Name: Shivani Narayan L

Regno: 21BLC1119

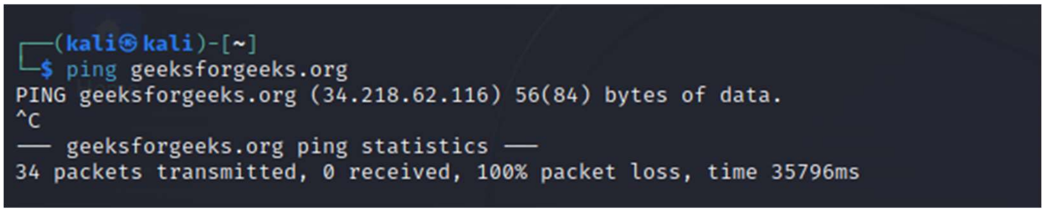
Week 2 Assignment: Kali Linux Tools

1. Information Gathering:

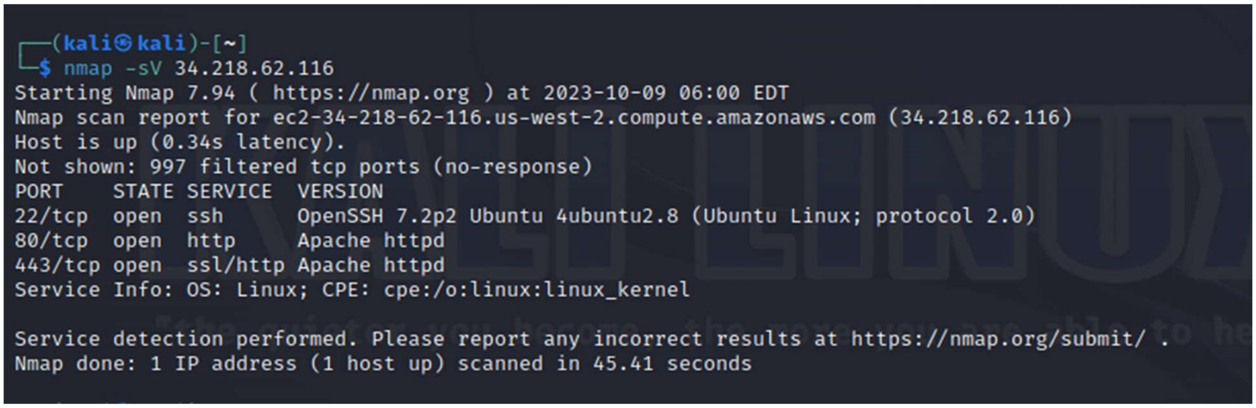
Information gathering in Kali Linux involves the process of collecting and analysing data about a target or a network to understand its structure, vulnerabilities, and potential attack surfaces. This phase is crucial for security testing, penetration testing, and vulnerability assessments.

Nmap:

Nmap, an open-source network scanning tool, is utilized for reconnaissance and analysis of networks. Its purpose is to uncover hosts, ports, and services, including their respective versions within a network. By sending packets to hosts and analysing their responses, Nmap gathers crucial information. This versatile tool is effective for tasks such as identifying hosts, detecting operating systems, and scanning for accessible ports. As a prominent reconnaissance tool, Nmap plays a vital role in network analysis.



```
┌──(kali㉿kali)-[~]
└─$ ping geeksforgeeks.org
PING geeksforgeeks.org (34.218.62.116) 56(84) bytes of data.
^C
── geeksforgeeks.org ping statistics ──
34 packets transmitted, 0 received, 100% packet loss, time 35796ms
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 34.218.62.116
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 06:00 EDT
Nmap scan report for ec2-34-218-62-116.us-west-2.compute.amazonaws.com (34.218.62.116)
Host is up (0.34s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http     Apache httpd
443/tcp open  ssl/http Apache httpd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.41 seconds
```

Recon-ng:

Recon-ng is a powerful open-source web reconnaissance tool available in Kali Linux. Designed for Open-Source Intelligence (OSINT), it excels at gathering information about target domains. Its interface, reminiscent of Metasploit, is user-friendly, operating through a command-line interface on Kali Linux. Recon-ng, written in Python, provides a robust environment for conducting web-based reconnaissance. It offers numerous modules, database interaction, built-in functions, interactive help, and command completion, making it an invaluable tool for information gathering and analysis during security testing and assessments.

Ammas:

Amass is a robust open-source subdomain enumeration tool available in Kali Linux. It's designed for discovering subdomains associated with a target domain. By leveraging various sources like search engines, web archives, and DNS records, Amass efficiently gathers a comprehensive list of subdomains.

theHarvester:

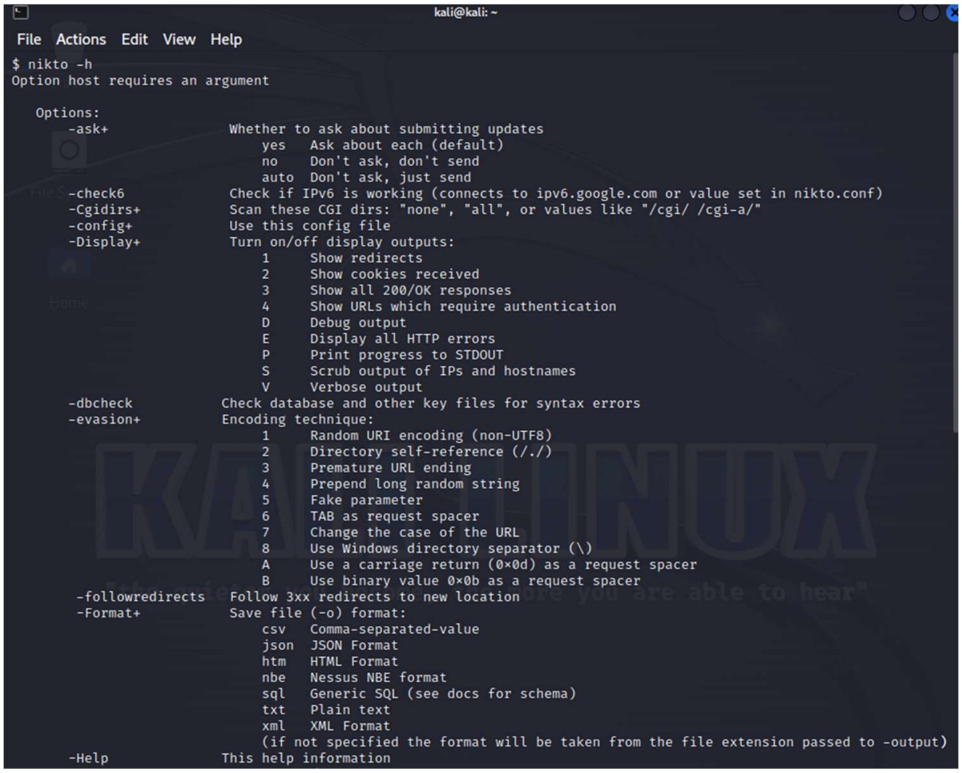
theHarvester is a popular OSINT (Open Source Intelligence) tool available in Kali Linux. It's utilized for collecting information such as email addresses, subdomains, virtual hosts, and more from public sources. The tool supports multiple search engines, PGP key servers, and public SHODAN databases, allowing users to perform reconnaissance and gather critical data about a target.

2. Vulnerability Analysis:

Vulnerability analysis is a critical hacking phase following information gathering, crucial in application design. It involves identifying vulnerabilities, the program loopholes hackers exploit for attacks. These vulnerabilities serve as entry points for cyber-attacks. Kali Linux, equipped with 300+ tools, offers a plethora of options for vulnerability analysis.

Nikto:

Nikto is an open-source Perl-based tool that scans web servers to uncover exploitable vulnerabilities that could compromise the server. It checks over 1200 servers for outdated versions and identifies issues with specific version details for more than 200 servers. Key features include SSL support, subdomain detection, HTTP Proxy compatibility, outdated component reporting, and username guessing.



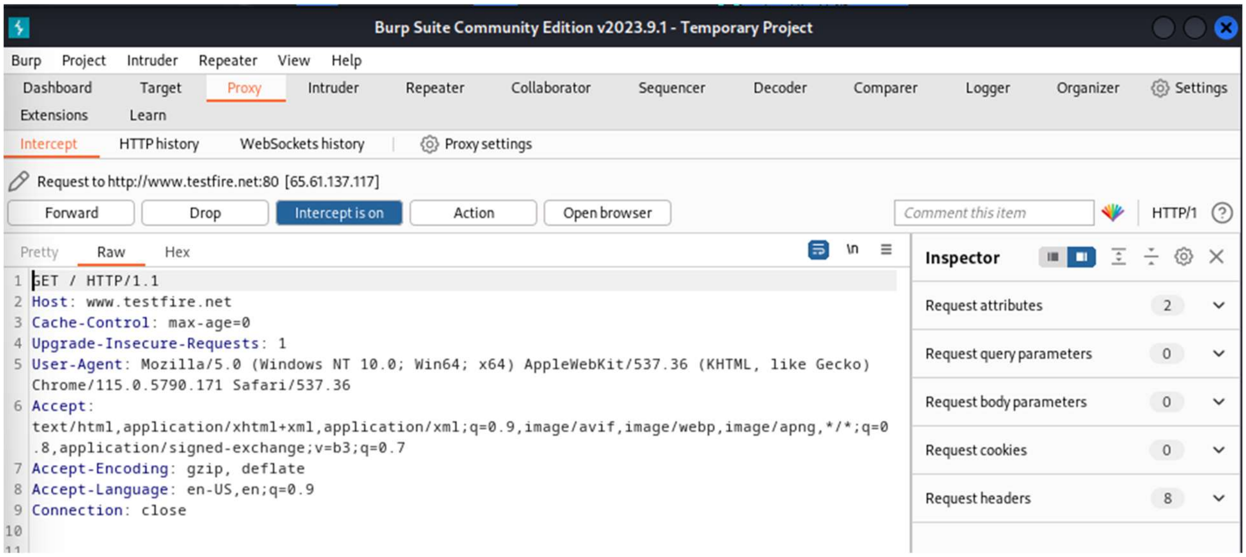
```
$ nikto -h
Option host requires an argument

   Options:
       -ask+               Whether to ask about submitting updates
                               yes   Ask about each (default)
                               no    Don't ask, don't send
                               auto  Don't ask, just send
       -check6             Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
       -Cgidirs+           Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
       -config+            Use this config file
       -Display+           Turn on/off display outputs:
                               1     Show redirects
                               2     Show cookies received
                               3     Show all 200/OK responses
                               4     Show URLs which require authentication
                               D     Debug output
                               E     Display all HTTP errors
                               P     Print progress to STDOUT
                               S     Scrub output of IPs and hostnames
                               V     Verbose output
       -dbcheck           Check database and other key files for syntax errors
       -evasion+          Encoding technique:
                               1     Random URI encoding (non-UTF8)
                               2     Directory self-reference (/./)
                               3     Premature URL ending
                               4     Prepend long random string
                               5     Fake parameter
                               6     TAB as request spacer
                               7     Change the case of the URL
                               8     Use Windows directory separator (\)
                               A     Use a carriage return (0×0d) as a request spacer
                               B     Use binary value 0×0b as a request spacer
        -followredirects   Follow 3xx redirects to new location
        -Format+           Save file (-o) format:
                               csv   Comma-separated-value
                               json  JSON Format
                               htm   HTML Format
                               nbe   Nessus NBE format
                               sql   Generic SQL (see docs for schema)
                               txt   Plain text
                               xml   XML Format
                               (if not specified the format will be taken from the file extension passed to -output)
       -Help              This help information
```

3. Web Application Analysis:

Kali Linux comes preloaded with numerous tools for web application analysis. These tools cater to different aspects of web application analysis, including vulnerability scanning, directory enumeration, SQL injection testing, cross-site scripting detection, and more.

Burp Suite:

Burp Suite is a widely used web application security testing tool, functioning as a proxy for browser requests. It enables modifying requests, making it valuable for testing web vulnerabilities like XSS and SQLi. Kali Linux includes the free Burp Suite Community Edition, but there's also a paid Professional edition offering additional features for comprehensive web security testing.



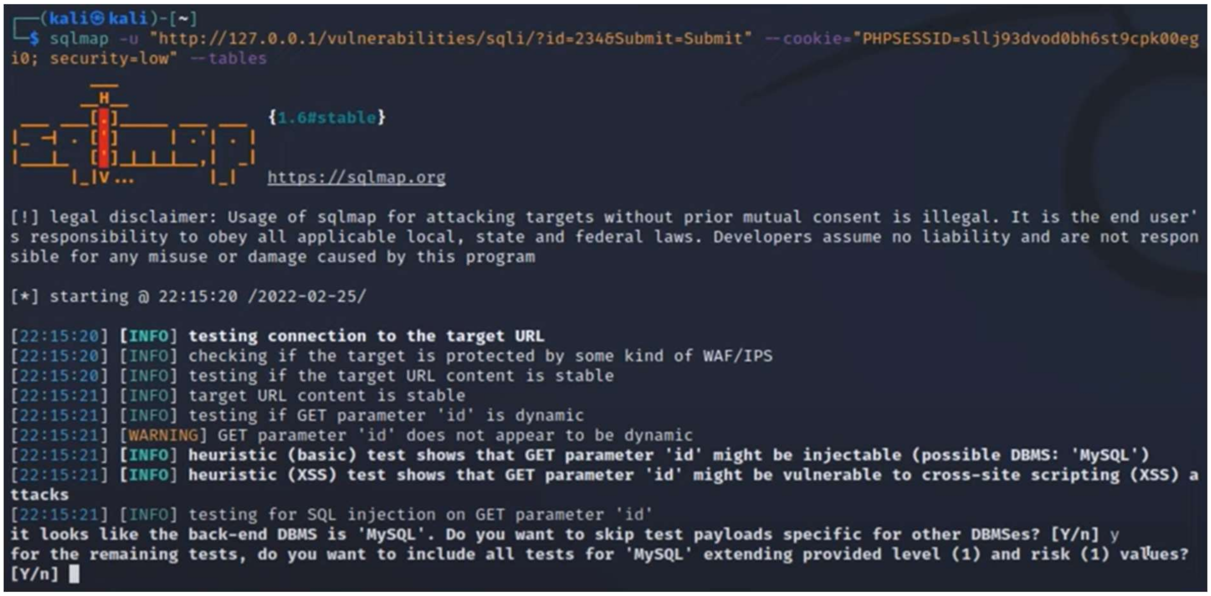
```
GET / HTTP/1.1
Host: www.testfire.net
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/115.0.5790.171 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

4. Database Assessment:

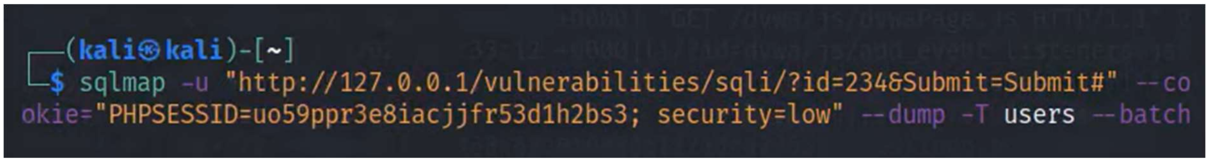
Kali Linux provides several database assessment tools to help test, analyse, and secure databases.

SqlMap:

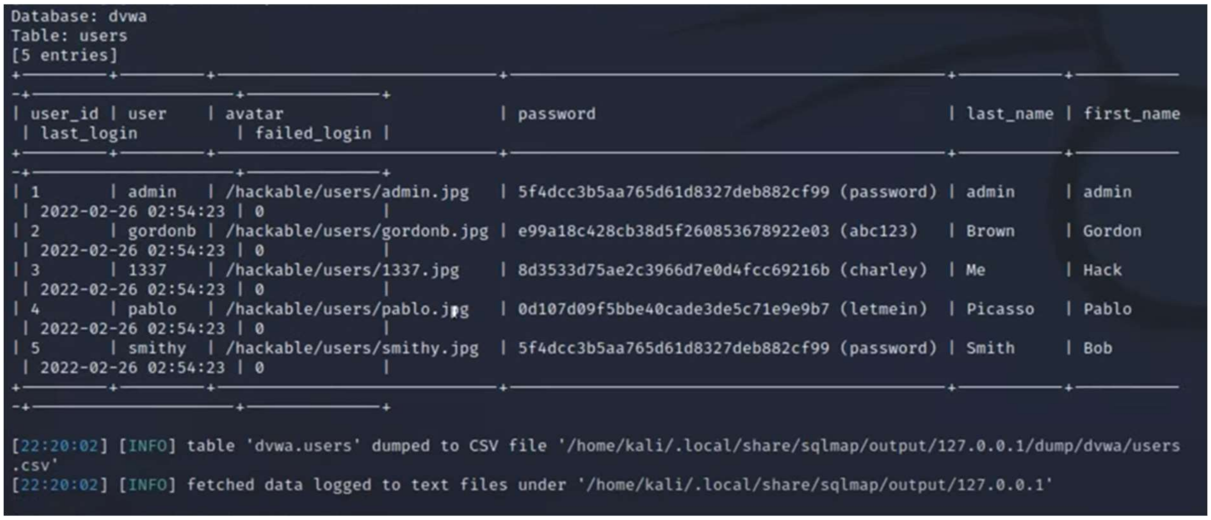
Sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from 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.



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://127.0.0.1/vulnerabilities/sqli/?id=234&Submit=Submit" --cookie="PHPSESSID=sllj93dvod0bh6st9cpk00eg
i0; security=low" --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   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 respon
sible for any misuse or damage caused by this program

[*] starting @ 22:15:20 /2022-02-25/

[22:15:20] [INFO] testing connection to the target URL
[22:15:20] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:15:20] [INFO] testing if the target URL content is stable
[22:15:21] [INFO] target URL content is stable
[22:15:21] [INFO] testing if GET parameter 'id' is dynamic
[22:15:21] [WARNING] GET parameter 'id' does not appear to be dynamic
[22:15:21] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[22:15:21] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) a
ttacks
[22:15:21] [INFO] testing for SQL injection on GET parameter 'id'
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] █
```



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://127.0.0.1/vulnerabilities/sqli/?id=234&Submit=Submit#" --co
okie="PHPSESSID=uo59ppr3e8iacjjfr53d1h2bs3; security=low" --dump -T users --batch
```



```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------+---------------------------------------------+-----------+-----------
-+---------------------+--------------+
| user_id | user    | avatar                      | password                                    | last_name | first_name
 | last_login          | failed_login |
+---------+---------+-----------------------------+---------------------------------------------+-----------+-----------
-+---------------------+--------------+
| 1       | admin   | /hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin
 | 2022-02-26 02:54:23 | 0            |
| 2       | gordonb | /hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon
 | 2022-02-26 02:54:23 | 0            |
| 3       | 1337    | /hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack
 | 2022-02-26 02:54:23 | 0            |
| 4       | pablo   | /hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo
 | 2022-02-26 02:54:23 | 0            |
| 5       | smithy  | /hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob
 | 2022-02-26 02:54:23 | 0            |
+---------+---------+-----------------------------+---------------------------------------------+-----------+-----------
-+---------------------+--------------+

[22:20:02] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/127.0.0.1/dump/dvwa/users
.csv'
[22:20:02] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/127.0.0.1'
```

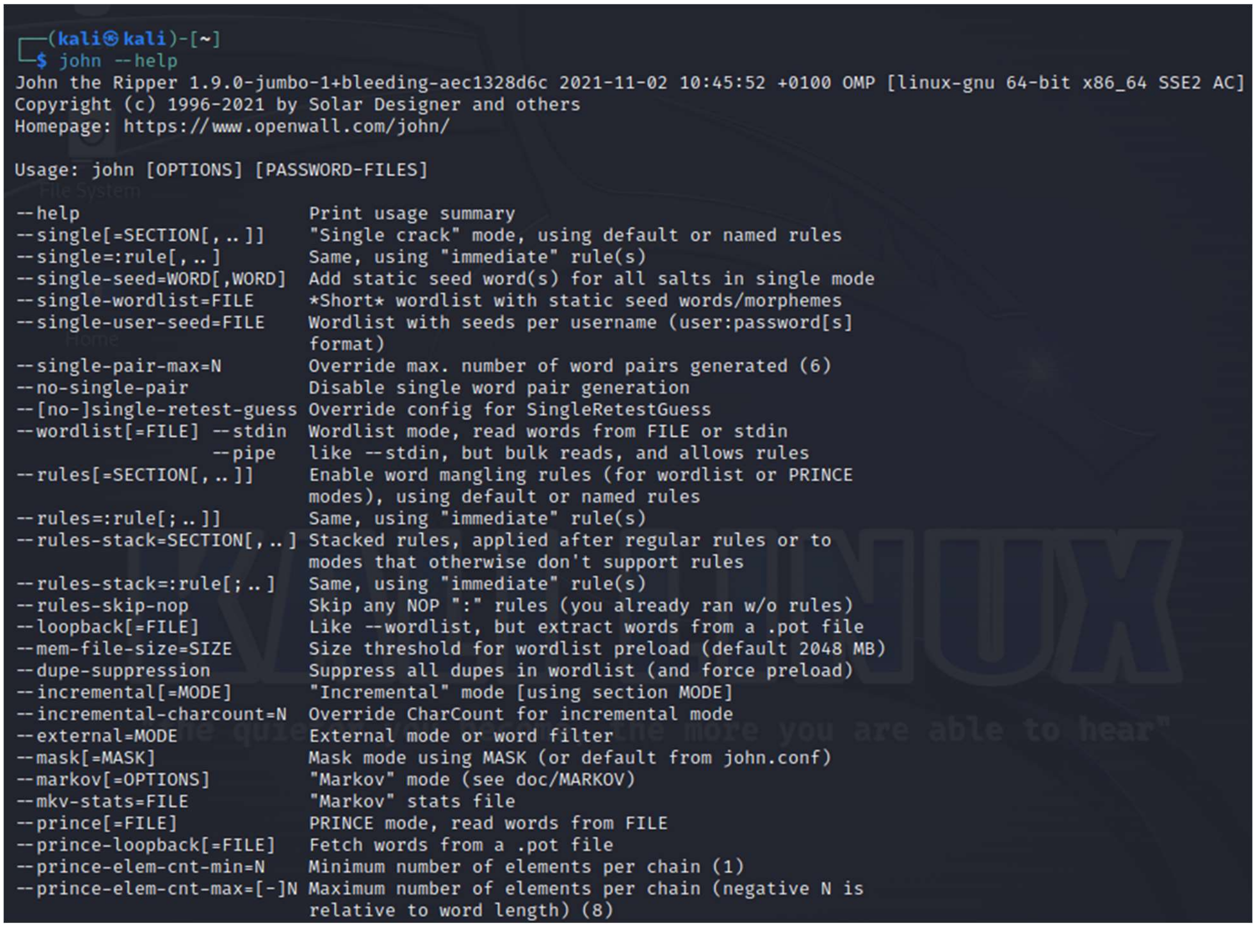
5. Password Attacks:

In Kali Linux, you can find various password attack tools that are designed to test and evaluate the security of passwords, hash algorithms, and authentication mechanisms.

John the Ripper:

John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired.

The rate at which John the Ripper will guess the password is going to depends on the password's strength and the offered wordlist. JTR will keep attempting to break the password continuously unless there is a termination command.



```
┌──(kali㉿kali)-[~]
└─$ john --help
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 SSE2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

--help                     Print usage summary
--single[=SECTION[,..]]    "Single crack" mode, using default or named rules
--single=:rule[,..]        Same, using "immediate" rule(s)
--single-seed=WORD[,WORD]  Add static seed word(s) for all salts in single mode
--single-wordlist=FILE     *Short* wordlist with static seed words/morphemes
--single-user-seed=FILE    Wordlist with seeds per username (user:password[s]
                           format)
--single-pair-max=N        Override max. number of word pairs generated (6)
--no-single-pair           Disable single word pair generation
--[no-]single-retest-guess Override config for SingleRetestGuess
--wordlist[=FILE] --stdin  Wordlist mode, read words from FILE or stdin
                   --pipe  like --stdin, but bulk reads, and allows rules
--rules[=SECTION[,..]]     Enable word mangling rules (for wordlist or PRINCE
                           modes), using default or named rules
--rules=:rule[;..]]        Same, using "immediate" rule(s)
--rules-stack=SECTION[,..] Stacked rules, applied after regular rules or to
                           modes that otherwise don't support rules
--rules-stack=:rule[;..]   Same, using "immediate" rule(s)
--rules-skip-nop           Skip any NOP ":" rules (you already ran w/o rules)
--loopback[=FILE]          Like --wordlist, but extract words from a .pot file
--mem-file-size=SIZE       Size threshold for wordlist preload (default 2048 MB)
--dupe-suppression         Suppress all dupes in wordlist (and force preload)
--incremental[=MODE]       "Incremental" mode [using section MODE]
--incremental-charcount=N  Override CharCount for incremental mode
--external=MODE            External mode or word filter
--mask[=MASK]              Mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]         "Markov" mode (see doc/MARKOV)
--mkv-stats=FILE           "Markov" stats file
--prince[=FILE]            PRINCE mode, read words from FILE
--prince-loopback[=FILE]   Fetch words from a .pot file
--prince-elem-cnt-min=N    Minimum number of elements per chain (1)
--prince-elem-cnt-max=[-]N Maximum number of elements per chain (negative N is
                           relative to word length) (8)
```

Hydra:

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

6. Wireless Attacks:

These tools are employed for exploiting wireless networks, enabling activities such as breaking wireless passwords, injecting harmful code into wireless data, and potentially gaining control over wireless access points. Key tools for wireless attacks in Kali Linux encompass Aircrack-ng, Kismet, and Reaver, recognized for their popularity and effectiveness in this domain.

7. Reverse Engineering:

Reverse engineering tools in Kali Linux are software applications aimed at dissecting and analyzing existing programs or software. Their primary purpose is to uncover the inner workings, vulnerabilities, and functionalities of the software. This process helps identify weaknesses, potential security flaws, and areas for improvement. Notable tools like Ghidra, IDA Pro, and Radare2, available in Kali Linux, are highly effective for reverse engineering tasks, making them essential for software analysis and security enhancement.

8. Exploitation Tools:

Exploitation tools in Kali Linux are specialized software designed to take advantage of vulnerabilities within a target system or network. They enable unauthorized access, the installation of malware, or disruption of normal operations. Notable tools like Metasploit Framework, BeEF, and SET are widely used in Kali Linux for carrying out these actions, making them crucial assets for penetration testing and security assessments.

9. Sniffing & Spoofing:

Sniffing and spoofing tools in Kali Linux are software utilities used to intercept and manipulate network traffic for various purposes. Sniffing tools capture and analyse data packets passing through a network, allowing users to inspect the content and extract valuable information. Spoofing tools, on the other hand, manipulate network data to deceive or impersonate devices, thus altering the traffic's source or destination. Kali Linux provides a range of powerful sniffing and spoofing tools, such as Wireshark, Ettercap, and Scapy, assisting in comprehensive network analysis and testing

10. Post Exploitation:

Post-exploitation tools in Kali Linux are software utilities used after an initial breach or successful infiltration of a target system or network. These tools assist in maintaining control, gathering further intelligence, and performing malicious actions within the compromised environment. They are crucial for activities like privilege escalation, lateral movement, data exfiltration, and establishing persistent access. Post-exploitation tools aid in the manipulation and exploration of compromised systems, making them significant assets in advanced cybersecurity assessments and ethical hacking scenarios. Kali Linux provides Meterpreter, Cobalt Strike, and Powershell Empire.

11.Forensics:

Forensics tools in Kali Linux are specialized software used for digital forensics and investigative analysis. These tools assist in collecting, preserving, and analysing digital evidence from various sources such as computers, networks, and storage devices. They help investigators uncover crucial information, identify patterns, and reconstruct events, enabling them to draw conclusions and support legal proceedings. Kali Linux provides a comprehensive range of forensics tools, including Autopsy, Sleuth Kit, Volatility, and many more, making it a powerful platform for digital forensics investigations.