

REPORT ON SCANNING NETWORK

A photograph of a person's hands typing on a dark-colored keyboard. The background is a deep blue, and there are glowing blue energy fields or data patterns visible around the keys, particularly around the number pad and the right-hand keys, suggesting a theme of digital scanning or network analysis.

-TANMAY KHEDEKAR

Table of Content:

Sr.No	INDEX
1	Introduction
2	Types of Scanning
3	Objective
4	Lab 1 – Host Discovery
5	ARP Ping Scan
6	UDP Ping Scan
7	ICMP Echo Scan
8	ICMP Timestamp Scan
9	ICMP Address Mask Scan
10	Lab 2 – Port & Service Discovery
11	TCP Connect Scan
12	Stealth Scan
13	Xmas Scan
14	TCP Maimon Scan
15	ACK Flag Probe Scan
16	UDP Scan
17	Nmap Advanced Scanning
18	Angry IP Scanner Results
19	Host Discovery
20	Scan Completion Statistics
21	Firewall & Evasion Techniques
22	smb-os-discovery Script
23	hping3 Probing & Analysis
24	ICMP Probes
25	TCP Timestamp / ACK / SYN Probes
26	Wireshark Packet Capture Analysis
27	Flood Testing (--flood)
28	Metasploit Port Scanning Modules

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

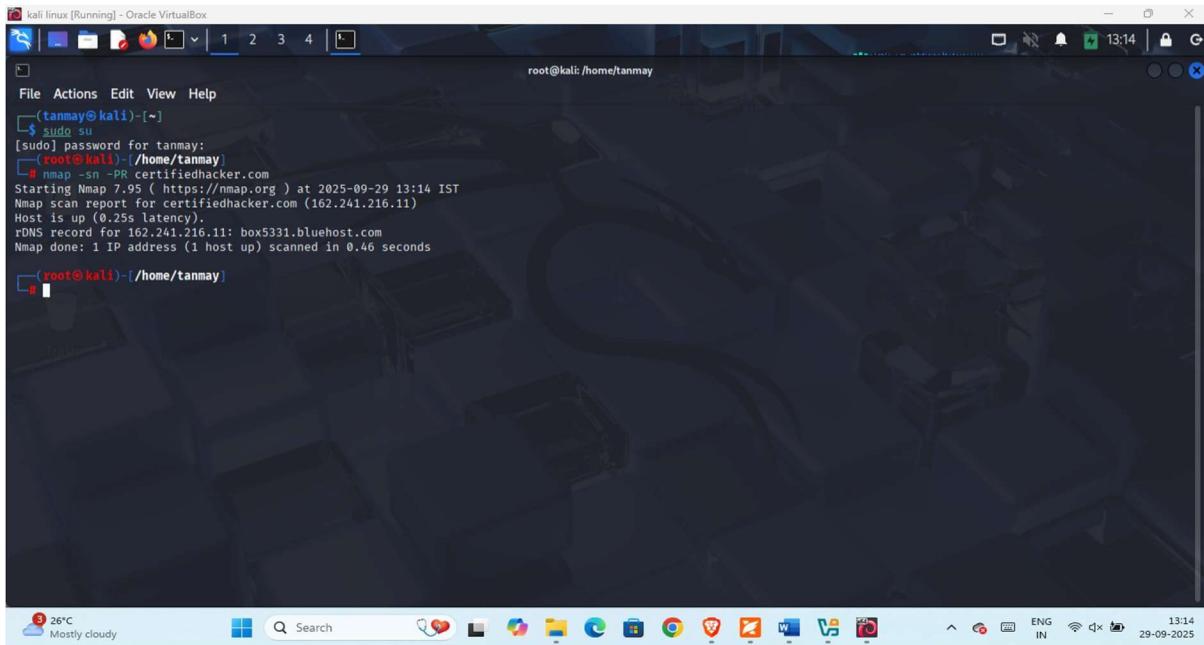
WHAT IS NMAP?

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



```
(tanmay㉿kali)-[~]
$ sudo su
[sudo] password for tanmay:
(root㉿kali)-[~/home/tanmay]
# nmap -sn -PR certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 13:14 IST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.25s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds

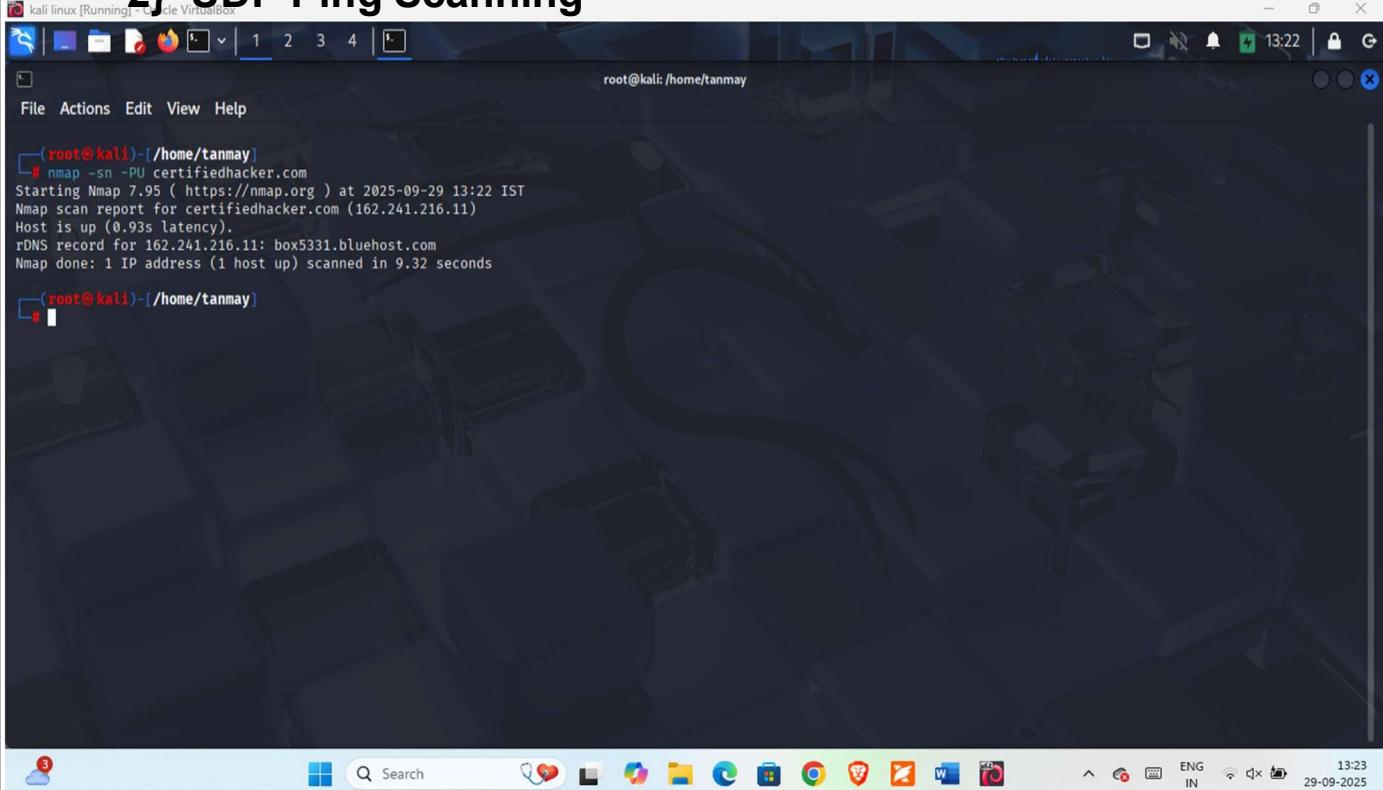
(root㉿kali)-[~/home/tanmay]
#
```

COMMAND - nmap -sn -PR (TARGET IP)

NOTE: sn- Disable port scan

PR- Performs APR ping Scanning

2} UDP Ping Scanning



```
(root㉿kali)-[~/home/tanmay]
# nmap -sn -PU certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 13:22 IST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.93s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Nmap done: 1 IP address (1 host up) scanned in 9.32 seconds

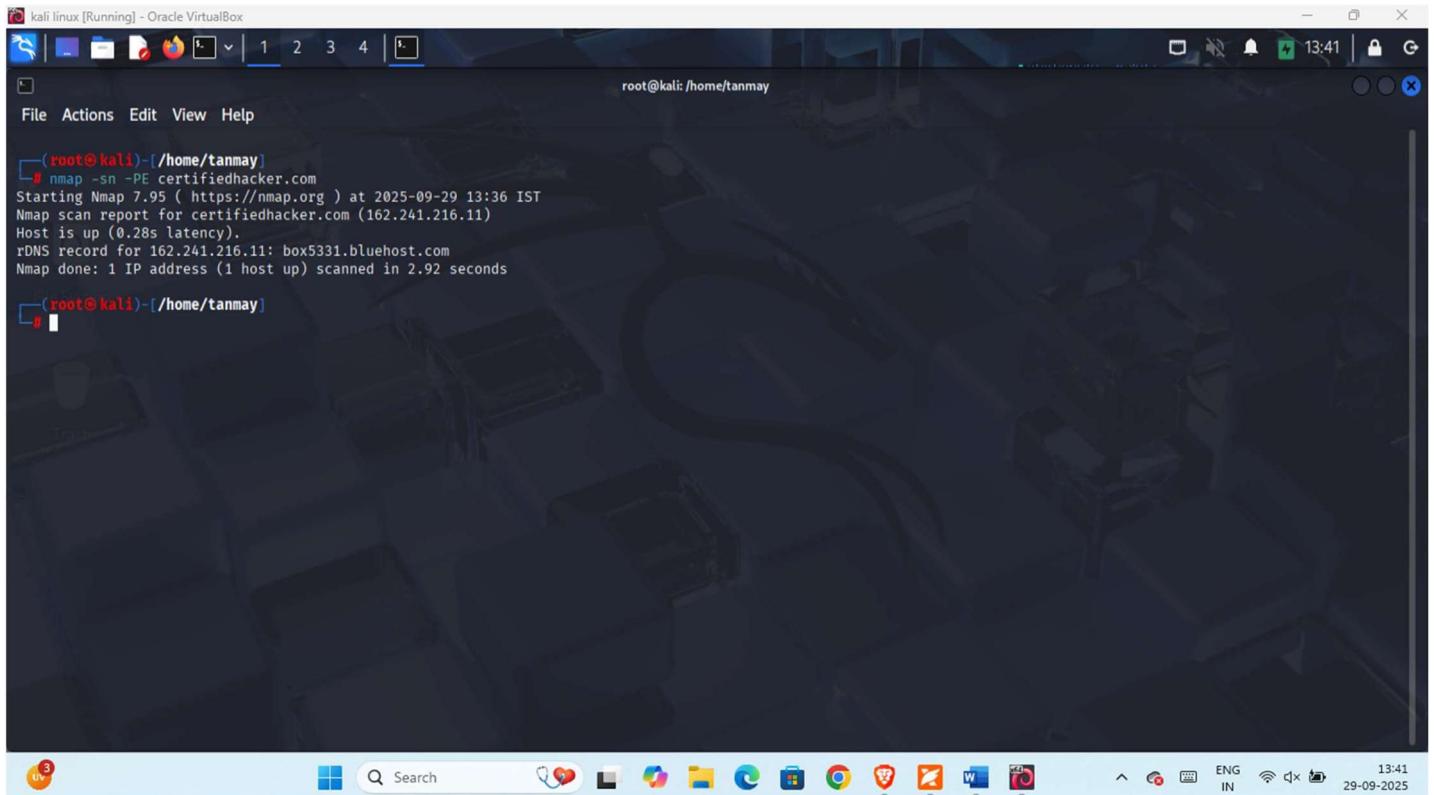
(root㉿kali)-[~/home/tanmay]
#
```

COMMAND - nmap -sn -PU (TARGET IP)

NOTE: sn- Disable port scan

PR- Performs UDP ping Scanning

3} ICMP ping Scanning



The screenshot shows a terminal window on a Kali Linux desktop. The terminal title is "root@kali: /home/tanmay". The command entered is "nmap -sn -PE certifiedhacker.com". The output shows the following details:

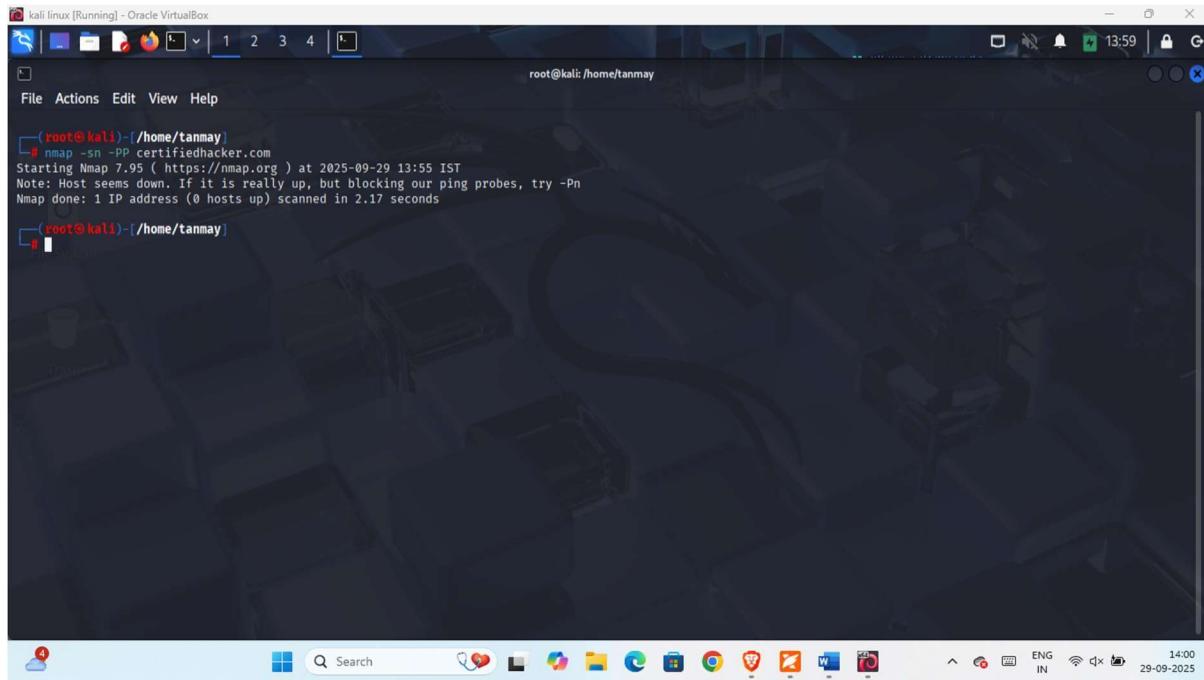
```
[root@kali]-[~/home/tanmay]
# nmap -sn -PE certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 13:36 IST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.28s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Nmap done: 1 IP address (1 host up) scanned in 2.92 seconds
[root@kali]-[~/home/tanmay]
#
```

COMMAND - nmap -sn -PE (TARGET IP)

NOTE: sn- Disable port scan

PE- Performs ICMP ECHO ping Scanning

4. ICMP Timestamp ping Scanning



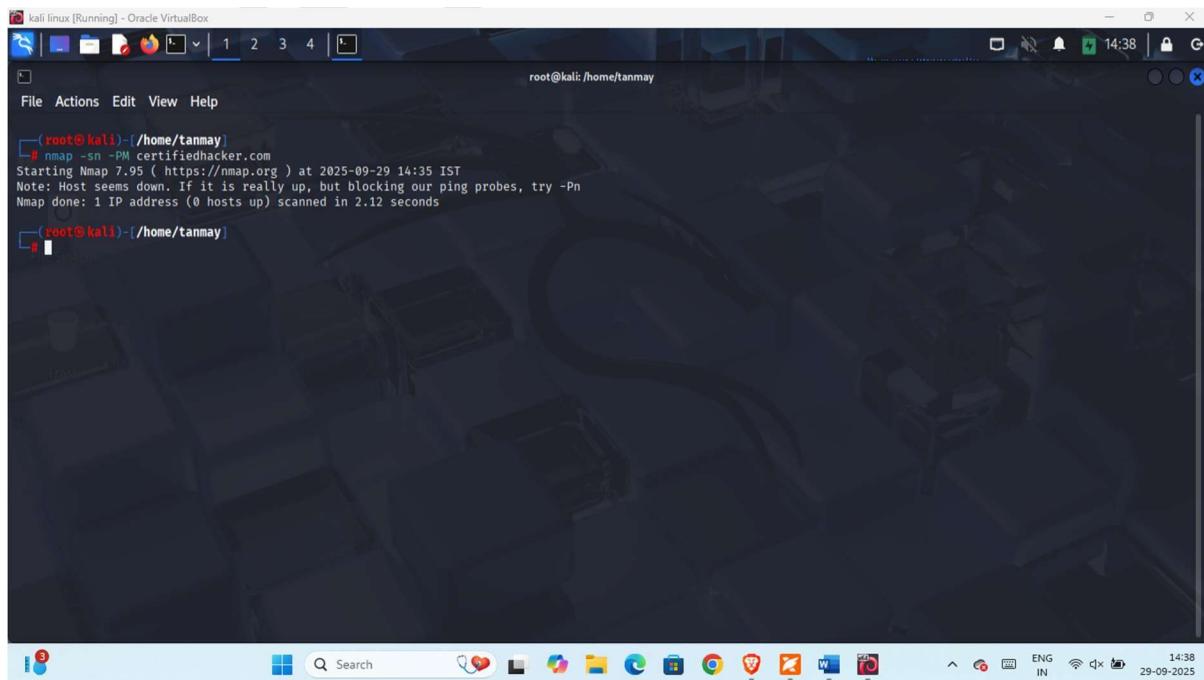
```
(root@kali)-[~/home/tanmay]
└─# nmap -sn -PP certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 13:55 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.17 seconds
└─#
```

COMMAND - nmap -sn -PP (TARGET IP)

NOTE: sn- Disable port scan

PP- Performs ICMP timestamp ping Scanning

5. ICMP Address mac Ping Scanning



```
(root@kali)-[~/home/tanmay]
└─# nmap -sn -PM certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 14:35 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.12 seconds
└─#
```

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:

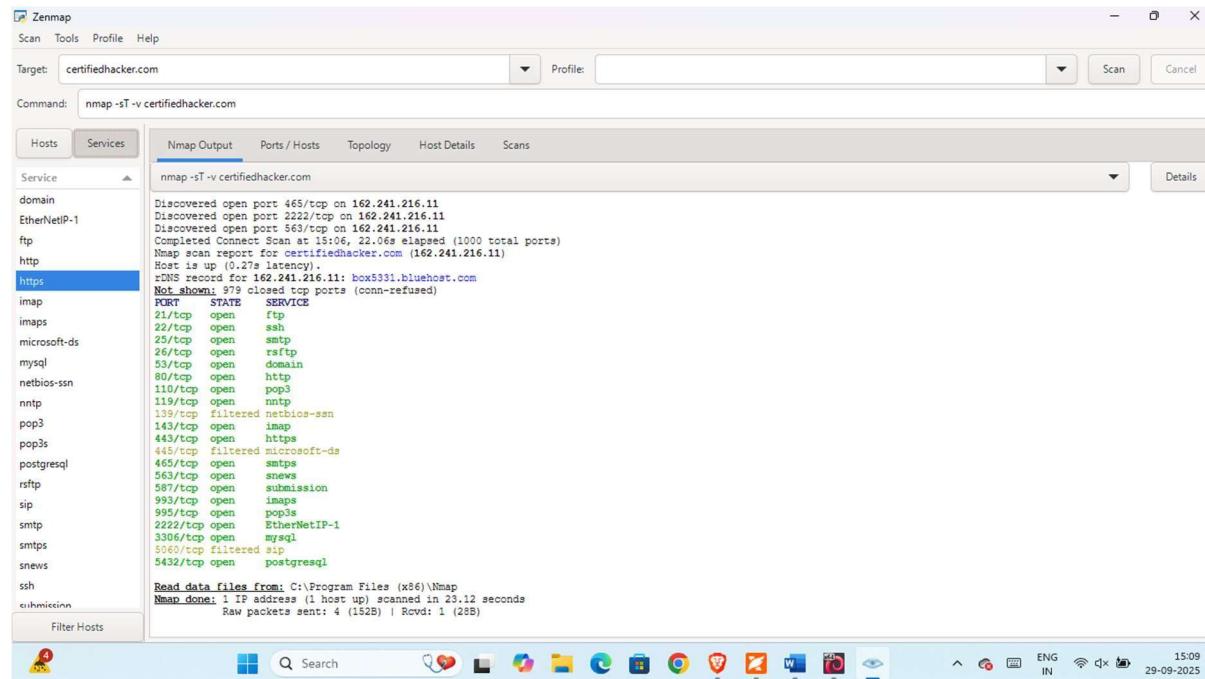
- TCP connect scan and SYN scan for finding open ports.
- UDP scan for identifying UDP-based services.
- Service/version detection (nmap -sV) to get detailed information.

LAB OBJECTIVE-

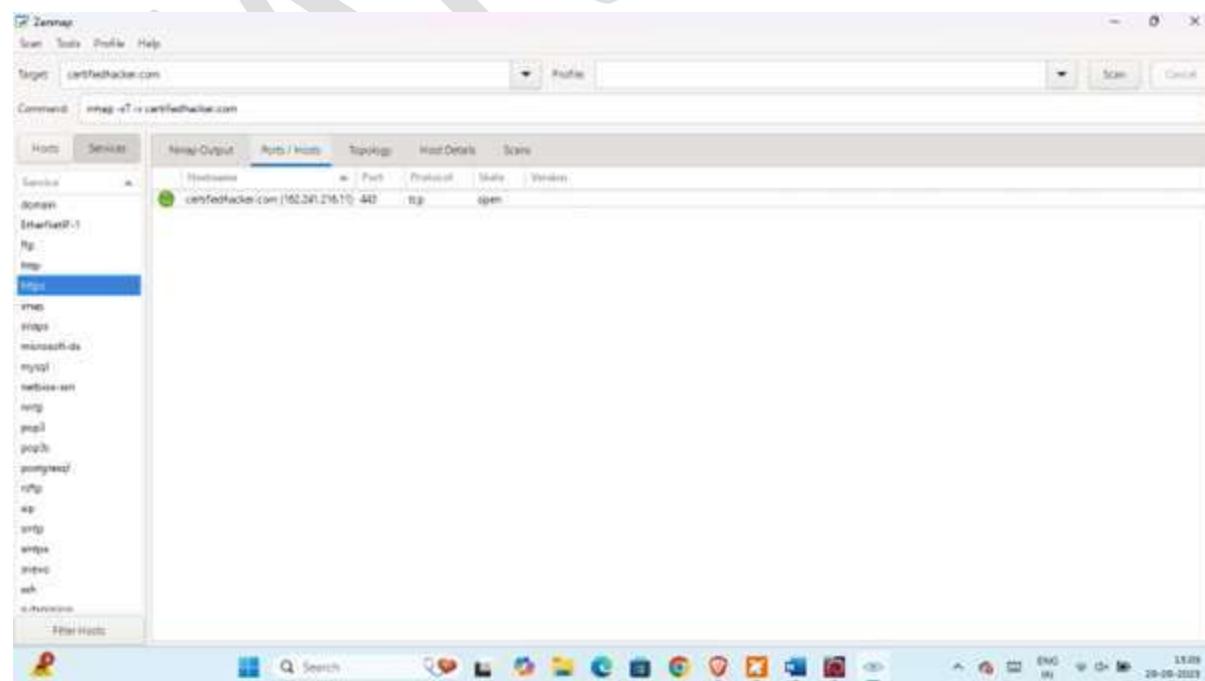
Explore Various networks scanning techniques using namp

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

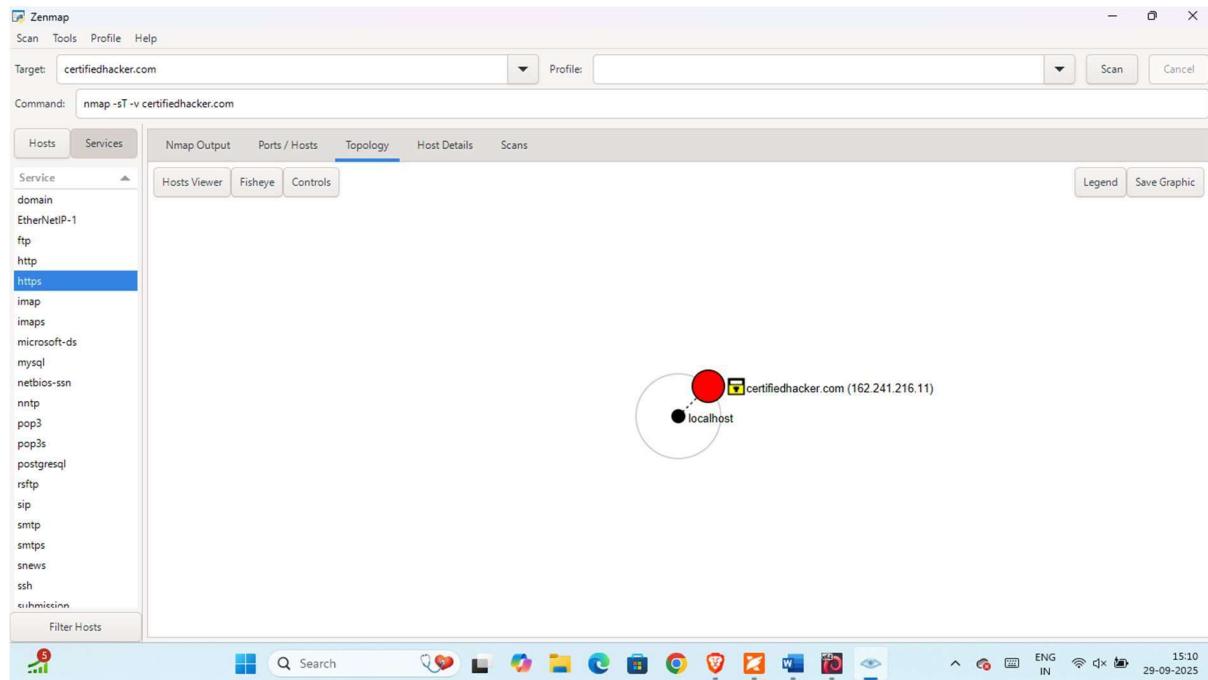
The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.



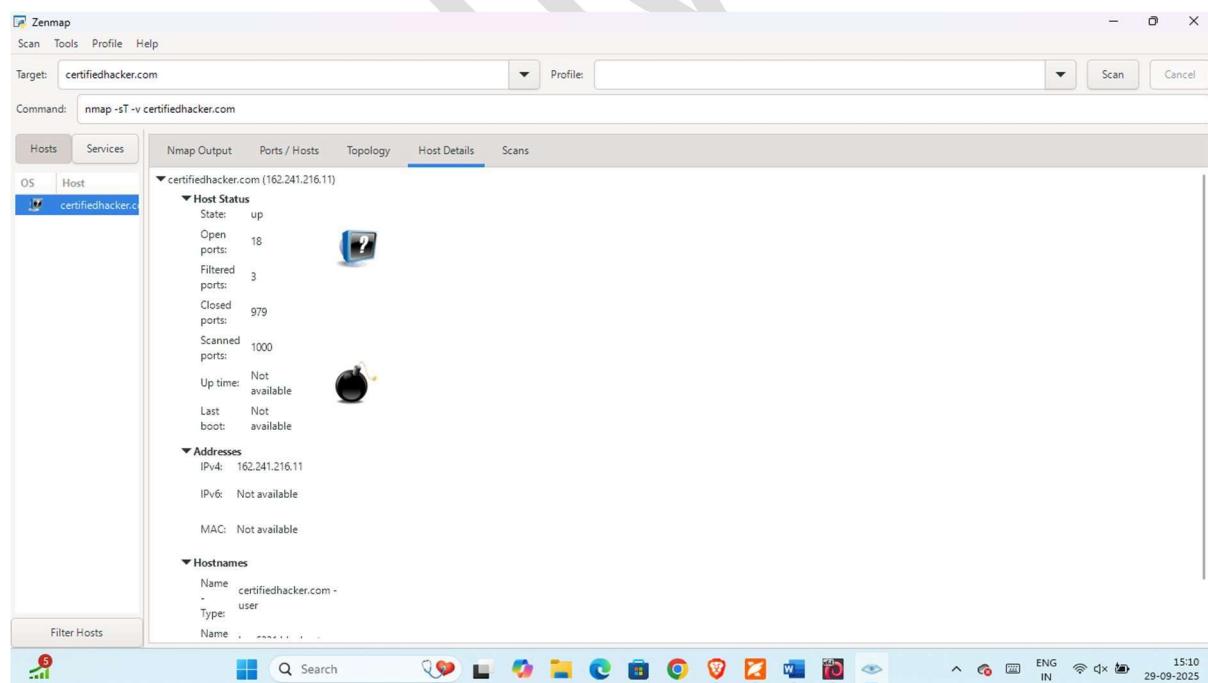
Clicking on the Ports/Hosts tab to gather more information on the scan results.



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.

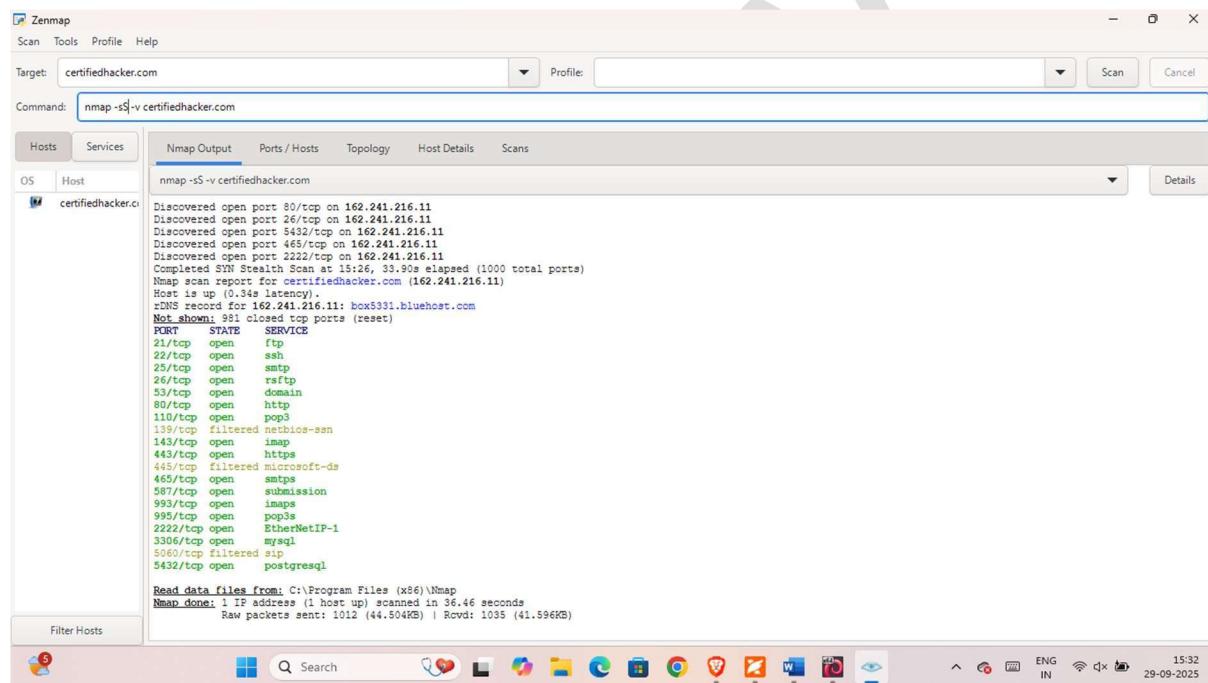


In this scenario we perform the stealth scan, Xmas scan, TCP Maimon scan and ACK Flag probe on a firewall-enabled machine.

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.



The screenshot shows the Zenmap interface with the following details:

- Target:** certifiedhacker.com
- Command:** nmap -sS -v certifiedhacker.com
- OS Host:** certifiedhacker.com
- Scans:** Nmap Output, Ports / Hosts, Topology, Host Details, Scans (selected)
- Output Content:**

```
Discovered open port 80/tcp on 162.241.216.11
Discovered open port 26/tcp on 162.241.216.11
Discovered open port 5432/tcp on 162.241.216.11
Discovered open port 465/tcp on 162.241.216.11
Discovered open port 2222/tcp on 162.241.216.11
Completed SYN Stealth Scan at 15:26: 33.98s elapsed (1000 total ports)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.34s latency).
rDNS record for 162.241.216.11: box531.bluehost.com
Not shown: 981 closed top ports (reset)
PORT      STATE     SERVICE
21/tcp    open      ftp
21/tcp    open      ssh
25/tcp    open      smtp
26/tcp    open      rsmtp
53/tcp    open      domain
80/tcp    open      http
110/tcp   open      pop3
139/tcp   filtered netbios-ssn
143/tcp   open      imap
443/tcp   open      https
465/tcp   open      smtp
587/tcp   open      submission
993/tcp   open      imaps
995/tcp   open      pop3s
2222/tcp  open      EtherNetIP-1
3306/tcp  open      mysql
5060/tcp  filtered sip
3432/tcp  open      postgresql

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 36.46 seconds
Raw packets sent: 1012 (44.504KB) | Rcvd: 1035 (41.596KB)
```
- Bottom Status Bar:** Filter Hosts, Search icon, Taskbar icons (File Explorer, Edge, File History, Task View, Taskbar Icons, Taskbar Buttons, Taskbar Buttons), ENG IN, 15:32, 29-09-2025

Command: - nmap -sS -v cetifedhacker.com

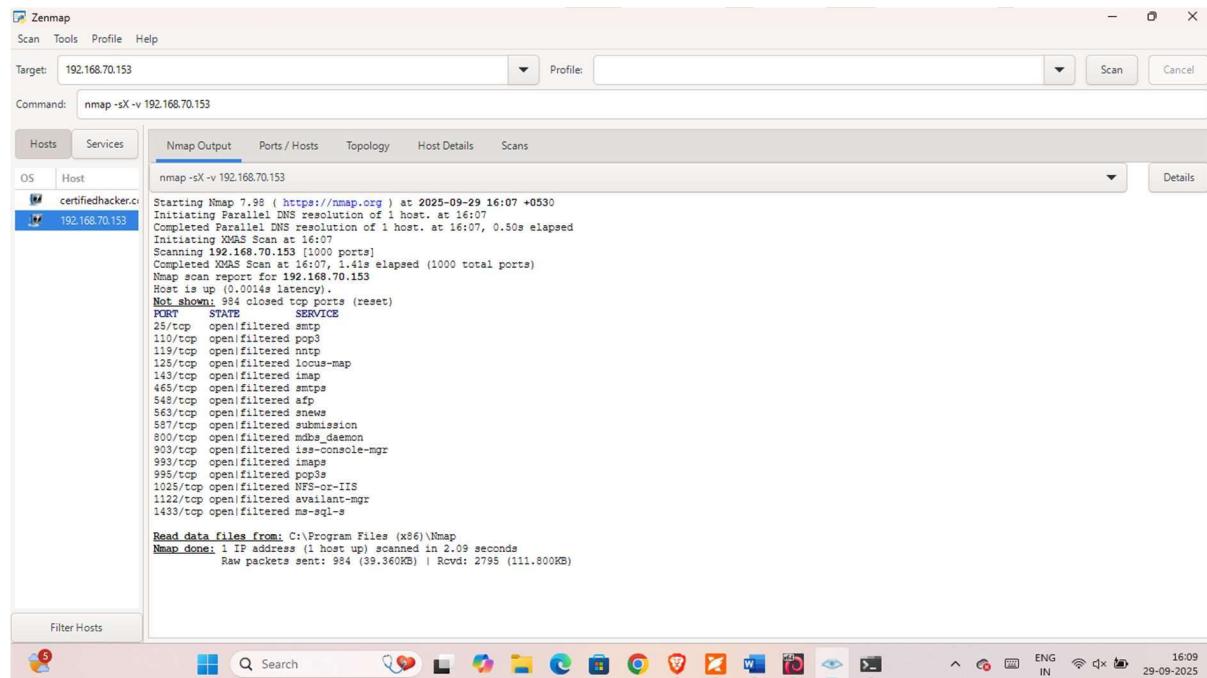
Note: -sS : perform the stealth scan/TCP half-open scan

-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.



The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.70.153
- Command:** nmap -sX -v 192.168.70.153
- Hosts:** certifiedhacker.c (Status: Up)
- Services:** 192.168.70.153 (Status: Up)
- Nmap Output:**

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-29 16:07 +0530
Initiating Parallel DNS resolution of 1 host at 16:07
Completed Parallel DNS resolution of 1 host at 16:07, 0.50s elapsed
Initiating XMAS Scan at 16:07
Scanning 192.168.70.153 [1000 ports]
Completed XMAS Scan at 16:07, 1.41s elapsed (1000 total ports)
Nmap scan report for 192.168.70.153
Host is up [0.014s latency].
Not shown: 934 closed ports (reset)
PORT      STATE      SERVICE
25/tcp    open       smtp
50/tcp    open       http
80/tcp    open       http
110/tcp   open       pop3
119/tcp   open       nntp
125/tcp   open       locus-map
143/tcp   open       imap
465/tcp   open       smtps
548/tcp   open       telnet
563/tcp   open       snews
587/tcp   open       submission
800/tcp   open       mdbs_daemon
903/tcp   open       iis-console-mgr
993/tcp   open       imaps
995/tcp   open       pop3s
1025/tcp  open       NFS-or-IIS
1122/tcp  open       availant-mgr
1433/tcp  open       ms-sql-s

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
Raw packets sent: 984 (39.360KB) | Rcvd: 2795 (111.800KB)
```

Command: - nmap -sX -v 192.168.70.153

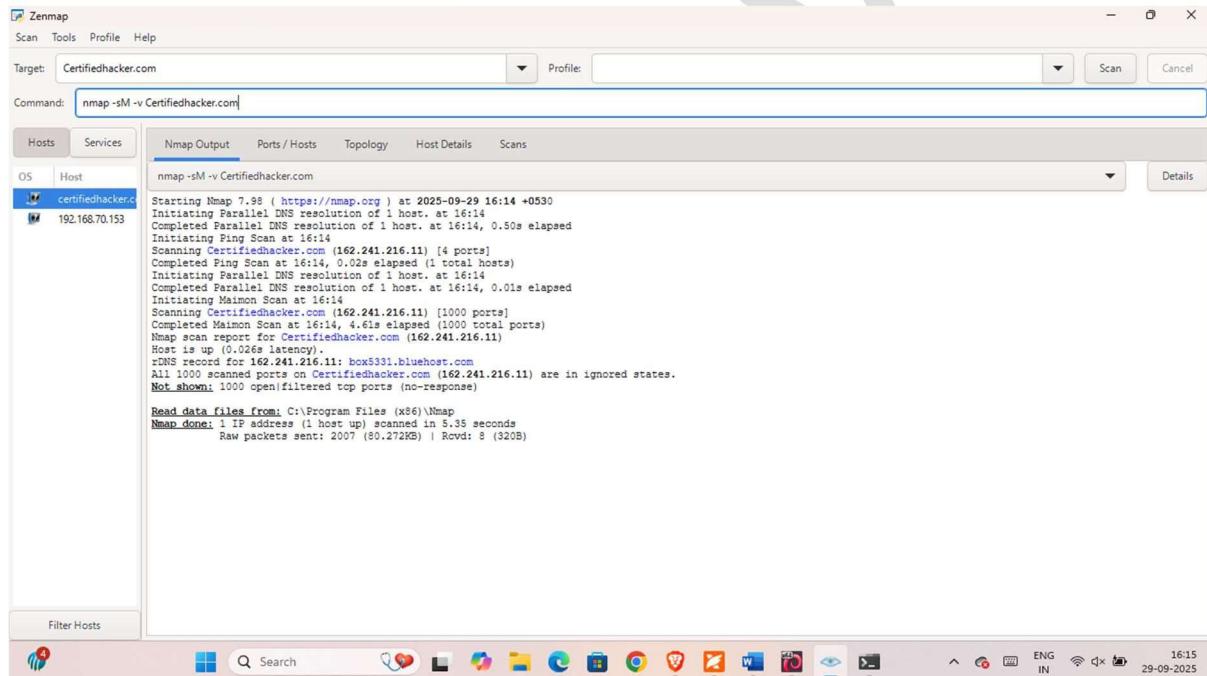
Note: -sX : perform the Xmas scan

-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.



Zenmap window showing the results of a TCP Maimon scan on host 192.168.70.153. The command entered is "nmap -sM -v Certifiedhacker.com". The output shows the scan process starting at 16:14 and completing at 16:14, with a total elapsed time of 0.50s. It lists various parallel DNS resolutions and a Maimon Scan at 16:14, which completed in 4.61s. The report concludes that the host is up with 0.026s latency and that all 1000 scanned ports are in ignored states. A note indicates that 1000 open/filtered top ports (no-response) were not shown. The scan report file was read from C:\Program Files (x86)\Nmap and the process took 5.35 seconds with 2007 raw packets sent and 320B received.

```
Starting Nmap 7.88 ( https://nmap.org ) at 2025-09-29 16:14 +0530
Initiating Parallel DNS resolution of 1 host at 16:14
Completed Parallel DNS resolution of 1 host at 16:14, 0.50s elapsed
Initiating Ping Scan at 16:14
Scanning Certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 16:14, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 16:14
Completed Parallel DNS resolution of 1 host at 16:14, 0.01s elapsed
Initiating Maimon Scan at 16:14
Scanning Certifiedhacker.com (162.241.216.11) [1000 ports]
Completed Maimon Scan at 16:14, 4.61s elapsed (1000 total ports)
Nmap scan report for Certifiedhacker.com (162.241.216.11)
Host is up (0.026s latency).
RDNS record for 162.241.216.11: box531.bluehost.com
All 1000 scanned ports on Certifiedhacker.com (162.241.216.11) are in ignored states.
Not shown: 1000 open/filtered top ports (no-response)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.35 seconds
Raw packets sent: 2007 (90.272KB) | Rcvd: 8 (320B)
```

Command: - nmap -sM -v 192.168.70.153

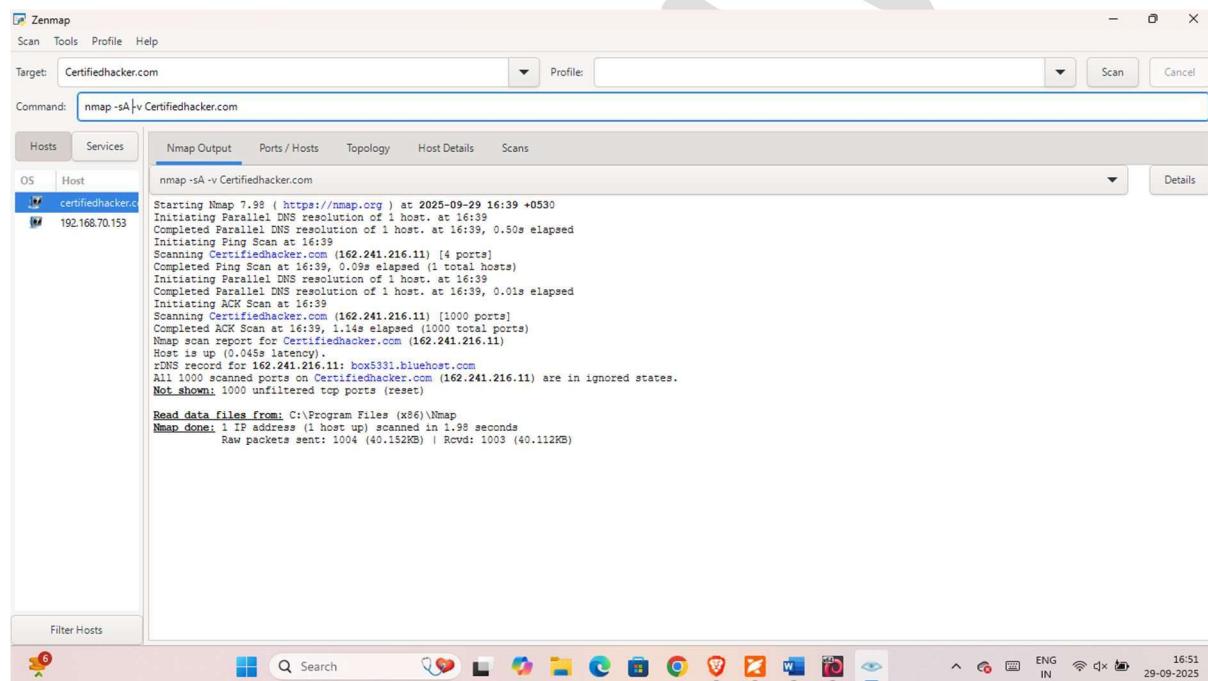
Note: -sM : perform the TCP Maimon scan

-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.



Zenmap

Scan Tools Profile Help

Target: Certifiedhacker.com

Command: nmap -sA -v Certifiedhacker.com

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

certifiedhacker.com
192.168.70.153

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-29 16:39 +0530
Initiating Parallel DNS resolution of 1 host. at 16:39
Completed Parallel DNS resolution of 1 host. at 16:39, 0.50s elapsed
Initiating Ping Scan at 16:39
Completed Ping Scan at 16:39, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:39
Completed Parallel DNS resolution of 1 host. at 16:39, 0.01s elapsed
Initiating ACK Scan at 16:39
Scanning Certifiedhacker.com (162.241.216.11) [1000 ports]
Completed ACK Scan at 16:39, 1.14s elapsed (1000 total ports)
Host up up (0.045s latency)
RDNS record for 162.241.216.11: box5331.bluehost.com
All 1000 scanned ports on Certifiedhacker.com (162.241.216.11) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 1.98 seconds
Raw packets sent: 1004 (40.152KB) | Rcvd: 1003 (40.112KB)
```

Filter Hosts

16:51 ENG IN 29-09-2025

Command: - nmap -sA -v 192.168.70.153

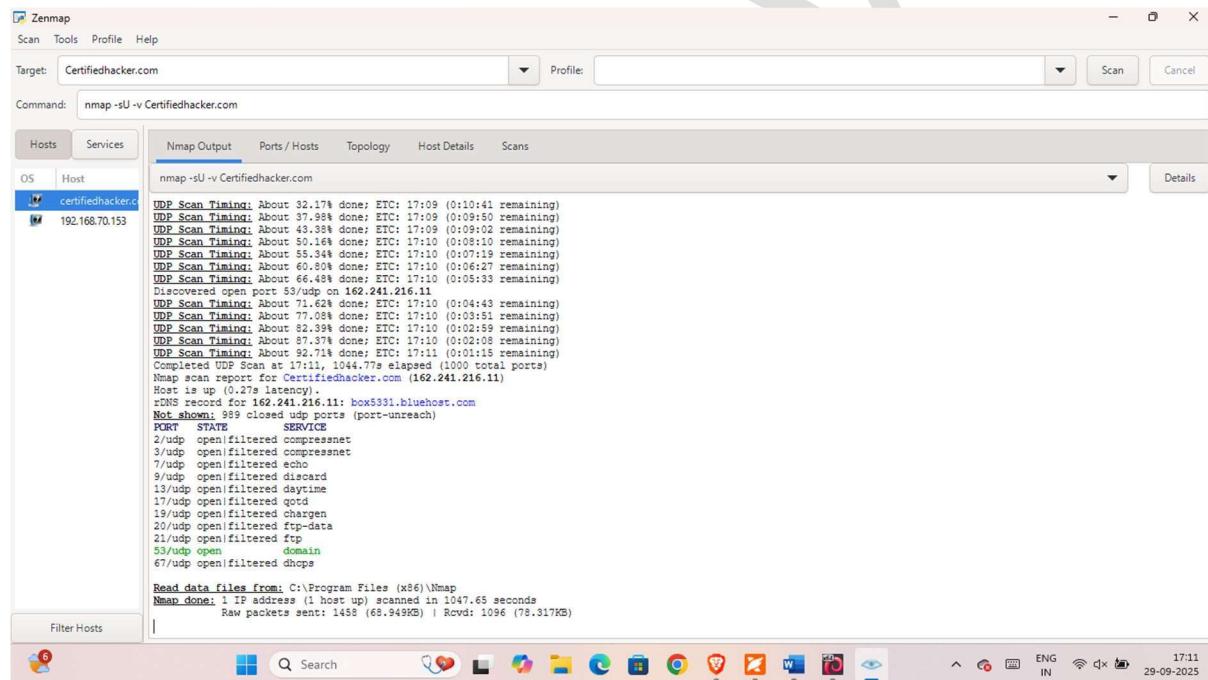
Note: -sA : performs the ACK flag probe scan

-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.



Zenmap

Scan Tools Profile Help

Target: Certifiedhacker.com

Command: nmap -sU -v Certifiedhacker.com

Hosts Services

OS Host

certifiedhacker.c
192.168.70.153

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sU -v Certifiedhacker.com

UDP Scan Timing: About 32.17% done; ETC: 17:09 (0:10:41 remaining)
UDP Scan Timing: About 37.98% done; ETC: 17:09 (0:09:50 remaining)
UDP Scan Timing: About 43.38% done; ETC: 17:09 (0:09:02 remaining)
UDP Scan Timing: About 48.68% done; ETC: 17:09 (0:08:14 remaining)
UDP Scan Timing: About 55.34% done; ETC: 17:10 (0:07:19 remaining)
UDP Scan Timing: About 60.80% done; ETC: 17:10 (0:06:27 remaining)
UDP Scan Timing: About 66.48% done; ETC: 17:10 (0:05:33 remaining)
Discovered open port 53/udp on 162.241.216.11
UDP Scan Timing: About 71.62% done; ETC: 17:11 (0:04:43 remaining)
UDP Scan Timing: About 77.08% done; ETC: 17:11 (0:03:51 remaining)
UDP Scan Timing: About 82.39% done; ETC: 17:11 (0:02:59 remaining)
UDP Scan Timing: About 86.57% done; ETC: 17:11 (0:02:10 remaining)
UDP Scan Timing: About 90.14% done; ETC: 17:11 (0:01:15 remaining)
Completed UDP Scan at 17:11: 1044.77s elapsed (1000 total ports)
Nmap scan report for Certifiedhacker.com (162.241.216.11)
Host is up (0.27s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 989 closed udp ports (port-unreach)

PORT	STATE	SERVICE
53/udp	open filtered	compressnet
3/udp	open filtered	compressnet
7/udp	open filtered	echo
9/udp	open filtered	discard
13/udp	open filtered	daytime
17/udp	open filtered	qotd
19/udp	open filtered	chargen
20/udp	open filtered	ftp-data
21/udp	open filtered	ftp
53/udp	open	domain
67/udp	open filtered	dhcps

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 1047.65 seconds
Raw packets sent: 1458 (68.949KB) | Rcvd: 1096 (78.317KB)

Filter Hosts

Search

17:11 ENG IN 29-09-2025

Command: - nmap -sU -v certifiedhacker.com

Note: -sU : performs the UDP scan

-v: enable the verbose output

```

Zenmap
Scan Tools Profile Help
Target: Certifiedhacker.com
Profile: Null Scan
Command: nmap -sN -sU -T4 -A -v Certifiedhacker.com
Hosts Services
OS Host
certifiedhacker.com
192.168.70.153
nmap -sN -sU -T4 -A -v Certifiedhacker.com
[...]

```

UDP Scan Timing: About 96.97% done; ETC: 17:37 (0:00:30 remaining)
Completed UDP Scan at 17:38, 1025.50s elapsed (1000 total ports)
Scanning 1012 services on Certifiedhacker.com (162.241.216.11)
Discovered open port 25/tcp on 162.241.216.11
Discovered open/filtered port 25/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open/filtered port 26/tcp on 162.241.216.11
Discovered open/filtered port 26/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open/filtered port 21/tcp on 162.241.216.11
Discovered open/filtered port 21/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open/filtered port 22/tcp on 162.241.216.11
Discovered open/filtered port 22/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 53/tcp on 162.241.216.11
Discovered open/filtered port 53/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 80/tcp on 162.241.216.11
Discovered open/filtered port 80/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 110/tcp on 162.241.216.11
Discovered open/filtered port 110/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 119/tcp on 162.241.216.11
Discovered open/filtered port 119/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 143/tcp on 162.241.216.11
Discovered open/filtered port 143/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 465/tcp on 162.241.216.11
Discovered open/filtered port 465/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 443/tcp on 162.241.216.11
Discovered open/filtered port 443/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 563/tcp on 162.241.216.11
Discovered open/filtered port 563/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 887/tcp on 162.241.216.11
Discovered open/filtered port 887/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 993/tcp on 162.241.216.11
Discovered open/filtered port 993/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Discovered open port 995/tcp on 162.241.216.11
Discovered open/filtered port 995/tcp on Certifiedhacker.com (162.241.216.11) is actually open
Service scan Timing: About 16.93% done; ETC: 17:41 (0:02:32 remaining)

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)

The screenshot shows the main interface of Angry IP Scanner. The title bar reads "IP Range - Angry IP Scanner". The menu bar includes Scan, Go to, Commands, Favorites, Tools, and Help. The IP Range is set to 192.168.1.1 to 192.168.1.254. The Hostname field contains "Tanmay". Below the menu is a toolbar with "IP+", "Netmask", "Start", and other icons. The main window displays a table of scanned hosts:

IP	Ping	Hostname	Ports [3+]
192.168.1.1	9 ms	[n/a]	443
192.168.1.2	2377 ms	[n/a]	[n/a]
192.168.1.3	[n/a]	[n/s]	[n/s]
192.168.1.4	[n/a]	[n/s]	[n/s]
192.168.1.5	[n/a]	[n/s]	[n/s]
192.168.1.6	2334 ms	[n/a]	[n/a]
192.168.1.7	53 ms	[n/a]	80
192.168.1.8	44 ms	[n/a]	[n/a]
192.168.1.9	[n/a]	[n/s]	[n/s]
192.168.1.10	[n/a]	[n/s]	[n/s]
192.168.1.11	[n/a]	[n/s]	[n/s]
192.168.1.12	846 ms	[n/a]	[n/a]
192.168.1.13	2759 ms	[n/a]	[n/a]
192.168.1.14	67 ms	SKALI	[n/a]
192.168.1.15	[n/a]	[n/s]	[n/s]
192.168.1.16	[n/a]	[n/s]	[n/s]
192.168.1.17	[n/a]	[n/s]	[n/s]
192.168.1.18	298 ms	[n/a]	[n/a]
192.168.1.19	393 ms	[n/a]	[n/a]
192.168.1.20	65 ms	[n/a]	[n/a]
192.168.1.21	2425 ms	[n/a]	[n/a]
192.168.1.22	[n/a]	[n/s]	[n/s]
192.168.1.23	[n/a]	[n/s]	[n/s]
192.168.1.24	69 ms	ANKITA	[n/a]
192.168.1.25	[n/a]	[n/s]	[n/s]
192.168.1.26	55 ms	[n/a]	[n/a]
192.168.1.27	74 ms	LAPTOP-ID8SD7CS	[n/a]
192.168.1.28	2 ms	Tanmay	[n/a]
192.168.1.29	2339 ms	[n/a]	[n/a]
192.168.1.30	975 ms	[n/a]	[n/a]

At the bottom, there are buttons for "Display: All" and "Threads: 0". The system tray shows icons for network, battery, and date/time (25-11-2025, 12:41). A status bar at the bottom indicates "Ready".

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

The screenshot shows the main interface of Angry IP Scanner with the same configuration as the previous screenshot. A modal dialog titled "Scan Statistics" is displayed in the center:

Scanning completed

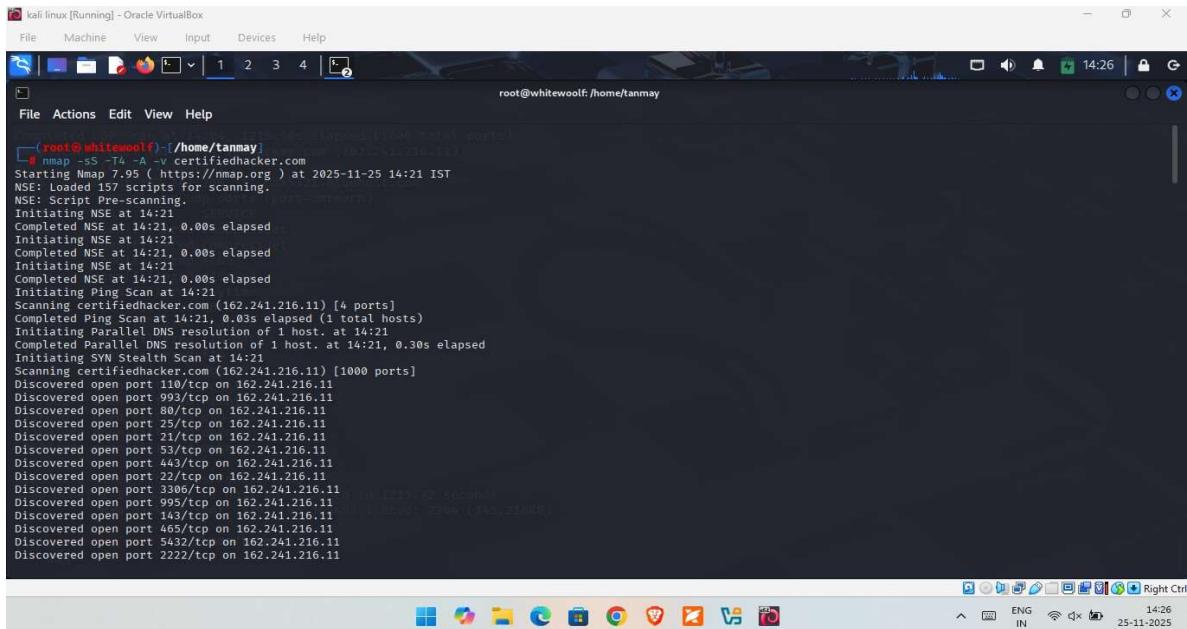
Total time: 37.16 sec
Average time per host: 0.15 sec
IP Range
192.168.1.1 - 192.168.1.254
Hosts scanned: 254
Hosts alive: 48
With open ports: 4

At the bottom right of the dialog is a "Close" button. The main window below shows the same list of hosts as the first screenshot. The system tray and status bar are also visible.

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

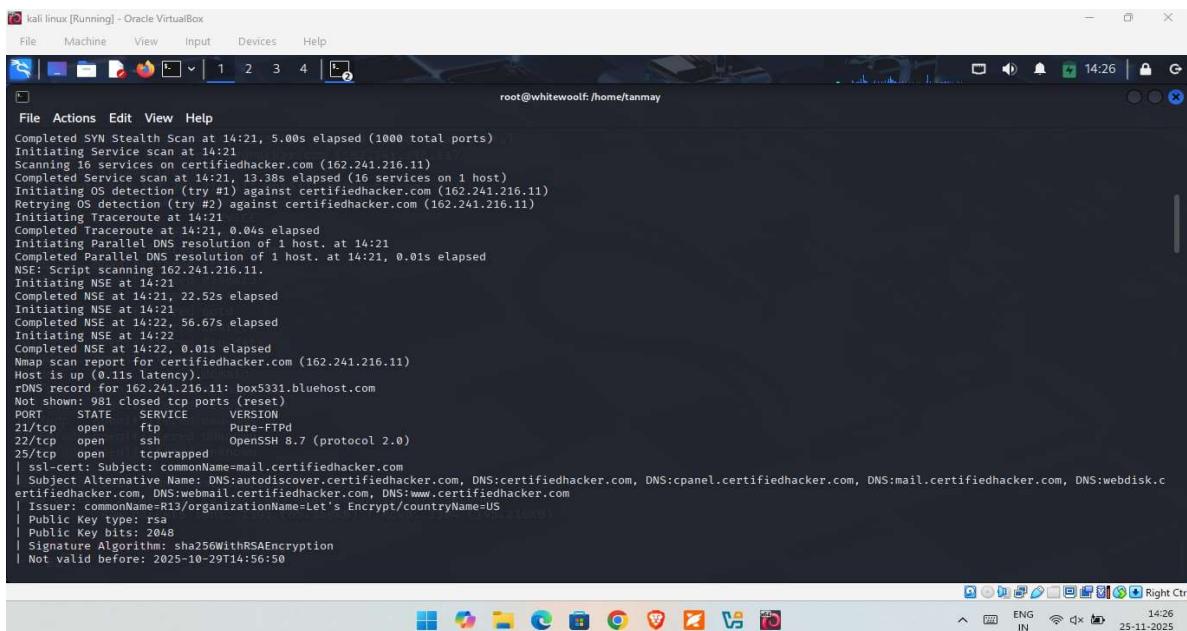


```
(root@whitewolf)-[~/home/tanmay]
└── nmap -sS -T4 -v certifiedhacker.com
Starting Nmap 7.91 ( https://nmap.org ) at 2025-11-25 14:21 IST
NSE: Script Pre-scanning.
Initiating NSE at 14:21
Completed NSE at 14:21, 0.00s elapsed
Initiating NSE at 14:21
Completed NSE at 14:21, 0.00s elapsed
Initiating NSE at 14:21
Completed NSE at 14:21, 0.00s elapsed
Initiating NSE at 14:21
Completed NSE at 14:21, 0.00s elapsed
Initiating Ping Scan at 14:21
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 14:21, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:21
Completed Parallel DNS resolution of 1 host. at 14:21, 0.30s elapsed
Initiating SYN Stealth Scan at 14:21
Scanning certifiedhacker.com (162.241.216.11) [1000 ports]
Completed SYN Stealth Scan at 14:21, 5.00s elapsed (1000 total ports)
Discovering open port 109/tcp on 162.241.216.11
Discovered open port 993/tcp on 162.241.216.11
Discovered open port 80/tcp on 162.241.216.11
Discovered open port 25/tcp on 162.241.216.11
Discovered open port 23/tcp on 162.241.216.11
Discovered open port 53/tcp on 162.241.216.11
Discovered open port 443/tcp on 162.241.216.11
Discovered open port 22/tcp on 162.241.216.11
Discovered open port 3306/tcp on 162.241.216.11
Discovered open port 995/tcp on 162.241.216.11
Discovered open port 143/tcp on 162.241.216.11
Discovered open port 465/tcp on 162.241.216.11
Discovered open port 5432/tcp on 162.241.216.11
Discovered open port 2222/tcp on 162.241.216.11
```

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

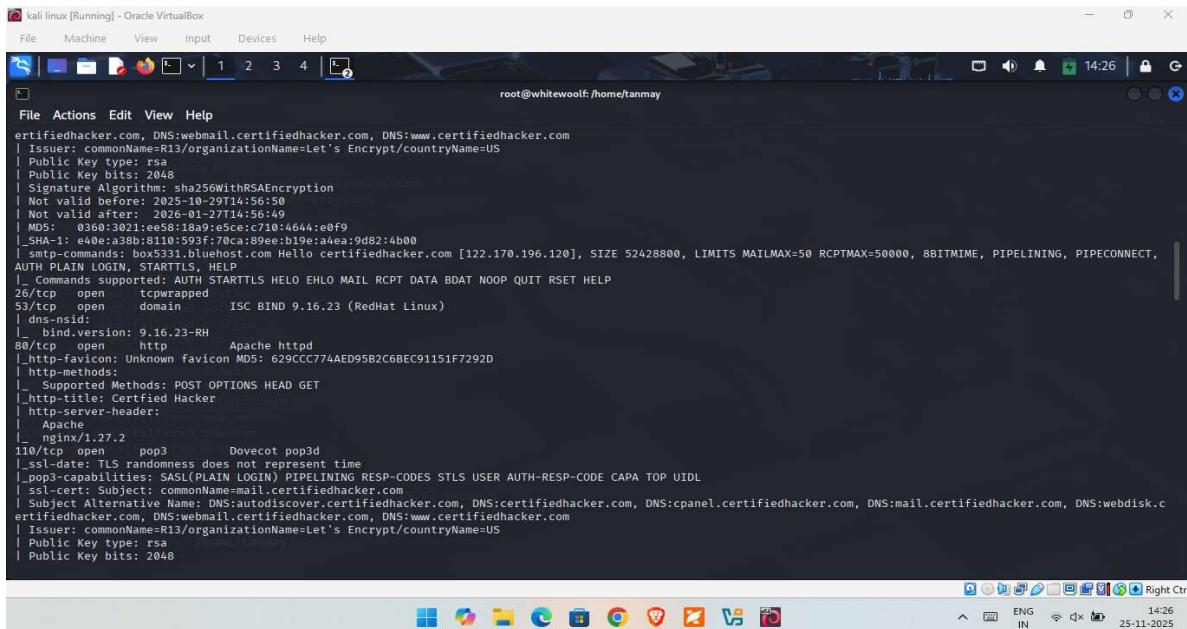


```
(root@whitewolf)-[~/home/tanmay]
└── nmap -sV -A certifiedhacker.com
Completed SYN Stealth Scan at 14:21, 5.00s elapsed (1000 total ports)
Initiating Service scan at 14:21
Scanning 16 services on certifiedhacker.com (162.241.216.11)
Completed Service scan at 14:21, 13.38s elapsed (16 services on 1 host)
Initiating OS detection (try #1) against certifiedhacker.com (162.241.216.11)
Retrying OS detection (try #2) against certifiedhacker.com (162.241.216.11)
Initiating Traceroute at 14:21
Completed Traceroute at 14:21, 0.04s elapsed
Initiating Parallel DNS resolution of 1 host. at 14:21
Completed Parallel DNS resolution of 1 host. at 14:21, 0.01s elapsed
NSE: Script scanning 162.241.216.11.
Initiating NSE at 14:21
Completed NSE at 14:21, 22.52s elapsed
Initiating NSE at 14:21
Completed NSE at 14:22, 56.67s elapsed
Initiating NSE at 14:22
Completed NSE at 14:22, 0.01s elapsed
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.11s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)
PORT      STATE     SERVICE      VERSION
21/tcp    open      ftp          Pure-FTPd
22/tcp    open      ssh          OpenSSH 8.7 (protocol 2.0)
25/tcp    open      tcpwrapped
|_ ssl-cert: Subject: commonName@mail.certifiedhacker.com
|_ subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:mail.certifiedhacker.com, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
|_ Issuer: commonName=R13/organizationName=Let's Encrypt/countryName=US
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2025-10-29T14:56:50
```

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

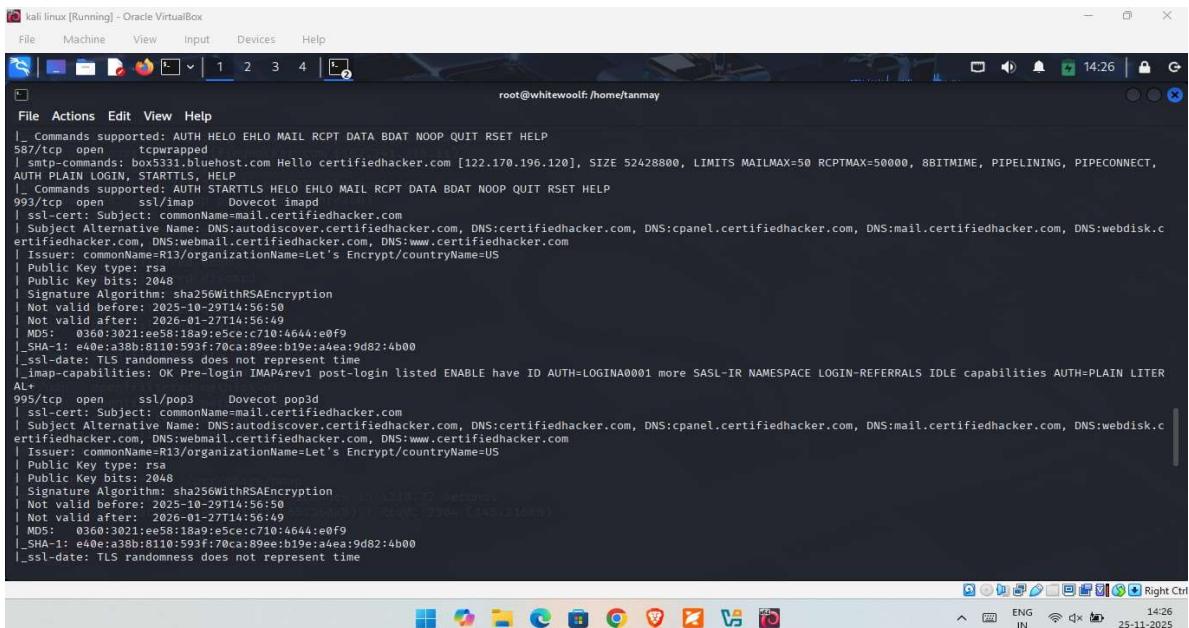


```
root@whitewolf:/home/tanmay
File Actions Edit View Help
certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
| Issuer: commonName=R13/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-10-29T14:56:50
| Not valid after: 2026-01-27T14:56:49
| MD5: 0360:3021:ee58:18a9:e5ce:c710:464:a:0ef9
| SHA-1: e40e:a38b:8110:593f:70ca:89ee:b19e:a4ea:9d82:4b00
|_ smtp-commands: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
26/tcp open tcpwrapped
53/tcp open domain ISC BIND 9.16.23 (RedHat Linux)
| dns-nsid:
|_ bind-version: 9.16.23-RH
80/tcp open http Apache httpd
| http-favicon: Unknown favicon MD5: 629CCC774AED95B2C6BEC91151F7292D
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
| http-title: Certified Hacker
| http-server-header:
|_ Apache
|_ nginx/1.27.2
110/tcp open pop3 Dovecot pop3d
|_ ssl-date: TLS randomness does not represent time
|_ ssl3-capabilities: SASL(PLAIN LOGIN) PIPELINING RESP-CODES STLS USER AUTH-RESP-CODE CAPA TOP UIDL
|_ ssl-cert: Subject: commonName=mail.certifiedhacker.com
|_ Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:mail.certifiedhacker.com, DNS:webdisk.c
certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
|_ Issuer: commonName=R13/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
```

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

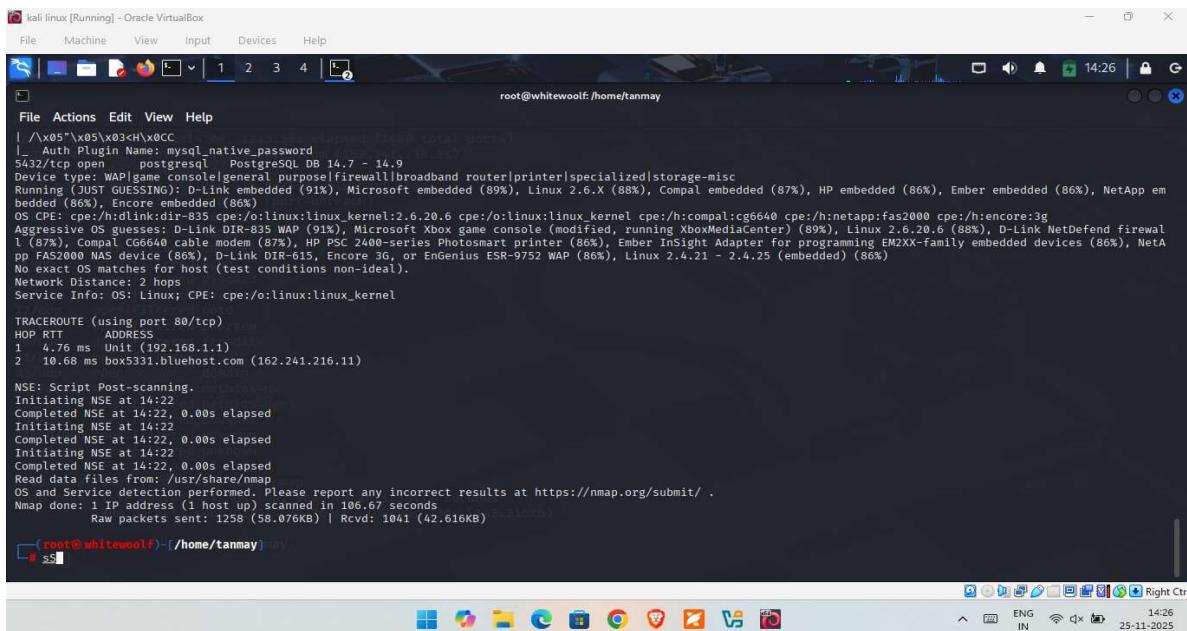


```
root@whitewolf:/home/tanmay
File Actions Edit View Help
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
587/tcp open tcpwrapped
|_ smtp-commands: box5331.bluehost.com Hello certifiedhacker.com [122.170.196.120], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT,
AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
993/tcp open ssl/imap Dovecot imapd
|_ ssl-cert: Subject: commonName=mail.certifiedhacker.com
|_ Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:mail.certifiedhacker.com, DNS:webdisk.c
certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
|_ Issuer: commonName=R13/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-10-29T14:56:50
| Not valid after: 2026-01-27T14:56:49
| MD5: 0360:3021:ee58:18a9:e5ce:c710:464:a:0ef9
| SHA-1: e40e:a38b:8110:593f:70ca:89ee:b19e:a4ea:9d82:4b00
|_ ssl-date: TLS randomness does not represent time
|_ imap-capabilities: OK Pre-login IMAP4rev1 post-login listed ENABLE have ID AUTH=LOGINA0001 more SASL-IR NAMESPACES LOGIN-REFERRALS IDLE capabilities AUTH=PLAIN LITER
AL+
995/tcp open ssl/pop3 Dovecot pop3d
|_ ssl-cert: Subject: commonName=mail.certifiedhacker.com
|_ Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:mail.certifiedhacker.com, DNS:webdisk.c
certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
|_ Issuer: commonName=R13/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-10-29T14:56:50
| Not valid after: 2026-01-27T14:56:49
| MD5: 0360:3021:ee58:18a9:e5ce:c710:464:a:0ef9
| SHA-1: e40e:a38b:8110:593f:70ca:89ee:b19e:a4ea:9d82:4b00
|_ ssl-date: TLS randomness does not represent time
```

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



```
|_ />x05">x05">x03<h>x0CC
|_ Auth Plugin Name: mysql_native_password
5432/tcp open  postgresql  PostgreSQL DB 14.7 - 14.9
Device type: WAP|game console|general purpose|firewall|broadband router|printer|specialized|storage-misc
Running OSes: JUST GUESSED! D-Link embedded (91%), Microsoft embedded (89%), Compaq embedded (87%), HP embedded (86%), Ember embedded (86%), NetApp embedded (86%), Encore embedded (86%)
OS: CPE: cpe:/h:dlink:dir-835 cpe:/o:linux:linux_kernel:2.6.20.6 cpe:/o:linux:linux_kernel cpe:/h:compal:cg6640 cpe:/h:netapp:fas2000 cpe:/h:encore:3g
Aggressive OS guesses: D-Link DIR-835 WAP (91%), Microsoft Xbox game console (modified, running XboxMediaCenter) (89%), Linux 2.6.20.6 (88%), D-Link NetDefend Firewall 1 (87%), Compaq CG6640 cable modem (87%), HP PSC 2400-series Photosmart printer (86%), Ember InSight Adapter for programming EM2XX-family embedded devices (86%), NetApp FAS2000 NAS device (86%), D-Link DIR-615, Encore 3G, or EnGenius ESR-9752 WAP (86%), Linux 2.4.21 - 2.4.25 (embedded) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

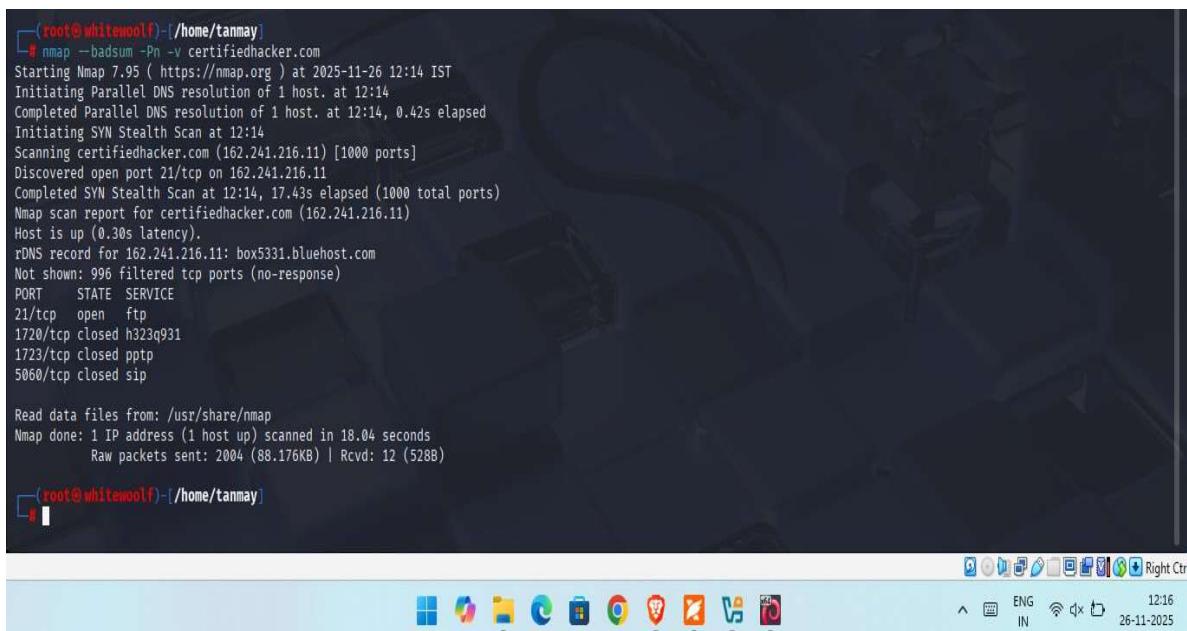
TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  4.76 ms  Unit (192.168.1.1)
2  10.68 ms box5331.bluehost.com (162.241.216.11)

NSE: Script Post-scanning.
Initiating NSE at 14:22
Completed NSE at 14:22, 0.00s elapsed
Initiating NSE at 14:22
Completed NSE at 14:22, 0.00s elapsed
Initiating NSE at 14:22
Completed NSE at 14:22, 0.00s elapsed
Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.67 seconds
Raw packets sent: 1258 (58.076KB) | Rcvd: 1041 (42.616KB)
```

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)



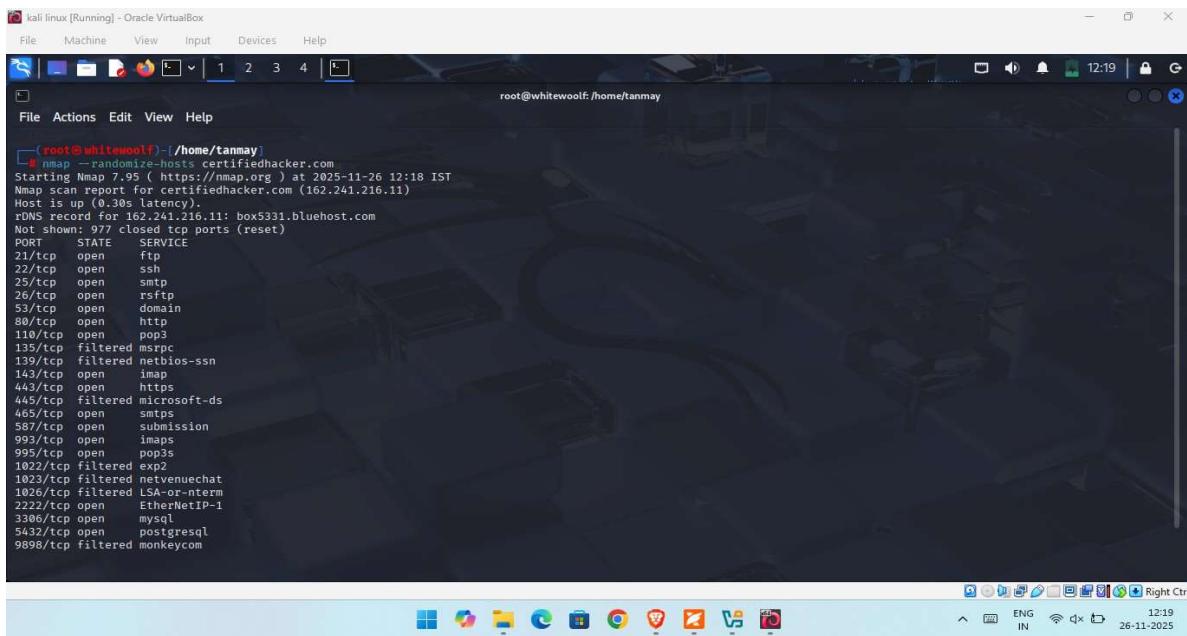
```
[root@whitewolf ~]# nmap --badsum -Pn -v certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 12:14 IST
Initiating Parallel DNS resolution of 1 host. at 12:14
Completed Parallel DNS resolution of 1 host. at 12:14, 0.42s elapsed
Initiating SYN Stealth Scan at 12:14
Scanning certifiedhacker.com (162.241.216.11) [1000 ports]
Discovered open port 21/tcp on 162.241.216.11
Completed SYN Stealth Scan at 12:14, 17.43s elapsed (1000 total ports)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.03s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
1723/tcp  closed pptp
5060/tcp  closed sip

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 18.04 seconds
Raw packets sent: 2004 (88.176KB) | Rcvd: 12 (528B)
```

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)

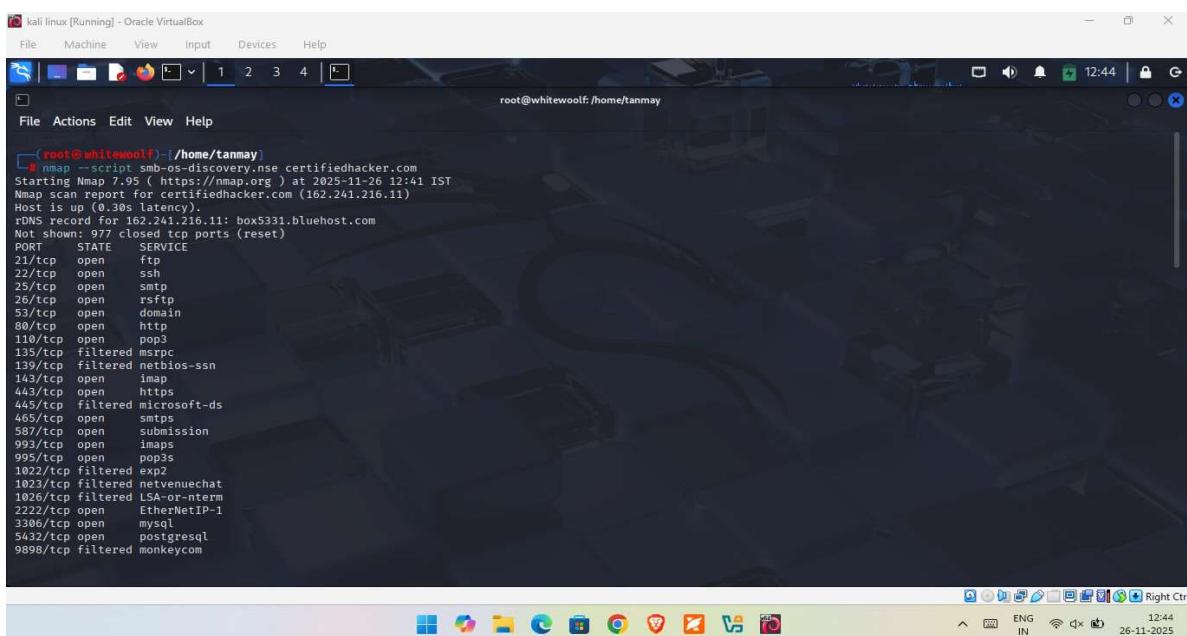


```
root@whitewoolf: /home/tanmay
# nmap --randomize-hosts certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 12:18 IST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.03s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 977 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
25/tcp    open     smtp
26/tcp    open     rsftp
53/tcp    open     domain
80/tcp    open     http
110/tcp   open     pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
445/tcp   filtered microsoft-ds
465/tcp   open     smtps
587/tcp   open     submission
993/tcp   open     imaps
995/tcp   open     pop3s
1022/tcp  filtered exp2
1023/tcp  filtered netvenuechat
1026/tcp  filtered LSA-or-nterm
2222/tcp  open     EtherNetIP-1
3306/tcp  open     mysql
5432/tcp  open     postgresql
9898/tcp  filtered monkeycom
```

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)

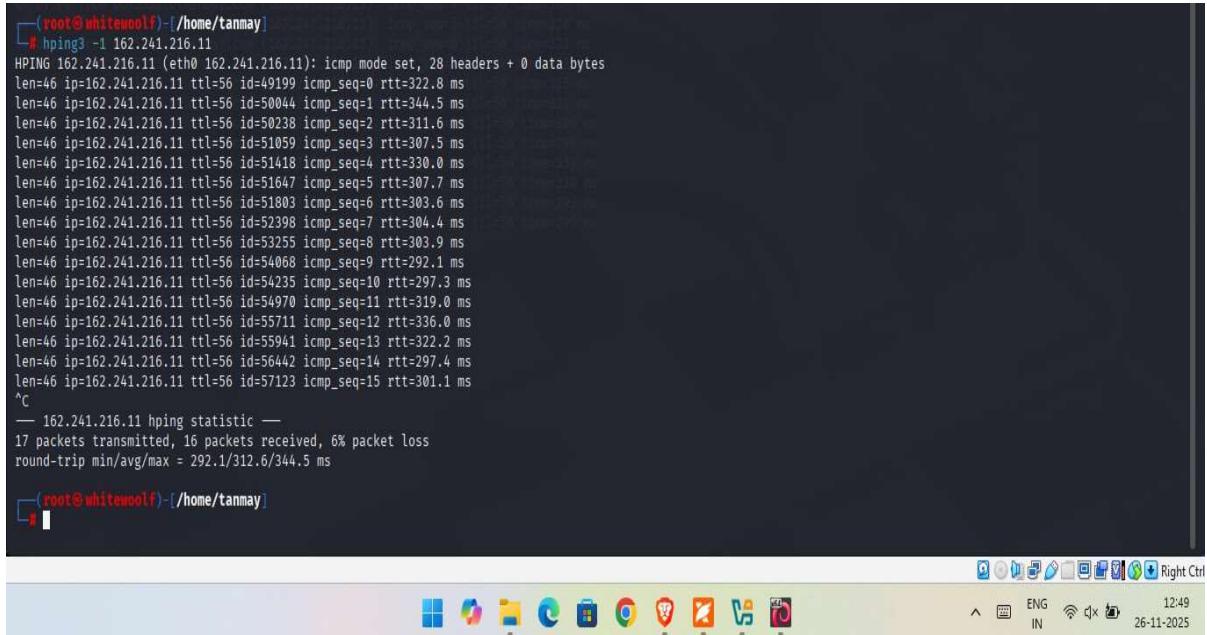


```
root@whitewoolf: /home/tanmay
# nmap --script smb-os-discovery.nse certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 12:41 IST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.03s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 977 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
25/tcp    open     smtp
26/tcp    open     rsftp
53/tcp    open     domain
80/tcp    open     http
110/tcp   open     pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
445/tcp   filtered microsoft-ds
465/tcp   open     smtps
587/tcp   open     submission
993/tcp   open     imaps
995/tcp   open     pop3s
1022/tcp  filtered exp2
1023/tcp  filtered netvenuechat
1026/tcp  filtered LSA-or-nterm
2222/tcp  open     EtherNetIP-1
3306/tcp  open     mysql
5432/tcp  open     postgresql
9898/tcp  filtered monkeycom
```

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)

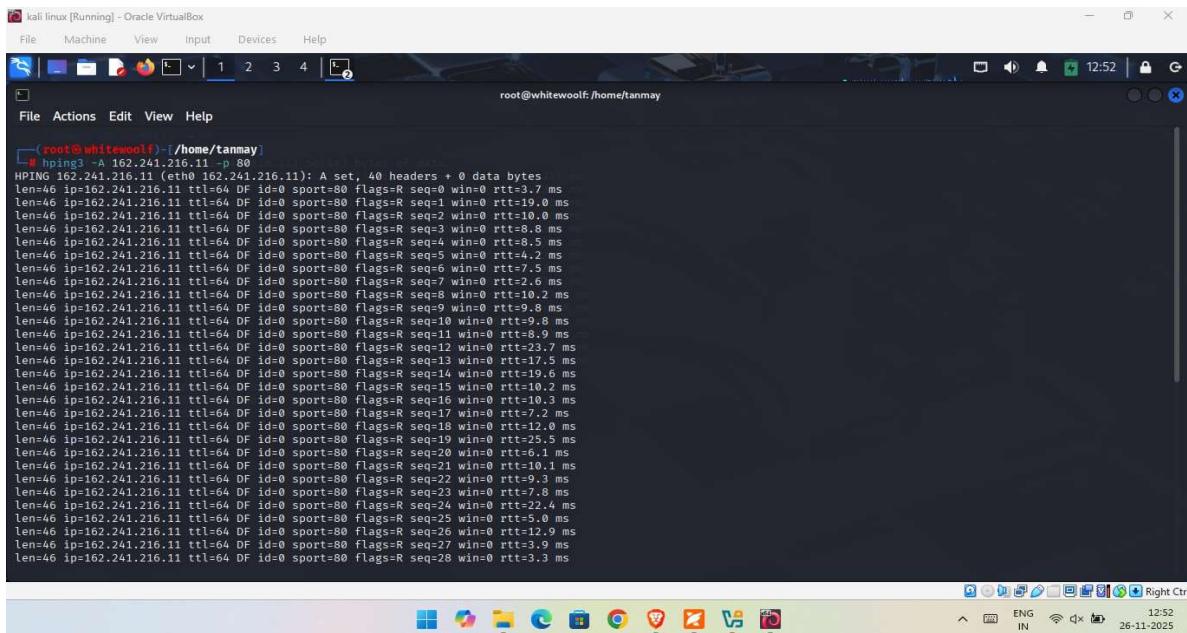


```
[root@whitewoolf ~]# hping3 -1 162.241.216.11
HPING 162.241.216.11 (eth0 162.241.216.11): icmp mode set, 28 headers + 0 data bytes
len=46 ip=162.241.216.11 ttl=56 id=49199 icmp_seq=0 rtt=322.8 ms
len=46 ip=162.241.216.11 ttl=56 id=50044 icmp_seq=1 rtt=344.5 ms
len=46 ip=162.241.216.11 ttl=56 id=50238 icmp_seq=2 rtt=311.6 ms
len=46 ip=162.241.216.11 ttl=56 id=51059 icmp_seq=3 rtt=307.5 ms
len=46 ip=162.241.216.11 ttl=56 id=51418 icmp_seq=4 rtt=330.0 ms
len=46 ip=162.241.216.11 ttl=56 id=51647 icmp_seq=5 rtt=307.7 ms
len=46 ip=162.241.216.11 ttl=56 id=51803 icmp_seq=6 rtt=303.6 ms
len=46 ip=162.241.216.11 ttl=56 id=52398 icmp_seq=7 rtt=304.4 ms
len=46 ip=162.241.216.11 ttl=56 id=53255 icmp_seq=8 rtt=303.9 ms
len=46 ip=162.241.216.11 ttl=56 id=54088 icmp_seq=9 rtt=292.1 ms
len=46 ip=162.241.216.11 ttl=56 id=54235 icmp_seq=10 rtt=297.3 ms
len=46 ip=162.241.216.11 ttl=56 id=54970 icmp_seq=11 rtt=319.0 ms
len=46 ip=162.241.216.11 ttl=56 id=55711 icmp_seq=12 rtt=336.0 ms
len=46 ip=162.241.216.11 ttl=56 id=55941 icmp_seq=13 rtt=322.2 ms
len=46 ip=162.241.216.11 ttl=56 id=56442 icmp_seq=14 rtt=297.4 ms
len=46 ip=162.241.216.11 ttl=56 id=57123 icmp_seq=15 rtt=301.1 ms
^C
-- 162.241.216.11 hping statistic --
17 packets transmitted, 16 packets received, 6% packet loss
round-trip min/avg/max = 292.1/312.6/344.5 ms
```

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)



```
[root@whitewoolf ~]# hping3 -S-A-p --tcp-timestamp 162.241.216.11
HPING 162.241.216.11 (eth0 162.241.216.11): A set, 40 headers + 0 data bytes
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0 rtt=3.7 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=1 win=0 rtt=19.0 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=2 win=0 rtt=10.0 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=3 win=0 rtt=8.8 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=4 win=0 rtt=8.5 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=5 win=0 rtt=4.2 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=6 win=0 rtt=7.5 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=7 win=0 rtt=2.6 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=8 win=0 rtt=10.2 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=9 win=0 rtt=9.8 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=10 win=0 rtt=9.6 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=11 win=0 rtt=8.9 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=12 win=0 rtt=23.7 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=13 win=0 rtt=19.3 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=14 win=0 rtt=19.9 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=15 win=0 rtt=10.2 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=16 win=0 rtt=10.3 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=17 win=0 rtt=7.2 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=18 win=0 rtt=12.0 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=19 win=0 rtt=25.5 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=20 win=0 rtt=6.1 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=21 win=0 rtt=10.1 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=22 win=0 rtt=9.3 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=23 win=0 rtt=7.8 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=24 win=0 rtt=22.4 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=25 win=0 rtt=5.0 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=26 win=0 rtt=12.9 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=27 win=0 rtt=3.9 ms
len=46 ip=162.241.216.11 ttl=64 DF id=0 sport=80 flags=R seq=28 win=0 rtt=3.3 ms
```

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

```
(root@whitewolf:~/home/tanmay)
# hping3 -c 1 -t -p 80 --tcp-timestamp
HPING 162.241.216.11 (eth0 162.241.216.11): S set, 40 headers + 0 data bytes
len=56 ip=162.241.216.11 ttl=56 id=0 sport=80 flags=SA seq=0 win=62636 rtt=311.8 ms
TCP timestamp: tcpts=3161186956

len=56 ip=162.241.216.11 ttl=56 id=0 sport=80 flags=SA seq=1 win=62636 rtt=298.4 ms
TCP timestamp: tcpts=3161187961
HZ seems hz=1000
System uptime seems: 36 days, 14 hours, 6 minutes, 27 seconds

len=56 ip=162.241.216.11 ttl=56 id=0 sport=80 flags=SA seq=2 win=62636 rtt=305.5 ms
TCP timestamp: tcpts=3161188956
HZ seems hz=1000
System uptime seems: 36 days, 14 hours, 6 minutes, 28 seconds

len=56 ip=162.241.216.11 ttl=56 id=0 sport=80 flags=SA seq=3 win=62636 rtt=308.4 ms
TCP timestamp: tcpts=3161189960
HZ seems hz=1000
System uptime seems: 36 days, 14 hours, 6 minutes, 29 seconds

len=56 ip=162.241.216.11 ttl=56 id=0 sport=80 flags=SA seq=4 win=62636 rtt=291.7 ms
TCP timestamp: tcpts=3161190950
HZ seems hz=1000
System uptime seems: 36 days, 14 hours, 6 minutes, 30 seconds

len=56 ip=162.241.216.11 ttl=56 id=0 sport=80 flags=SA seq=5 win=62636 rtt=307.9 ms
TCP timestamp: tcpts=3161191954
HZ seems hz=1000
System uptime seems: 36 days, 14 hours, 6 minutes, 31 seconds

len=56 ip=162.241.216.11 ttl=56 id=0 sport=80 flags=SA seq=6 win=62636 rtt=294.8 ms
```

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

```
> Frame 1: 1308 bytes on wire (10464 bits), 1308 bytes captured (10464 bits) on interface [Device: Intel_b7:54:30]
> Ethernet II, Src: NokiaSolutio_62:bb:61 (00:91:ca:62:bb:61), Dst: Intel_b7:54:30 (48:a4:72:b7)
> 802.1Q Virtual LAN, PPI: 0, DEI: 0, ID: 0
> Internet Protocol Version 4, Src: 20.216.166.59, Dst: 192.168.1.28
> Transmission Control Protocol, Src Port: 443, Dst Port: 7039, Seq: 1, Ack: 1, Len: 1250
0000  48 a4 72 b7 54 30 a9 91 ca 62 b6 61 81 00 00 H-r-T0- b-a...
0001  00 00 42 00 05 3e d5 00 00 00 00 00 00 00 00 .-E->-> G-
0002  00 3b 00 a9 1c 0d 00 00 00 00 00 00 00 00 00 .-P-> Y-.
0003  f4 02 50 10 00 3f 21 7b 00 00 17 03 03 40 11 86 p-?{ .....@-
0004  01 01 2c 08 b2 3c 61 c6 78 51 a1 16 6d ae ..Z,...< a:ZQ..m.
0005  62 3d 00 b9 54 d1 9d cc 20 74 16 28 20 28 ad 3d 75 b=+T...-p-4u
0006  c1 68 1a c7 cd 63 dd 7b 9a 9f 7d 35 82 00 99 h->c- ....S...
0007  9f 8e cc 74 23 b7 bc e8 a4 d1 82 bc da 51 50 ...ts-.....QP
0008  ce 38 0b 19 b6 e7 61 ac c6 cc a4 f3 dd aa 24 8-..w- .....$.
0009  ce 38 cs 1e 0d 22 1e d0 00 00 00 00 00 00 00 00 .8-]-> P-X-.
0009  57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 w-K-....8-fs-.
0009  c4 1e d1 32 2d 94 93 d2 7c 20 db 55 19 55 cb aa ..>2-... | _U-U..
0009  b7 72 f7 8b 67 76 75 83 d3 72 b4 ca 18 3e 2a 5d r->gvu cr->"]
0009  c9 8e al e3 81 02 b6 09 c5 74 6a 7e b9 af 77 .....>tj...>w
0009  3f 6d b6 22 3f 62 cd bd 69 55 48 9a dc 45 1f 7m="b... i-H-E-
00f0  9c 77 fa 3e c6 5d ad 61 24 1b ba fe ee 6e d0 d9 w->]-a $-...n-.
0100  05 59 b0 a2 a7 35 c1 1b 09 72 db 69 fc 68 8f 14 .Y-...S-...r-h-.
0110  cb a8 79 5a a1 3c 93 78 c3 b2 4a 78 c1 9a 27 4b .Y2-<x ..3x..K
0120  61 73 44 2b 82 fb 6d c8 c8 52 0e c4 82 20 a3 86 asD+-m- R...-
```

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)



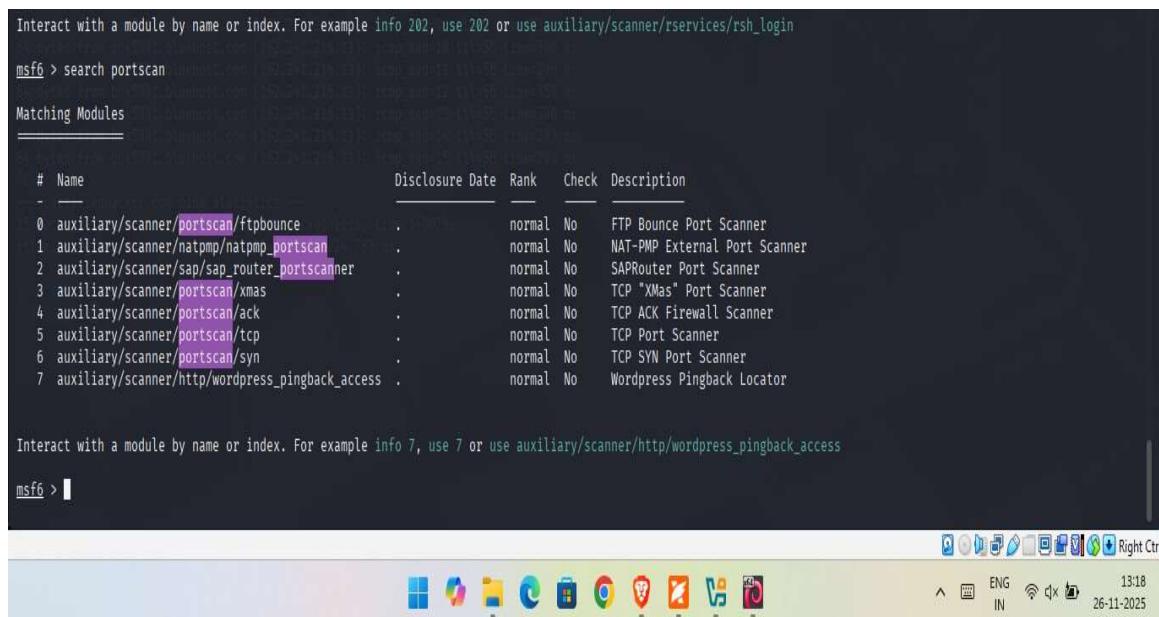
```
(root@whitehole)-[~/home/tanmay]
└─# hping3 -1 162.241.216.11 -a 162.241.216.11 -p 80 --flood
HPING 162.241.216.11 (eth0 162.241.216.11): icmp mode set, 28 headers + 0 data bytes
hpng in flood mode, no replies will be shown
^C
— 162.241.216.11 hping statistic —
701733 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

[root@whitehole)-[~/home/tanmay]
```

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



```
Interact with a module by name or index. For example info 202, use 202 or use auxiliary/scanner/rservices/rsh_login

msf6 > search portscan
Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
--  --
0  auxiliary/scanner/ftpbounce              .             normal  No     FTP Bounce Port Scanner
1  auxiliary/scanner/natpmp/natpmp_portscan .             normal  No     NAT-PMP External Port Scanner
2  auxiliary/scanner/sap/sap_router_portscanner .             normal  No     SAPRouter Port Scanner
3  auxiliary/scanner/portscan/xmas          .             normal  No     TCP "XMas" Port Scanner
4  auxiliary/scanner/portscan/ack           .             normal  No     TCP ACK Firewall Scanner
5  auxiliary/scanner/portscan/tcp           .             normal  No     TCP Port Scanner
6  auxiliary/scanner/portscan/syn          .             normal  No     TCP SYN Port Scanner
7  auxiliary/scanner/http/wordpress_pingback_access .             normal  No     Wordpress Pingback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access

msf6 > |
```

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.

