ASSIGNMENT – 2

UNDERSTANDING AND IMPLEMENTING KALI LINUX TOOLS

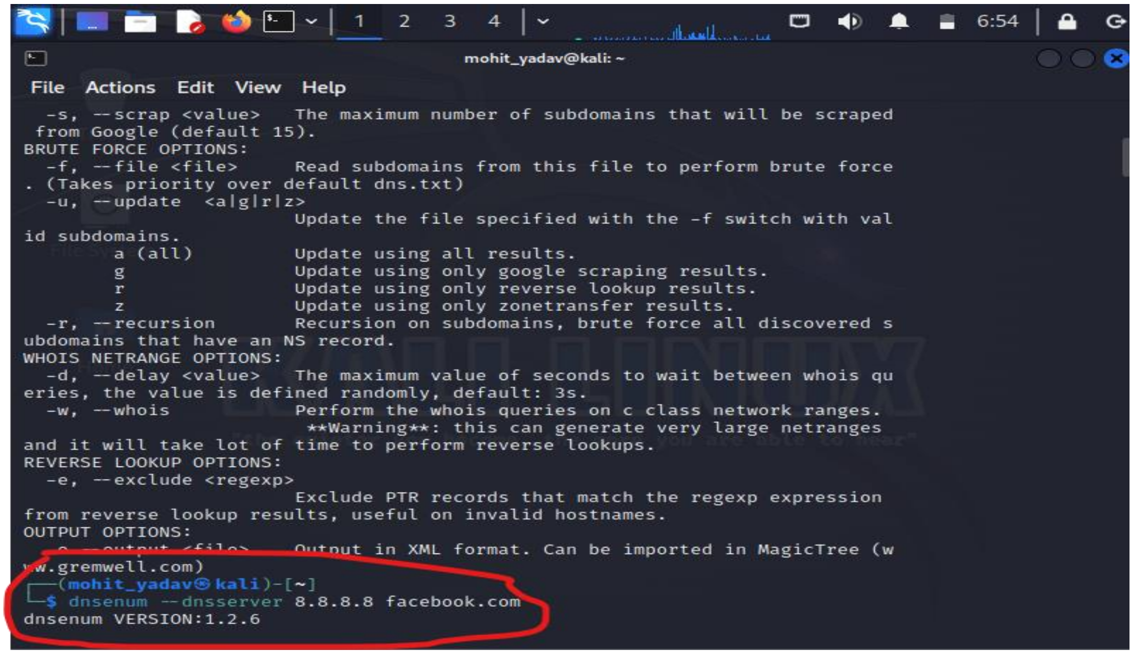
===

1. DNSENUM:

Information gathering, often referred to as reconnaissance or OSINT (Open-Source Intelligence), is the initial phase of the cybersecurity and hacking process. It involves the systematic collection of data, facts, and intelligence about a target system, organization, or individual.

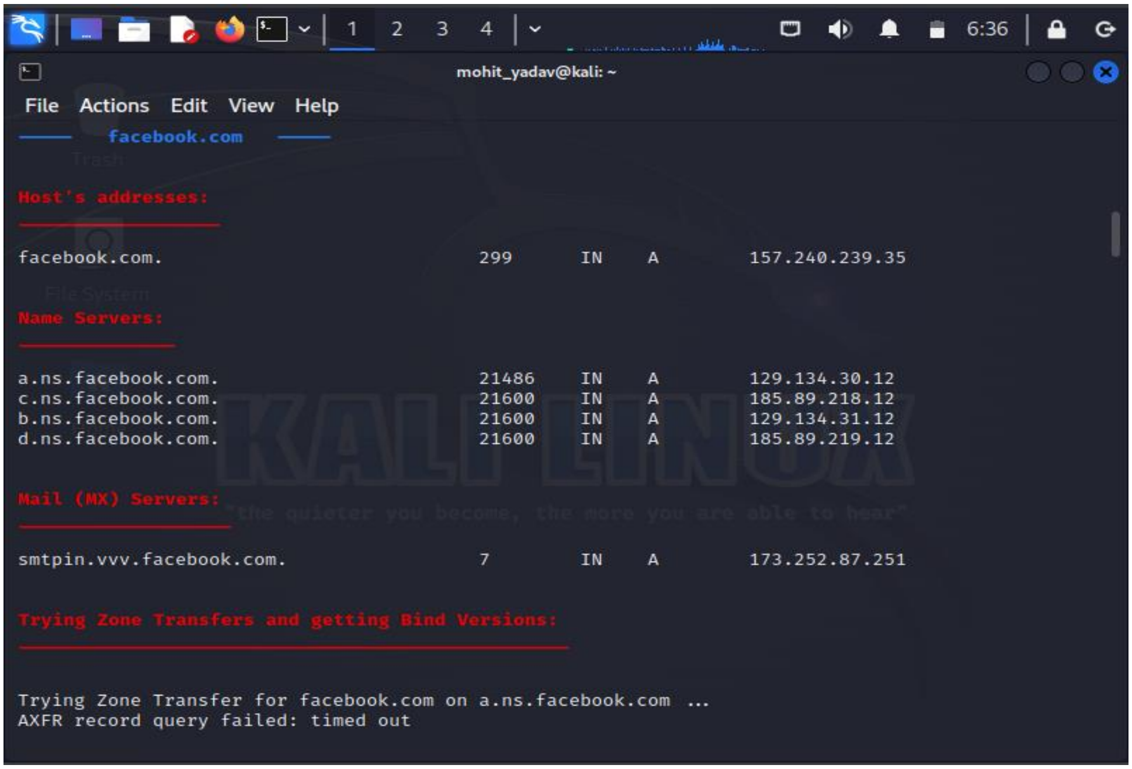
Kali Linux provides various tools for implementing the first and crucial stage of penetration testing, i.e., Information Gathering.

I have chosen DNS analysis i.e., Domain Name System Analysis. The Domain Name System is a hierarchical and distributed naming system for computers, services, and other resources on the Internet or other Internet Protocol networks. It associates various information with domain names assigned to each of the associated entities. We will implement this by using the tool DNSENUM to get as much information as we can related to the target's DNS.

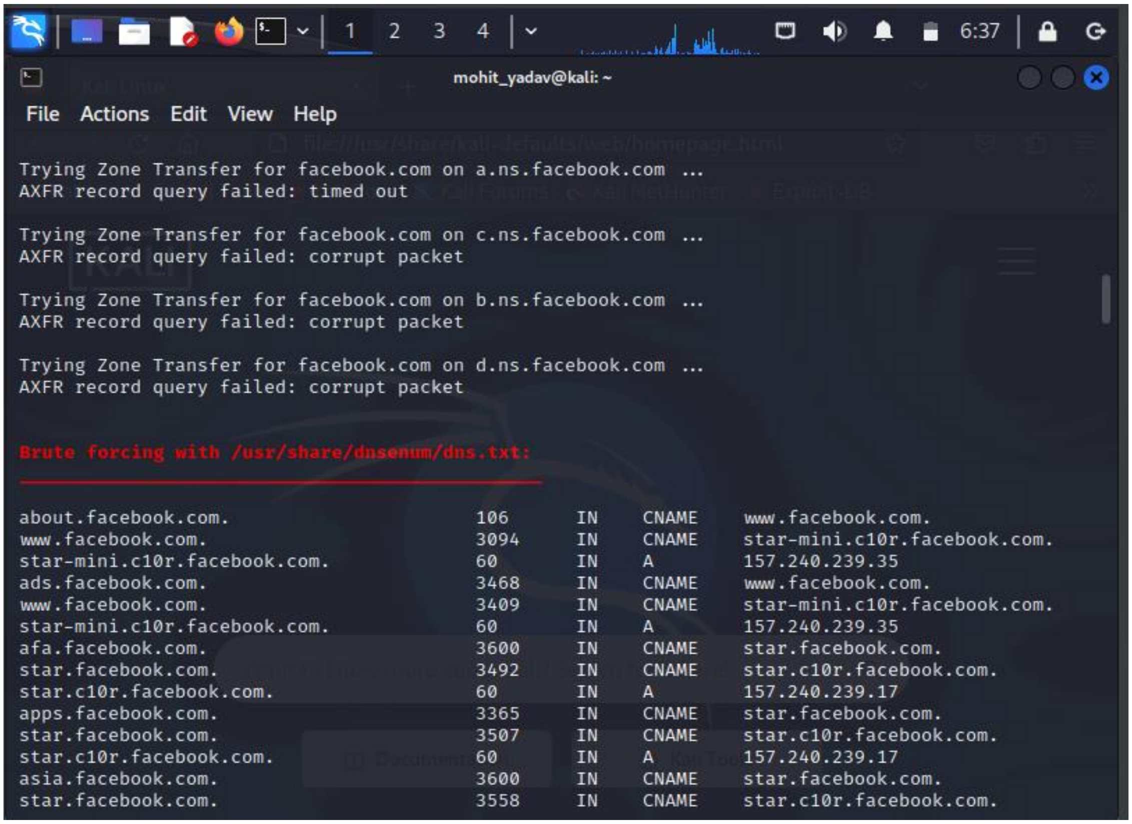


```
  -s, --scrap <value>   The maximum number of subdomains that will be scraped
 from Google (default 15).
BRUTE FORCE OPTIONS:
  -f, --file <file>     Read subdomains from this file to perform brute force
. (Takes priority over default dns.txt)
  -u, --update  <a|g|r|z>
                        Update the file specified with the -f switch with val
id subdomains.
        a (all)         Update using all results.
        g               Update using only google scraping results.
        r               Update using only reverse lookup results.
        z               Update using only zonetransfer results.
  -r, --recursion       Recursion on subdomains, brute force all discovered s
ubdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
  -d, --delay <value>   The maximum value of seconds to wait between whois qu
eries, the value is defined randomly, default: 3s.
  -w, --whois           Perform the whois queries on c class network ranges.
                         **Warning**: this can generate very large netranges
and it will take lot of time to perform reverse lookups.
REVERSE LOOKUP OPTIONS:
  -e, --exclude <regexp>
                        Exclude PTR records that match the regexp expression
from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
  -o, --output <file>   Output in XML format. Can be imported in MagicTree (w
ww.gremwell.com)
┌──(mohit_yadav㉿kali)-[~]
└─$ dnsenum --dnsserver 8.8.8.8 facebook.com
dnsenum VERSION:1.2.6
```

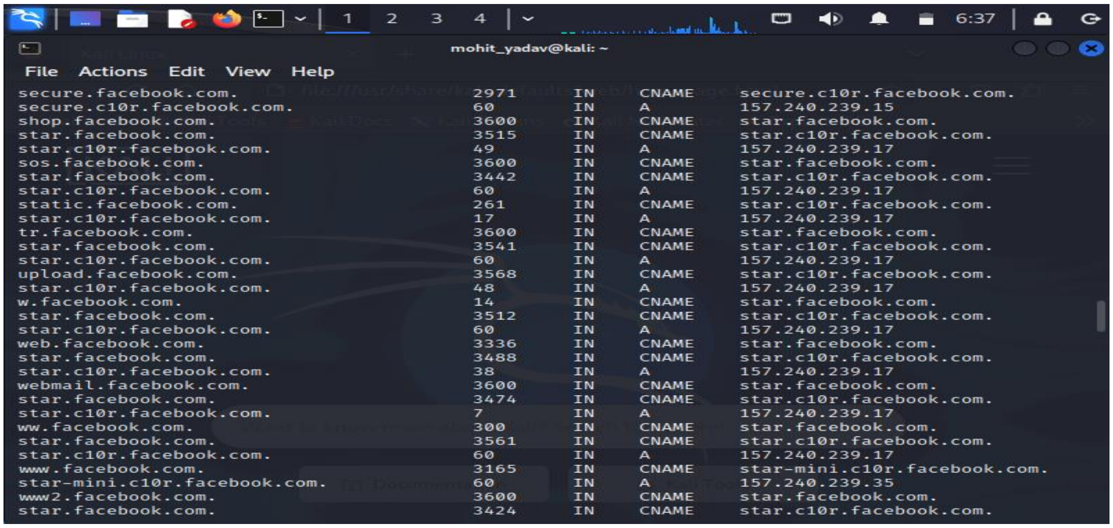
I have chosen Facebook as my target. We enter the google domain IP with the dnsserver command to reach the server. Following this we get,



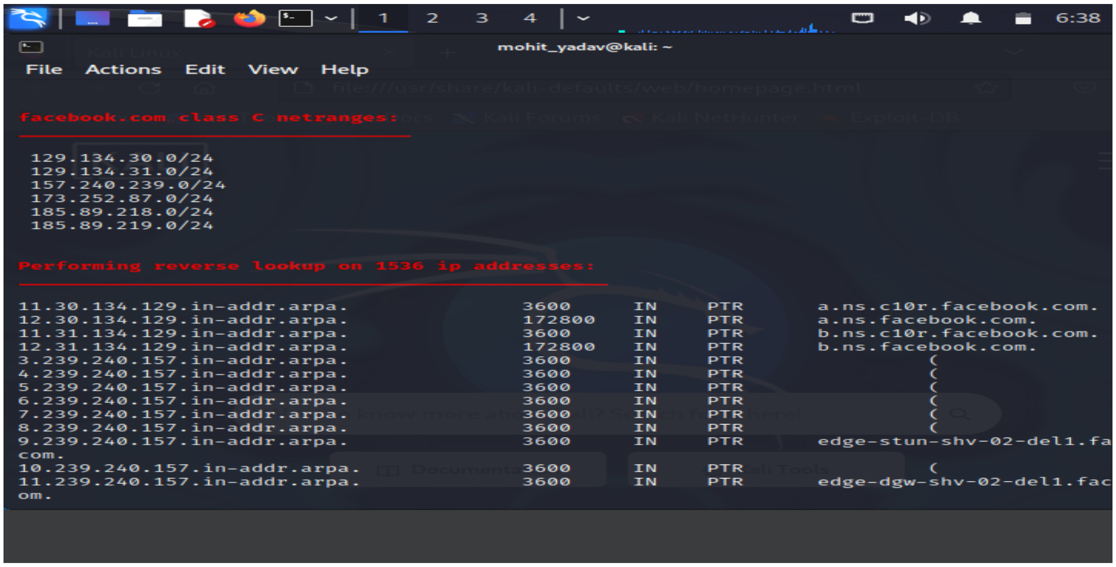
```
-----   facebook.com   -----


Host's addresses:
__________________

facebook.com.                            299      IN    A        157.240.239.35


Name Servers:
______________

a.ns.facebook.com.                       21486    IN    A        129.134.30.12
c.ns.facebook.com.                       21600    IN    A        185.89.218.12
b.ns.facebook.com.                       21600    IN    A        129.134.31.12
d.ns.facebook.com.                       21600    IN    A        185.89.219.12


Mail (MX) Servers:
___________________

smtpin.vvv.facebook.com.                 7        IN    A        173.252.87.251


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for facebook.com on a.ns.facebook.com ...
AXFR record query failed: timed out
```



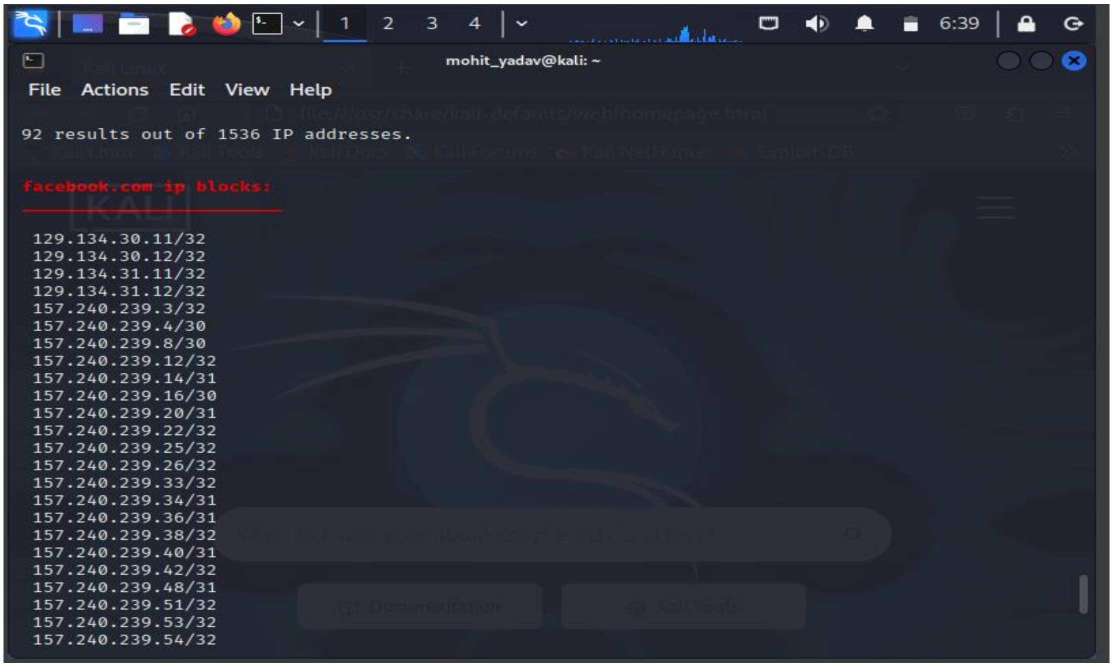
```
Trying Zone Transfer for facebook.com on a.ns.facebook.com ...
AXFR record query failed: timed out

Trying Zone Transfer for facebook.com on c.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on b.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on d.ns.facebook.com ...
AXFR record query failed: corrupt packet


Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________

about.facebook.com.                      106      IN    CNAME    www.facebook.com.
www.facebook.com.                        3094     IN    CNAME    star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.             60       IN    A        157.240.239.35
ads.facebook.com.                        3468     IN    CNAME    www.facebook.com.
www.facebook.com.                        3409     IN    CNAME    star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.             60       IN    A        157.240.239.35
afa.facebook.com.                        3600     IN    CNAME    star.facebook.com.
star.facebook.com.                       3492     IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.                  60       IN    A        157.240.239.17
apps.facebook.com.                       3365     IN    CNAME    star.facebook.com.
star.facebook.com.                       3507     IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.                  60       IN    A        157.240.239.17
asia.facebook.com.                       3600     IN    CNAME    star.facebook.com.
star.facebook.com.                       3558     IN    CNAME    star.c10r.facebook.com.
```



```
secure.facebook.com.              2971    IN   CNAME   secure.c10r.facebook.com.
secure.c10r.facebook.com.         60      IN   A       157.240.239.15
shop.facebook.com.                3600    IN   CNAME   star.facebook.com.
star.facebook.com.                3515    IN   CNAME   star.c10r.facebook.com.
star.c10r.facebook.com.           49      IN   A       157.240.239.17
sos.facebook.com.                 3600    IN   CNAME   star.facebook.com.
star.facebook.com.                3442    IN   CNAME   star.c10r.facebook.com.
star.c10r.facebook.com.           60      IN   A       157.240.239.17
static.facebook.com.              261     IN   CNAME   star.c10r.facebook.com.
star.c10r.facebook.com.           17      IN   A       157.240.239.17
tr.facebook.com.                  3600    IN   CNAME   star.facebook.com.
star.facebook.com.                3541    IN   CNAME   star.c10r.facebook.com.
star.c10r.facebook.com.           60      IN   A       157.240.239.17
upload.facebook.com.              3568    IN   CNAME   star.c10r.facebook.com.
star.c10r.facebook.com.           48      IN   A       157.240.239.17
w.facebook.com.                   14      IN   CNAME   star.facebook.com.
star.facebook.com.                3512    IN   CNAME   star.c10r.facebook.com.
star.c10r.facebook.com.           60      IN   A       157.240.239.17
web.facebook.com.                 3336    IN   CNAME   star.facebook.com.
star.facebook.com.                3488    IN   CNAME   star.c10r.facebook.com.
star.c10r.facebook.com.           38      IN   A       157.240.239.17
webmail.facebook.com.             3600    IN   CNAME   star.facebook.com.
star.facebook.com.                3474    IN   CNAME   star.c10r.facebook.com.
star.c10r.facebook.com.           7       IN   A       157.240.239.17
ww.facebook.com.                  300     IN   CNAME   star.facebook.com.
star.facebook.com.                3561    IN   CNAME   star.c10r.facebook.com.
star.c10r.facebook.com.           60      IN   A       157.240.239.17
www.facebook.com.                 3165    IN   CNAME   star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.      60      IN   A       157.240.239.35
www2.facebook.com.                3600    IN   CNAME   star.facebook.com.
star.facebook.com.                3424    IN   CNAME   star.c10r.facebook.com.
```



```
facebook.com class C netranges:
_______________________________

 129.134.30.0/24
 129.134.31.0/24
 157.240.239.0/24
 173.252.87.0/24
 185.89.218.0/24
 185.89.219.0/24

Performing reverse lookup on 1536 ip addresses:
________________________________________________

11.30.134.129.in-addr.arpa.              3600      IN     PTR      a.ns.c10r.facebook.com.
12.30.134.129.in-addr.arpa.              172800    IN     PTR      a.ns.facebook.com.
11.31.134.129.in-addr.arpa.              3600      IN     PTR      b.ns.c10r.facebook.com.
12.31.134.129.in-addr.arpa.              172800    IN     PTR      b.ns.facebook.com.
3.239.240.157.in-addr.arpa.              3600      IN     PTR              (
4.239.240.157.in-addr.arpa.              3600      IN     PTR              (
5.239.240.157.in-addr.arpa.              3600      IN     PTR              (
6.239.240.157.in-addr.arpa.              3600      IN     PTR              (
7.239.240.157.in-addr.arpa.              3600      IN     PTR              (
8.239.240.157.in-addr.arpa.              3600      IN     PTR              (
9.239.240.157.in-addr.arpa.              3600      IN     PTR      edge-stun-shv-02-del1.fa
com.
10.239.240.157.in-addr.arpa.             3600      IN     PTR              (
11.239.240.157.in-addr.arpa.             3600      IN     PTR      edge-dgw-shv-02-del1.fac
om.
```



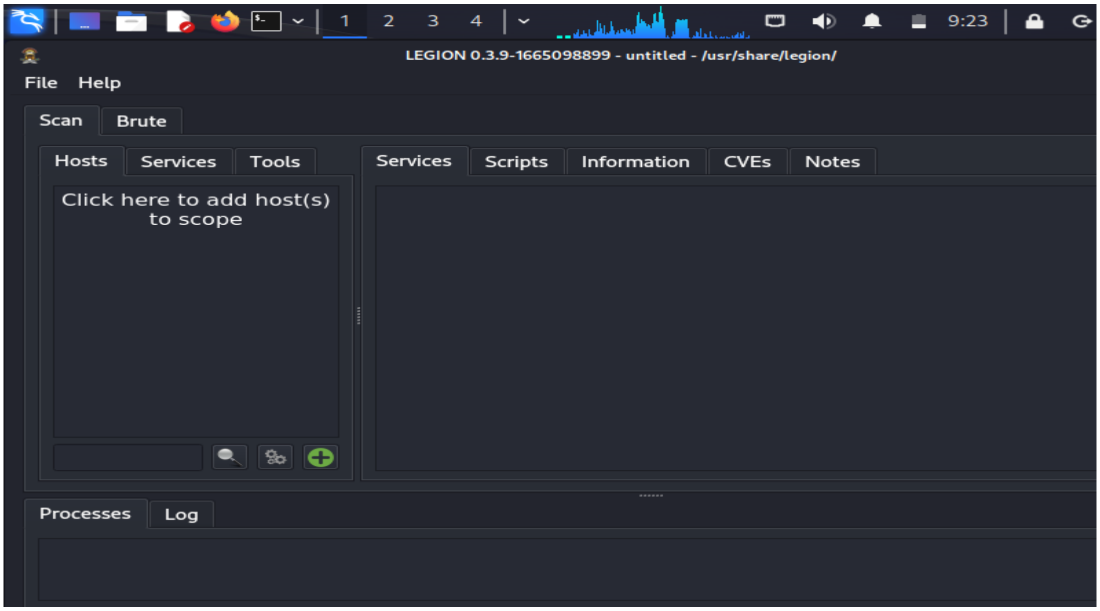
```
92 results out of 1536 IP addresses.

facebook.com ip blocks:
_______________________

 129.134.30.11/32
 129.134.30.12/32
 129.134.31.11/32
 129.134.31.12/32
 157.240.239.3/32
 157.240.239.4/30
 157.240.239.8/30
 157.240.239.12/32
 157.240.239.14/31
 157.240.239.16/30
 157.240.239.20/31
 157.240.239.22/32
 157.240.239.25/32
 157.240.239.26/32
 157.240.239.33/32
 157.240.239.34/31
 157.240.239.36/31
 157.240.239.38/32
 157.240.239.40/31
 157.240.239.42/32
 157.240.239.48/31
 157.240.239.51/32
 157.240.239.53/32
 157.240.239.54/32
```

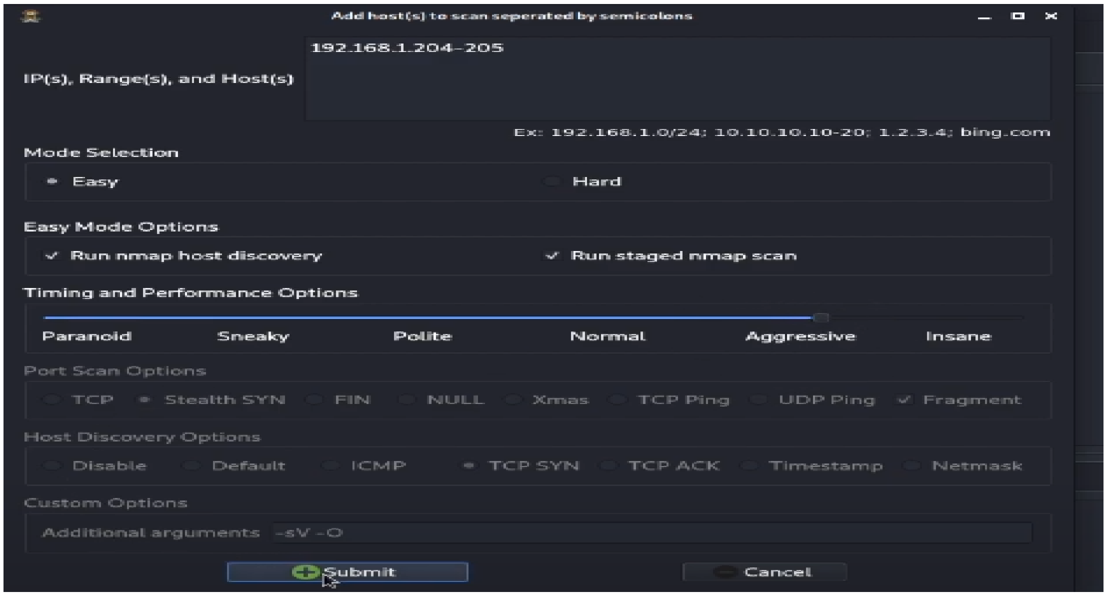
We get all the information regarding the DNS of our target server.

2. LEGION:

Vulnerability analysis is the process of identifying, assessing, and prioritizing security weaknesses or vulnerabilities in computer systems, software, networks, or applications. The goal of vulnerability analysis is to proactively find and address these weaknesses to prevent potential security breaches or unauthorized access.

We will go with Legion, which one of the tools provided by the kali Linux for vulnerability analysis. i.e., This package contains an open source, easy-to-use, super-extensible and semi-automated network penetration testing tool that aids in discovery, reconnaissance and exploitation of information systems.




Add host(s) to scan seperated by semicolons

IP(s), Range(s), and Host(s): 192.168.1.204-205

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

Mode Selection: ● Easy ○ Hard

Easy Mode Options: ✓ Run nmap host discovery ✓ Run staged nmap scan

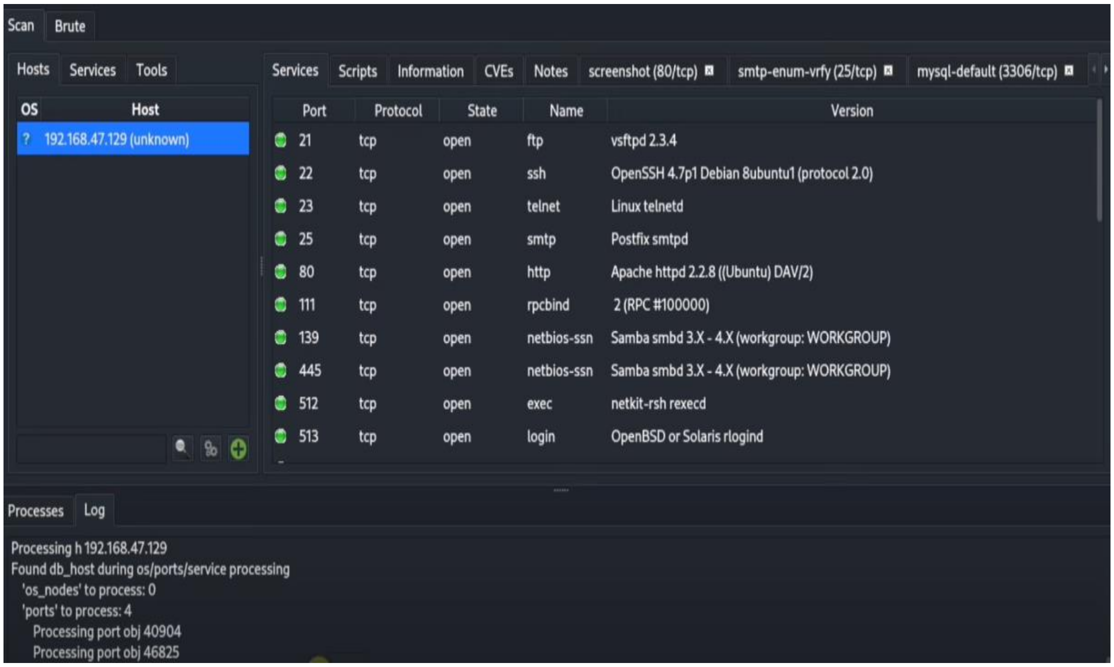
Timing and Performance Options: Paranoid Sneaky Polite Normal Aggressive Insane

Port Scan Options: ○ TCP ● Stealth SYN ○ FIN ○ NULL ○ Xmas ○ TCP Ping ○ UDP Ping ✓ Fragment

Host Discovery Options: ○ Disable ○ Default ○ ICMP ● TCP SYN ○ TCP ACK ○ Timestamp ○ Netmask

Custom Options: Additional arguments -sV -O

We get all the ports which are open:

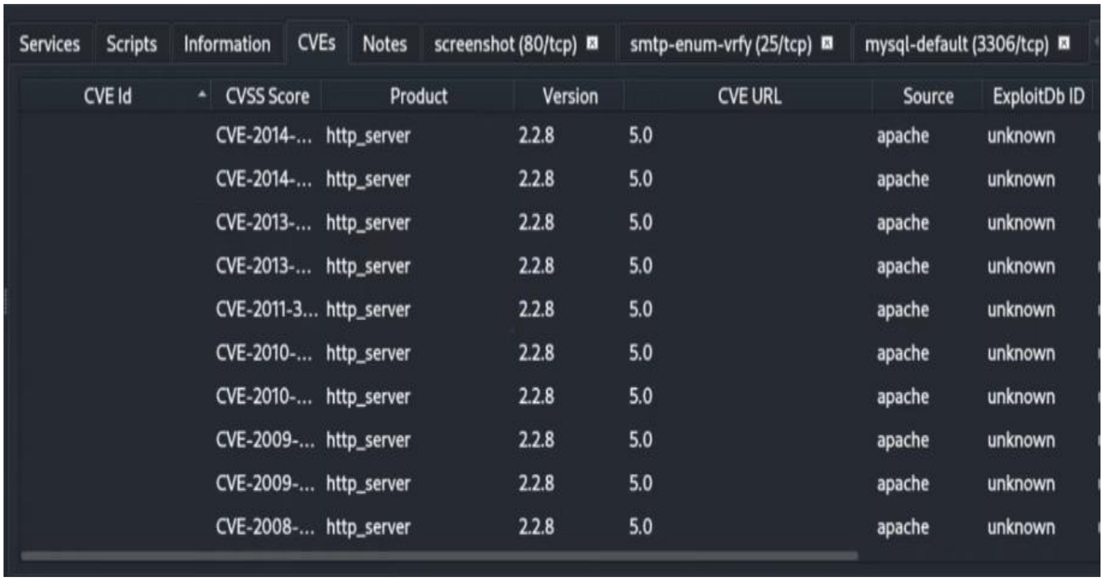


OS	Host
?	192.168.47.129 (unknown)

Port	Protocol	State	Name	Version
21	tcp	open	ftp	vsftpd 2.3.4
22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	tcp	open	telnet	Linux telnetd
25	tcp	open	smtp	Postfix smtpd
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	open	rpcbind	2 (RPC #100000)
139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	tcp	open	exec	netkit-rsh rexecd
513	tcp	open	login	OpenBSD or Solaris rlogind

```
Processing h 192.168.47.129
Found db_host during os/ports/service processing
  'os_nodes' to process: 0
  'ports' to process: 4
    Processing port obj 40904
    Processing port obj 46825
```

We can also see the basic level vulnerabilities which are present on the target:



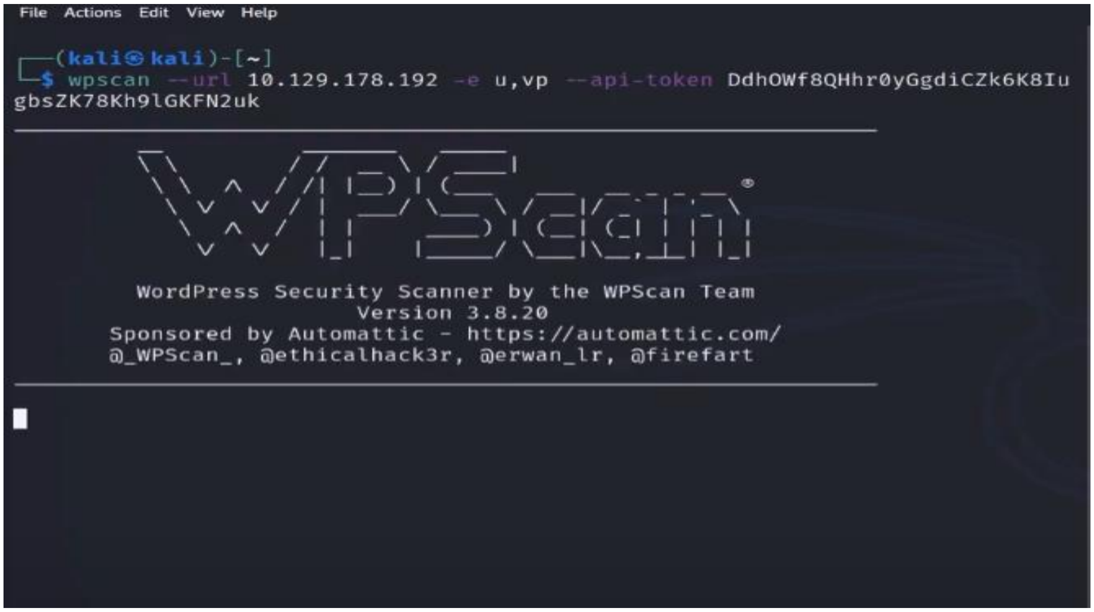
CVE Id	CVSS Score	Product	Version	CVE URL	Source	ExploitDb ID
	CVE-2014-...	http_server	2.2.8	5.0	apache	unknown
	CVE-2014-...	http_server	2.2.8	5.0	apache	unknown
	CVE-2013-...	http_server	2.2.8	5.0	apache	unknown
	CVE-2013-...	http_server	2.2.8	5.0	apache	unknown
	CVE-2011-3...	http_server	2.2.8	5.0	apache	unknown
	CVE-2010-...	http_server	2.2.8	5.0	apache	unknown
	CVE-2010-...	http_server	2.2.8	5.0	apache	unknown
	CVE-2009-...	http_server	2.2.8	5.0	apache	unknown
	CVE-2009-...	http_server	2.2.8	5.0	apache	unknown
	CVE-2008-...	http_server	2.2.8	5.0	apache	unknown

It has many more functionality, but We will only explore till here.

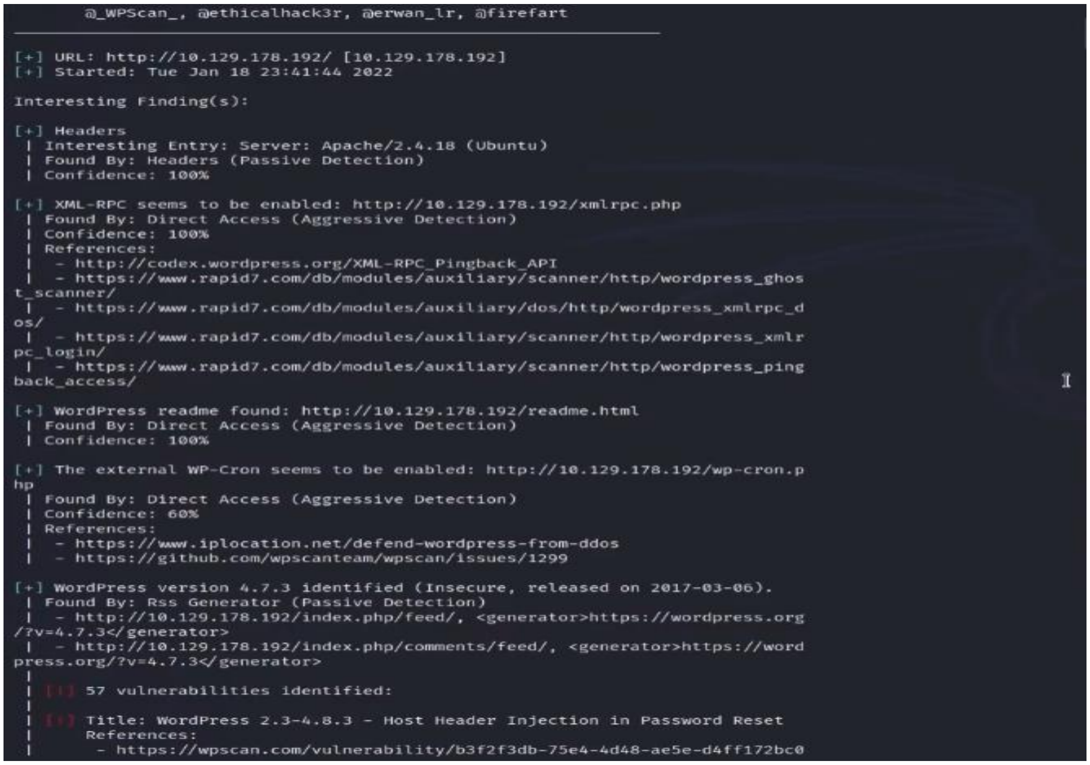
3. WPScan:

Web application analysis involves the examination and evaluation of web-based software applications to identify security vulnerabilities, such as SQL injection, cross-site scripting (XSS), and other potential threats. This analysis is essential for ensuring the security of web applications.

I have chosen Wpscan to perform this analysis on Kali Linux, Wpscan is a WordPress security scanner used to test WordPress installations and WordPress-powered websites.



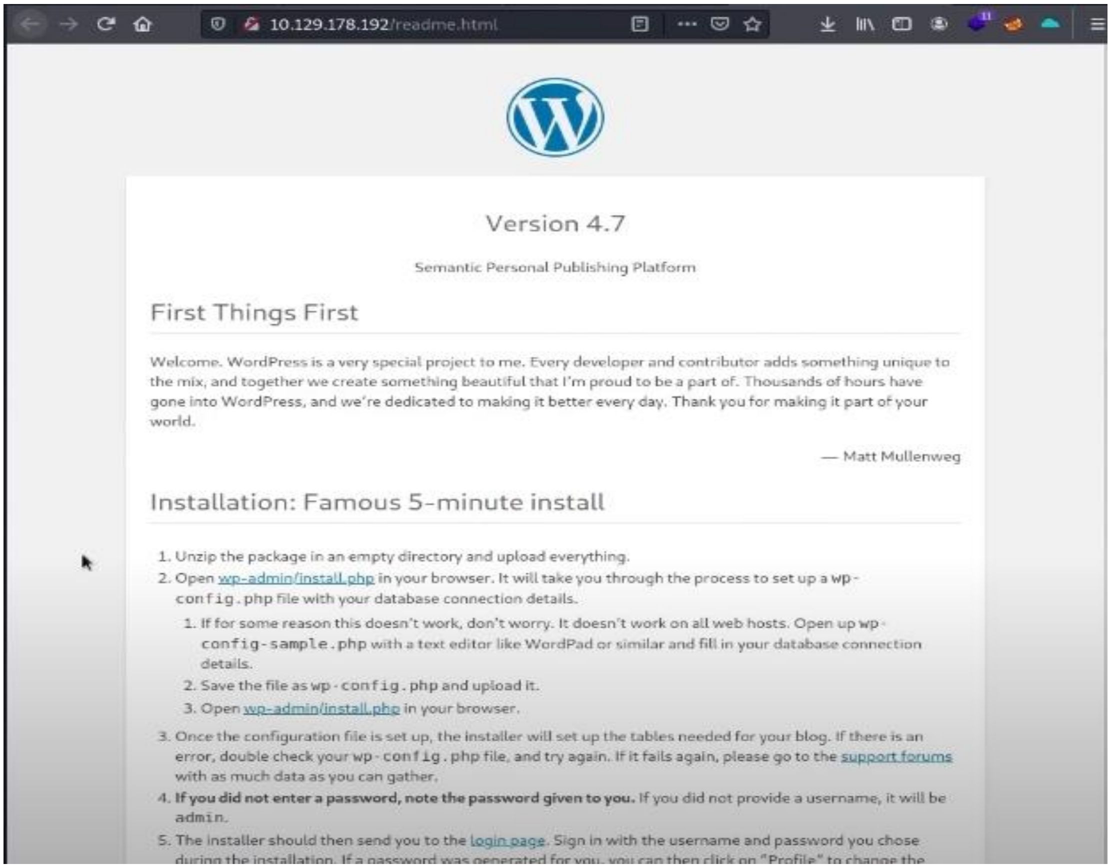
```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 10.129.178.192 -e u,vp --api-token DdhOWf8QHhr0yGgdiCZk6K8Iu
gbsZK78Kh9lGKFN2uk
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.20
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```



```
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.129.178.192/ [10.129.178.192]
[+] Started: Tue Jan 18 23:41:44 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.129.178.192/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghos
t_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_d
os/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlr
pc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ping
back_access/

[+] WordPress readme found: http://10.129.178.192/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.129.178.192/wp-cron.p
hp
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.7.3 identified (Insecure, released on 2017-03-06).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.129.178.192/index.php/feed/, <generator>https://wordpress.org
/?v=4.7.3</generator>
 |  - http://10.129.178.192/index.php/comments/feed/, <generator>https://word
press.org/?v=4.7.3</generator>
 |
 | [!] 57 vulnerabilities identified:
 |
 | [!] Title: WordPress 2.3-4.8.3 - Host Header Injection in Password Reset
 |     References:
 |      - https://wpscan.com/vulnerability/b3f2f3db-75e4-4d48-ae5e-d4ff172bc0
```

We found a readme file.

```
http://10.129.178.192/readme.html
(Aggressive Detection)
```



Version 4.7

Semantic Personal Publishing Platform

First Things First

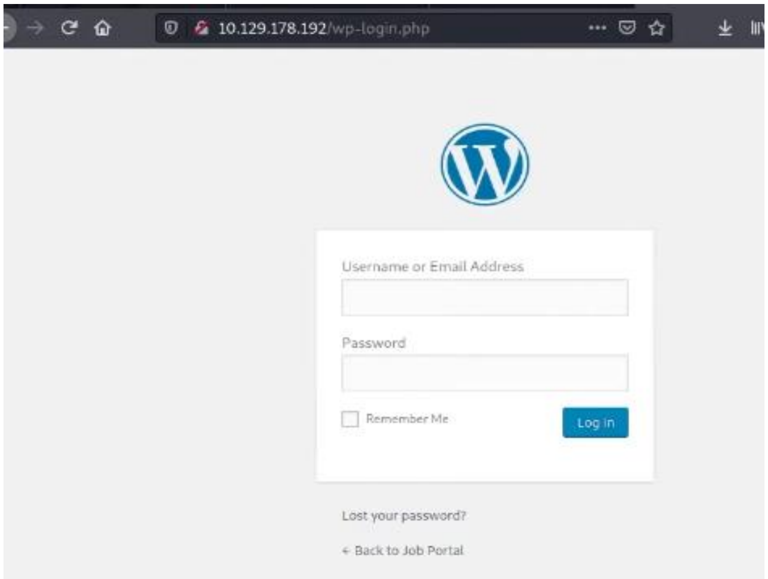
Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I'm proud to be a part of. Thousands of hours have gone into WordPress, and we're dedicated to making it better every day. Thank you for making it part of your world.

— Matt Mullenweg

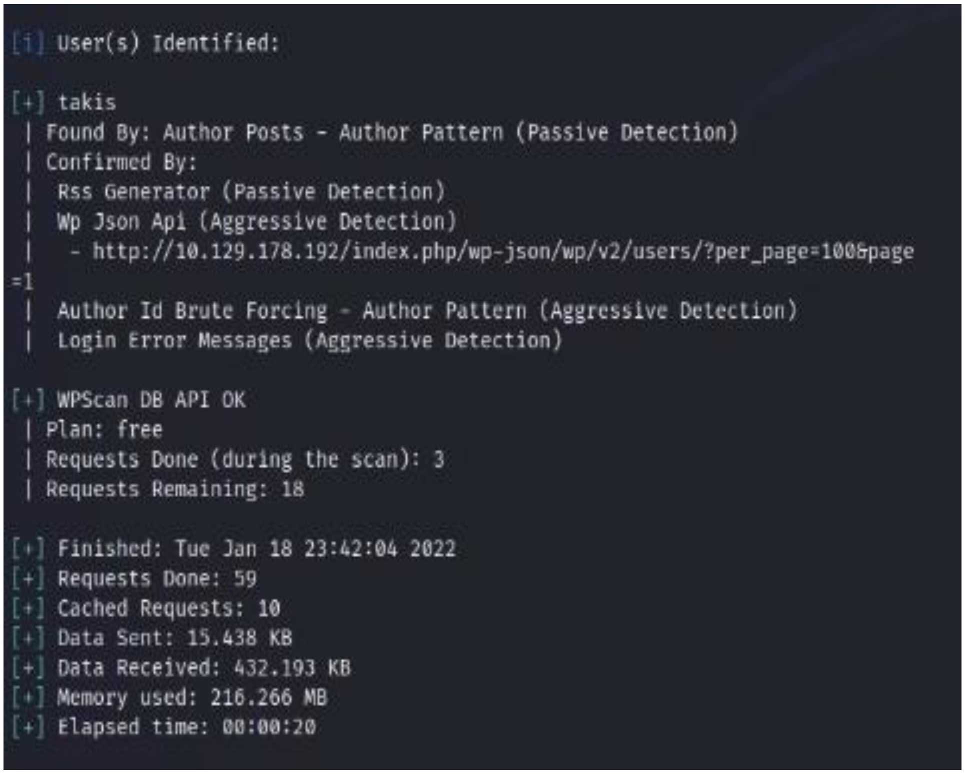
Installation: Famous 5-minute install

1. Unzip the package in an empty directory and upload everything.
2. Open wp-admin/install.php in your browser. It will take you through the process to set up a `wp-config.php` file with your database connection details.
   1. If for some reason this doesn't work, don't worry. It doesn't work on all web hosts. Open up `wp-config-sample.php` with a text editor like WordPad or similar and fill in your database connection details.
   2. Save the file as `wp-config.php` and upload it.
   3. Open wp-admin/install.php in your browser.
3. Once the configuration file is set up, the installer will set up the tables needed for your blog. If there is an error, double check your `wp-config.php` file, and try again. If it fails again, please go to the support forums with as much data as you can gather.
4. **If you did not enter a password, note the password given to you.** If you did not provide a username, it will be `admin`.
5. The installer should then send you to the login page. Sign in with the username and password you chose during the installation. If a password was generated for you, you can then click on "Profile" to change the

Here we found the URL for the login page for WordPress:



We also got the user info:



```
[i] User(s) Identified:

[+] takis
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.129.178.192/index.php/wp-json/wp/v2/users/?per_page=100&page
=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 3
 | Requests Remaining: 18

[+] Finished: Tue Jan 18 23:42:04 2022
[+] Requests Done: 59
[+] Cached Requests: 10
[+] Data Sent: 15.438 KB
[+] Data Received: 432.193 KB
[+] Memory used: 216.266 MB
[+] Elapsed time: 00:00:20
```

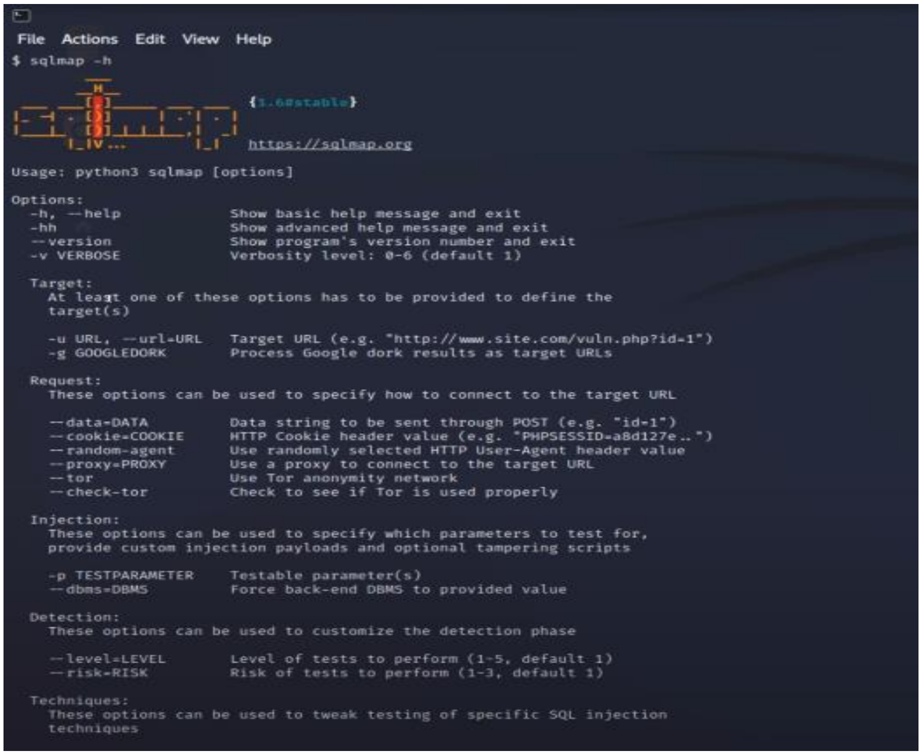
Similarly, we can use this tool to further analysis the whole target application.

4. SQLMAP:

Database assessment is the process of evaluating the security, performance, and overall health of a database system. It includes examining database configurations, access controls, and data integrity to identify potential issues and vulnerabilities.

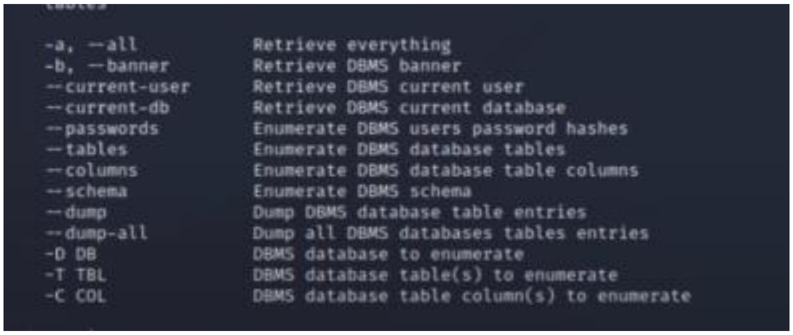
I have chosen SQLMAP tool for the data evaluation process. sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.



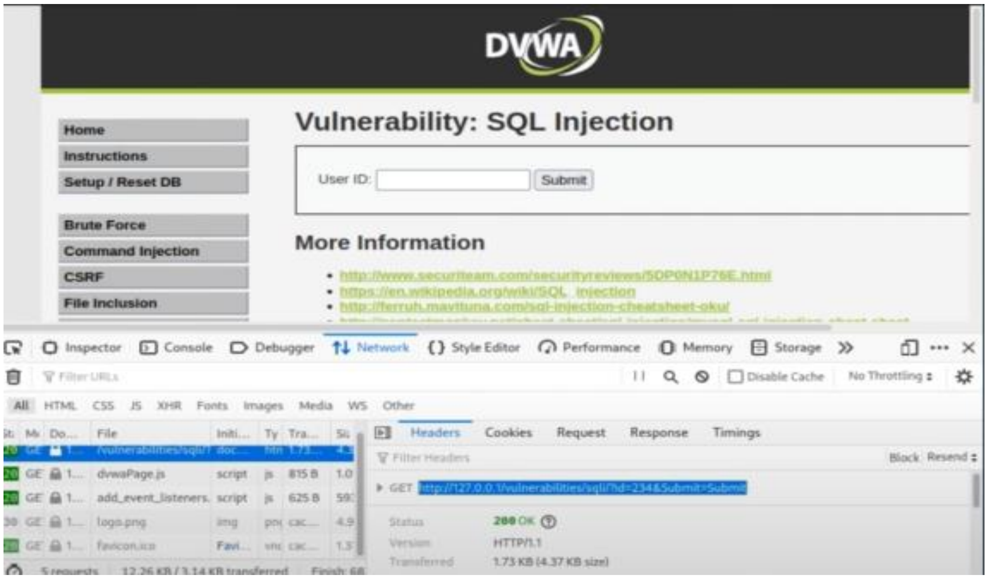
```
$ sqlmap -h
                                    {1.6#stable}

                                    https://sqlmap.org

Usage: python3 sqlmap [options]

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

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
    These options can be used to customize the detection phase

    --level=LEVEL       Level of tests to perform (1-5, default 1)
    --risk=RISK         Risk of tests to perform (1-3, default 1)

  Techniques:
    These options can be used to tweak testing of specific SQL injection
    techniques
```

We also get different functionalities to perform scanning.



```
  -a, --all           Retrieve everything
  -b, --banner        Retrieve DBMS banner
  --current-user      Retrieve DBMS current user
  --current-db        Retrieve DBMS current database
  --passwords         Enumerate DBMS users password hashes
  --tables            Enumerate DBMS database tables
  --columns           Enumerate DBMS database table columns
  --schema            Enumerate DBMS schema
  --dump              Dump DBMS database table entries
  --dump-all          Dump all DBMS databases tables entries
  -D DB               DBMS database to enumerate
  -T TBL              DBMS database table(s) to enumerate
  -C COL              DBMS database table column(s) to enumerate
```

We get the following information about the target.



Vulnerability: SQL Injection

User ID:

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/

```
St  Me  Do...  File                       Initi...  Ty   Tra...  Si
20  GE  1...   /vulnerabilities/sqli/?    doc...    htn  1.73... 4.3
20  GE  1...   dvwaPage.js                script    js   815 B   1.0
20  GE  1...   add_event_listeners.       script    js   625 B   59
30  GE  1...   logo.png                   img       pn   cac...  4.9
20  GE  1...   favicon.ico                Favi...   vnc  cac...  1.3
5 requests   12.26 KB / 3.14 KB transferred   Finish: 68
```

```
GET http://127.0.0.1/vulnerabilities/sqli/?id=234&Submit=Submit

Status        200 OK
Version       HTTP/1.1
Transferred   1.73 KB (4.37 KB size)
```

5. HASHCAT:

Password attacks refer to various techniques and methods used by attackers to gain unauthorized access to computer systems, networks, or accounts by attempting to guess or crack passwords. Common password attacks include brute force attacks, dictionary attacks, and rainbow table attacks.

I have chosen Hashcat for this attack. Hashcat is a password cracking tool used for licit and illicit purposes. HashCat is a particularly fast, efficient, and versatile hacking tool that assists brute-force attacks by conducting them with hash values of passwords that the tool is guessing or applying.

Hashcat supports several attack modes. Common ones include:
Dictionary Attack: This mode uses a wordlist or dictionary file.
Mask Attack: You specify a mask for the password format, such as "?????123" to crack passwords following that pattern.
Rule-Based Attack: You can create custom rules to manipulate and generate password combinations.
Hashcat will start its cracking process and display progress updates, including the number of hashes cracked and the estimated time remaining.
Once Hashcat completes its task, it will display the cracked passwords, if successful. These passwords will be displayed on the terminal screen.
Hashcat offers various options and flags to customize and optimize your cracking process. You can set attack-specific parameters, use rules for mutations, and specify performance-related options.

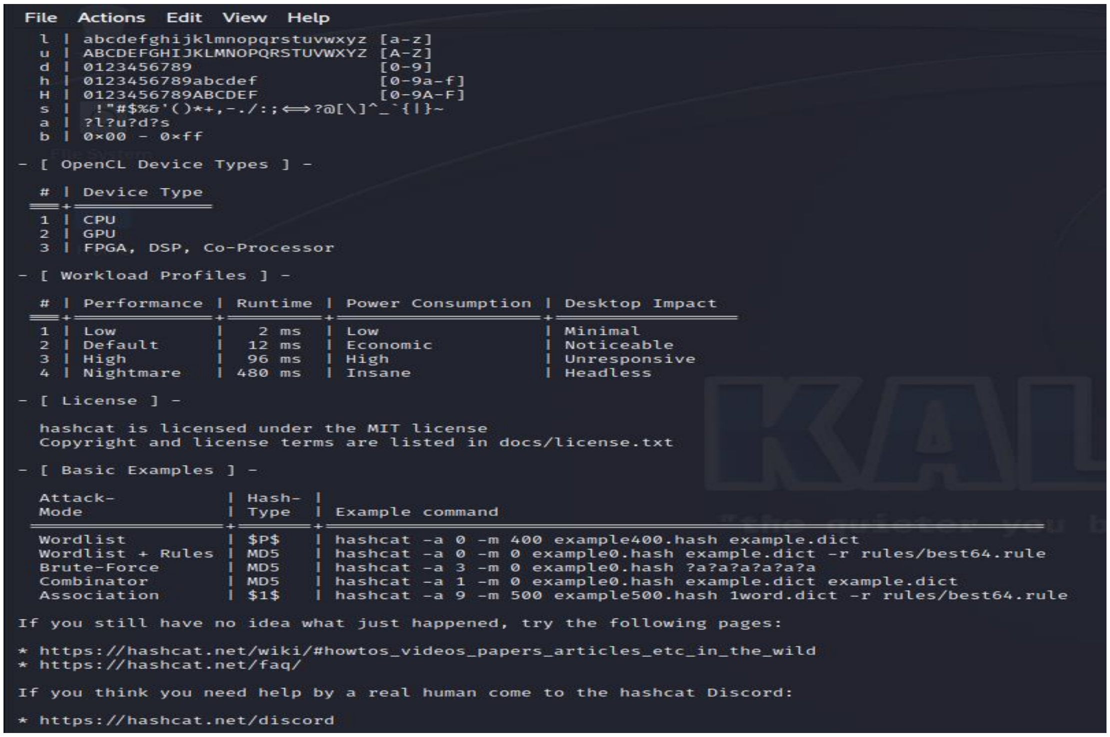
To use Hashcat, you'll need to specify the hash to crack, the attack mode, and the wordlist or mask. Here's a general command structure:

```
hashcat -m [HashingAlgorithm] [HashFile] [Wordlist]
```

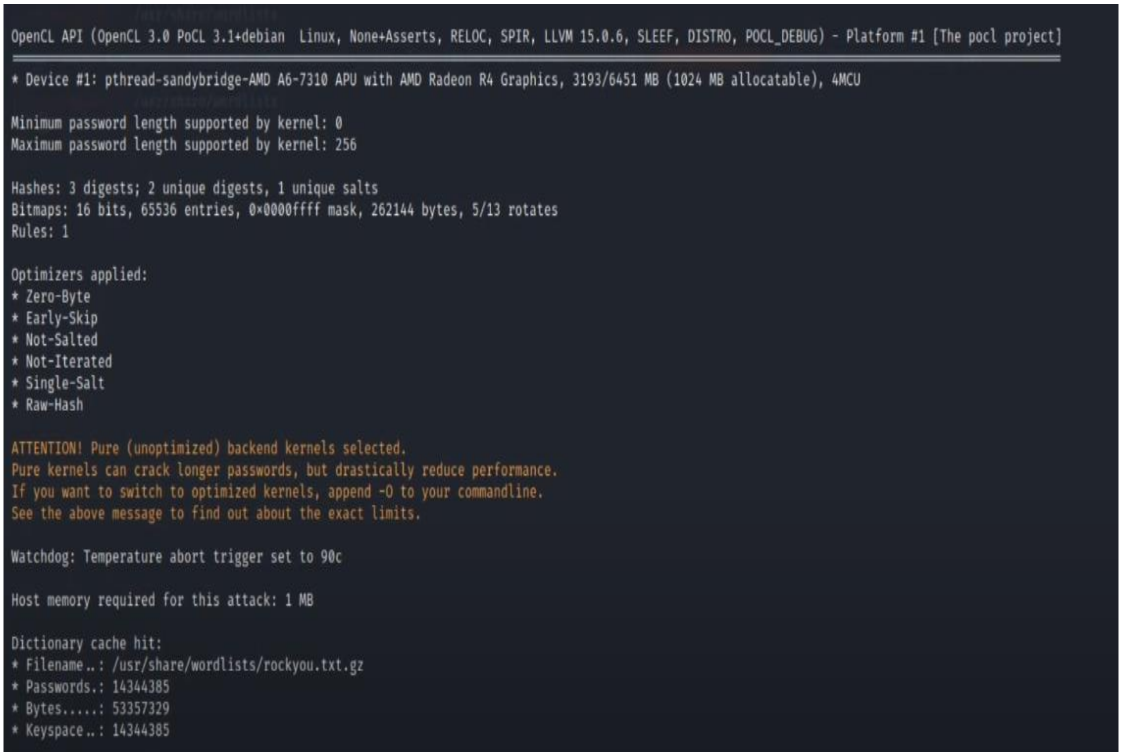
For example, to perform a dictionary attack on an MD5 hash with a wordlist called "wordlist.txt":

```
hashcat -m 0 hashfile.txt wordlist.txt
```

Replace [Hashing Algorithm] with the appropriate number for the hashing algorithm (e.g., 0 for MD5, 1000 for NTLM), [HashFile] with the file containing the target hash, and [Wordlist] with the path to your wordlist file.



```
  l | abcdefghijklmnopqrstuvwxyz [a-z]
  u | ABCDEFGHIJKLMNOPQRSTUVWXYZ [A-Z]
  d | 0123456789                 [0-9]
  h | 0123456789abcdef           [0-9a-f]
  H | 0123456789ABCDEF           [0-9A-F]
  s |  !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
  a | ?l?u?d?s
  b | 0x00 - 0xff

- [ OpenCL Device Types ] -

  # | Device Type
 ===+=============
  1 | CPU
  2 | GPU
  3 | FPGA, DSP, Co-Processor

- [ Workload Profiles ] -

  # | Performance | Runtime | Power Consumption | Desktop Impact
 ===+=============+=========+===================+=================
  1 | Low         |   2 ms  | Low               | Minimal
  2 | Default     |  12 ms  | Economic          | Noticeable
  3 | High        |  96 ms  | High              | Unresponsive
  4 | Nightmare   | 480 ms  | Insane            | Headless

- [ License ] -

  hashcat is licensed under the MIT license
  Copyright and license terms are listed in docs/license.txt

- [ Basic Examples ] -

  Attack-          | Hash- |
  Mode             | Type  | Example command
 ==================+=======+==================================================================
  Wordlist         | $P$   | hashcat -a 0 -m 400 example400.hash example.dict
  Wordlist + Rules | MD5   | hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule
  Brute-Force      | MD5   | hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a
  Combinator       | MD5   | hashcat -a 1 -m 0 example0.hash example.dict example.dict
  Association      | $1$   | hashcat -a 9 -m 500 example500.hash 1word.dict -r rules/best64.rule

If you still have no idea what just happened, try the following pages:

* https://hashcat.net/wiki/#howtos_videos_papers_articles_etc_in_the_wild
* https://hashcat.net/faq/

If you think you need help by a real human come to the hashcat Discord:

* https://hashcat.net/discord
```

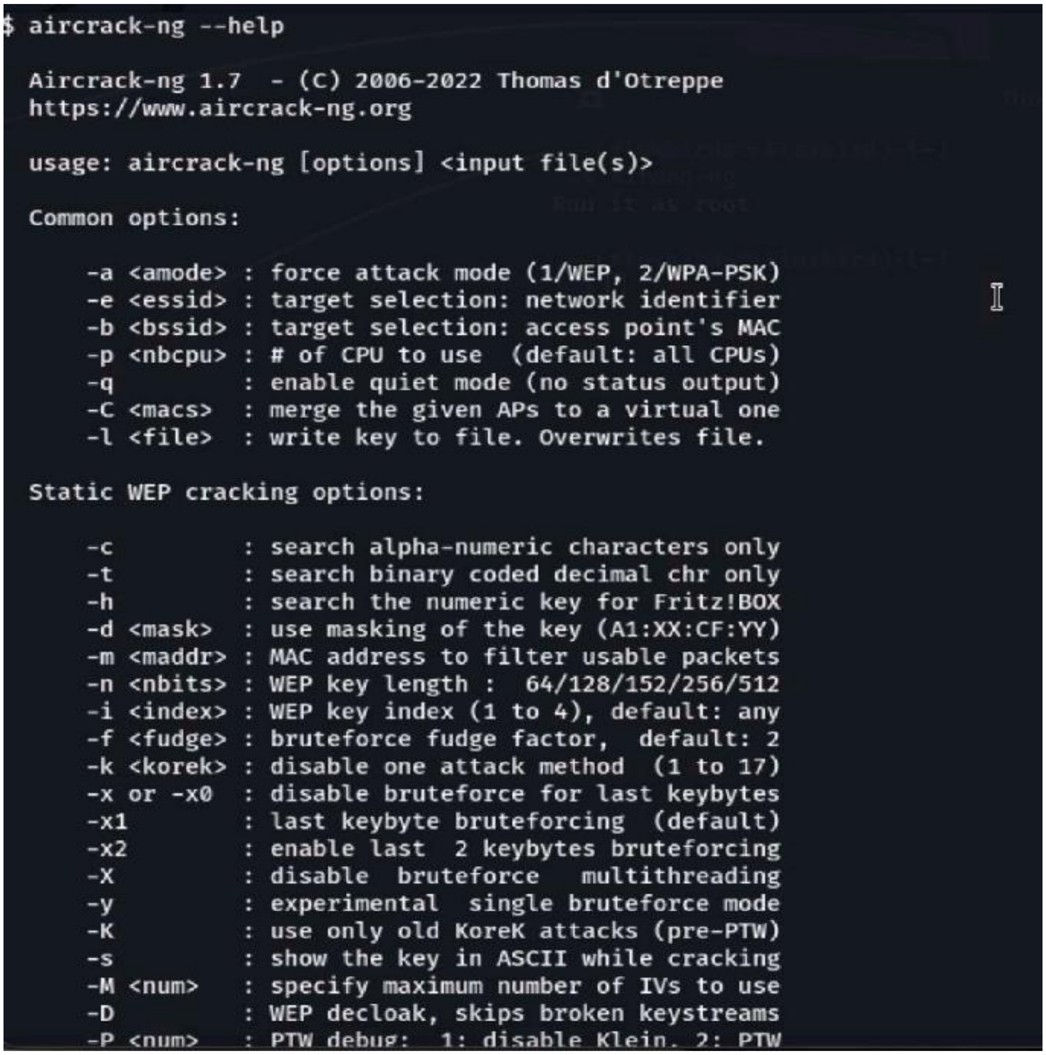


```
OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====================================================================================================================================================
* Device #1: pthread-sandybridge-AMD A6-7310 APU with AMD Radeon R4 Graphics, 3193/6451 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 3 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 14344385
* Bytes.....: 53357329
* Keyspace..: 14344385
```

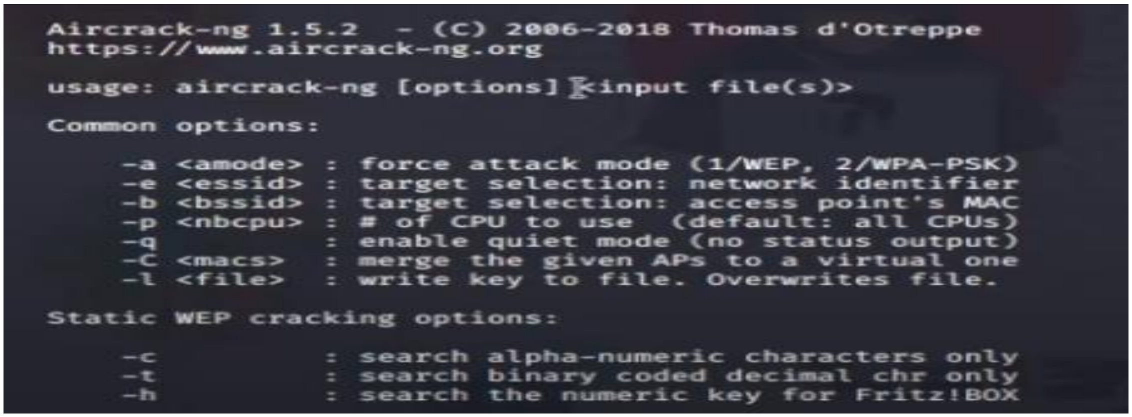
6. AIRCRACK-NG:

Wireless attacks involve exploiting vulnerabilities in wireless networks and devices, such as Wi-Fi networks. These attacks can include unauthorized access, eavesdropping, and interception of wireless communications.

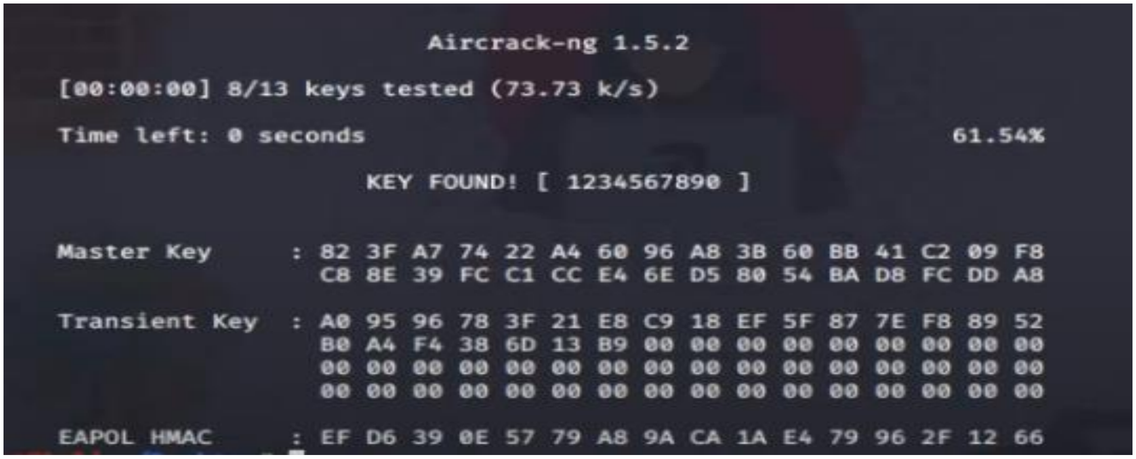
Aircrack-ng is a suite of tools that can be used to crack wireless security protocols, such as WEP and WPA. It can also be used to monitor wireless networks and capture packets. Aircrack-ng is a command-line tool, but there are also GUIs available. It is available for Linux, macOS, Windows, and FreeBSD. To use Aircrack-ng, you will need to have a wireless adapter that supports monitor mode. You can check if your adapter supports monitor mode by running the following command: If your adapter supports monitor mode, you will see a list of interfaces that can be used in monitor mode.



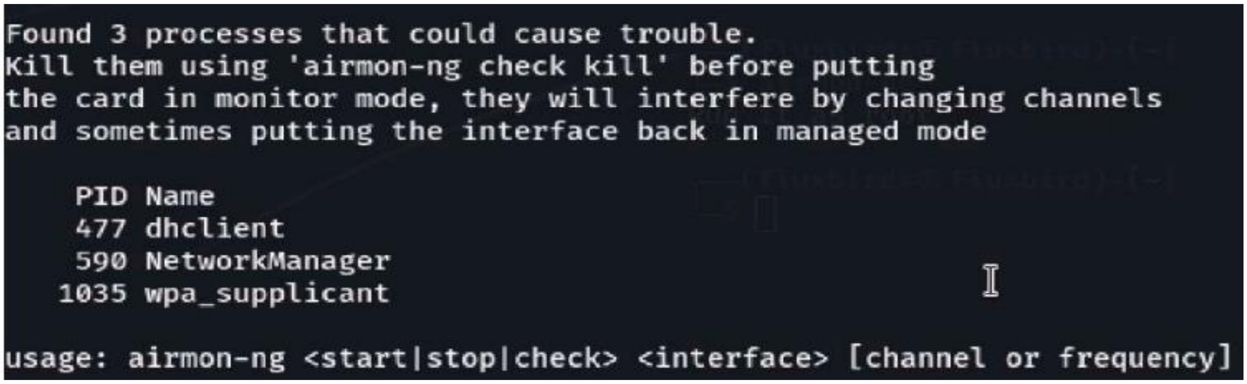
```
$ aircrack-ng --help

  Aircrack-ng 1.7  - (C) 2006-2022 Thomas d'Otreppe
  https://www.aircrack-ng.org

  usage: aircrack-ng [options] <input file(s)>

  Common options:

      -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
      -e <essid> : target selection: network identifier
      -b <bssid> : target selection: access point's MAC
      -p <nbcpu> : # of CPU to use  (default: all CPUs)
      -q         : enable quiet mode (no status output)
      -C <macs>  : merge the given APs to a virtual one
      -l <file>  : write key to file. Overwrites file.

  Static WEP cracking options:

      -c         : search alpha-numeric characters only
      -t         : search binary coded decimal chr only
      -h         : search the numeric key for Fritz!BOX
      -d <mask>  : use masking of the key (A1:XX:CF:YY)
      -m <maddr> : MAC address to filter usable packets
      -n <nbits> : WEP key length :  64/128/152/256/512
      -i <index> : WEP key index (1 to 4), default: any
      -f <fudge> : bruteforce fudge factor,  default: 2
      -k <korek> : disable one attack method  (1 to 17)
      -x or -x0  : disable bruteforce for last keybytes
      -x1        : last keybyte bruteforcing  (default)
      -x2        : enable last  2 keybytes bruteforcing
      -X         : disable  bruteforce   multithreading
      -y         : experimental  single bruteforce mode
      -K         : use only old KoreK attacks (pre-PTW)
      -s         : show the key in ASCII while cracking
      -M <num>   : specify maximum number of IVs to use
      -D         : WEP decloak, skips broken keystreams
      -P <num>   : PTW debug:  1: disable Klein, 2: PTW
```



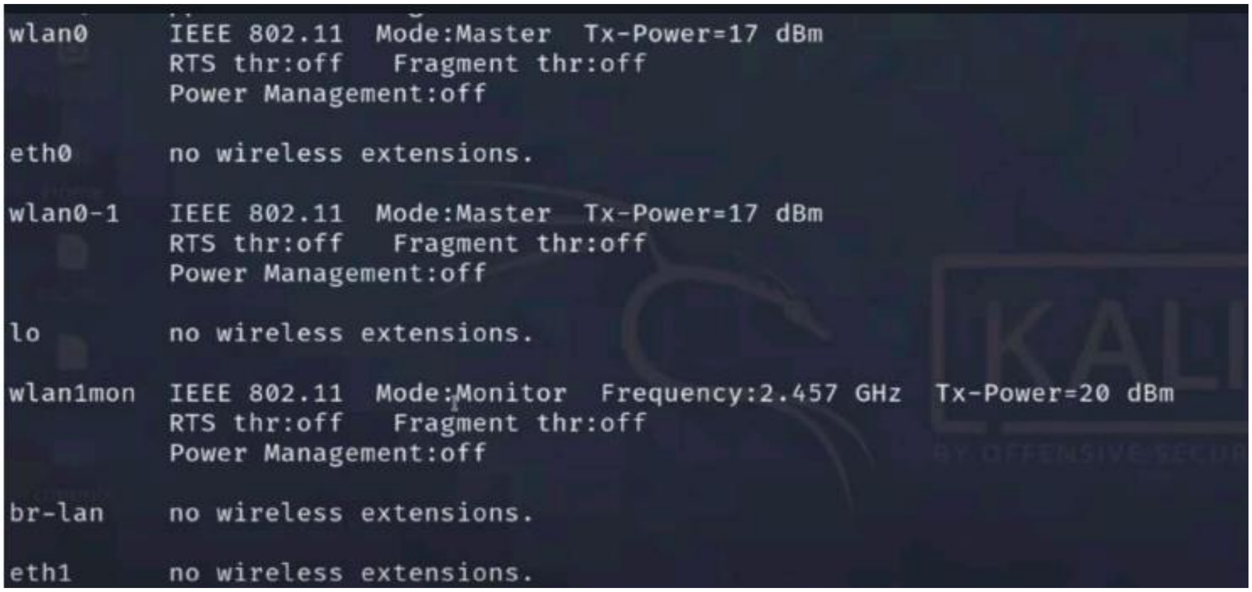
```
Aircrack-ng 1.5.2  - (C) 2006-2018 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: aircrack-ng [options] <input file(s)>

Common options:

    -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
    -e <essid> : target selection: network identifier
    -b <bssid> : target selection: access point's MAC
    -p <nbcpu> : # of CPU to use  (default: all CPUs)
    -q         : enable quiet mode (no status output)
    -C <macs>  : merge the given APs to a virtual one
    -l <file>  : write key to file. Overwrites file.

Static WEP cracking options:

    -c         : search alpha-numeric characters only
    -t         : search binary coded decimal chr only
    -h         : search the numeric key for Fritz!BOX
```



```
                          Aircrack-ng 1.5.2

 [00:00:00] 8/13 keys tested (73.73 k/s)

 Time left: 0 seconds                                       61.54%

                       KEY FOUND! [ 1234567890 ]


 Master Key     : 82 3F A7 74 22 A4 60 96 A8 3B 60 BB 41 C2 09 F8
                  C8 8E 39 FC C1 CC E4 6E D5 80 54 BA D8 FC DD A8

 Transient Key  : A0 95 96 78 3F 21 E8 C9 18 EF 5F 87 7E F8 89 52
                  B0 A4 F4 38 6D 13 B9 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 EAPOL HMAC     : EF D6 39 0E 57 79 A8 9A CA 1A E4 79 96 2F 12 66
```



```
Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    477 dhclient
    590 NetworkManager
   1035 wpa_supplicant

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```



```
wlan0     IEEE 802.11  Mode:Master  Tx-Power=17 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off

eth0      no wireless extensions.

wlan0-1   IEEE 802.11  Mode:Master  Tx-Power=17 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off

lo        no wireless extensions.

wlan1mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off

br-lan    no wireless extensions.

eth1      no wireless extensions.
```

7. WIRESHARK:

- Wireshark is a popular open-source packet analyzer that comes pre-installed on Kali Linux, a specialized Linux distribution for penetration testing and ethical hacking.

- It allows users to capture and analyze network traffic in real-time, making it a valuable tool for troubleshooting, security analysis, and monitoring network activity.
- Wireshark supports a wide range of network protocols, enabling users to dissect and inspect packets at various layers of the OSI model.

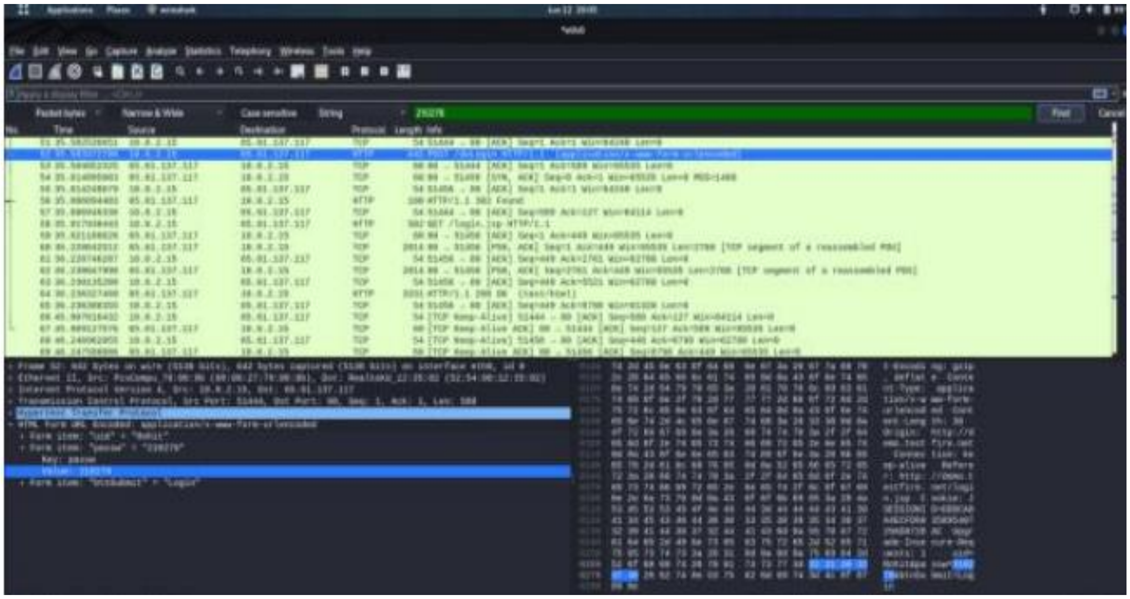
- With its user-friendly graphical interface, Wireshark simplifies the process of capturing and analyzing network packets, even for those without extensive networking knowledge.
- Network professionals use Wireshark to identify network issues, diagnose performance problems, and detect suspicious or malicious activities on a network.

- Wireshark offers advanced features like packet filtering, color coding, and protocol analysis, making it suitable for both beginners and experts in the field.
- It can capture traffic from a variety of sources, including Ethernet, Wi-Fi, and USB interfaces, allowing for comprehensive network analysis.

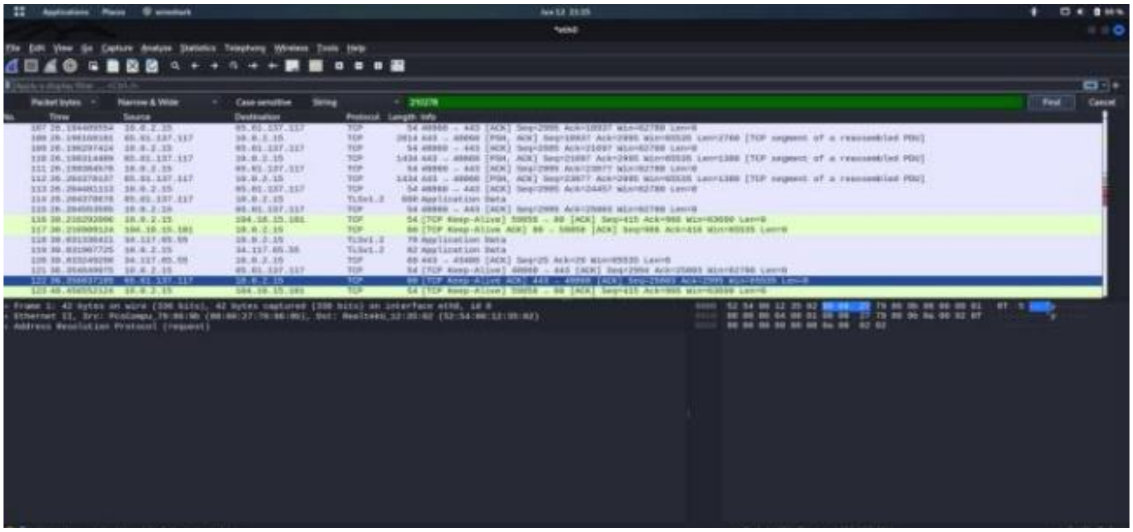
- Wireshark's "Follow TCP Stream" feature allows users to reconstruct and view the contents of a complete TCP session, aiding in the analysis of data exchanges.
- Kali Linux, with Wireshark, is a powerful combination for ethical hackers and penetration testers, as it helps identify vulnerabilities and assess network security.

- Continuous updates and a robust community support Wireshark, making it an essential tool for anyone working with network traffic analysis on Kali Linux or any other Linux distribution.

FOR HTTP PROTOCOL:



FOR HTTPS PROTOCOL:



So Wireshark works only for HTTP not for HTTPS protocol.

8. BURPSUITE:

Burp Suite is a comprehensive suite of tools for web applica6on security tes6ng. It can be used to iden6fy and exploit vulnerabili6es in web applica6ons, as well as to improve the security of web applica6ons.

Burp Suite consists of several different tools, including:

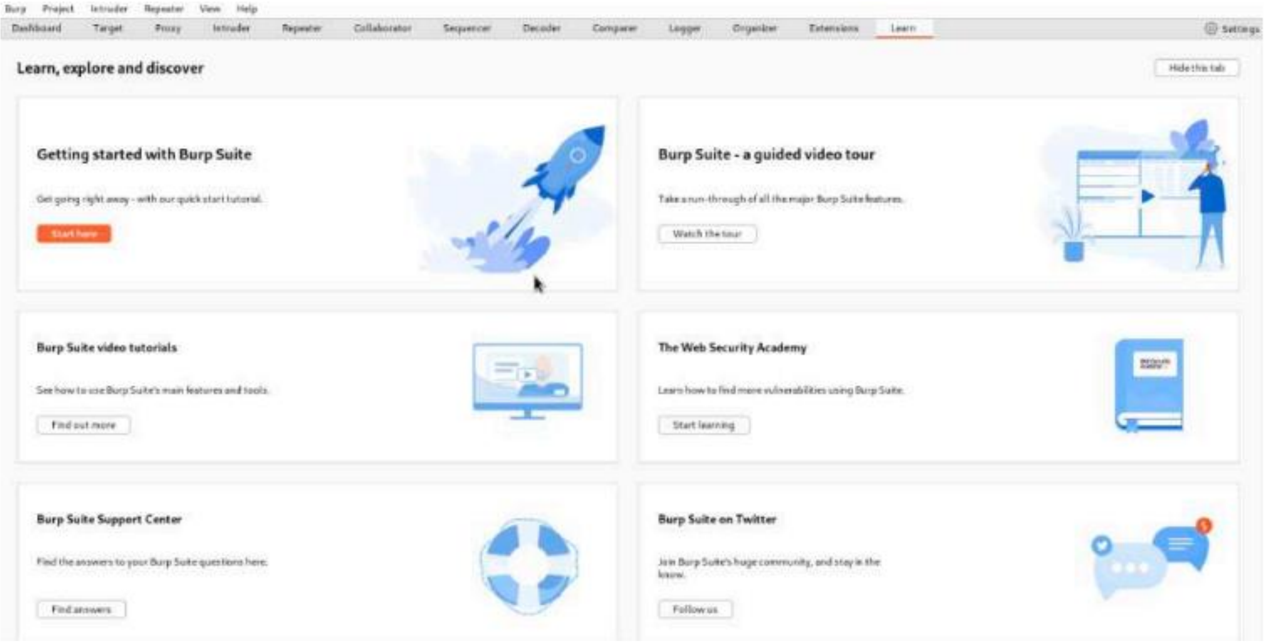
- **Proxy: The proxy intercepts all traffic between the user's browser and the web applica6on. This allows Burp Suite to examine the traffic and iden6fy poten6al vulnerabili6es.**

- **Scanner: The scanner automa6cally scans web applica6ons for known vulnerabili6es.**

- **Intruder: The intruder tool can be used to fuzz web applica6ons and to iden6fy vulnerabili6es that are not detected by the scanner.**

- **Repeater: The repeater tool allows the user to manually send requests to the web applica6on and to see the responses. This can be used to debug web applica6ons and to identify vulnerabilities.**

- **Sequencer: The sequencer tool can be used to analyze the sequence of requests and responses in a web applica6on. This can be used to identify vulnerabili6es that are not detected by the other tools.**
- **Spider: The spider tool can be used to crawl a web applica6on and to iden6fy all the pages and resources that are available. This can be used to find vulnerabili6es that are not easily accessible.**
- **Extender: The extender allows the user to add custom func6onality to Burp Suite. This can be used to extend the capabili6es of Burp Suite and to automate Tasks**



Learn, explore and discover

Getting started with Burp Suite

Get going right away - with our quick start tutorial.

Burp Suite - a guided video tour

Take a run-through of all the major Burp Suite features.

Burp Suite video tutorials

See how to use Burp Suite's main features and tools.

The Web Security Academy

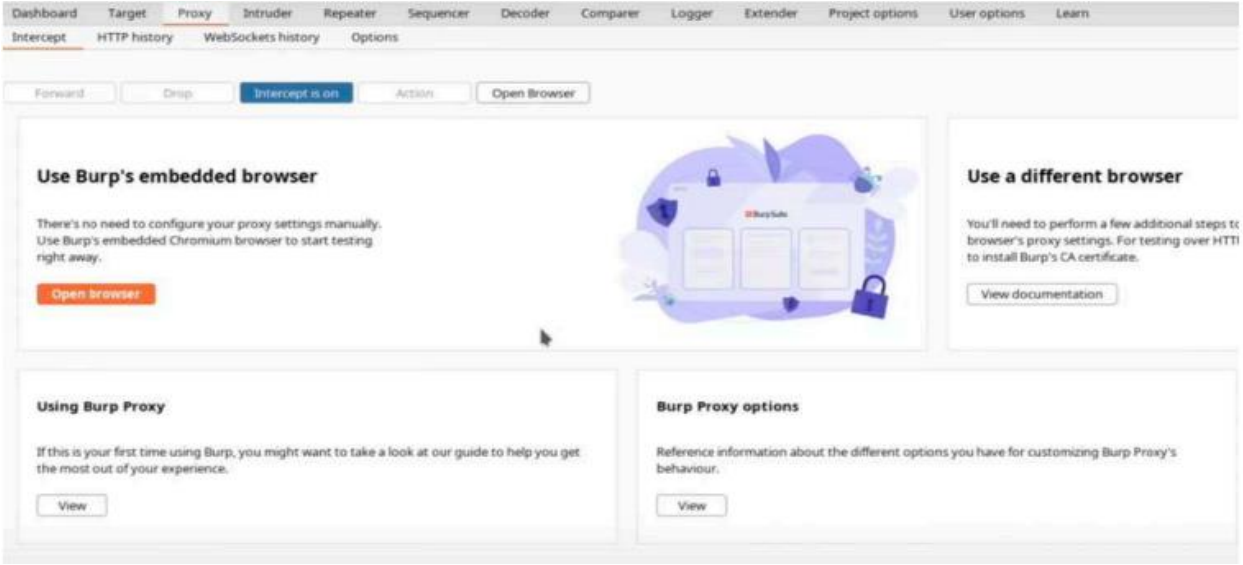
Learn how to find more vulnerabilities using Burp Suite.

Burp Suite Support Center

Find the answers to your Burp Suite questions here.

Burp Suite on Twitter

Join Burp Suite's huge community, and stay in the know.



Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Use a different browser

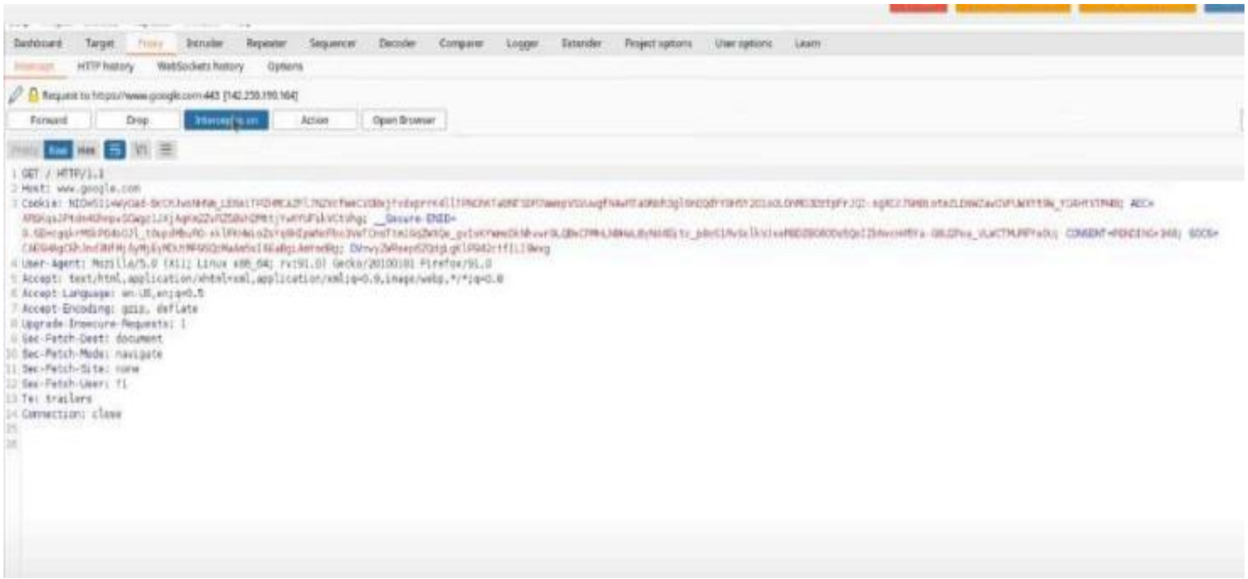
You'll need to perform a few additional steps to browser's proxy settings. For testing over HTTI to install Burp's CA certificate.

Using Burp Proxy

If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

Burp Proxy options

Reference information about the different options you have for customizing Burp Proxy's behaviour.



Request to https://www.google.com:443 [142.250.190.164]

```
GET / HTTP/1.1
Host: www.google.com
Cookie: NID=511=[illegible] __Secure-ENID=
[illegible]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

9. Metaspolit:

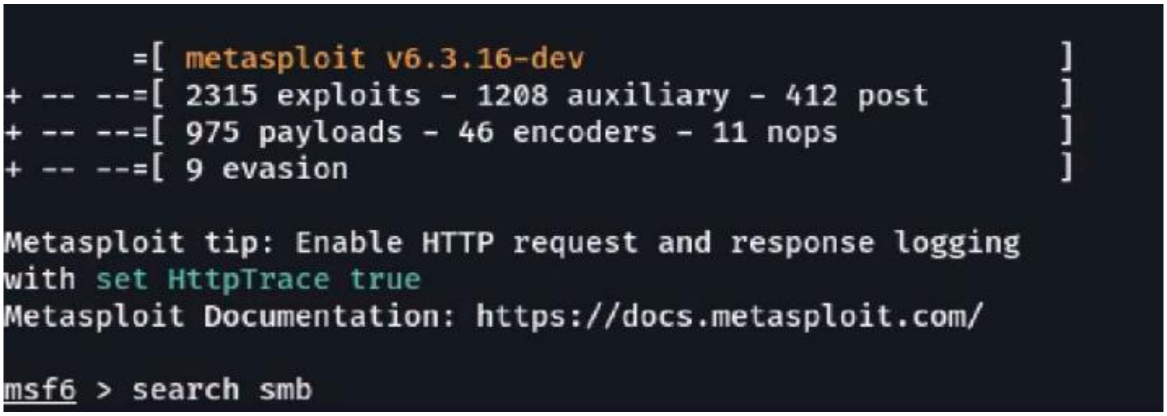
Metasploit is a penetration testing framework that is used to find and exploit vulnerabili6es in computer systems and networks. It is a powerful tool that can be used by security professionals to test the security of their systems and by attackers to exploit vulnerabilities.

Metasploit has a large library of exploits that can be used to exploit known vulnerabili6es. It also has a variety of tools that can be used to automate tasks, such as scanning for vulnerabili6es and genera6ng reports.

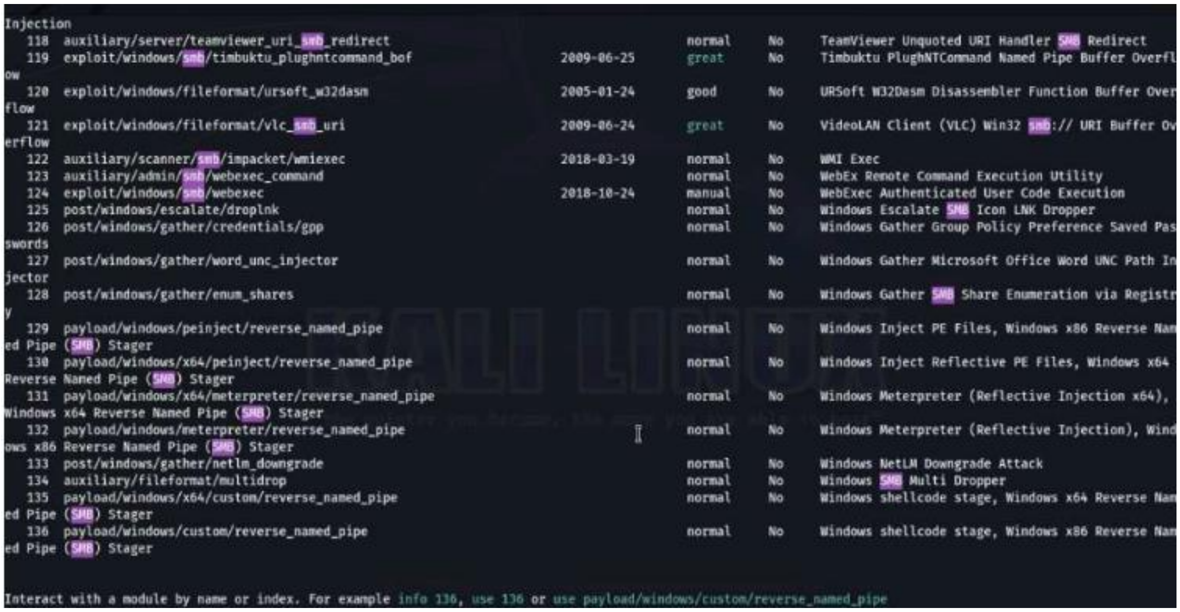
- Penetra6on tes6ng: Metasploit can be used by penetra6on testers to iden6fy and exploit vulnerabili6es in computer systems and applica6ons. This helps to improve the security of the systems and applica6ons.
- Vulnerability scanning: Metasploit can be used to scan networks and systems

for vulnerabili6es. This can help organiza6ons to iden6fy and fix vulnerabilities before they can be exploited by attackers.

- Security research: Metasploit can be used by security researchers to study vulnerabili6es and to develop new ways to exploit them. This helps to improve the understanding of vulnerabili6es and how to prevent them.
- Cyberwarfare: Metasploit can be used by governments and militaries to exploit vulnerabili6es in enemy systems. This can be used to gain intelligence or to disrupt enemy opera6ons.



```
       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search smb
```

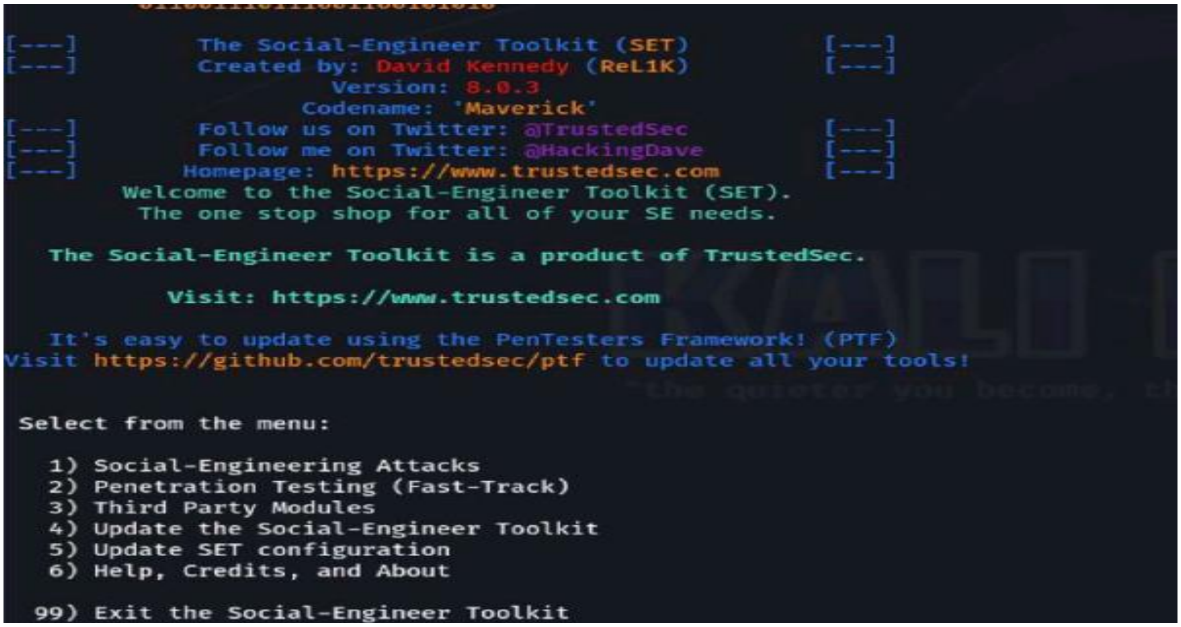


```
Injection
   118  auxiliary/server/teamviewer_uri_smb_redirect                                  normal   No     TeamViewer Unquoted URI Handler SMB Redirect
   119  exploit/windows/smb/timbuktu_plughntcommand_bof            2009-06-25         great    No     Timbuktu PlughNTCommand Named Pipe Buffer Overfl
ow
   120  exploit/windows/fileformat/ursoft_w32dasm                  2005-01-24         good     No     URSoft W32Dasm Disassembler Function Buffer Over
flow
   121  exploit/windows/fileformat/vlc_smb_uri                     2009-06-24         great    No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Ov
erflow
   122  auxiliary/scanner/smb/impacket/wmiexec                     2018-03-19         normal   No     WMI Exec
   123  auxiliary/admin/smb/webexec_command                                           normal   No     WebEx Remote Command Execution Utility
   124  exploit/windows/smb/webexec                                2018-10-24         manual   No     WebExec Authenticated User Code Execution
   125  post/windows/escalate/droplnk                                                 normal   No     Windows Escalate SMB Icon LNK Dropper
   126  post/windows/gather/credentials/gpp                                           normal   No     Windows Gather Group Policy Preference Saved Pas
swords
   127  post/windows/gather/word_unc_injector                                         normal   No     Windows Gather Microsoft Office Word UNC Path In
jector
   128  post/windows/gather/enum_shares                                               normal   No     Windows Gather SMB Share Enumeration via Registr
y
   129  payload/windows/peinject/reverse_named_pipe                                   normal   No     Windows Inject PE Files, Windows x86 Reverse Nam
ed Pipe (SMB) Stager
   130  payload/windows/x64/peinject/reverse_named_pipe                               normal   No     Windows Inject Reflective PE Files, Windows x64
Reverse Named Pipe (SMB) Stager
   131  payload/windows/x64/meterpreter/reverse_named_pipe                            normal   No     Windows Meterpreter (Reflective Injection x64),
Windows x64 Reverse Named Pipe (SMB) Stager
   132  payload/windows/meterpreter/reverse_named_pipe                                normal   No     Windows Meterpreter (Reflective Injection), Wind
ows x86 Reverse Named Pipe (SMB) Stager
   133  post/windows/gather/netlm_downgrade                                           normal   No     Windows NetLM Downgrade Attack
   134  auxiliary/fileformat/multidrop                                                normal   No     Windows SMB Multi Dropper
   135  payload/windows/x64/custom/reverse_named_pipe                                 normal   No     Windows shellcode stage, Windows x64 Reverse Nam
ed Pipe (SMB) Stager
   136  payload/windows/custom/reverse_named_pipe                                     normal   No     Windows shellcode stage, Windows x86 Reverse Nam
ed Pipe (SMB) Stager


Interact with a module by name or index. For example info 136, use 136 or use payload/windows/custom/reverse_named_pipe
```

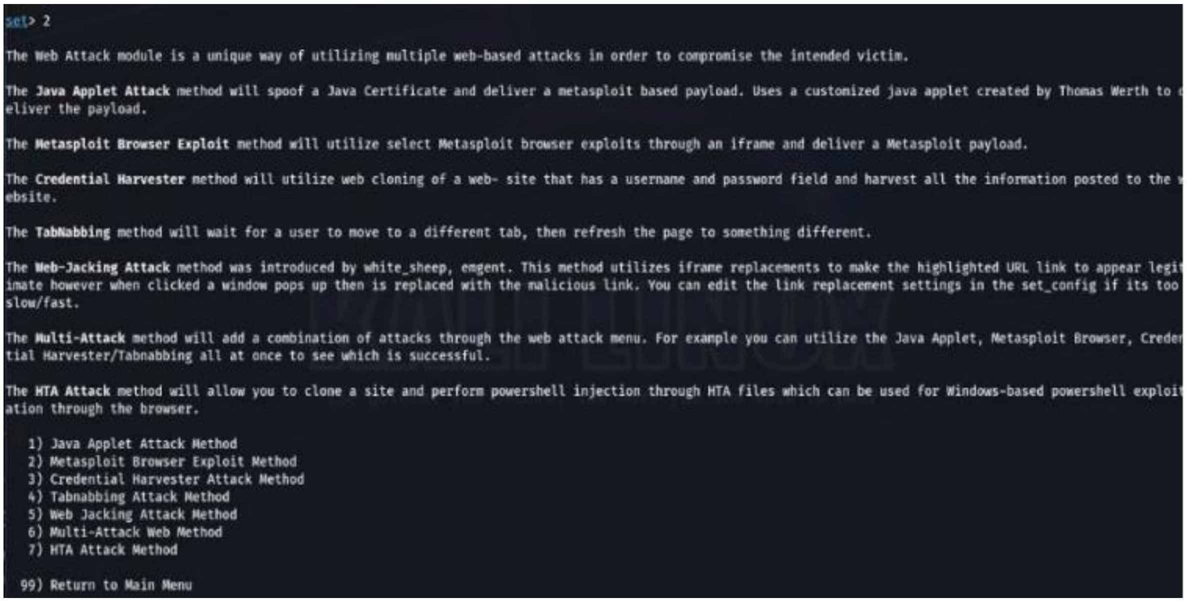
10. SETOOLKIT:

Setoolkit, short for the Social Engineering Toolkit, is a potent and versatile tool that can be found in Kali Linux, a popular distribution for penetration testing and ethical hacking. It has gained notoriety for its effectiveness in simulating and testing social engineering attacks, making it an essential component of any ethical hacker's toolkit.

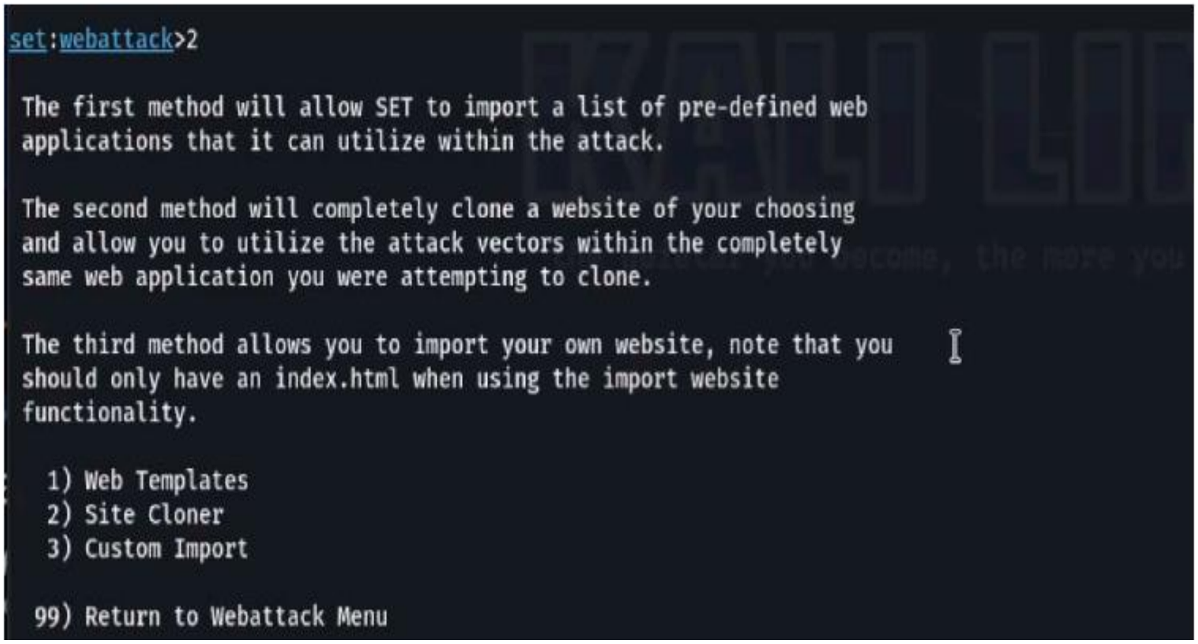
Setoolkit is designed to help cybersecurity professionals and penetration testers assess and strengthen the security of systems and networks by exploiting human vulnerabilities rather than technical weaknesses.



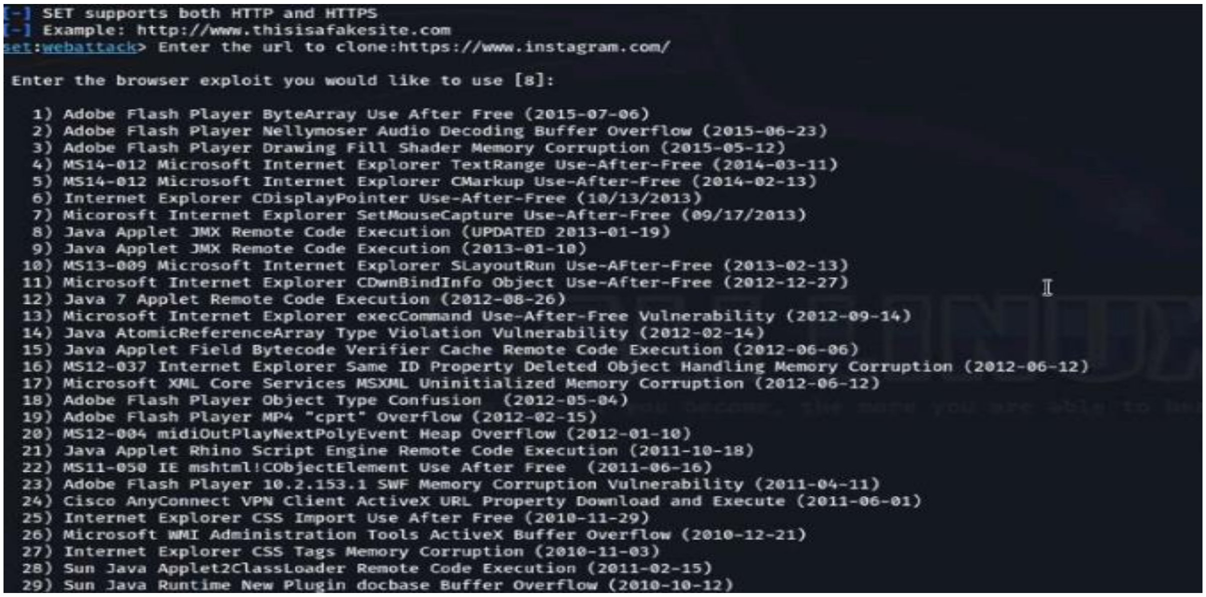
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave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

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

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


 Select from the menu:

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

  99) Exit the Social-Engineer Toolkit
```



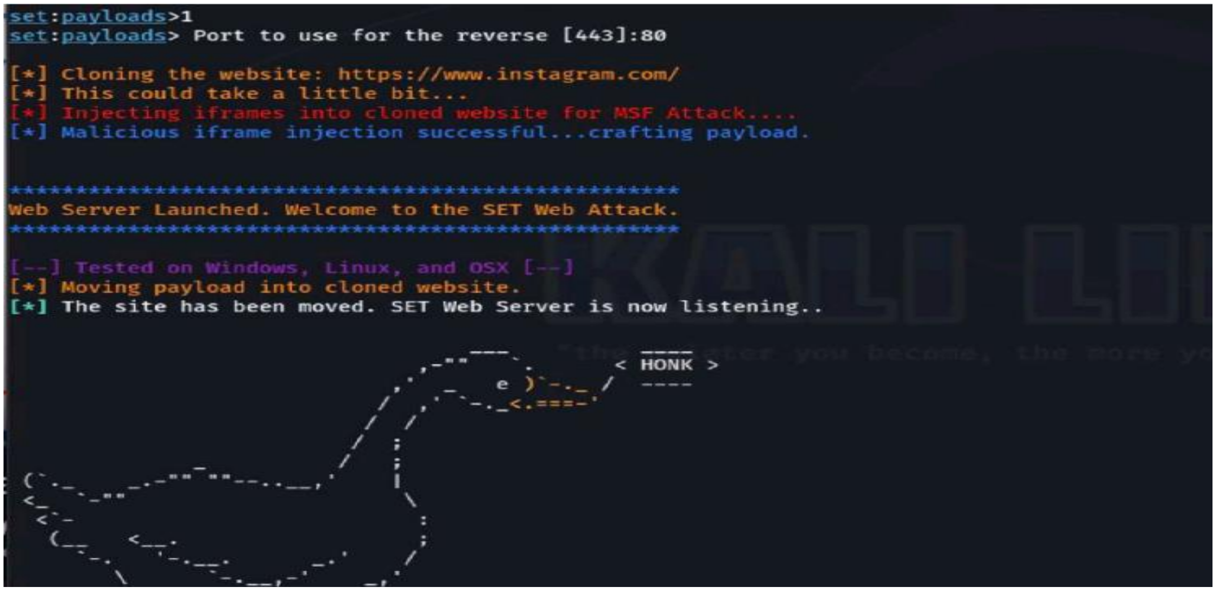
```
set> 2

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

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

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

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the
ebsite.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legit
imate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too
slow/fast.

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

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploit
ation 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>2

 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 supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.instagram.com/

 Enter the browser exploit you would like to use [8]:

   1) Adobe Flash Player ByteArray Use After Free (2015-07-06)
   2) Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow (2015-06-23)
   3) Adobe Flash Player Drawing Fill Shader Memory Corruption (2015-05-12)
   4) MS14-012 Microsoft Internet Explorer TextRange Use-After-Free (2014-03-11)
   5) MS14-012 Microsoft Internet Explorer CMarkup Use-After-Free (2014-02-13)
   6) Internet Explorer CDisplayPointer Use-After-Free (10/13/2013)
   7) Micorosft Internet Explorer SetMouseCapture Use-After-Free (09/17/2013)
   8) Java Applet JMX Remote Code Execution (UPDATED 2013-01-19)
   9) Java Applet JMX Remote Code Execution (2013-01-10)
  10) MS13-009 Microsoft Internet Explorer SLayoutRun Use-AFter-Free (2013-02-13)
  11) Microsoft Internet Explorer CDwnBindInfo Object Use-After-Free (2012-12-27)
  12) Java 7 Applet Remote Code Execution (2012-08-26)
  13) Microsoft Internet Explorer execCommand Use-After-Free Vulnerability (2012-09-14)
  14) Java AtomicReferenceArray Type Violation Vulnerability (2012-02-14)
  15) Java Applet Field Bytecode Verifier Cache Remote Code Execution (2012-06-06)
  16) MS12-037 Internet Explorer Same ID Property Deleted Object Handling Memory Corruption (2012-06-12)
  17) Microsoft XML Core Services MSXML Uninitialized Memory Corruption (2012-06-12)
  18) Adobe Flash Player Object Type Confusion  (2012-05-04)
  19) Adobe Flash Player MP4 "cprt" Overflow (2012-02-15)
  20) MS12-004 midiOutPlayNextPolyEvent Heap Overflow (2012-01-10)
  21) Java Applet Rhino Script Engine Remote Code Execution (2011-10-18)
  22) MS11-050 IE mshtml!CObjectElement Use After Free  (2011-06-16)
  23) Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability (2011-04-11)
  24) Cisco AnyConnect VPN Client ActiveX URL Property Download and Execute (2011-06-01)
  25) Internet Explorer CSS Import Use After Free (2010-11-29)
  26) Microsoft WMI Administration Tools ActiveX Buffer Overflow (2010-12-21)
  27) Internet Explorer CSS Tags Memory Corruption (2010-11-03)
  28) Sun Java Applet2ClassLoader Remote Code Execution (2011-02-15)
  29) Sun Java Runtime New Plugin docbase Buffer Overflow (2010-10-12)
```



```
set:payloads>1
set:payloads> Port to use for the reverse [443]:80

[*] Cloning the website: https://www.instagram.com/
[*] This could take a little bit...
[*] Injecting iframes into cloned website for MSF Attack....
[*] Malicious iframe injection successful...crafting payload.


***************************************************
Web Server Launched. Welcome to the SET Web Attack.
***************************************************

[--] Tested on Windows, Linux, and OSX [--]
[*] Moving payload into cloned website.
[*] The site has been moved. SET Web Server is now listening..
```