Scan ordering evasion)



Command / Tool used: nmap --randomize-hosts (randomize scan order)

Detailed Explanation: Randomizing host order helps evade simple rate-limiting or detection systems that assume sequential scans. This screenshot shows a scan where Nmap randomized probe order to reduce predictability.

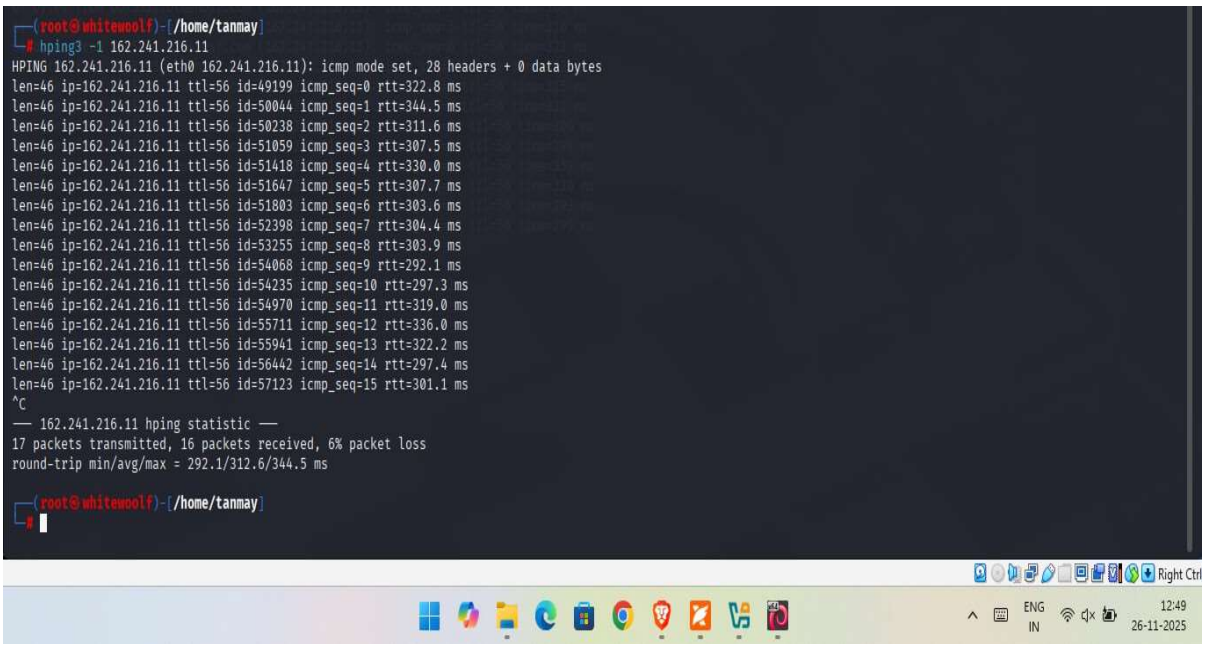
SMB OS Discovery (smb-os-discovery.nse)



Command / Tool used: nmap --script smb-os-discovery.nse (enumerate SMB and OS info)

Detailed Explanation: The smb-os-discovery NSE queries SMB services to extract OS and NetBIOS information, share lists and machine names. It is effective within LANs or hosts exposing SMB.

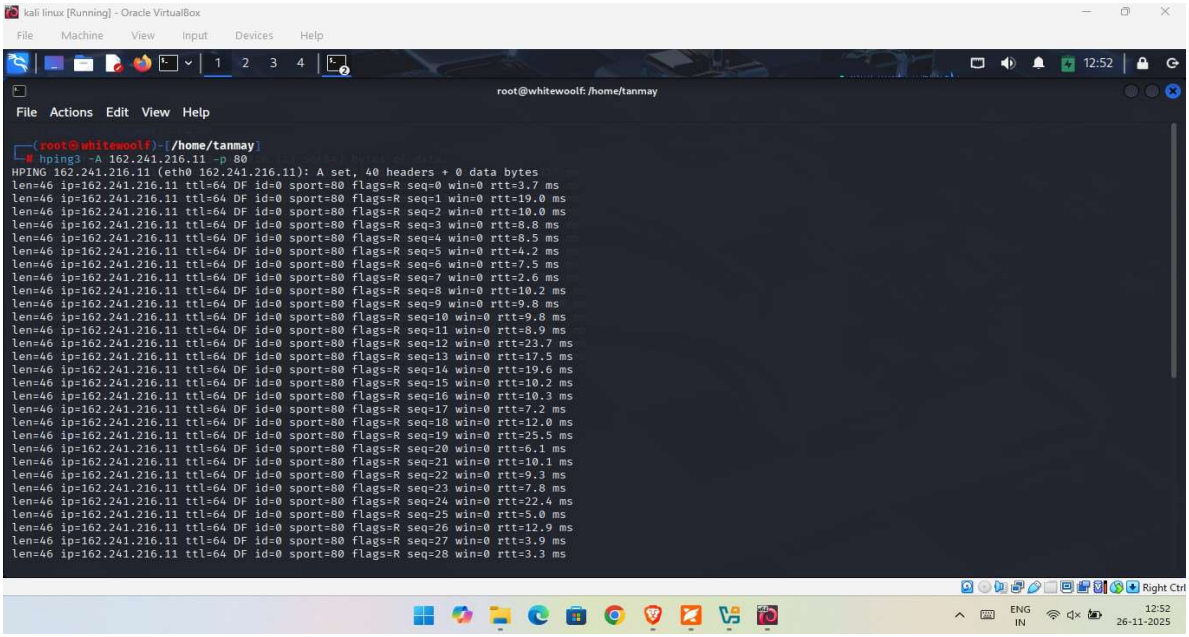
hping3 — ICMP probes and latency (hping3 -1)



Command / Tool used: hping3 -1 (ICMP mode, measure RTT and packet responses)

Detailed Explanation: This screenshot shows hping3 sending ICMP echo probes and reporting per-packet RTTs. hping3 provides finer control than ping and can craft custom packets for testing firewalls and measuring latency.

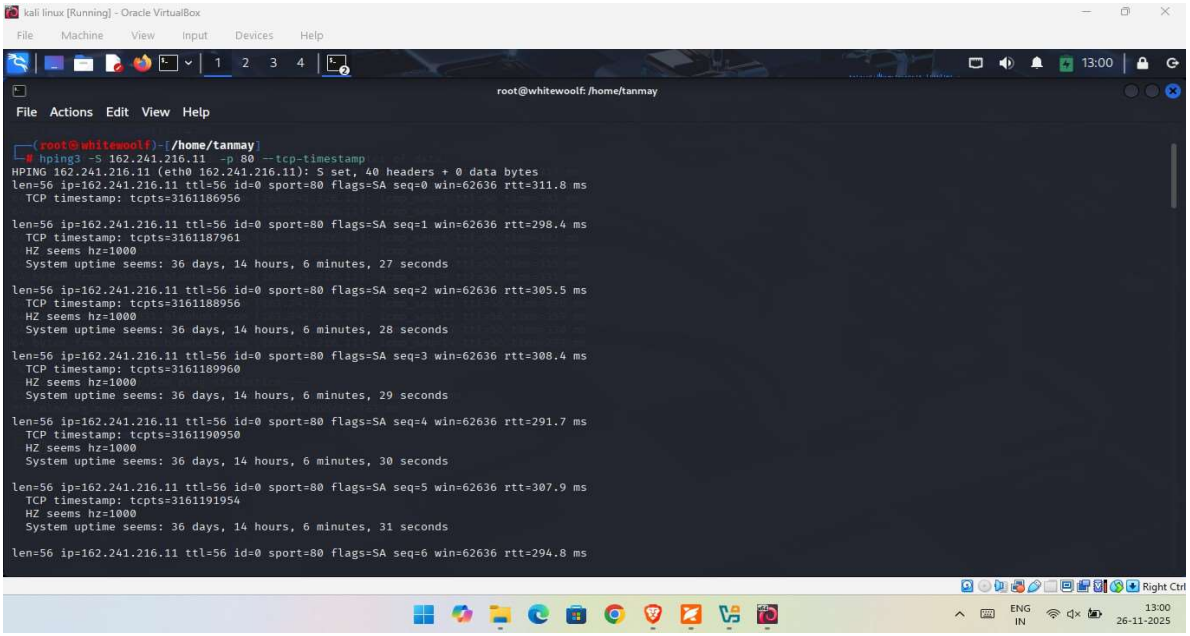
hping3 — TCP probes (ACK / Timestamp / Uptime detection)



Command / Tool used: hping3 -S/-A/-p --tcp-timestamp (custom TCP probes)

Detailed Explanation: These crafted TCP packets test firewall responses and can extract TCP timestamp values. Timestamps and TCP window values help infer system uptime and OS characteristics when interpreted correctly.

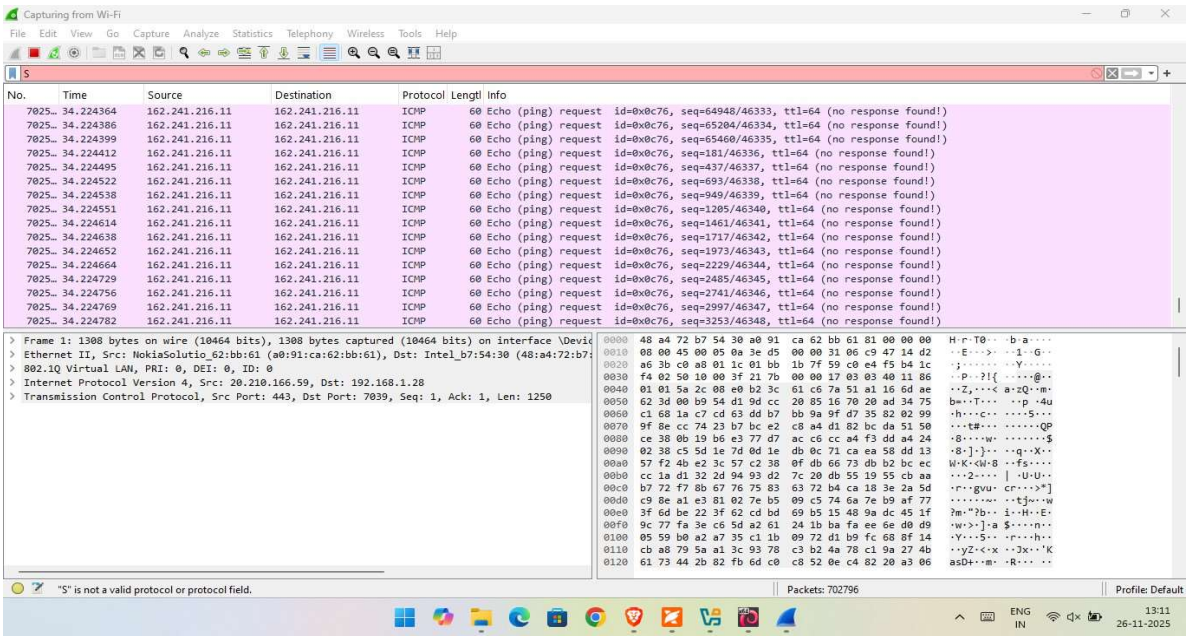
hping3 — TCP timestamp uptime extraction



Command / Tool used: hping3 with --tcp-timestamp to read remote TCP timestamp values

Detailed Explanation: TCP timestamps returned by some systems include a counter that increases regularly; by sampling and converting, an approximate uptime can be inferred. This screenshot demonstrates deriving uptime information from timestamp replies

Wireshark — ICMP Packet Capture Analysis



Command / Tool used: Wireshark capture of ICMP traffic generated during tests (interface: Wi■Fi)

Detailed Explanation: The capture window displays ICMP echo requests with 'no response found' messages and a hex/ASCII pane showing packet bytes. This confirms that some probes were sent but no replies were seen (possible filtering or rate-limiting).

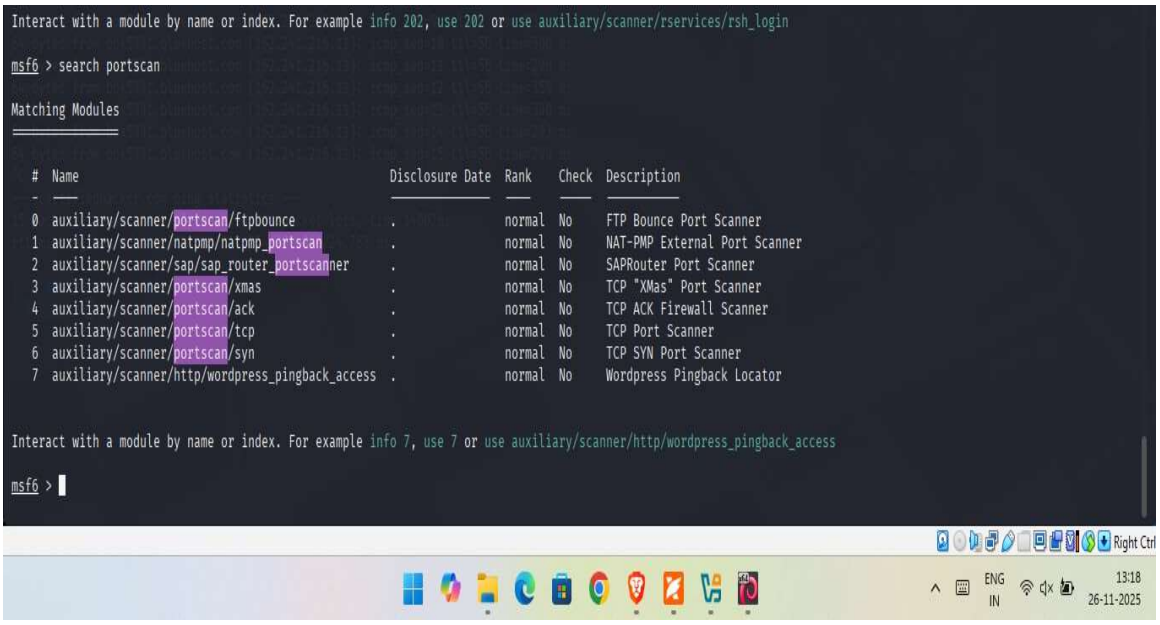
.

hping3 — ICMP Flood Test (--flood)

Command / Tool used: hping3 -1 -p 80 --flood (ICMP flood to test DoS behavior)

Detailed Explanation: This screenshot documents a flood test where hping3 transmitted many packets in rapid succession. The statistics show 701,733 packets transmitted and 0 replies — indicating the target/route dropped floods or rate-limited responses.

Metasploit — Portscan Module Search



Command / Action: msfconsole -> search port scan

What the image shows: Shows matching auxiliary scanner modules in Metasploit (ftp bounce, nat-pmp, sap/router, xmas, ack, tcp, syn, WordPress pingback).

Step-by-step interpretation: Interpretation: The list helps choose a module tailored to target/network. For example, 'auxiliary/scanner/port scan/syn' performs SYN scans within Metasploit; 'ftp bounce' uses FTP bounce technique (requires vulnerable FTP server). Selecting proper module reduces noise and can exploit protocol-specific behaviors.