LOYOLA ACADEMY DEGREE & PG COLLEGE
(AUTONOMOUS)

ALWAL, SECUNDERABAD-500010

ACCREDITED BY NAAC WITH 'A' GRADE

A COLLEGE WITH POTENTIAL AND EXCELLENCE

B.Sc Computer Science and Cyber Security

THIS IS TO CERTIFY THAT THIS IS A BONAFIDE RECORD ON

Ethical Hacking

DONE DURING THE **SECOND YEAR, THIRD SEMESTER** FOR THE **ACADEMIC YEAR 2024-2025**

Name :
Class : NCSCS
UID :

Internal examiner **Principal** **External examiner**

INDEX

S.No.	Topic	Page No.	Signature
1	Open Source Reconnaissance Tool Recon-ng		
2	Enumeration of resources in a Local Machine using Hyena		
3	Enumerating Services on a Target Machine		
4	Open Source Information Gathering- Windows Command Line Utilities		
5	Collecting Information about Target Website - Firebug		
6	Network Scanning – Nmap Tool		
7	Detecting Phishing using Netcraft		
8	Sniffing Facebook Credentials- Social Engineering Toolkit		
9	Basic Disk encryption - VeraCrypt		

1. Open Source reconnaissance tool Recon-ng

Aim : Use Recong-ng tool together personal information

Step 1: Install Recon-ng

Recon-ng should come pre-installed on Kali Linux. If not, you can install it using the following command:
sudo apt-get update
sudo apt-get install recon-ng

Step 2 :Launch Recon-ng

Open a terminal and start Recon-ng by typing:

recon-ng

Step 3: Create a Workspace

Create a new workspace to keep your session organized: workspaces create google_info

Step 4: Add the Target Domain

Add the target domain (google.com) to the Recon-ng database: add **domains google.com**

Step 5: List Available Modules

View the available modules in Recon-ng. These modules are categorized for different types of information gathering:
show modules

Step 6: Use Specific Modules to Gather Information

a. Gather Hosts Information

Use the recon/domains-hosts/bing_domain_web module to find hosts within the google.com domain:
use
recon/domains-hosts/bing_domain_web
set SOURCE google.com
run

b. Gather Contacts Information

Use the recon/domains-contacts/whois_pocs module to gather point of contact information from WHOIS records:
use
recon/domains-contacts/whois_pocs
set SOURCE
run google.com

c. Gather Subdomains

Use the recon/domains-hosts/brute_hosts module to brute force subdomains:

use recon/domains-hosts/brute_hosts

set SOURCE www.google.com

Run

d. Gather DNS Information

Use the recon/hosts-hosts/resolve module to resolve hostnames to IP addresses:

use recon/hosts-hosts/resolve

Run

Step 7: List Collected Data

You can view the collected data using the show command:

show hosts

show

contacts

show

domains

Step 8: Generate Reports

Generate reports in various formats like CSV, JSON, or HTML to share with your students:

use reporting/csv

set FILENAME

googlereport.csv run

Step 9: Exit Recon-ng

Once you have gathered all the necessary information, you can exit

Recon-ng: exit

```
[1] Recon modules

[recon-ng][default] > workspaces create google_info
[recon-ng][google_info] > marketplace search

+-------------------------------------------------------------------------------------------+
|                          Path                          | Version |     Status    | Updated    | D | K |
+-------------------------------------------------------------------------------------------+
| discovery/info_disclosure/cache_snoop                  | 1.1     | not installed | 2020-10-13 |   |   |
| discovery/info_disclosure/interesting_files            | 1.2     | not installed | 2021-10-04 |   |   |
| exploitation/injection/command_injector                | 1.0     | not installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter                    | 1.2     | not installed | 2019-10-08 |   |   |
| import/csv_file                                        | 1.1     | not installed | 2019-08-09 |   |   |
| import/list                                            | 1.1     | not installed | 2019-06-24 |   |   |
| import/masscan                                         | 1.0     | not installed | 2020-04-07 |   |   |
| import/nmap                                            | 1.1     | not installed | 2020-10-06 |   |   |
| recon/companies-contacts/bing_linkedin_cache           | 1.0     | not installed | 2019-06-24 |   | * |
| recon/companies-contacts/censys_email_address          | 2.1     | not installed | 2022-01-31 | * | * |
| recon/companies-contacts/pen                           | 1.1     | not installed | 2019-10-15 |   |   |
| recon/companies-domains/censys_subdomains              | 2.1     | not installed | 2022-01-31 | * | * |
```

```
| recon/companies-domains/pen                          | 1.1     | not installed | 2019-10-15 |    |    |
| recon/companies-domains/viewdns_reverse_whois        | 1.1     | installed     | 2021-08-24 |    |    |
| recon/companies-domains/whoxy_dns                    | 1.1     | not installed | 2020-06-17 |    | *  |
| recon/companies-multi/censys_org                     | 2.1     | not installed | 2022-01-31 | *  | *  |
| recon/companies-multi/censys_tls_subjects            | 2.1     | not installed | 2022-01-31 | *  | *  |
| recon/companies-multi/github_miner                   | 1.1     | not installed | 2020-05-15 |    | *  |
| recon/companies-multi/shodan_org                     | 1.1     | not installed | 2020-07-01 | *  | *  |
| recon/companies-multi/whois_miner                    | 1.1     | not installed | 2019-10-15 |    |    |
| recon/contacts-contacts/abc                          | 1.0     | not installed | 2019-10-11 | *  |    |
| recon/contacts-contacts/mailtester                   | 1.0     | not installed | 2019-06-24 |    |    |
| recon/contacts-contacts/mangle                       | 1.0     | not installed | 2019-06-24 |    |    |
| recon/contacts-contacts/unmangle                     | 1.1     | not installed | 2019-10-27 |    |    |
| recon/contacts-credentials/hibp_breach               | 1.2     | not installed | 2019-09-10 |    | *  |
| recon/contacts-credentials/hibp_paste                | 1.1     | not installed | 2019-09-10 |    | *  |
| recon/contacts-domains/censys_email_to_domains       | 2.1     | not installed | 2022-01-31 | *  | *  |
| recon/contacts-domains/migrate_contacts              | 1.1     | not installed | 2020-05-17 |    |    |
| recon/contacts-profiles/fullcontact                  | 1.1     | not installed | 2019-07-24 |    | *  |
| recon/credentials-credentials/adobe                  | 1.0     | not installed | 2019-06-24 |    |    |
| recon/credentials-credentials/bozocrack              | 1.0     | not installed | 2019-06-24 |    |    |
| recon/credentials-credentials/hashes_org             | 1.0     | not installed | 2019-06-24 |    | *  |
| recon/domains-companies/censys_companies             | 2.1     | not installed | 2022-01-31 | *  | *  |
| recon/domains-companies/pen                          | 1.1     | not installed | 2019-10-15 |    |    |
| recon/domains-companies/whoxy_whois                  | 1.1     | not installed | 2020-06-24 |    | *  |
| recon/domains-contacts/hunter_io                     | 1.3     | not installed | 2020-04-14 |    | *  |
| recon/domains-contacts/metacrawler                   | 1.1     | not installed | 2019-06-24 | *  |    |
| recon/domains-contacts/pen                           | 1.1     | not installed | 2019-10-15 |    |    |
| recon/domains-contacts/pgp_search                    | 1.4     | not installed | 2019-10-16 |    |    |
| recon/domains-contacts/whois_pocs                    | 1.0     | not installed | 2019-06-24 |    |    |
| recon/domains-contacts/wikileaker                    | 1.0     | not installed | 2020-04-08 |    |    |
| recon/domains-domains/brute_suffix                   | 1.1     | not installed | 2020-05-17 |    |    |
| recon/domains-hosts/binaryedge                       | 1.2     | not installed | 2020-06-18 |    | *  |
| recon/domains-hosts/bing_domain_api                  | 1.0     | not installed | 2019-06-24 |    | *  |
| recon/domains-hosts/bing_domain_web                  | 1.1     | not installed | 2019-07-04 |    |    |
| recon/domains-hosts/brute_hosts                      | 1.0     | not installed | 2019-06-24 |    |    |
| recon/domains-hosts/builtwith                        | 1.1     | not installed | 2021-08-24 |    | *  |
| recon/domains-hosts/censys_domain                    | 2.1     | not installed | 2022-01-31 | *  | *  |
| recon/domains-hosts/certificate_transparency         | 1.3     | not installed | 2019-09-16 |    |    |
| recon/domains-hosts/google_site_web                  | 1.0     | not installed | 2019-06-24 |    |    |
| recon/domains-hosts/hackertarget                     | 1.1     | not installed | 2020-05-17 |    |    |
| recon/domains-hosts/mx_spf_ip                        | 1.0     | not installed | 2019-06-24 |    |    |
| recon/domains-hosts/netcraft                         | 1.1     | not installed | 2020-02-05 |    |    |
| recon/domains-hosts/shodan_hostname                  | 1.1     | not installed | 2020-07-01 | *  | *  |
```

```
| recon/repositories-profiles/github_commits           | 1.0     | not installed | 2019-06-24 |    | *  |
| recon/repositories-vulnerabilities/gists_search      | 1.0     | not installed | 2019-06-24 |    |    |
| recon/repositories-vulnerabilities/github_dorks      | 1.0     | not installed | 2019-06-24 |    | *  |
| reporting/csv                                        | 1.0     | not installed | 2019-06-24 |    |    |
| reporting/html                                       | 1.0     | not installed | 2019-06-24 |    |    |
| reporting/json                                       | 1.0     | not installed | 2019-06-24 |    |    |
| reporting/list                                       | 1.0     | not installed | 2019-06-24 |    |    |
| reporting/proxifier                                  | 1.0     | not installed | 2019-06-24 |    |    |
| reporting/pushpin                                    | 1.0     | not installed | 2019-06-24 |    | *  |
| reporting/xlsx                                       | 1.0     | not installed | 2019-06-24 |    |    |
| reporting/xml                                        | 1.1     | not installed | 2019-06-24 |    |    |
+------------------------------------------------------+---------+---------------+------------+----+----+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][google_info] > marketplace install recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Reloading modules ...
```

```
[recon-ng][google_info] > marketplace info
Shows detailed information about available modules

Usage: marketplace info <<path>|<prefix>|all>

[recon-ng][google_info] > marketplace info recon/companies-domains/viewdns_reverse_whois

  +--------------+-----------------------------------------------------------------------------------+
  | path         | recon/companies-domains/viewdns_reverse_whois                                     |
  | name         | Viewdns Reverse Whois Domain Harvester                                            |
  | author       | Gaetan Ferry (@_mabote_) from @synacktiv                                          |
  | version      | 1.1                                                                               |
  | last_updated | 2021-08-24                                                                        |
  | description  | Harvests domain names belonging to a company by using the viewdns.info free reverse whois tool. |
  | required_keys | []                                                                               |
  | dependencies | []                                                                                |
  | files        | []                                                                                |
  | status       | installed                                                                         |
  +--------------+-----------------------------------------------------------------------------------+

[recon-ng][google_info] > modules load recon/companies-domains/viewdns_reverse_whois
[recon-ng][google_info][viewdns_reverse_whois] > options set SOURCE google.com
SOURCE => google.com
```

2. Enumeration Resources in a Local Machine using Hyena

Aim : To enumerate the resources in a local machine using Hyena

Step 1 . Download and Install Hyena:

- Visit the Hyena website (https://www.hyena.com/) and download the latest version for your operating system (Windows, Linux, or macOS).
- Follow the installation instructions provided in the downloaded package.

Step 2: Open Hyena:

- Once installed, launch Hyena from your start menu or desktop shortcut

Step 3: Connect to Your Local Machine:

- In the Hyena interface, click on the "Connect" button.
- In the "Connect to" dialog box, select "Local Machine" and click “ok "

Step 4: Navigate to the Resources View:

- In the main Hyena window, navigate to the "Resources" view. This might be located under the "View" menu or directly in the toolbar.

Step 5: Enumerate Resources:

- The "Resources" view will display a list of resources available on your local machine. These might include:
  - **Shared Folders:** Folders that are shared with other users on the network.
  - **Printers:** Printers connected to your machine.
  - **Services:** Background processes running on your machine.
  - **Users:** User accounts on your machine.
  - **Groups:** Groups of users with specific permissions.
  - **Processes:** Running applications and services.
  - **Registry Keys:** Entries in the Windows Registry.
- To enumerate a specific resource, double-click on it to open its properties.
- You can use the search bar in the "Resources" view to quickly find specific resources.

Step 6: Explore Resource Properties:

- When you double-click on a resource, Hyena will display its properties in a separate window. This window will provide detailed information about the resource, such as:
  - **Name:** The name of the resource.
  - **Description:** A brief description of the resource.
  - **Location:** The path to the resource.
  - **Type:** The type of resource (e.g., file, folder, printer).

○ **Permissions:** The permissions granted to different users and groups for the resource.

○ **Other properties:** Depending on the resource type, there might be additional properties.

Step 7: Perform Additional Actions:

● Hyena allows you to perform various actions on resources, such as:

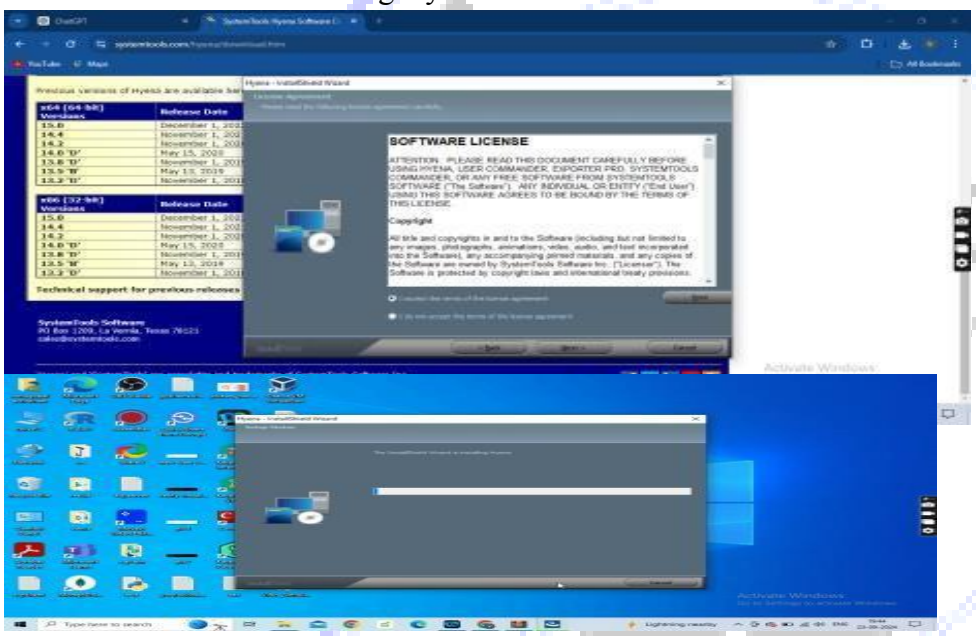
○ **Modifying permissions:** Changing who can access and modify the resource. ○ **Creating or deleting resources:** Creating new resources or deleting existing ones.

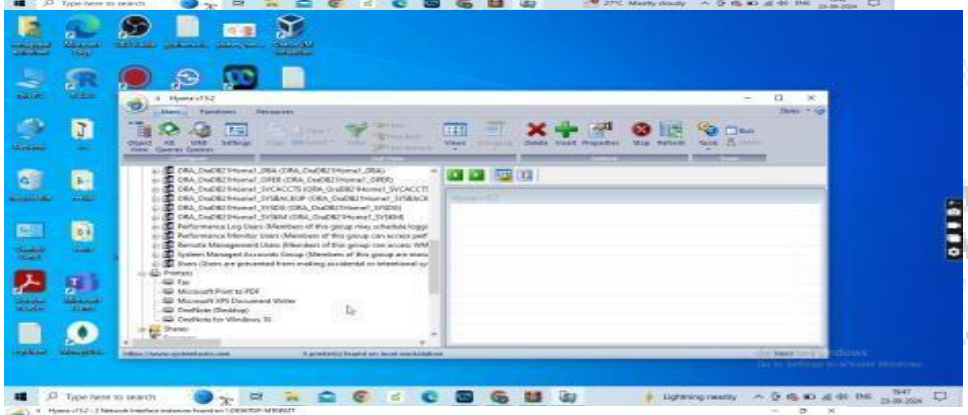
○ **Starting or stopping services:** Controlling the running of background processes.

○ **Printing files:** Printing documents and other files.

○ **And more:** The specific actions available will depend on the type of resource.

By following these steps, you can effectively enumerate and explore resources on your local machine using Hyena.





3. Enumerating Services on a Target Machine

Aim

To enumerate services running on a target machine using tools in Kali Linux.

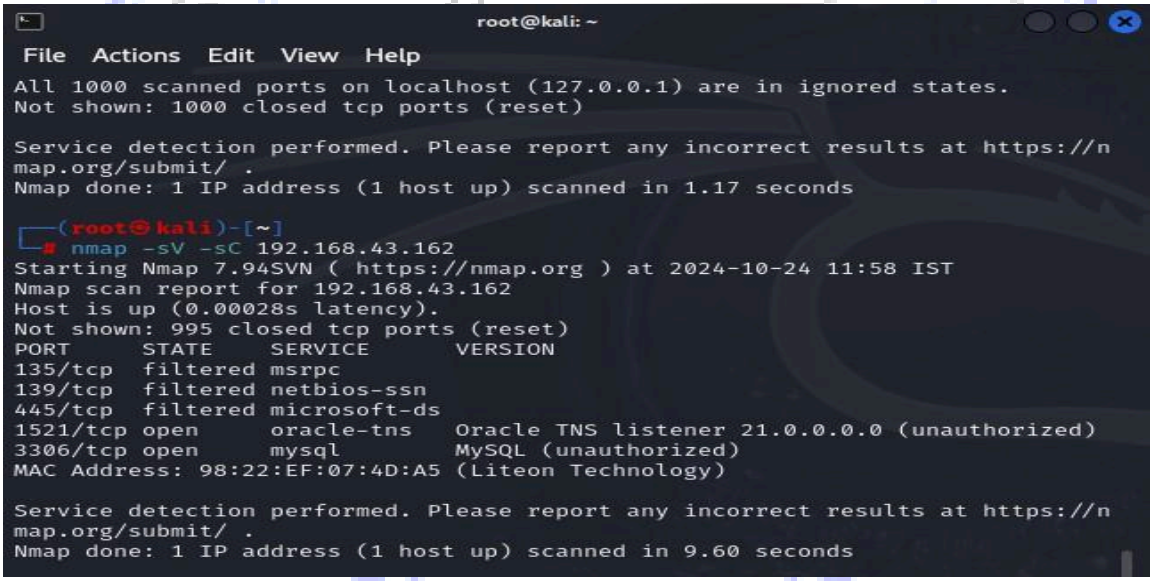
Tools

- Kali Linux
- Nmap
- Netcat
- Nikto
- Enum4linux
- snmpwalk

Step 1: Conduct a service scan using Nmap to identify open ports and services.

Command: nmap -sV -sC <Target_IP>

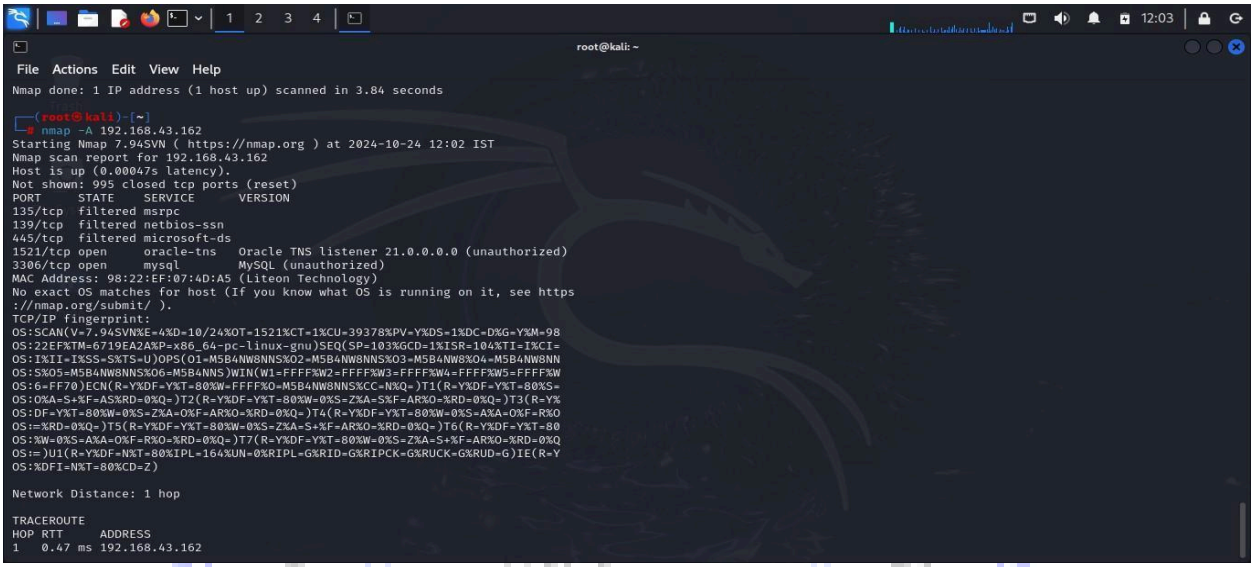
nmap -sV -sC 192.168.43.162



Step -2

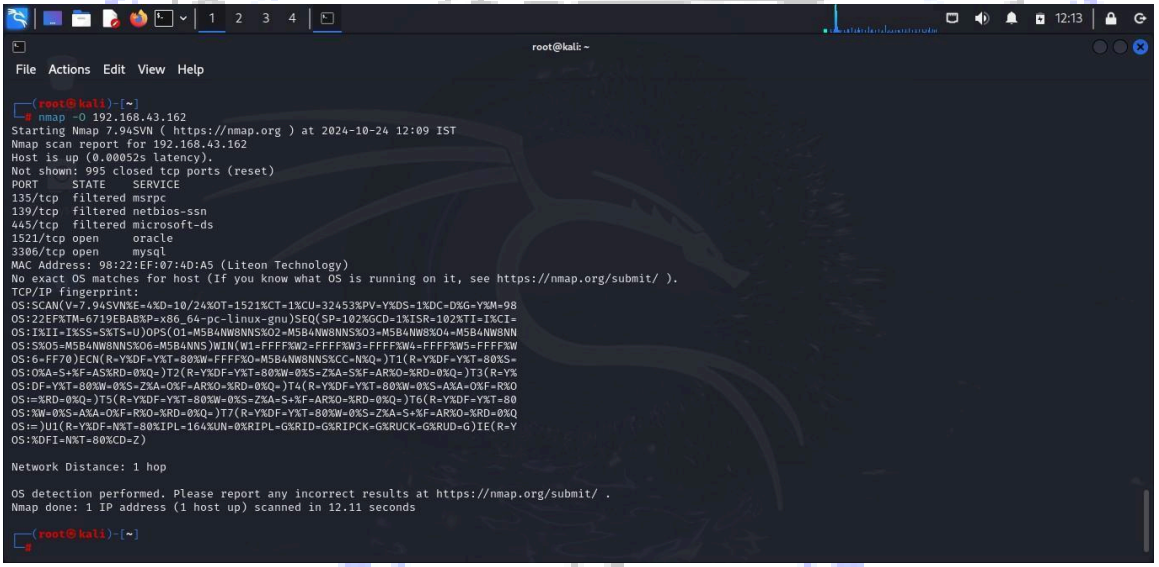
Use the Command Option -A to get combine several functionalities like OS detection, version detection, script scanning

nmap - A 192.168.43.162



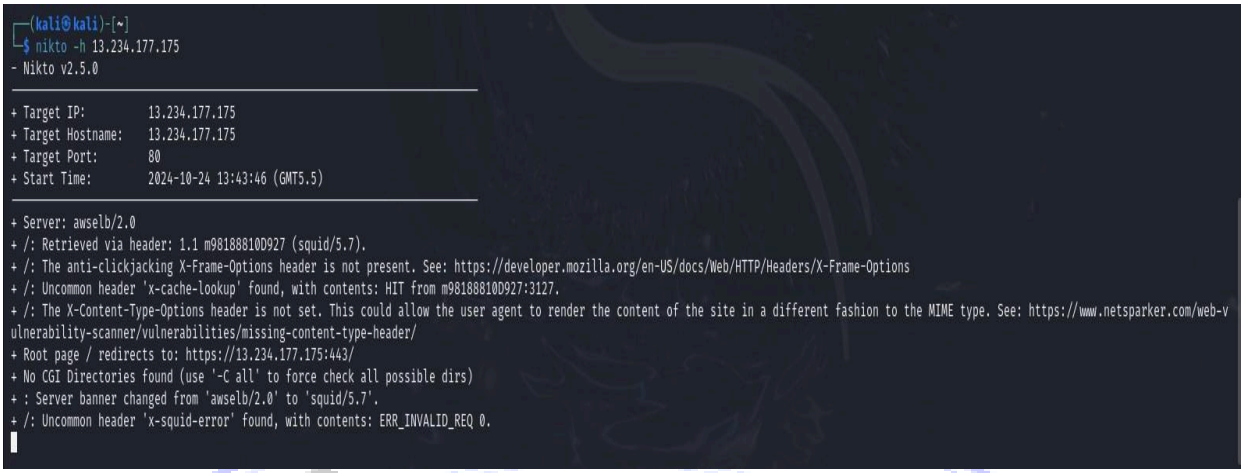
step 3: Use the command option -O for getting the OS details nmap -O <target Address>

nmap -O 192.168.43.162



Step 4: Perform web server enumeration using Nikto if applicable.

- Command: nikto -h <Target_IP> nikto -h 192.168.43.162



Step 5: Run Enum4linux to gather SMB service information. Command: enum4linux -a <Target_IP>

enum4linux -a 157.248.241.174

4. Open Source Information Gathering using Windows Command Line

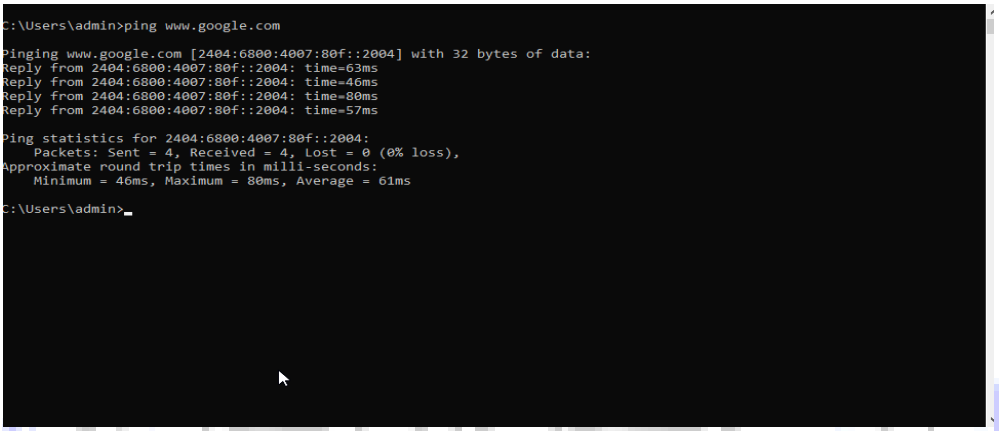
Aim : To collect open source information using Windows command line.

1. **Basic Network Information Gathering:**

- **Identify Target:** Define the domain name or IP address you're investigating.

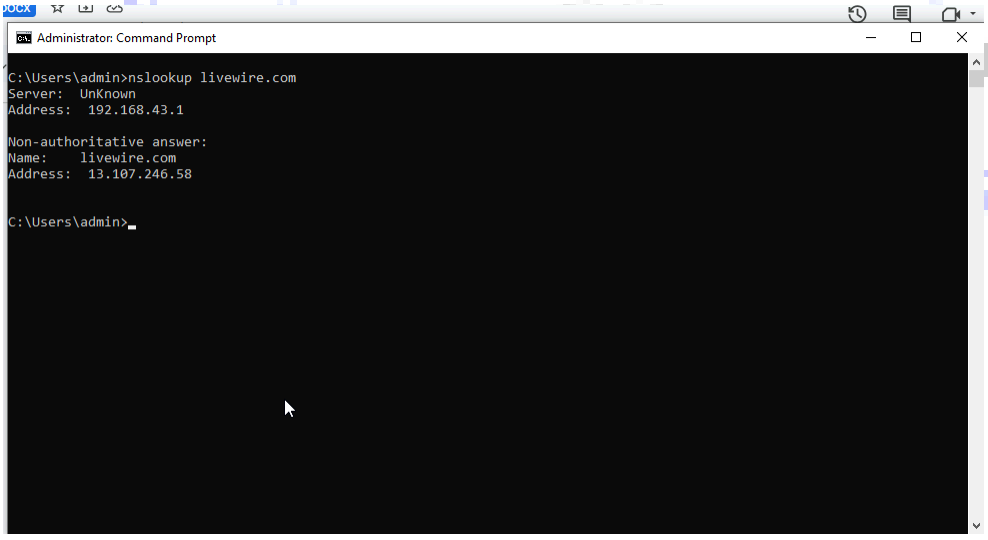
- **Ping (ICMP Echo Request):** Use the **ping** command followed by the target domain or IP to check reachability and measure response time.

ping google.com



- **Hostname Resolution (DNS Lookup):** Utilize the **nslookup** command to translate a domain name to its corresponding IP address(es) and vice versa.

nslookup lifewire.com



2. Finding Maximum Frame Size

```
C:\WINDOWS\system32>ping www.google.com -f -l 1500

Pinging www.google.com [142.250.67.164] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 142.250.67.164:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINDOWS\system32>
```

```
C:\Windows\System32\cmd.exe

C:\WINDOWS\system32>ping www.google.com -f -l 1500

Pinging www.google.com [142.250.67.164] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 142.250.67.164:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINDOWS\system32>ping www.google.com -f -l 1300

Pinging www.google.com [142.250.67.164] with 1300 bytes of data:
Reply from 142.250.67.164: bytes=1300 time=18ms TTL=59
Reply from 142.250.67.164: bytes=1300 time=17ms TTL=59
Reply from 142.250.67.164: bytes=1300 time=17ms TTL=59
Reply from 142.250.67.164: bytes=1300 time=18ms TTL=59

Ping statistics for 142.250.67.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 18ms, Average = 17ms

C:\WINDOWS\system32>
```

3. TTL - Ping with option -i

It allows you to specify the Time-to-Live (TTL) value for the ICMP echo request packets. This can be useful for tracing the path a packet takes to its destination

ping -i<TTL_value> <target_address>
ping –i 2 www.google.com

The -i option in the ping command is used to specify the interval between pings in seconds

```
C:\WINDOWS\system32>ping -i 2 www.google.com

Pinging www.google.com [142.250.67.164] with 32 bytes of data:
Reply from 202.160.160.57: TTL expired in transit.
Reply from 202.160.160.57: TTL expired in transit.
Reply from 202.160.160.57: TTL expired in transit.
Reply from 202.160.160.57: TTL expired in transit.

Ping statistics for 142.250.67.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\WINDOWS\system32>ping  www.google.com -i 2

Pinging www.google.com [142.250.67.132] with 32 bytes of data:
Reply from 202.160.160.57: TTL expired in transit.
Reply from 202.160.160.57: TTL expired in transit.
Reply from 202.160.160.57: TTL expired in transit.
Reply from 202.160.160.57: TTL expired in transit.

Ping statistics for 142.250.67.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\WINDOWS\system32>
```

4. **Trace Route (Path Mapping):** Employ the tracert command (Windows) or **traceroute** command (Linux/macOS) to visualize the route packets take from your system to the target, identifying any intermediate network hops.

   tracert microsoft.com (Windows)

   traceroute google.com (Linux/macOS)

```
C:\WINDOWS\system32>tracert www.google.com

Tracing route to www.google.com [142.250.67.132]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     3 ms     3 ms     3 ms  undefined.hostname.localhost [202.160.160.57]
  3     *        *        *     Request timed out.
  4    22 ms    23 ms    22 ms  72.14.202.41
  5    25 ms    25 ms    24 ms  74.125.37.7
  6    18 ms    19 ms    20 ms  142.250.227.71
  7    19 ms    19 ms    20 ms  bom12s06-in-f4.1e100.net [142.250.67.132]

Trace complete.

C:\WINDOWS\system32>
```

5. DNS Record Exploration:

● **DNS Record Lookup:** ●

nslookup wikipedia.com

```
C:\WINDOWS\system32>nslookup wikipedia.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    wikipedia.com
Addresses:  2001:df2:e500:ed1a::3
          103.102.166.226


C:\WINDOWS\system32>
```

5. Collecting information about target website using Firebug

Aim: To collect information about target website using Firebug

Firebug was a popular web development tool for inspecting HTML, CSS, and JavaScript on web pages, but it has been discontinued. Similar functionality is now integrated into modern browsers like Google Chrome and Firefox Developer Tools.

Step 1: Open the Developer Tools:

- In **Google Chrome** or **Firefox**, right-click anywhere on the web page you want to inspect and select **"Inspect"** or **"Inspect Element"**.
- Alternatively, you can press **F12** or **Ctrl + Shift + I** (Windows/Linux) or **Cmd + Option + I** (Mac) to open Developer Tools.

Step 2: Inspect Elements (HTML):

- In the Developer Tools window, the default view is often the **"Elements"** panel, which displays the HTML structure of the webpage.
- Hover over different HTML elements in this panel to see their visual representation on the webpage highlighted.
- You can also click on any HTML tag to see its properties, attributes (like class, id), and associated styles (CSS rules).

Step 3:View CSS (Cascading Style Sheets):

- The **"Styles"** pane on the right side of the "Elements" panel shows the CSS rules applied to the selected HTML element.
- You can edit the CSS here in real-time to see how changes affect the page's layout and styling.

Step 4: JavaScript Console:

- Click on the **"Console"** tab to view any JavaScript errors or logs on the webpage.
- You can also use the console to execute JavaScript commands, which is useful for testing or modifying JavaScript functionality on the fly.

Step 5:Network Activity (Request/Response Data):

- Click the **"Network"** tab to track all network requests made by the webpage, including API requests, AJAX calls, and asset loading (like images, CSS, and JavaScript files).
- Each request displays its status, type, size, and response time. Click on a request to view more detailed headers, response data, and timing breakdown.
- This is particularly useful for identifying endpoints or tracking how the website communicates with a backend server.

Step 6: View Cookies and Storage:

- Click the **"Application"** tab to inspect data related to storage, including cookies, local storage, and session storage.
- You can view stored data, add, delete, or modify entries. This is useful for understanding what

information the site stores in your browser.

Step 7: View JavaScript Events:

- In the **"Event Listeners"** section of the "Elements" panel, you can see JavaScript events attached to specific elements on the webpage.
- This allows you to trace how the page interacts with user actions, like clicks, mouse movements, or key presses.

Step 8: View Page Source:

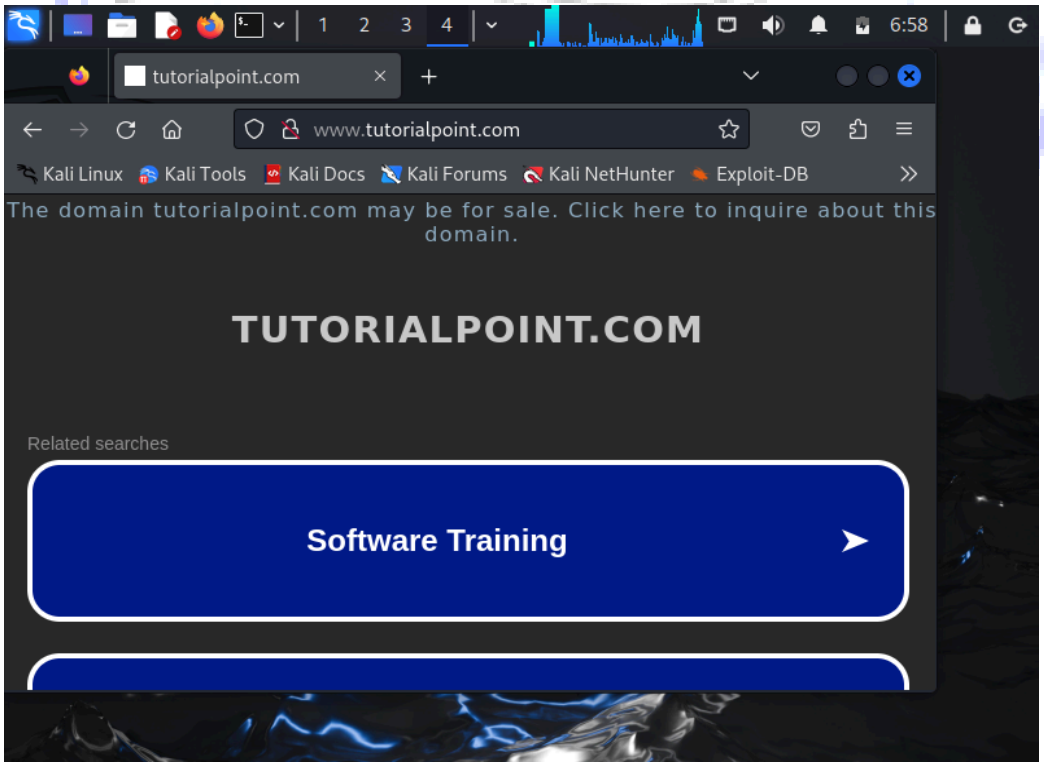
- To see the raw HTML, you can right-click on the webpage and select **"View Page Source"**. This will show the full HTML document, including scripts and resources linked to the page.

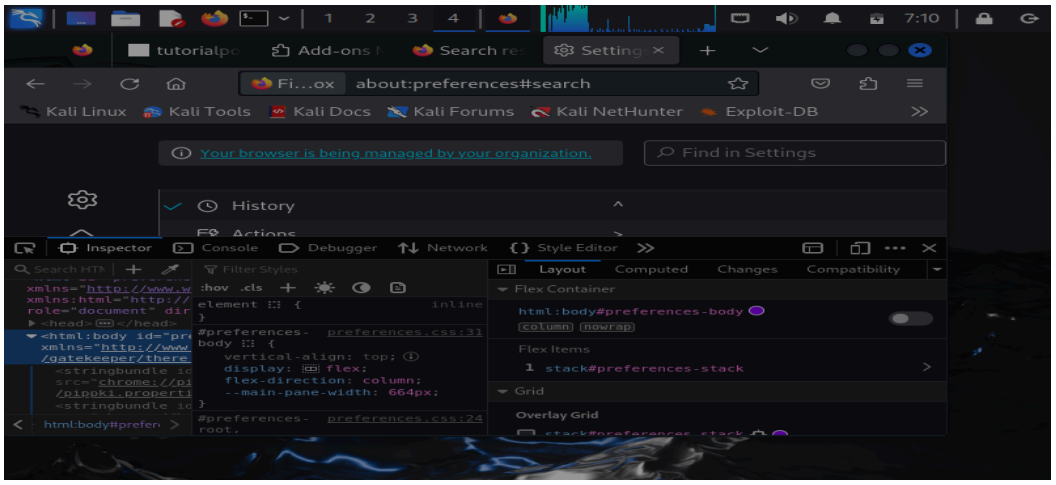
Step 9:Debug JavaScript:

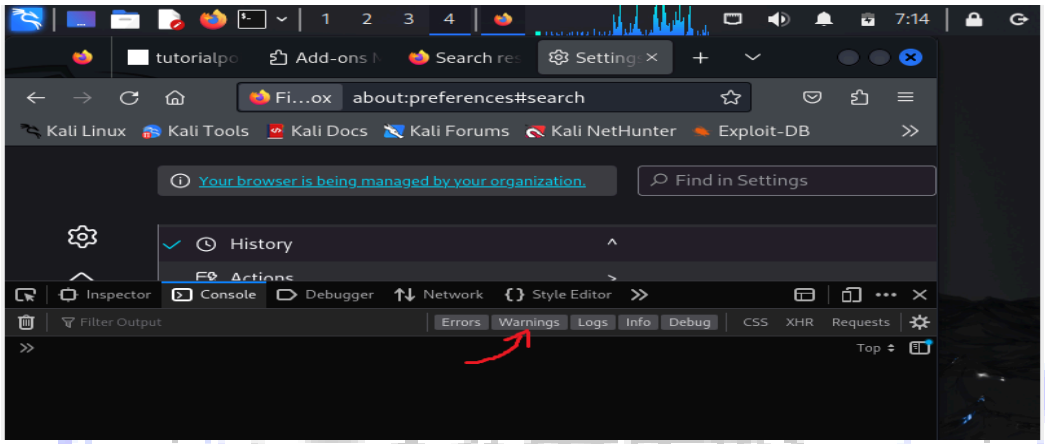
- In the **"Sources"** tab, you can view and debug JavaScript files loaded on the webpage. You can set breakpoints, step through code, and inspect variable values to debug or understand the website's code flow.

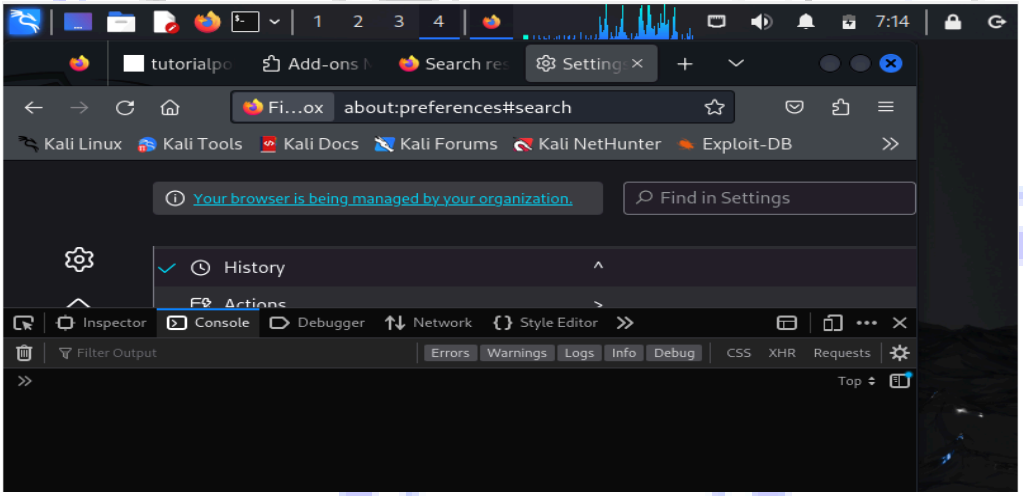
Step 10: Performance Monitoring:

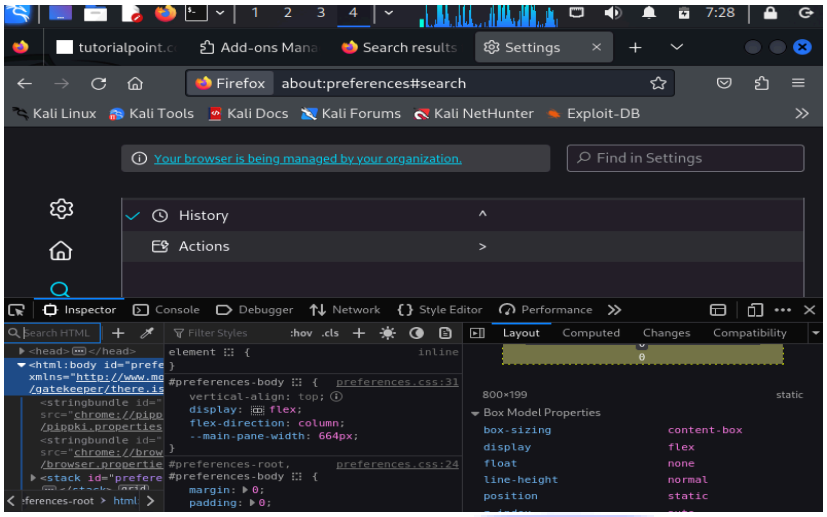
- The **"Performance"** tab allows you to record the performance of the webpage, including load times, CPU usage, and rendering.
- This is helpful to understand how the site performs under different conditions, such as during navigation or complex interactions.

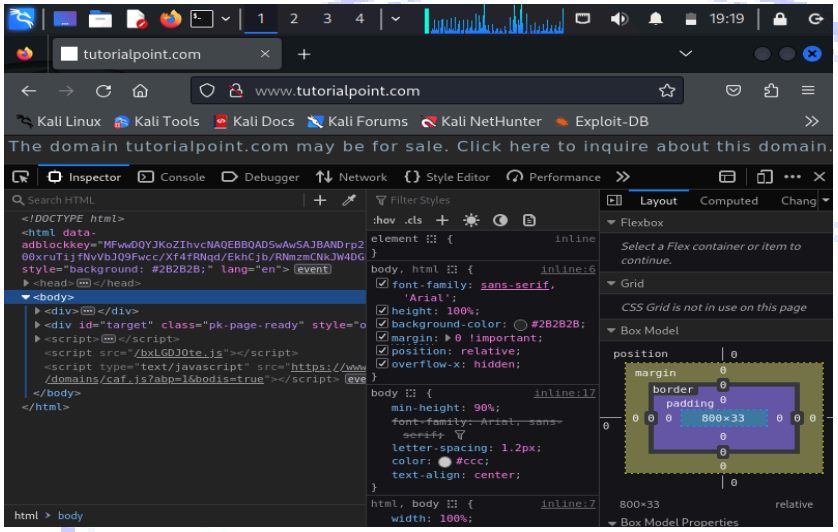



about:preferences#search
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Your browser is being managed by your organization.
Find in Settings
History
Inspector
Console
Debugger
Network
Style Editor
Layout
Computed
Changes
Compatibility
Flex Container
Flex Items
Grid
Overlay Grid


about:preferences#search
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Your browser is being managed by your organization.
Find in Settings
History
Inspector
Console
Debugger
Network
Style Editor
Filter Output
Errors
Warnings
Logs
Info
Debug
CSS
XHR
Requests
Top


about:preferences#search
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Your browser is being managed by your organization.
Find in Settings
History
Inspector
Console
Debugger
Network
Style Editor
Filter Output
Errors
Warnings
Logs
Info
Debug
CSS
XHR
Requests
Top





6. Network Scanning using NMAP

Aim : Yo understand the importance of network scanning using nmap tool commands

Step 1: **Basic Scan**

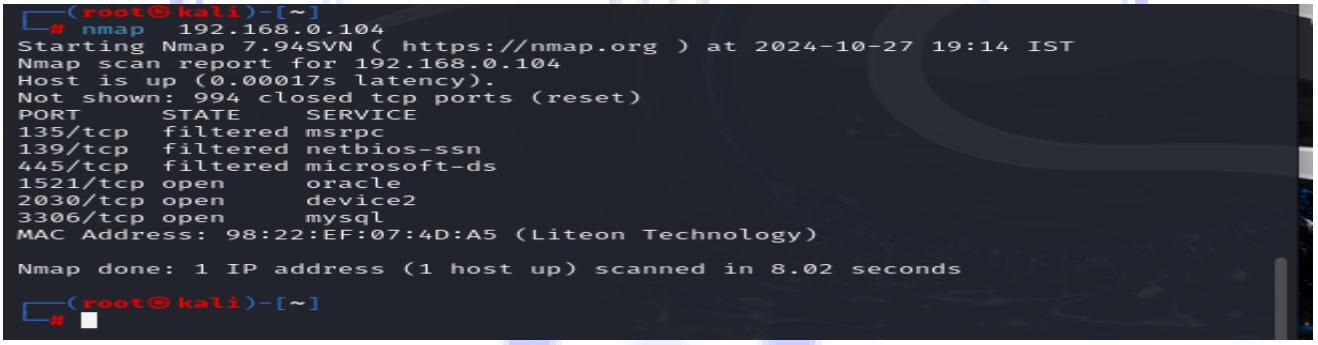
This performs a basic ping scan to check if the target machine is up by sending ICMP echo request

nmap -sn <target IPaddress>

nmap -sn 192.168.0.1431

2. Port Scanning for Open Ports

This scans the target for open TCP ports using the default Nmap scan.
nmap <target-IP>
nmap 192.168.0.104



3. Service Version Detection

This command detects the version of the services running on open ports.
nmap -sV <target-IP>

nmap -sV 192.168.0.104

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.0.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 19:35 IST
Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 19:39 (0:01:08 remaining)
Nmap scan report for 192.168.0.104
Host is up (0.00035s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1521/tcp open     oracle-tns   Oracle TNS listener 21.0.0.0.0 (unauthorized)
2030/tcp open     device2?
3306/tcp open     mysql        MySQL (unauthorized)
MAC Address: 98:22:EF:07:4D:A5 (Liteon Technology)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 166.05 seconds
```

4. Operating System Detection

This detects the operating system running on the target machine by analyzing network responses.

nmap -O <target-IP>

```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.0.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 19:50 IST
Nmap scan report for 192.168.0.104
Host is up (0.00024s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE    SERVICE
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1521/tcp open     oracle
2030/tcp open     device2
3306/tcp open     mysql
MAC Address: 98:22:EF:07:4D:A5 (Liteon Technology)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.98 seconds

┌──(root㉿kali)-[~]
└─#
```

5. Aggressive Scan (includes OS, Services, and more)

This is an aggressive scan that combines multiple Nmap features, including OS detection, version detection, script scanning, and traceroute.

nmap -A <target-IP>
nmap -A 192.168.0.104

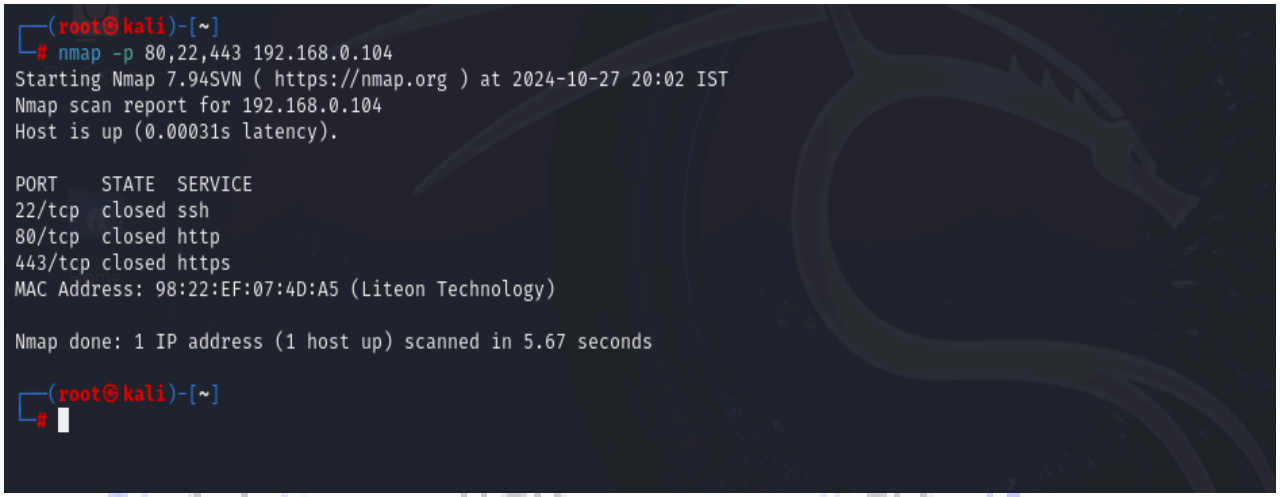
```
└─# nmap -A 192.168.0.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 19:54 IST
Nmap scan report for 192.168.0.104
Host is up (0.00039s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1521/tcp open     oracle-tns   Oracle TNS listener 21.0.0.0.0 (unauthorized)
2030/tcp open     device2?
3306/tcp open     mysql        MySQL (unauthorized)
MAC Address: 98:22:EF:07:4D:A5 (Liteon Technology)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/27%OT=1521%CT=1%CU=32398%PV=Y%DS=1%DC=D%G=Y%M=98
OS:22EF%TM=671E4DE0%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=106%TI=I%CI=
OS:I%II=I%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NN
OS:S%O5=M5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W
OS:6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%
OS:DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80
OS:%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y
OS:%DFI=N%T=80%CD=Z)

Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms 192.168.0.104

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.08 seconds
```

6. Scan Specific Ports

This command scans specific ports (80, 443, and 22 in this case) on the target.

nmap -p <port-range> <target-IP>

nmap -p 80,22,443 192.168.0.104



7. Detecting Phishing using Netcraft

Aim : To Detect phishing using Netcraft

Step 1: Install Netcraft Extension

Netcraft offers a browser extension that can be used for phishing detection. The extension alerts you if a site is unsafe and helps you report suspected phishing sites.

1. Open Firefox on your Kali Linux system (Firefox comes pre-installed on Kali).
2. Visit the Netcraft website and navigate to the “Browser Extension” section.
3. Download and install the Netcraft extension for Firefox.

Alternatively, you can install it directly from the Firefox Add-ons page:

- Open the Firefox Add-ons store by clicking on the hamburger menu (three horizontal lines) in the top right corner of the browser.
- Click on "Add-ons and themes."
- Search for "Netcraft Anti-Phishing."
- Click "Add to Firefox" and then "Add" to confirm.

Step 2: Enable the Netcraft Extension

Once installed, make sure the extension is enabled:

1. Go to the "Add-ons" menu in Firefox.
2. Verify that the Netcraft Anti-Phishing extension is toggled "On."

Step 3: Start Browsing

With the Netcraft extension enabled, you can start browsing websites. The extension will display a banner or warning if a website is identified as malicious or a phishing attempt.

- If the site is safe, you'll see a small green shield icon.
- If the site is suspicious, the extension will notify you with a warning.

Step 4: Report Phishing Sites

If you encounter a site that you believe to be phishing but hasn't been flagged, you can report it:

1. Click on the Netcraft icon in the toolbar.
2. Select the option to "Report this site."
3. Fill in the necessary details about why you believe the site is phishing.

Step 5: Check Site Reports

You can also manually check site reports by going to the Netcraft website:

1. Open Firefox and go to the Netcraft Phishing Protection page.
2. Enter the URL of any site you want to investigate.
3. The service will provide details about the safety of the website and whether it has been reported as a phishing site.

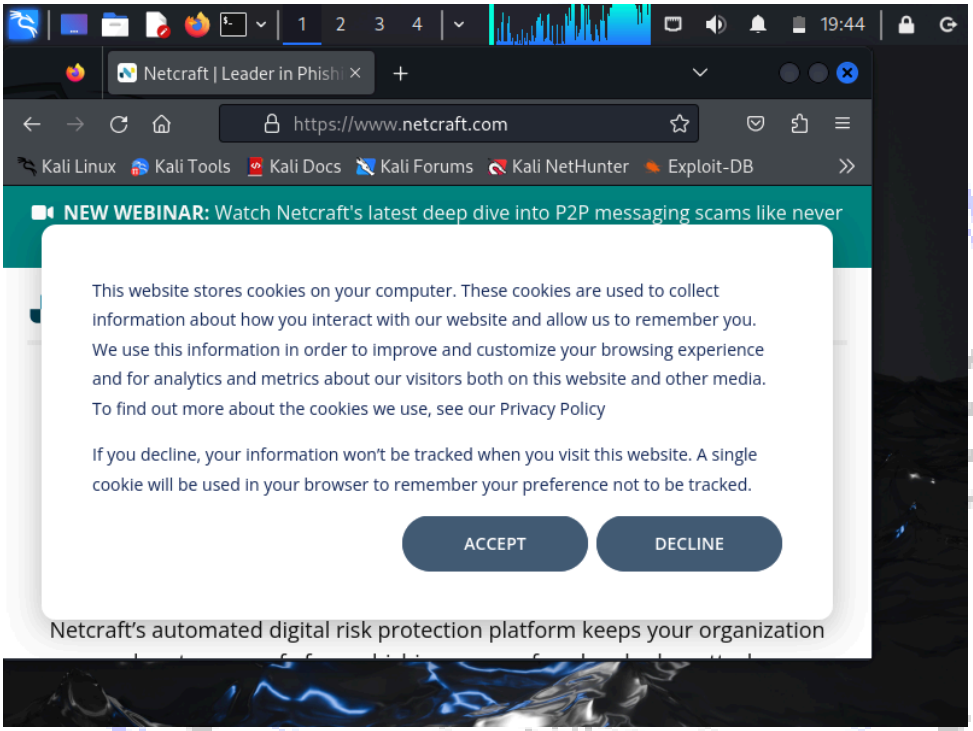
Step 6: Analyze Suspicious URLs

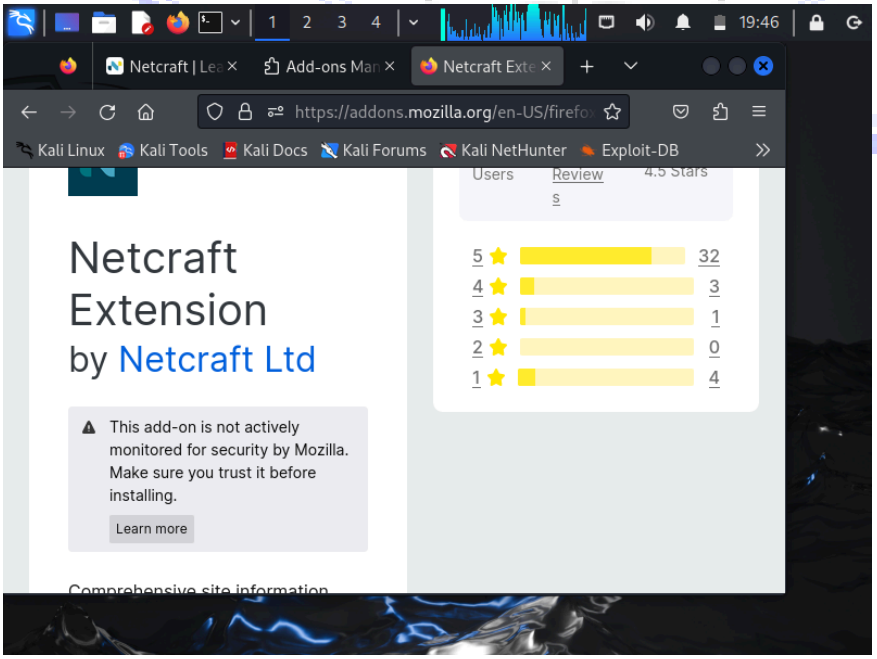
For beginners, Netcraft provides an easy way to analyze suspicious URLs. If you're visiting sites via emails or social media and are unsure about their legitimacy, you can:

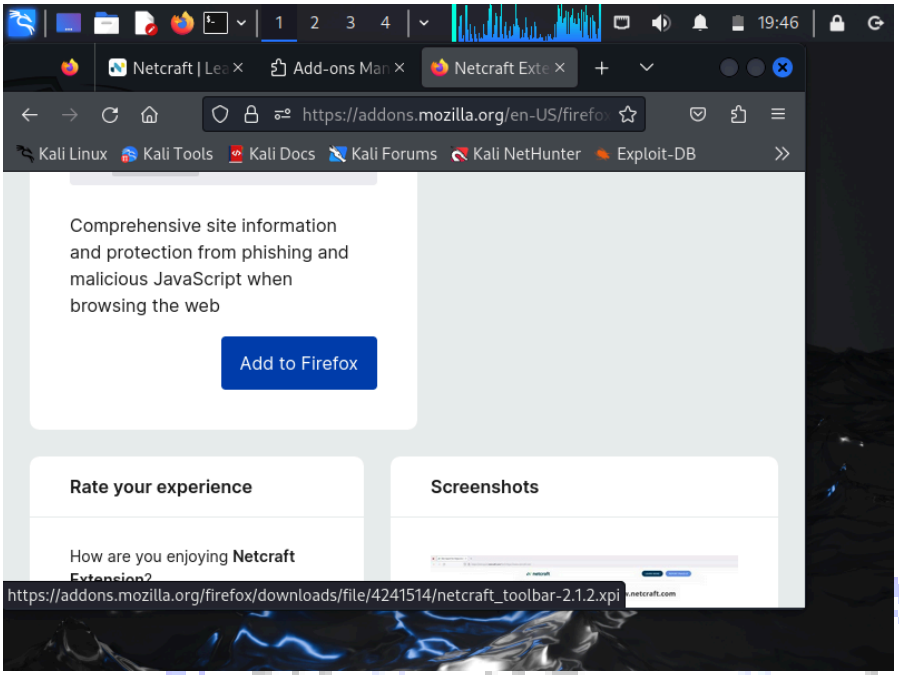
1. Right-click the link and copy the URL.
2. Paste the URL into Netcraft's “Search” or “Check a site” feature to check its safety.

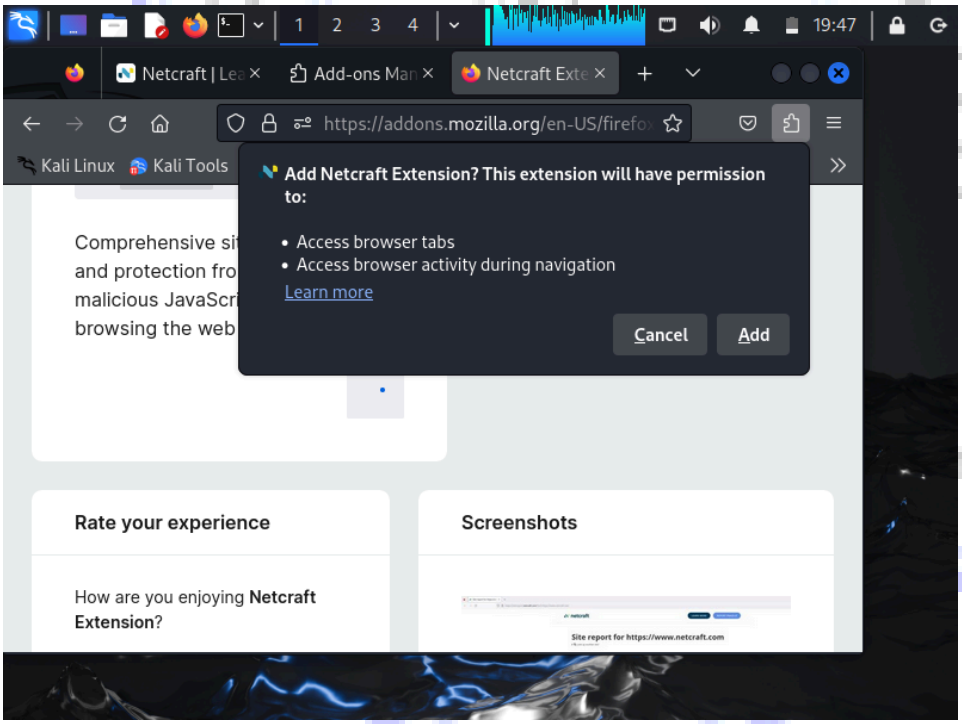
Step 7: Stay Vigilant

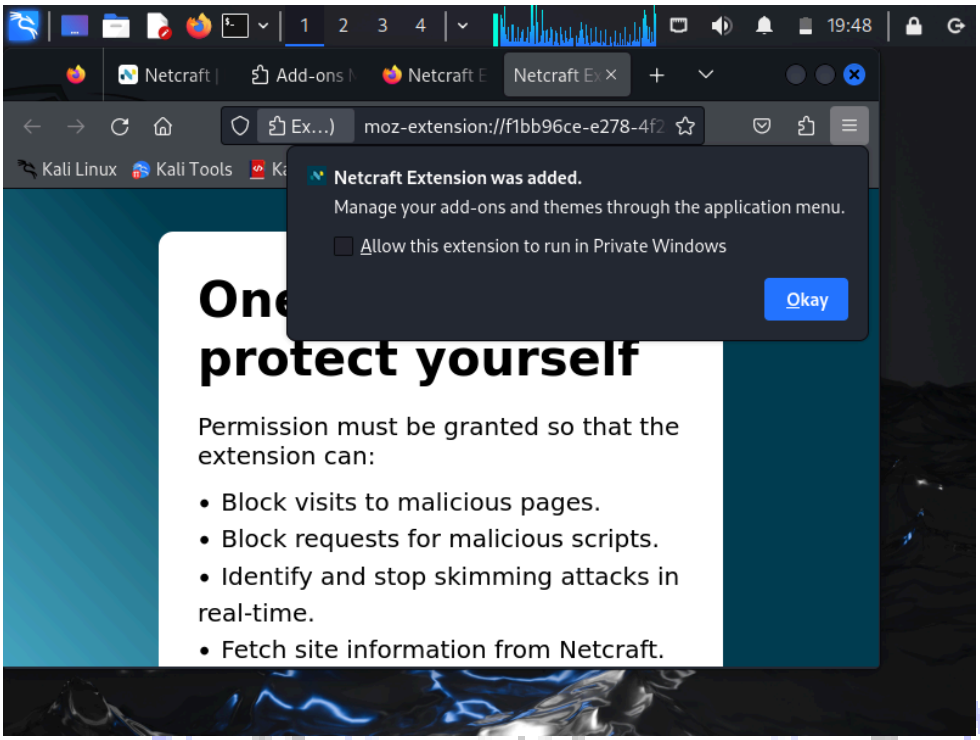
While Netcraft is a useful tool, always remain cautious when clicking on unknown links, especially from unsolicited emails or messages. Even legitimate-looking sites could be phishing traps.






19:46
Netcraft | Lea
Add-ons Man
Netcraft Exte
https://addons.mozilla.org/en-US/firefo
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web
Add to Firefox
Rate your experience
Screenshots
How are you enjoying Netcraft Extension?
https://addons.mozilla.org/firefox/downloads/file/4241514/netcraft_toolbar-2.1.2.xpi


19:47
Netcraft | Lea
Add-ons Man
Netcraft Exte
https://addons.mozilla.org/en-US/firefox
Kali Linux
Kali Tools
Add Netcraft Extension? This extension will have permission to:
Access browser tabs
Access browser activity during navigation
Learn more
Cancel
Add
Rate your experience
Screenshots
How are you enjoying Netcraft Extension?


Netcraft Extension was added.
Manage your add-ons and themes through the application menu.
Allow this extension to run in Private Windows
Okay
protect yourself
Permission must be granted so that the extension can:
• Block visits to malicious pages.
• Block requests for malicious scripts.
• Identify and stop skimming attacks in real-time.
• Fetch site information from Netcraft.

8.Sniffing facebook credential Using Social Engineering Toolkit (SET)

Aim : To sniff facebook credentials using SET

Step 1: Install Social Engineering Toolkit (SET)

If SET is not already installed, follow these steps to install it on Kali Linux:

1. Open a terminal and run:
   sudo apt update
   sudo apt install
   set

2. Confirm installation by running:
   setoolkit

Step 2: Open Social Engineering Toolkit (SET)

1. Run the following command to launch the SET:
   sudo setoolkit

2. Accept the disclaimer if prompted, and you'll see the SET main menu.

Step 3: Select the Attack Vector

1. From the menu, choose Social-Engineering Attacks:

   1) Social-Engineering Attacks

2. Next, choose Website Attack Vectors:

   2) Website Attack Vectors

Step 4: Choose Credential Harvester Attack Method

1. From the next menu, choose Credential Harvester Attack Method:

   3) Credential Harvester Attack Method

2. Then, select Site Cloner:

   2) Site Cloner

```
```

Step 5: Enter the URL to Clone (Facebook Login Page)

1. When prompted to enter the URL to clone, input Facebook's login page URL:

```
Enter the URL to clone: https://www.facebook.com
```

2. SET will clone this page, making it look identical to the legitimate Facebook login.

Step 6: Enter the Local IP Address

1. SET will ask you to provide the IP address where you want to host the fake Facebook login page. To find your local IP, run:

```
ifconfig
```

2. Enter your local IP address (e.g., 192.168.x.x).

Step 7: Start Apache Server

1. If Apache is not already running, you will need to start it:

```
sudo service apache2 start
```

Step 8: Send the Phishing Link

1. SET will now host the cloned Facebook login page on your local server. To test this, send the phishing URL (your local IP address, e.g., http://192.168.x.x) to a dummy system or a virtual machine within your lab setup.

Step 9: Test the Phishing Page (Credential Entry)

1. **Open a Browser on the Dummy System**:
    - Use a system in your lab environment, like a virtual machine or a separate device, and open a browser.
    - In the browser, go to the phishing URL you created (e.g., http://192.168.x.x).
2. **Enter Credentials**:
    - On the cloned Facebook login page, enter some dummy credentials (username and password).
    - Since this is a test, **DO NOT** use real credentials. Just input random values.

Step 10: Check for Captured Credentials in SET

1. **Go back to your SET terminal**:
    - After the dummy credentials are entered in the browser, return to the terminal window where the Social Engineering Toolkit (SET) is running.

2. **View Harvested Credentials**:
    - SET will capture and display the credentials entered on the phishing page in real-time.
      [*] WE GOT A HIT! Printing the details:

      [*] User: abc@123

      [*] Password: AbC@456

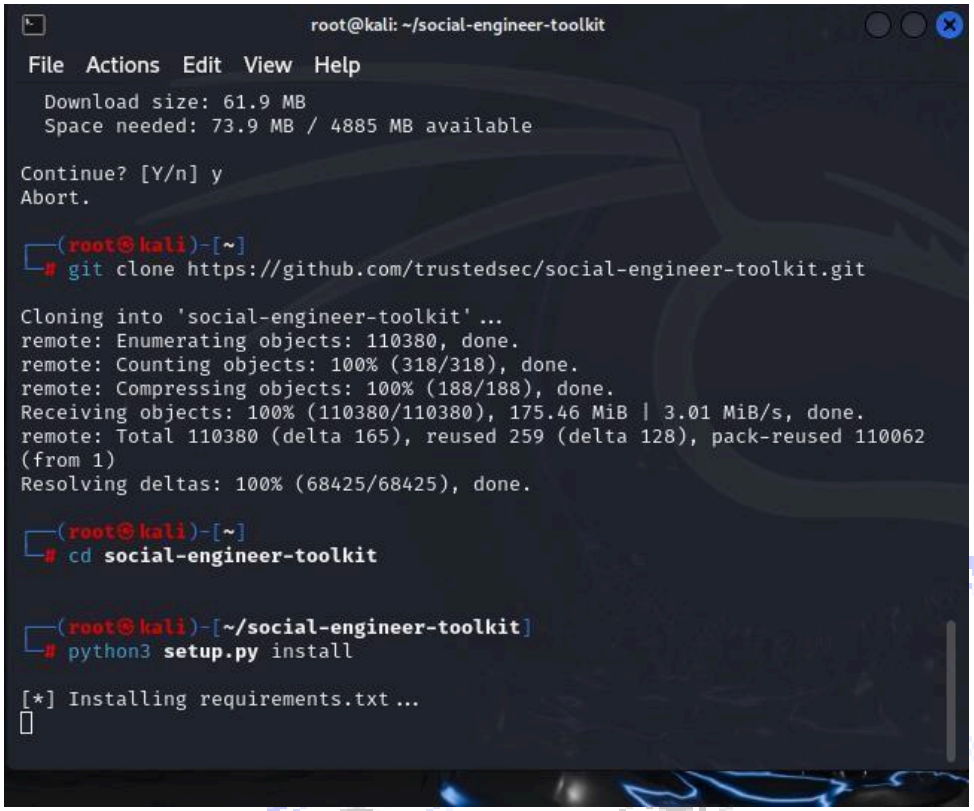
Step 11: Analyze the Results

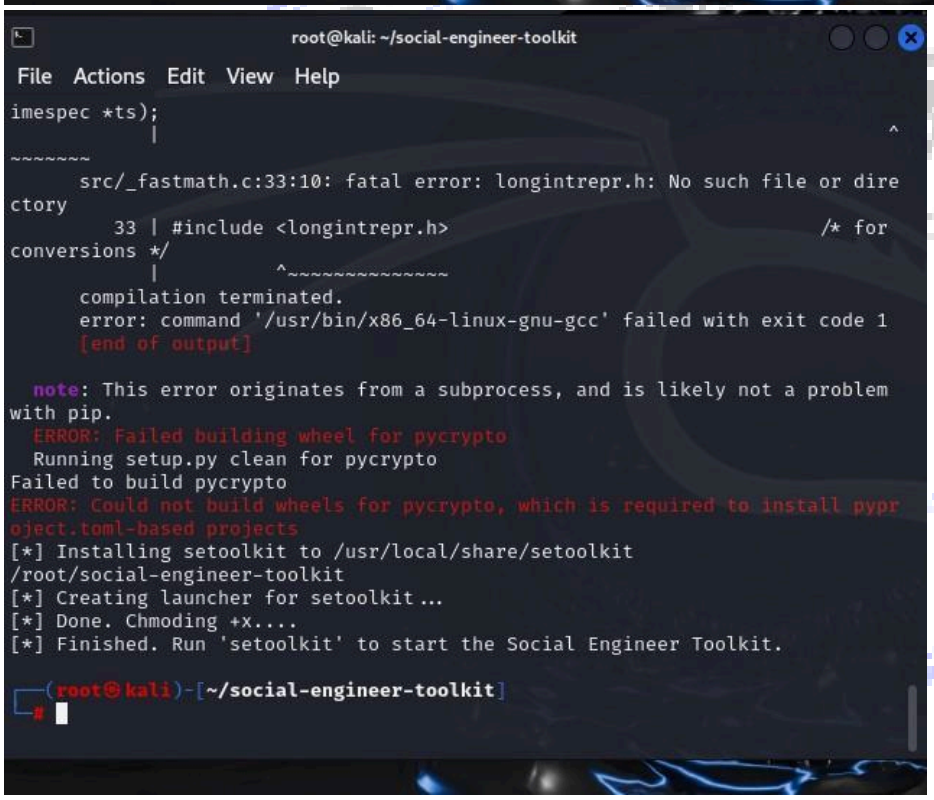
- Review the credentials displayed in the SET terminal. These credentials would have been sent to the server you set up using Apache, simulating a phishing attack.
- **Important**: Since this is an ethical hacking test in a controlled lab environment, ensure you never perform such actions on live systems or without proper authorization.

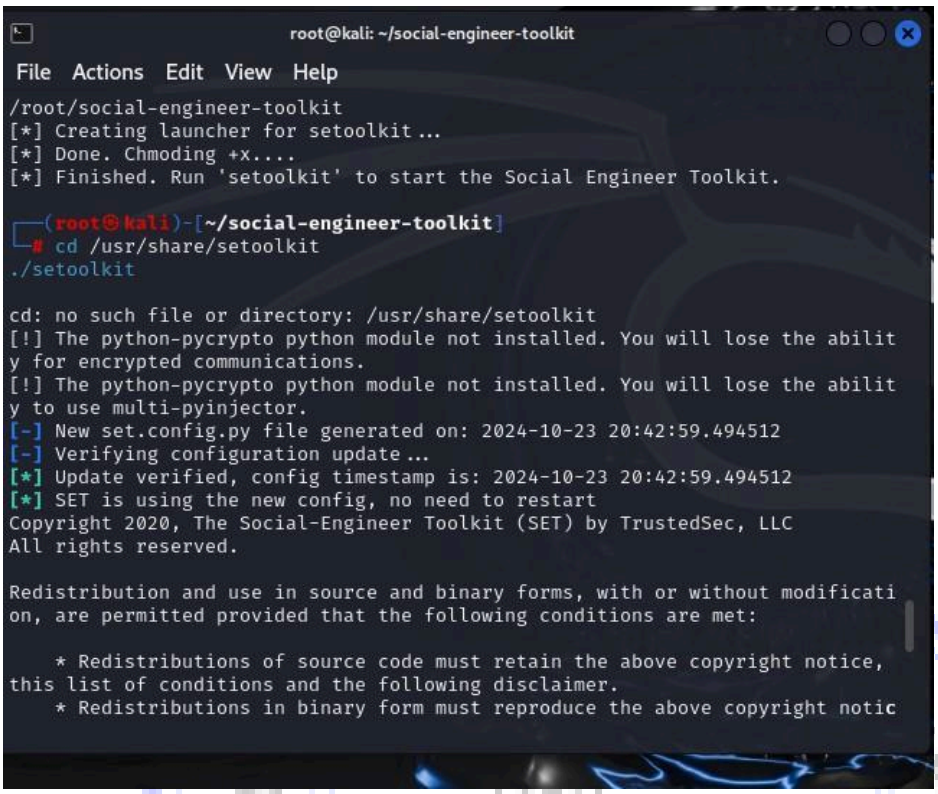
Step 12: Clean Up the Environment

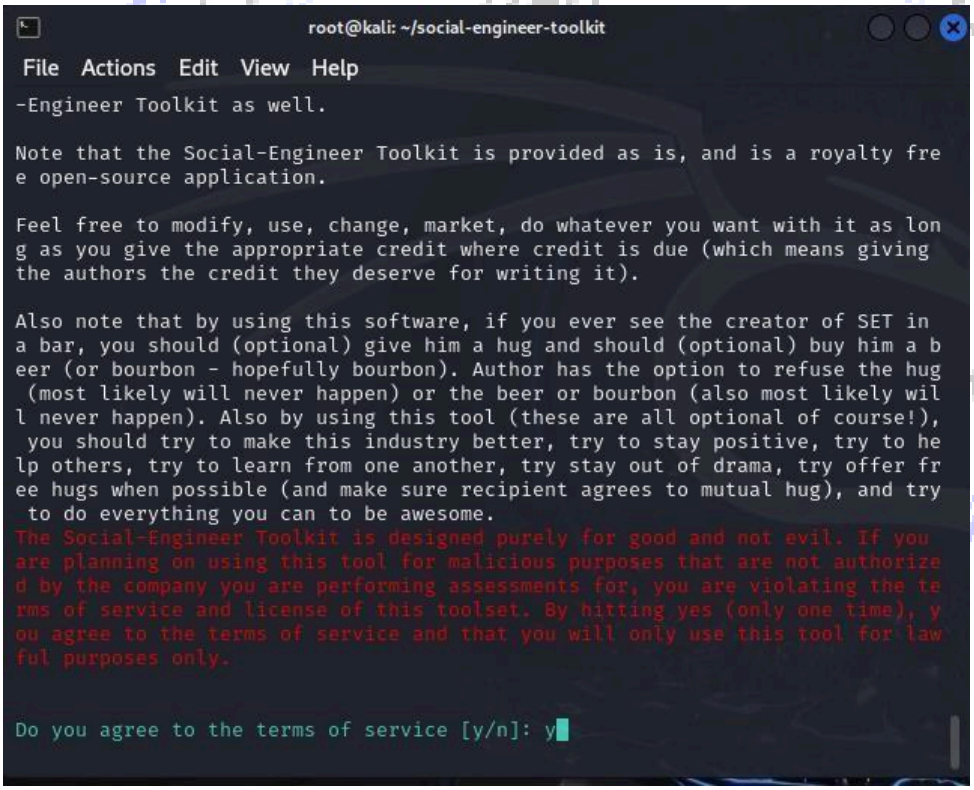
Once you've tested the credentials:

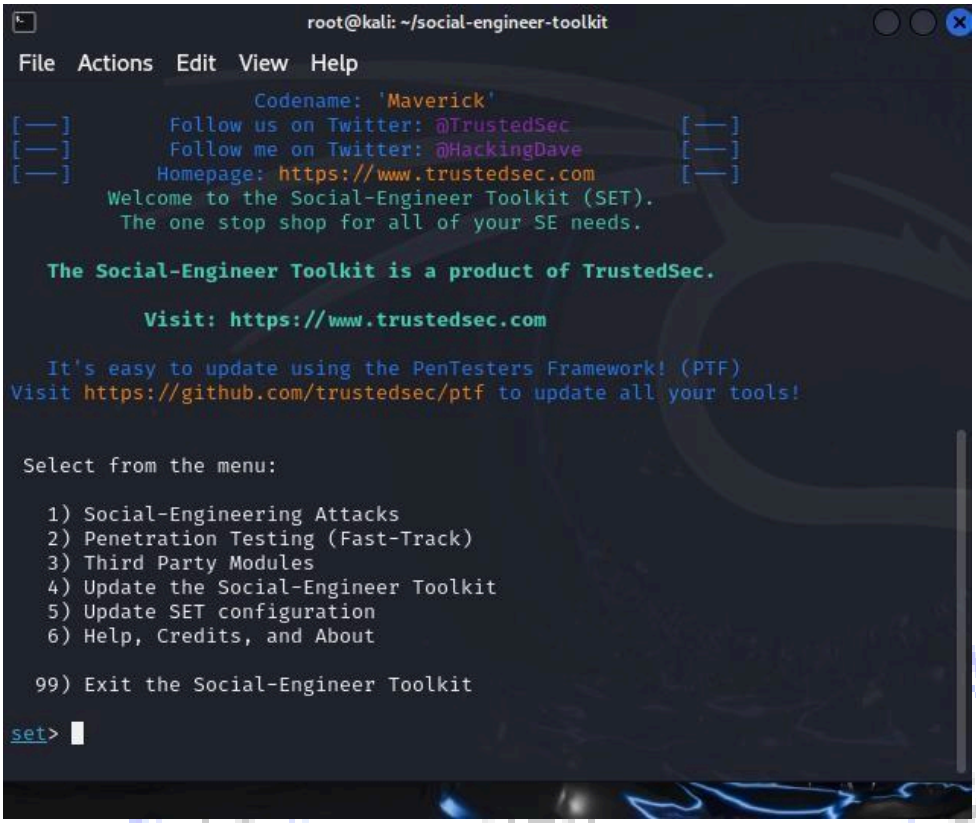
1. **Stop the Apache Server**: sudo service apache2 stop
2. **Clear any remaining cloned files** (if necessary):
   sudo rm -rf /var/www/html/*

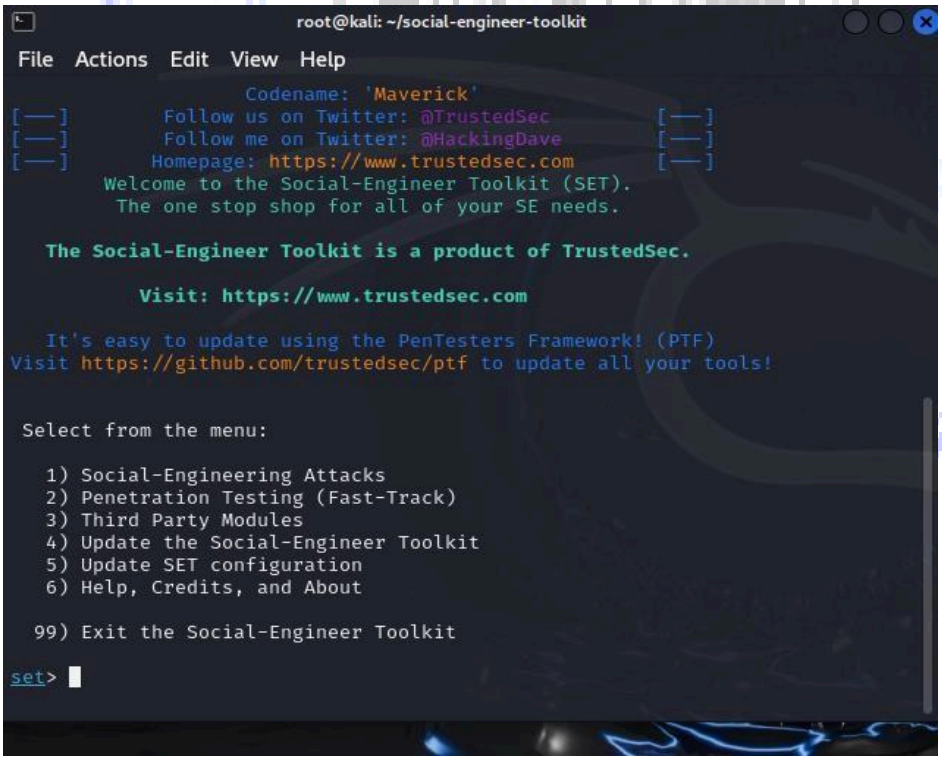

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
Download size: 61.9 MB
Space needed: 73.9 MB / 4885 MB available
Continue? [Y/n] y
Abort.
(root㉿kali)-[~]
git clone https://github.com/trustedsec/social-engineer-toolkit.git
Cloning into 'social-engineer-toolkit'...
remote: Enumerating objects: 110380, done.
remote: Counting objects: 100% (318/318), done.
remote: Compressing objects: 100% (188/188), done.
Receiving objects: 100% (110380/110380), 175.46 MiB | 3.01 MiB/s, done.
remote: Total 110380 (delta 165), reused 259 (delta 128), pack-reused 110062
(from 1)
Resolving deltas: 100% (68425/68425), done.
(root㉿kali)-[~]
cd social-engineer-toolkit
(root㉿kali)-[~/social-engineer-toolkit]
python3 setup.py install
[*] Installing requirements.txt...

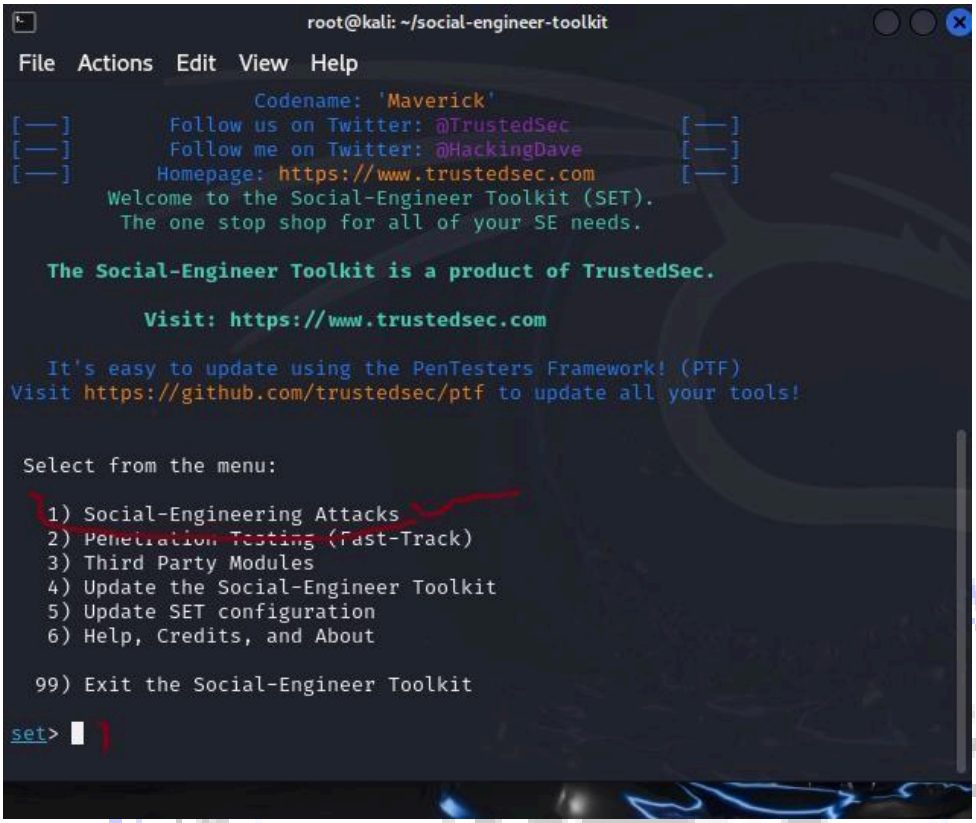

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
imespec *ts);
^
~~~~~~~
src/_fastmath.c:33:10: fatal error: longintrepr.h: No such file or dire
ctory
33 | #include <longintrepr.h> /* for
conversions */
^~~~~~~~~~~~~~
compilation terminated.
error: command '/usr/bin/x86_64-linux-gnu-gcc' failed with exit code 1
[end of output]
note: This error originates from a subprocess, and is likely not a problem
with pip.
ERROR: Failed building wheel for pycrypto
Running setup.py clean for pycrypto
Failed to build pycrypto
ERROR: Could not build wheels for pycrypto, which is required to install pypr
oject.toml-based projects
[*] Installing setoolkit to /usr/local/share/setoolkit
/root/social-engineer-toolkit
[*] Creating launcher for setoolkit...
[*] Done. Chmoding +x....
[*] Finished. Run 'setoolkit' to start the Social Engineer Toolkit.
(root㉿kali)-[~/social-engineer-toolkit]
#
~~~~~~~

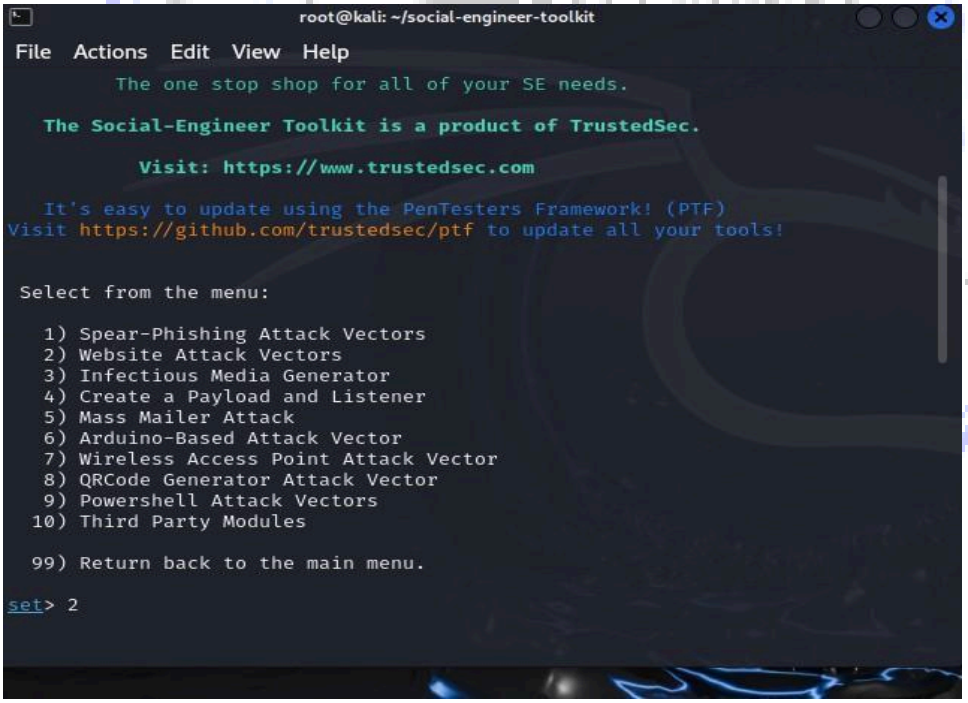

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
/root/social-engineer-toolkit
[*] Creating launcher for setoolkit ...
[*] Done. Chmoding +x....
[*] Finished. Run 'setoolkit' to start the Social Engineer Toolkit.
┌──(root㉿kali)-[~/social-engineer-toolkit]
└─# cd /usr/share/setoolkit
./setoolkit
cd: no such file or directory: /usr/share/setoolkit
[!] The python-pycrypto python module not installed. You will lose the abilit
y for encrypted communications.
[!] The python-pycrypto python module not installed. You will lose the abilit
y to use multi-pyinjector.
[-] New set.config.py file generated on: 2024-10-23 20:42:59.494512
[-] Verifying configuration update ...
[*] Update verified, config timestamp is: 2024-10-23 20:42:59.494512
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.
Redistribution and use in source and binary forms, with or without modificati
on, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notic

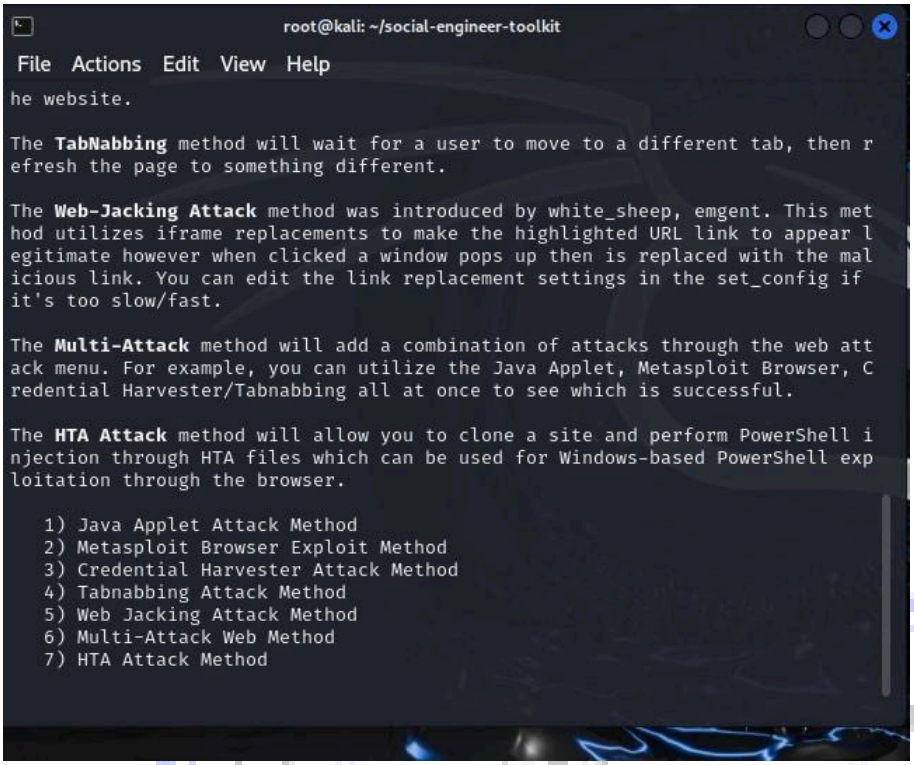

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
-Engineer Toolkit as well.
Note that the Social-Engineer Toolkit is provided as is, and is a royalty fre
e open-source application.
Feel free to modify, use, change, market, do whatever you want with it as lon
g as you give the appropriate credit where credit is due (which means giving
the authors the credit they deserve for writing it).
Also note that by using this software, if you ever see the creator of SET in
a bar, you should (optional) give him a hug and should (optional) buy him a b
eer (or bourbon - hopefully bourbon). Author has the option to refuse the hug
(most likely will never happen) or the beer or bourbon (also most likely wil
l never happen). Also by using this tool (these are all optional of course!),
you should try to make this industry better, try to stay positive, try to he
lp others, try to learn from one another, try stay out of drama, try offer fr
ee hugs when possible (and make sure recipient agrees to mutual hug), and try
to do everything you can to be awesome.
The Social-Engineer Toolkit is designed purely for good and not evil. If you
are planning on using this tool for malicious purposes that are not authorize
d by the company you are performing assessments for, you are violating the te
rms of service and license of this toolset. By hitting yes (only one time), y
ou agree to the terms of service and that you will only use this tool for law
ful purposes only.
Do you agree to the terms of service [y/n]: y

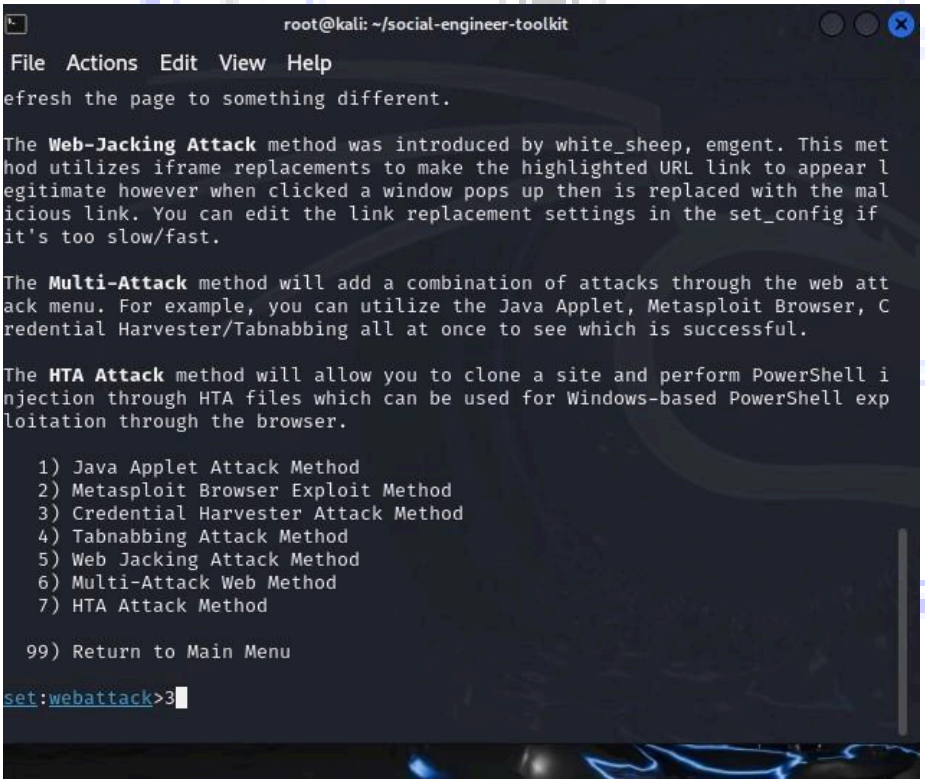

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set>

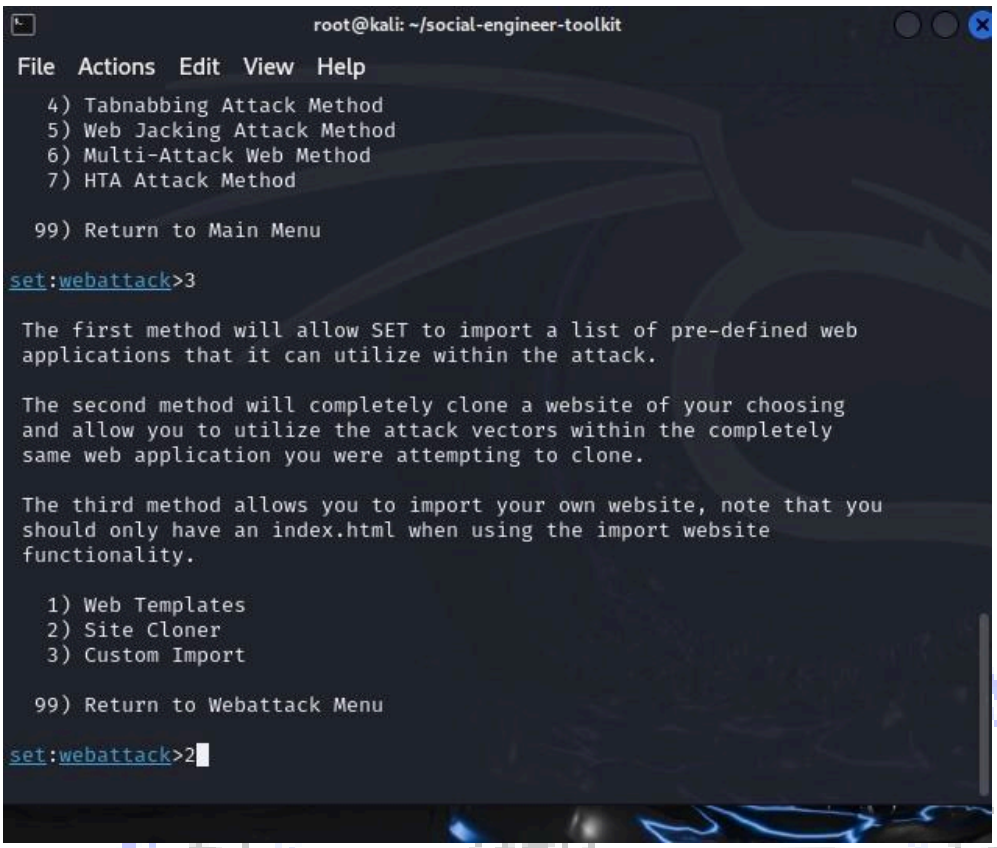

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set>

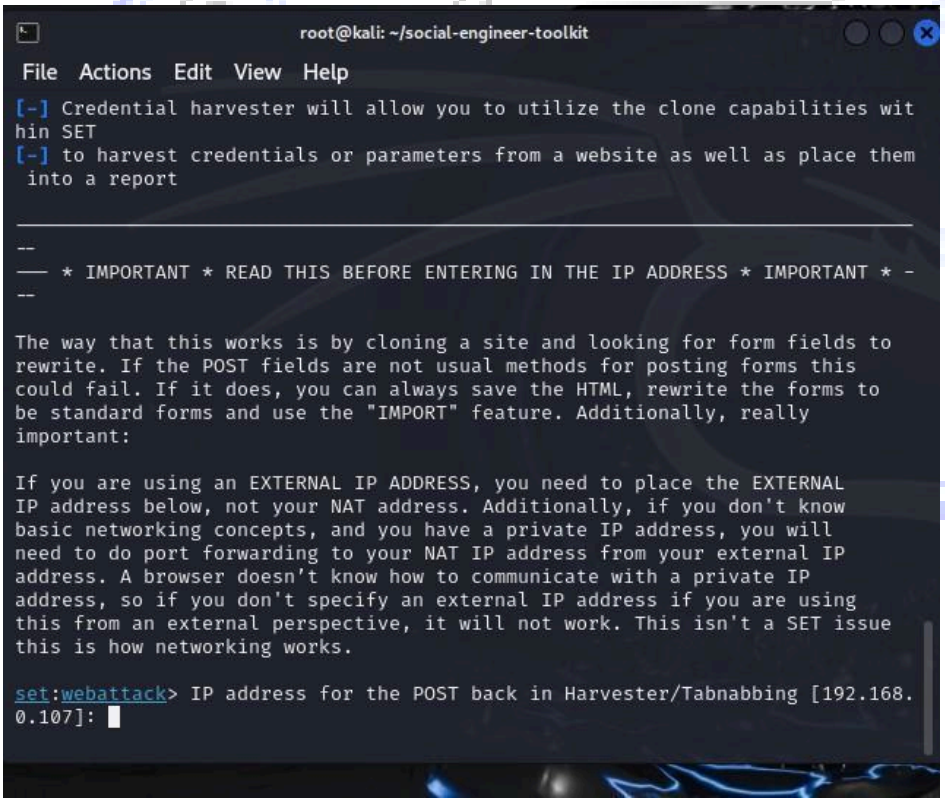

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set>

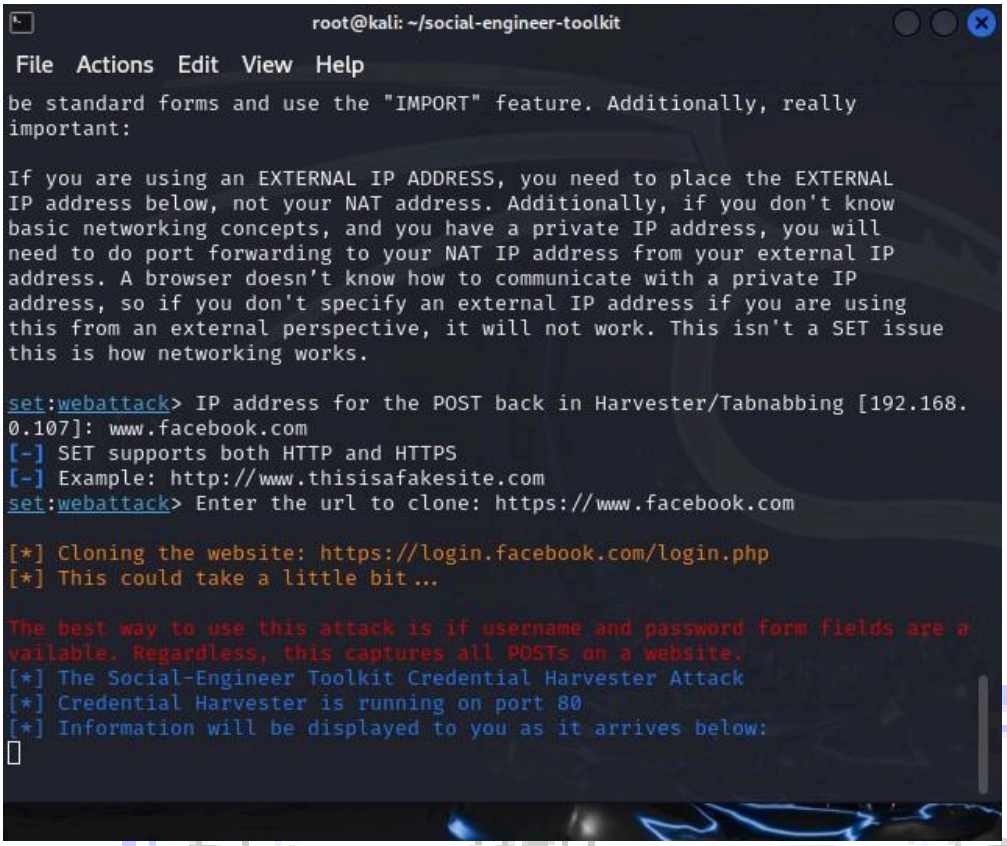

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2

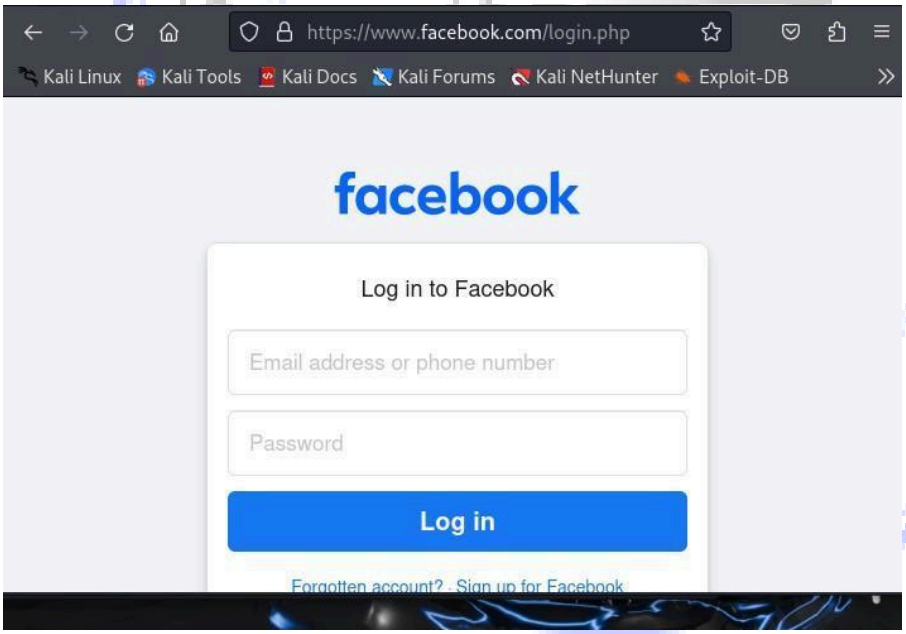

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
he website.
The TabNabbing method will wait for a user to move to a different tab, then r
efresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This met
hod utilizes iframe replacements to make the highlighted URL link to appear l
egitimate however when clicked a window pops up then is replaced with the mal
icious link. You can edit the link replacement settings in the set_config if
it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web att
ack menu. For example, you can utilize the Java Applet, Metasploit Browser, C
redential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform PowerShell i
njection through HTA files which can be used for Windows-based PowerShell exp
loitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

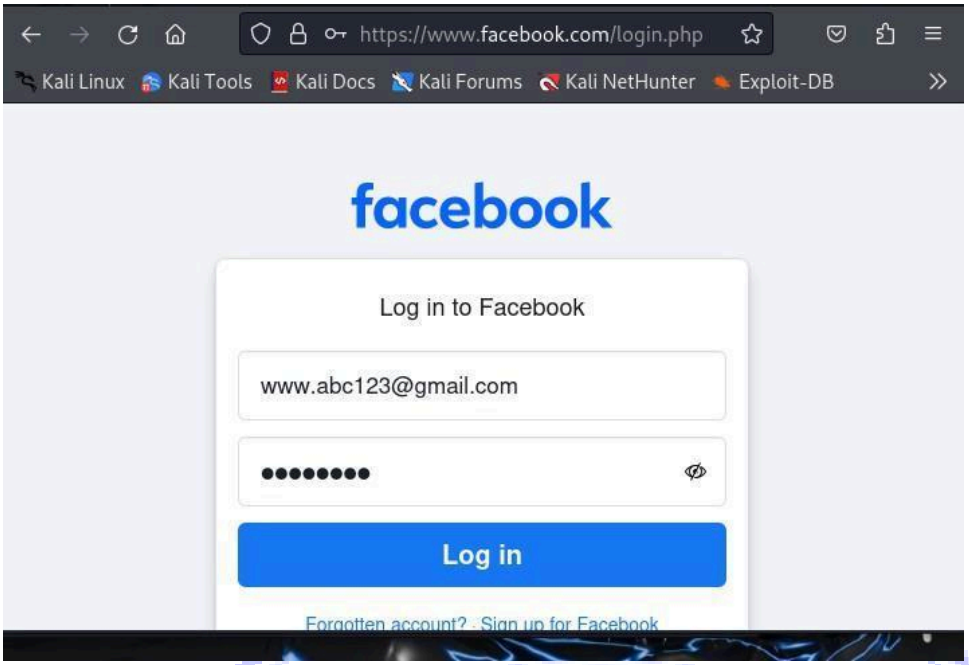

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
efresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This met
hod utilizes iframe replacements to make the highlighted URL link to appear l
egitimate however when clicked a window pops up then is replaced with the mal
icious link. You can edit the link replacement settings in the set_config if
it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web att
ack menu. For example, you can utilize the Java Applet, Metasploit Browser, C
redential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform PowerShell i
njection through HTA files which can be used for Windows-based PowerShell exp
loitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3

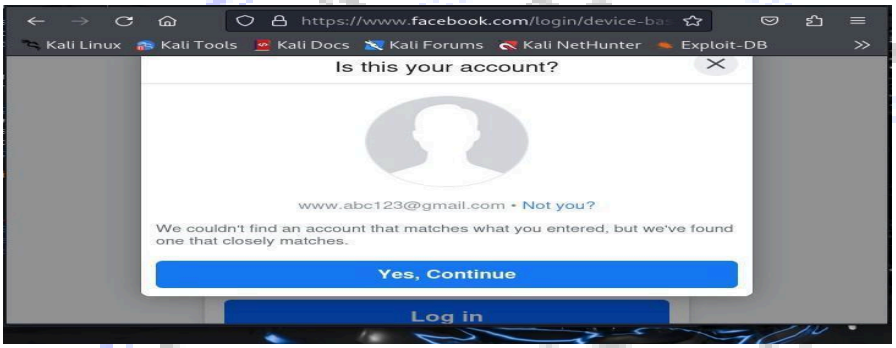

root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can 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>2


root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
* IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.107]:


root@kali: ~/social-engineer-toolkit
File Actions Edit View Help
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.
0.107]: www.facebook.com
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are a
vailable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:


https://www.facebook.com/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
facebook
Log in to Facebook
Email address or phone number
Password
Log in
Forgotten account? · Sign up for Facebook





Successfully tested the phishing attack simulation and credential harvesting using the Social Engineering Toolkit (SET).

9. Disk Encryption using VeraCrypt

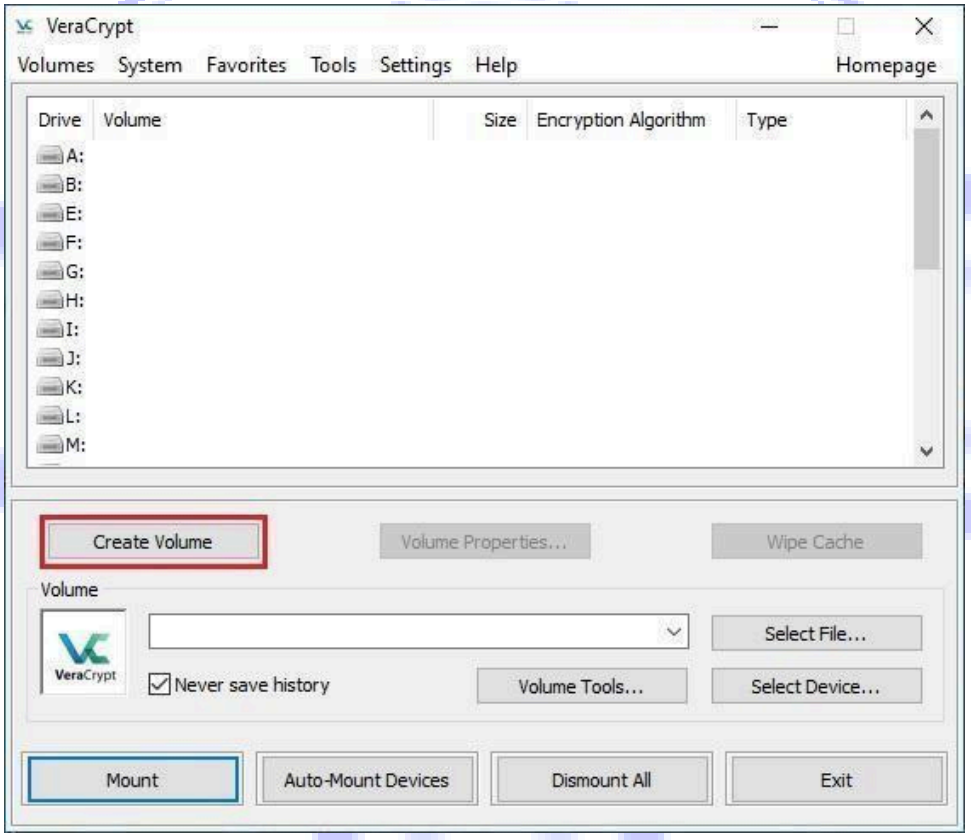
Aim : To perform disk encryption using VeraCrypt

STEP 1:

If you have not done so, download and install VeraCrypt. Then launch VeraCrypt by double-clicking the file VeraCrypt.exe or by clicking the VeraCrypt shortcut in your Windows Start menu.

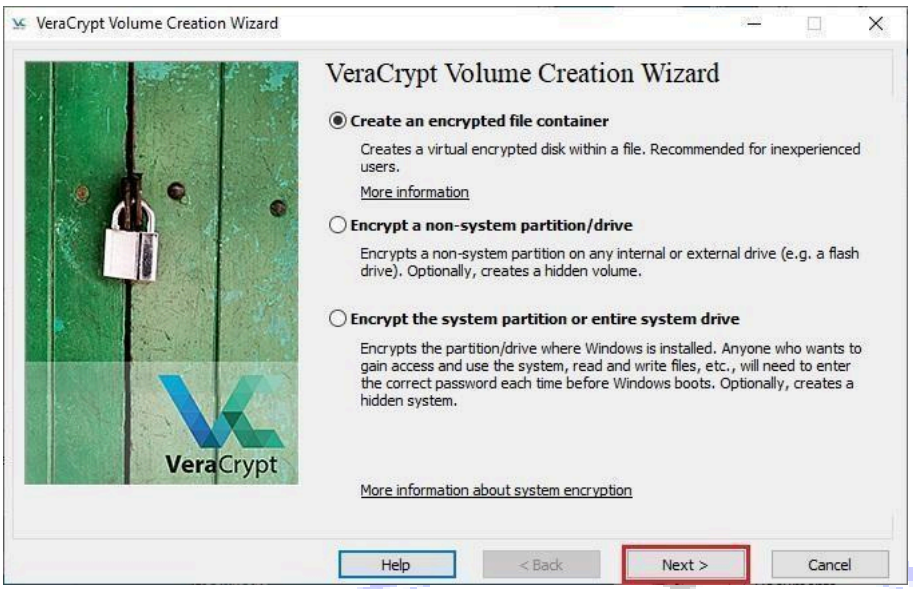
STEP 2:

The main VeraCrypt window should appear. Click **Create Volume** (marked with a red rectangle for clarity).



STEP 3:

The VeraCrypt Volume Creation Wizard window should appear. As the option is selected by default, you can just click **Next**.

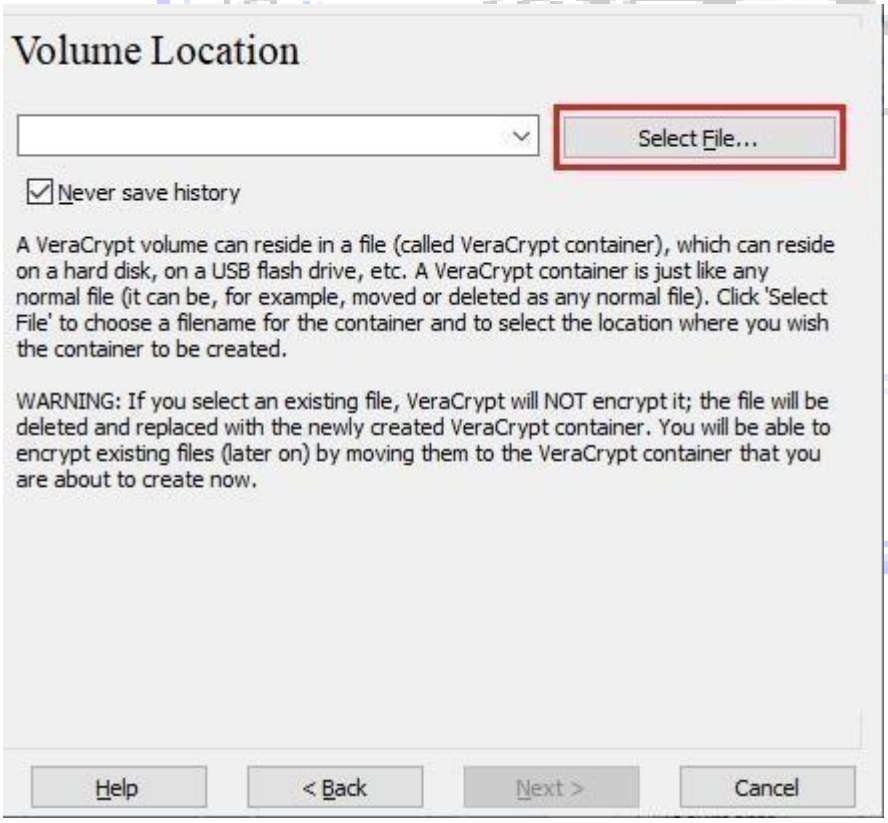


STEP 4:

In this step you need to choose whether to create a standard or hidden VeraCrypt volume. In this tutorial, we will choose the former option and create a standard VeraCrypt volume.

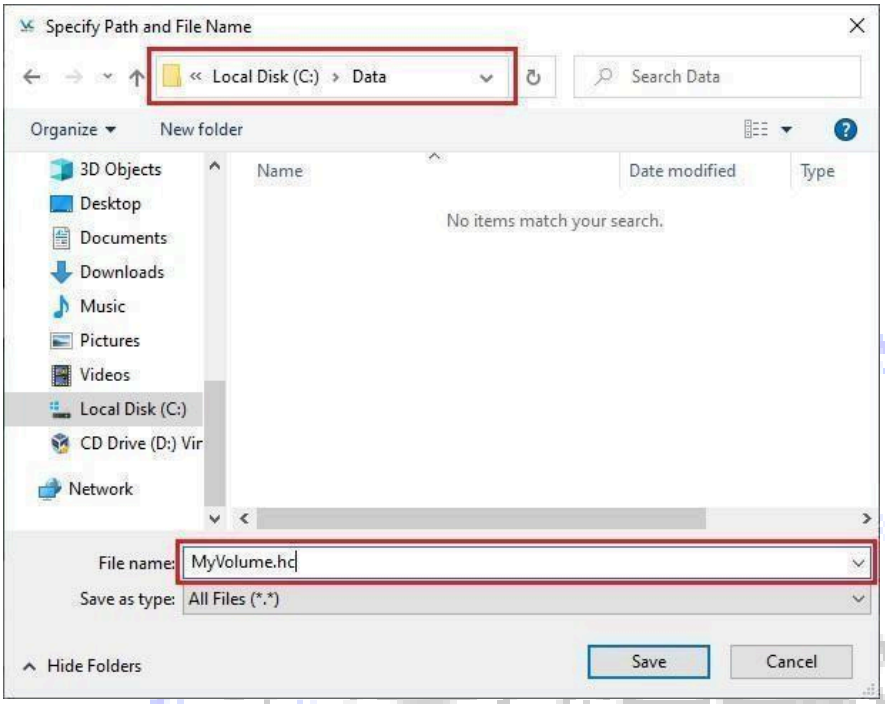
As the option is selected by default, you can just click **Next**.

STEP 5:



In this step you have to specify where you wish the VeraCrypt volume (file container) to be created. Note that a VeraCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step.

Click **Select File**.
The standard Windows file selector should appear (while the window of the VeraCrypt Volume Creation Wizard remains open in the background).
STEP 6:



Create our VeraCrypt volume in the folder C:*Data*\ and the filename of the volume (container) will be *MyVolume.hc*

IMPORTANT: **Note that VeraCrypt will *not* encrypt any existing files (when creating a VeraCrypt file container). If you select an existing file in this step, it will be overwritten and replaced by the newly created volume (so the overwritten file will be *lost*, *not* encrypted). You will be able to encrypt existing files (later on) by moving them to the VeraCrypt volume that we are creating now.***

Select the desired path (where you wish the container to be created) in the file selector. Type the desired container file name in the **Filename** box.

Click **Save**.
The file selector window should disappear.
In the following steps, we will return to the VeraCrypt Volume Creation Wizard.

* Note that after you copy existing unencrypted files to a VeraCrypt volume, you should securely erase (wipe) the original unencrypted files. There are software tools that can be used for the purpose of secure erasure (many of them are free).

STEP 7:

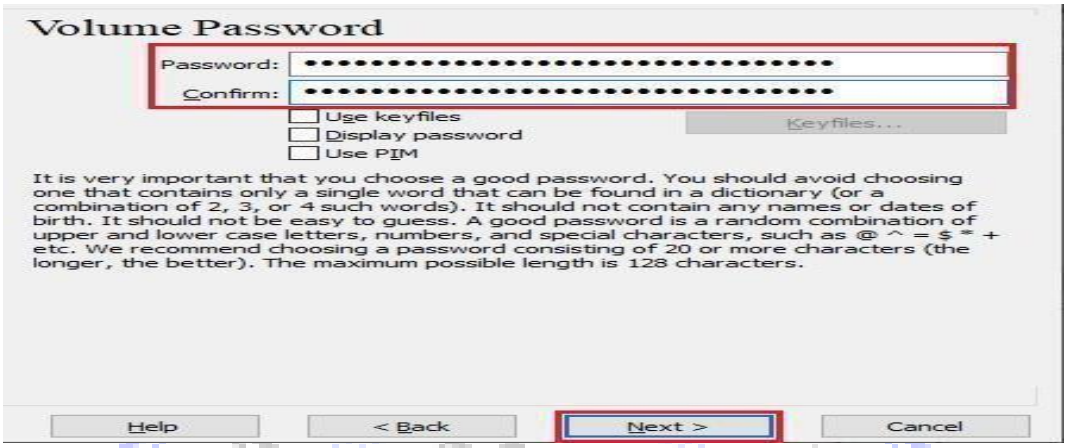
In the Volume Creation Wizard window, click **Next**. **STEP 8:**

Here you can choose an encryption algorithm and a hash algorithm for the volume. If you are not sure what to select here, you can use the default settings and click **Next** (for more information, see chapters *Encryption Algorithms* and *Hash Algorithms*).

STEP 9:

Here we specify that we wish the size of our VeraCrypt container to be 250 megabyte. You may, of course, specify a different size. After you type the desired size in the input field (marked with a red rectangle), click **Next**.

STEP 10:

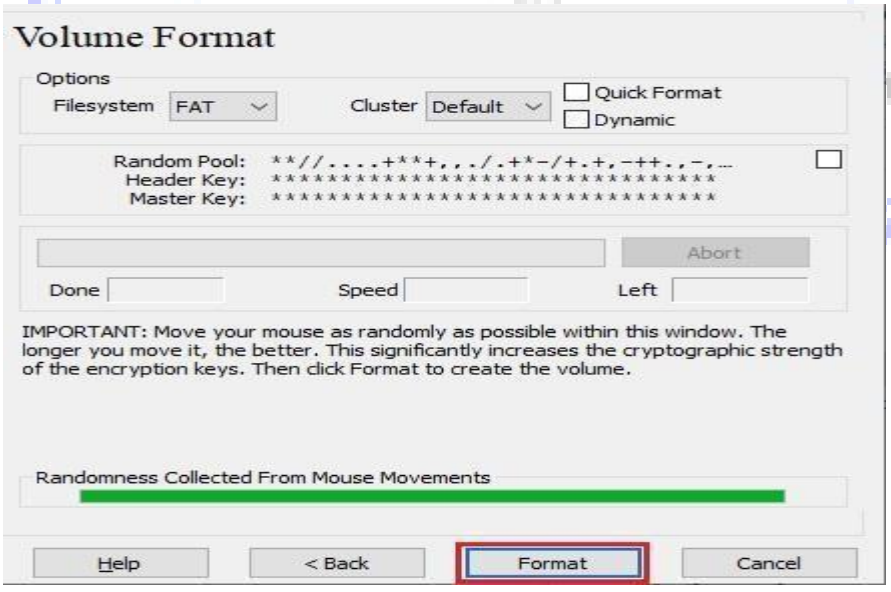


This is one of the most important steps. Here you have to choose a good volume password. Read carefully the information displayed in the Wizard window about what is considered a good password.

After you choose a good password, type it in the first input field. Then re-type it in the input field below the first one and click **Next**.

Note: The button **Next** will be disabled until passwords in both input fields are the same.

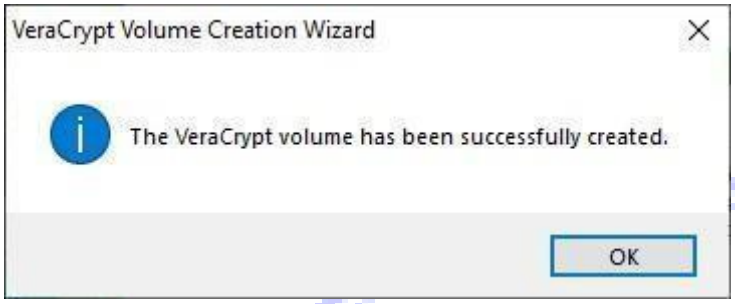
STEP 11:



Move your mouse as randomly as possible within the Volume Creation Wizard window at least until the randomness indicator becomes green. The longer you move the mouse, the better (moving the mouse for at least 30 seconds is recommended). This significantly

increases the cryptographic strength of the encryption keys (which increases security).

Click **Format**.
Volume creation should begin. VeraCrypt will now create a file called *MyVolume.hc* in the folder C:*Data*\ (as we specified in Step 6). This file will be a VeraCrypt container (it will contain the encrypted VeraCrypt volume). Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box will appear:



Click **OK** to close the dialog box.
STEP 12:

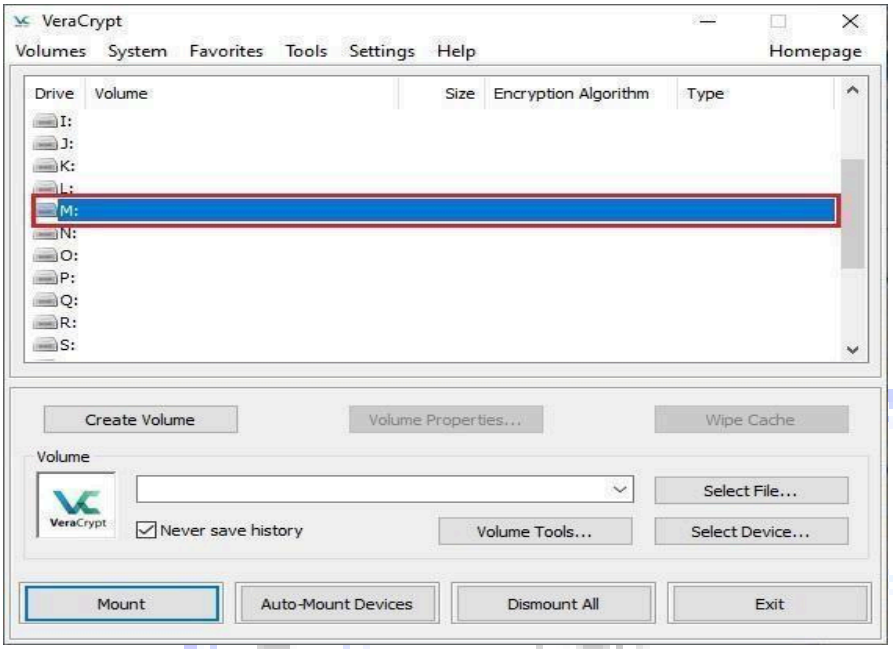
We have just successfully created a VeraCrypt volume (file container). In the VeraCrypt Volume Creation Wizard window, click **Exit**.

The Wizard window should disappear.

In the remaining steps, we will mount the volume we just created. We will return to the main

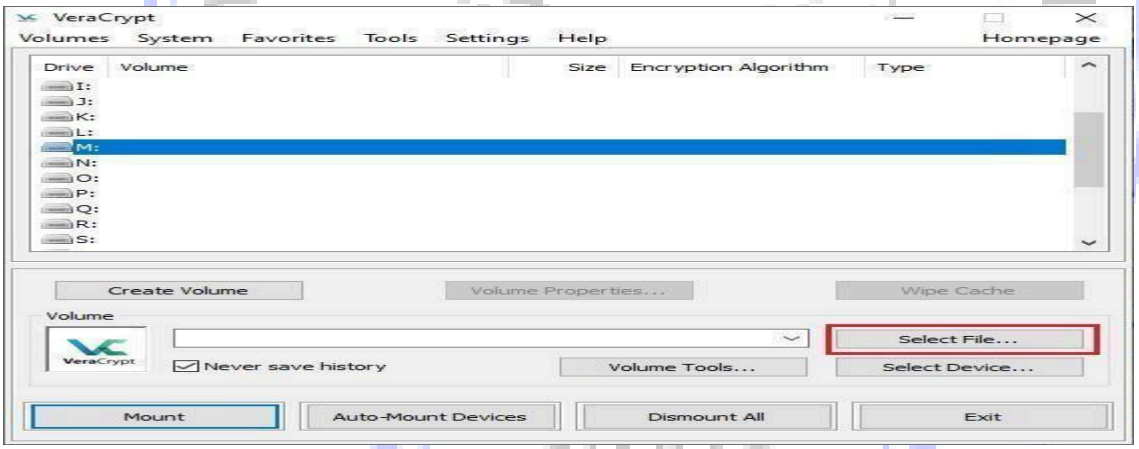
VeraCrypt window (which should still be open, but if it is not, repeat Step 1 to launch VeraCrypt and then continue from Step 13.)

STEP 13:



Select a drive letter from the list (marked with a red rectangle). This will be the drive letter to which the VeraCrypt container will be mounted.

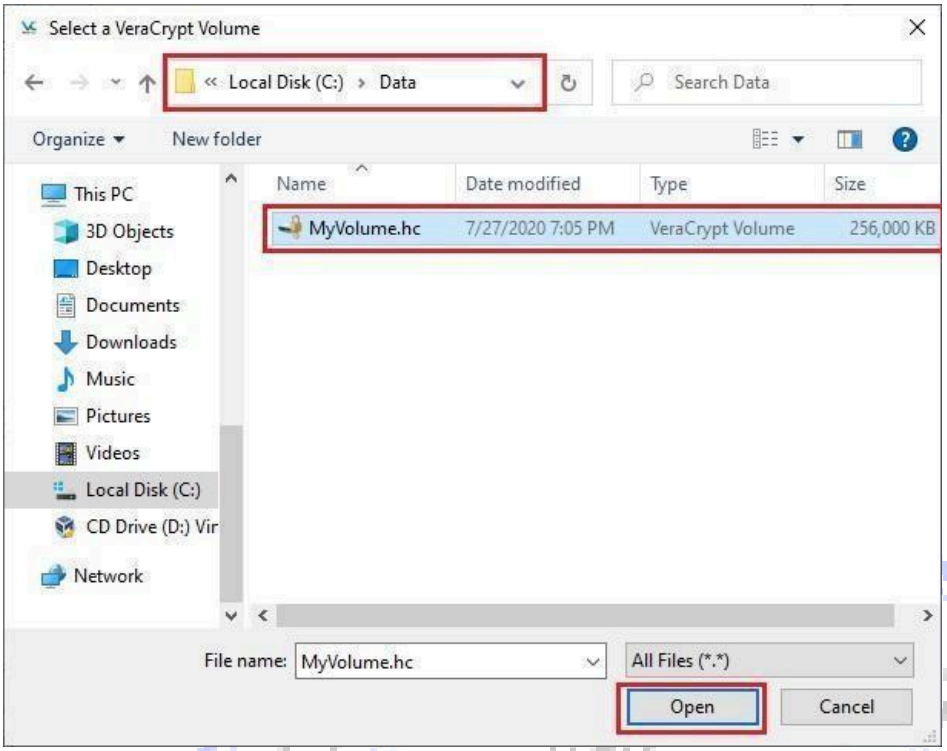
STEP 14:



Click **Select File**.

The standard file selector window should appear.

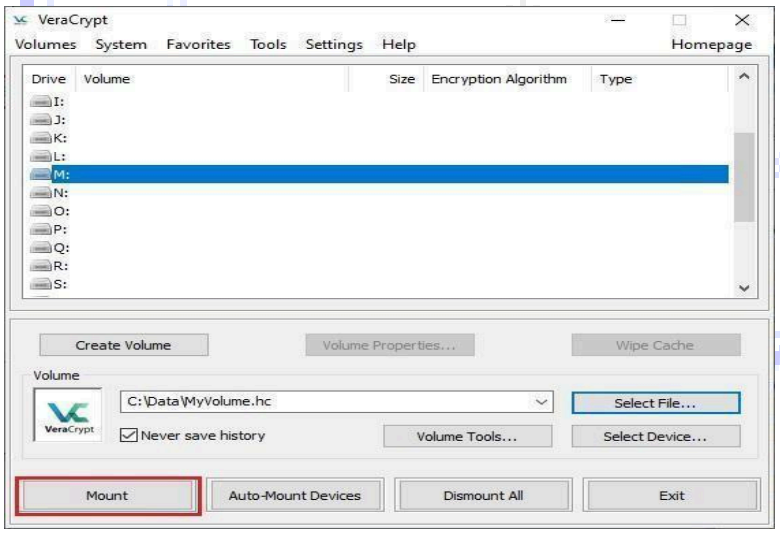
STEP 15:



In the file selector, browse to the container file (which we created in Steps 6-12) and select it. Click **Open** (in the file selector window).

The file selector window should disappear.

In the following steps, we will return to the main VeraCrypt window.

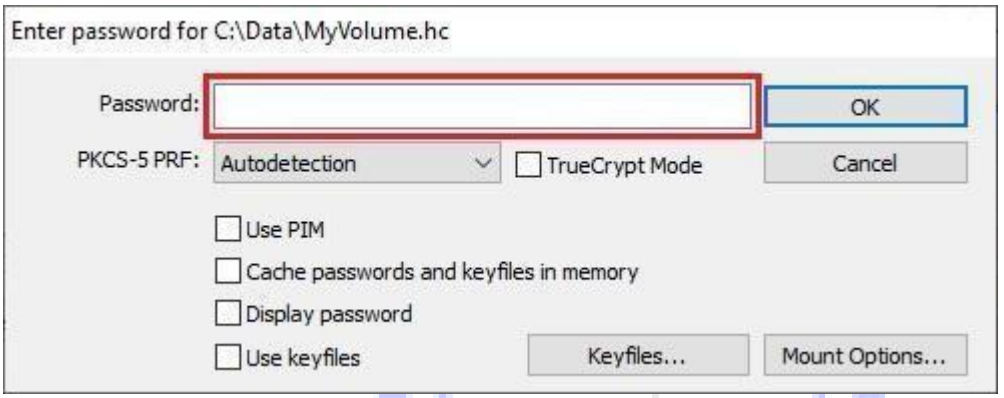


STEP 16:

In the main VeraCrypt window, click **Mount**. Password prompt dialog window should appear.

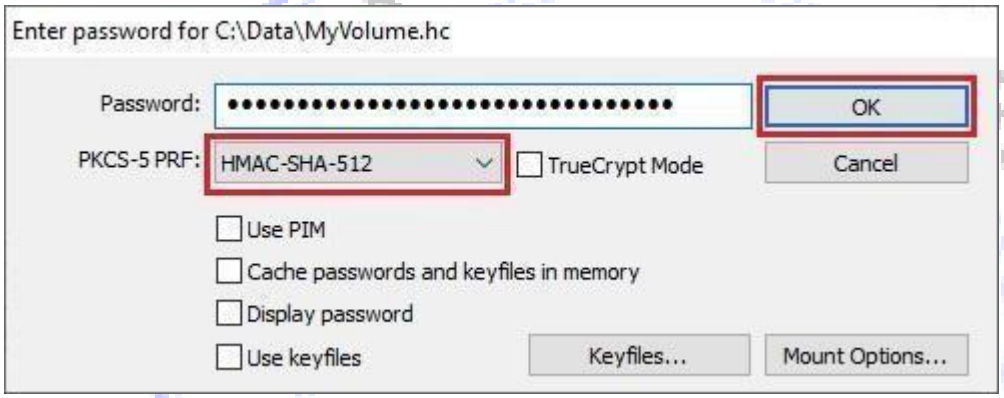
STEP 17:

Type the password (which you specified in Step 10) in the password input field (marked with



a red rectangle).

STEP 18:

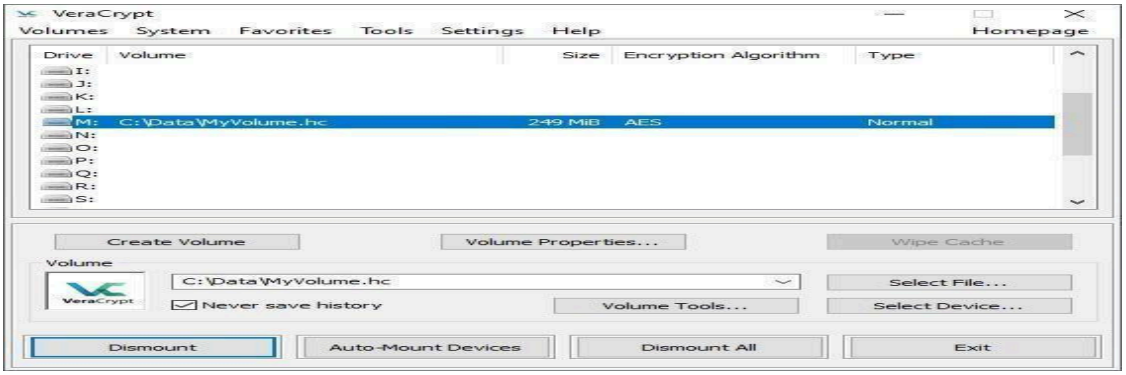


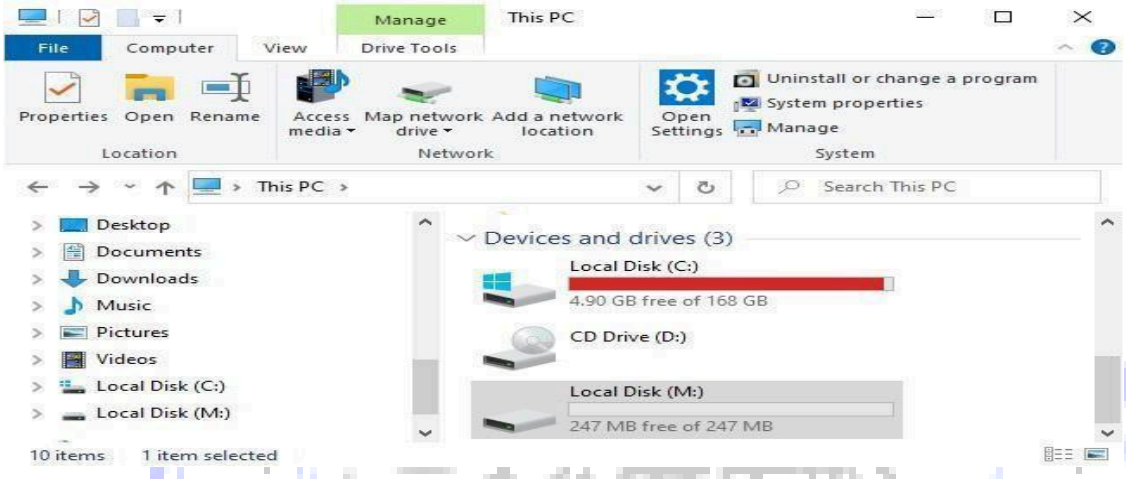
Select the PRF algorithm that was used during the creation of the volume (SHA-512 is the default PRF used by VeraCrypt). If you don't remember which PRF was used, just leave it set to "autodetection" but the mounting process will take more time. Click **OK** after entering the password.

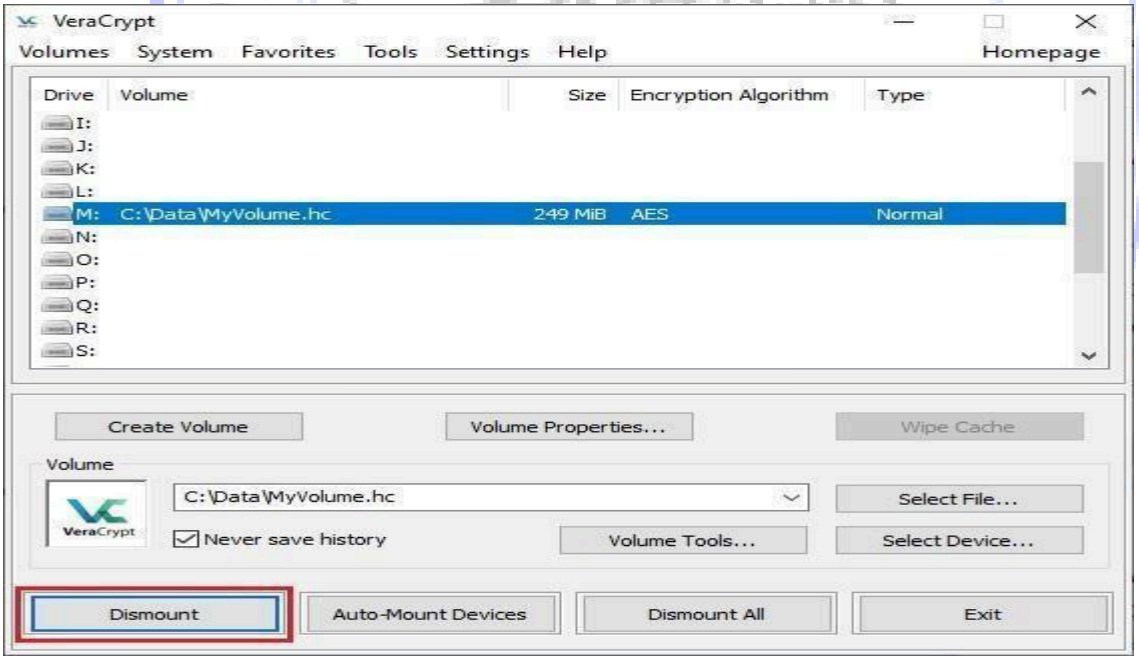
VeraCrypt will now attempt to mount the volume. If the password is incorrect (for example, if you typed it incorrectly), VeraCrypt will notify you and you will need to repeat the previous step (type the password again and click **OK**). If the password is correct, the volume will be mounted.

FINAL STEP:

Select the volume from the list of mounted volumes in the main VeraCrypt window (marked with a red rectangle in the screenshot above) and then click **Dismount** (also marked with a red rectangle in the screenshot above). To make files stored on the volume accessible again, you will have to mount the volume. To do so, repeat Steps 13-18.


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
M: C:\Data\MyVolume.hc 249 MiB AES Normal
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Data\MyVolume.hc
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit


This PC
File Computer View Manage Drive Tools
Properties Open Rename Access media Map network drive Add a network location Open Settings
Uninstall or change a program
System properties
Manage
Location Network System
This PC
Search This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (M:)
Devices and drives (3)
Local Disk (C:)
4.90 GB free of 168 GB
CD Drive (D:)
Local Disk (M:)
247 MB free of 247 MB
10 items 1 item selected


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
M: C:\Data\MyVolume.hc 249 MiB AES Normal
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Data\MyVolume.hc
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit