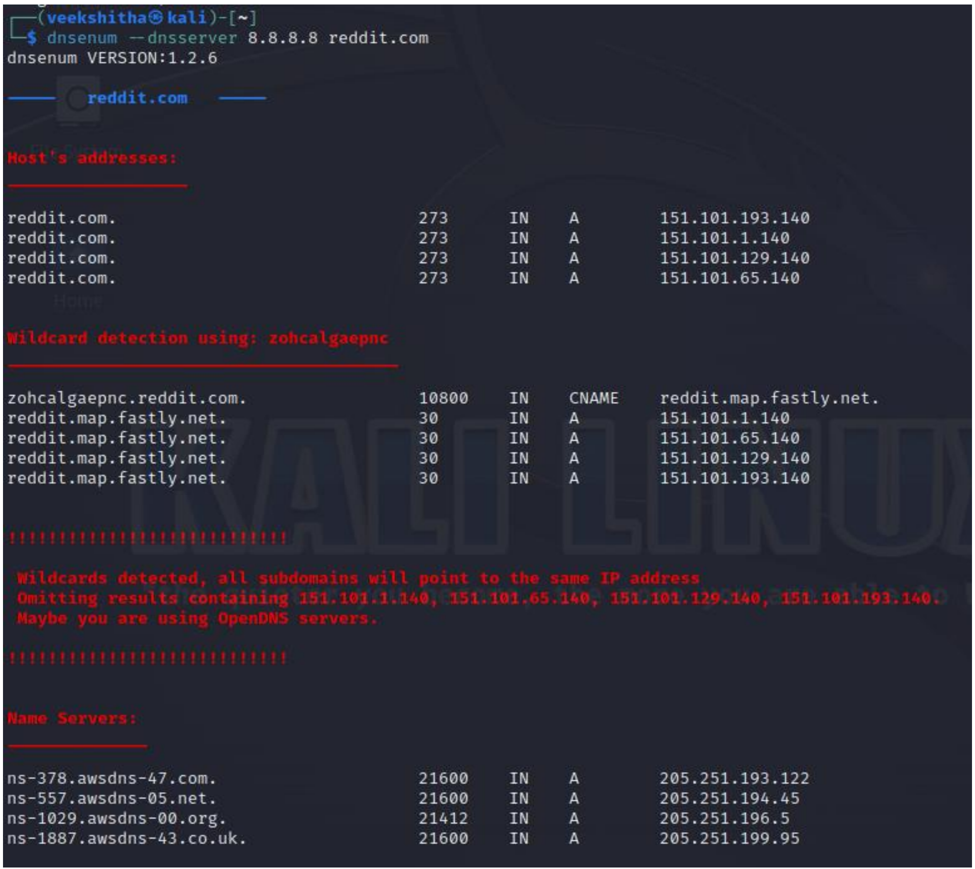
Name : Veekshitha
Regno : 21BCE8943

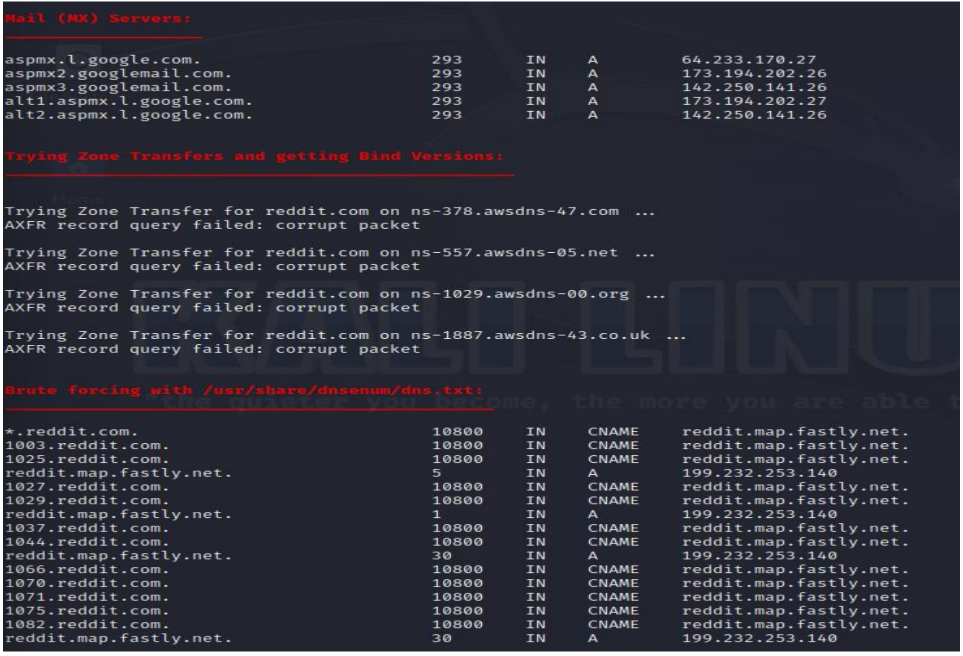
ASSIGNMENT - 2

1. Information Gathering

dnsenum :

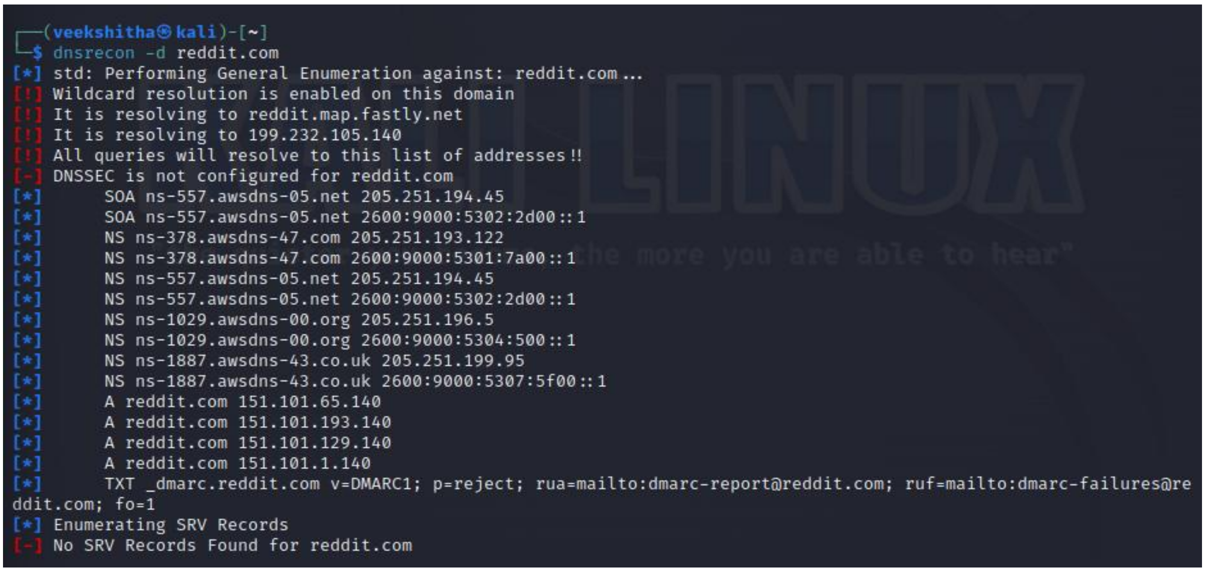


```
┌──(veekshitha㉿kali)-[~]
└─$ dnsenum --dnsserver 8.8.8.8 reddit.com
dnsenum VERSION:1.2.6

-----   reddit.com   -----


Host's addresses:
__________________

reddit.com.                              273      IN    A        151.101.193.140
reddit.com.                              273      IN    A        151.101.1.140
reddit.com.                              273      IN    A        151.101.129.140
reddit.com.                              273      IN    A        151.101.65.140


Wildcard detection using: zohcalgaepnc
_______________________________________

zohcalgaepnc.reddit.com.                 10800    IN    CNAME    reddit.map.fastly.net.
reddit.map.fastly.net.                   30       IN    A        151.101.1.140
reddit.map.fastly.net.                   30       IN    A        151.101.65.140
reddit.map.fastly.net.                   30       IN    A        151.101.129.140
reddit.map.fastly.net.                   30       IN    A        151.101.193.140


!!!!!!!!!!!!!!!!!!!!!!!!!!!!

 Wildcards detected, all subdomains will point to the same IP address
 Omitting results containing 151.101.1.140, 151.101.65.140, 151.101.129.140, 151.101.193.140.
 Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!


Name Servers:
______________

ns-378.awsdns-47.com.                    21600    IN    A        205.251.193.122
ns-557.awsdns-05.net.                    21600    IN    A        205.251.194.45
ns-1029.awsdns-00.org.                   21412    IN    A        205.251.196.5
ns-1887.awsdns-43.co.uk.                 21600    IN    A        205.251.199.95
```



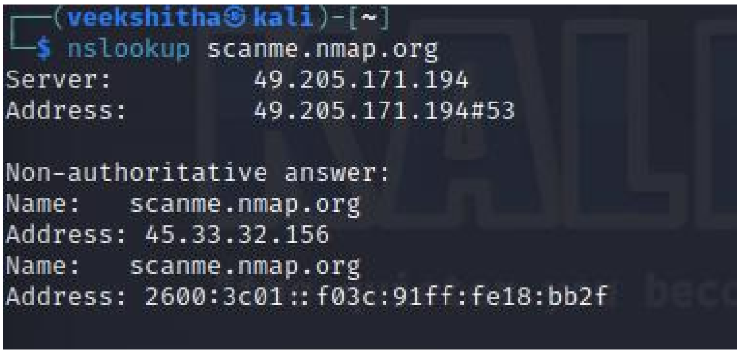
```
Mail (MX) Servers:
___________________

aspmx.l.google.com.                      293      IN    A        64.233.170.27
aspmx2.googlemail.com.                   293      IN    A        173.194.202.26
aspmx3.googlemail.com.                   293      IN    A        142.250.141.26
alt1.aspmx.l.google.com.                 293      IN    A        173.194.202.27
alt2.aspmx.l.google.com.                 293      IN    A        142.250.141.26


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for reddit.com on ns-378.awsdns-47.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for reddit.com on ns-557.awsdns-05.net ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for reddit.com on ns-1029.awsdns-00.org ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for reddit.com on ns-1887.awsdns-43.co.uk ...
AXFR record query failed: corrupt packet


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

*.reddit.com.                            10800    IN    CNAME    reddit.map.fastly.net.
1003.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
1025.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
reddit.map.fastly.net.                   5        IN    A        199.232.253.140
1027.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
1029.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
reddit.map.fastly.net.                   1        IN    A        199.232.253.140
1037.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
1044.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
reddit.map.fastly.net.                   30       IN    A        199.232.253.140
1066.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
1070.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
1071.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
1075.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
1082.reddit.com.                         10800    IN    CNAME    reddit.map.fastly.net.
reddit.map.fastly.net.                   30       IN    A        199.232.253.140
```

Dnsrecon :



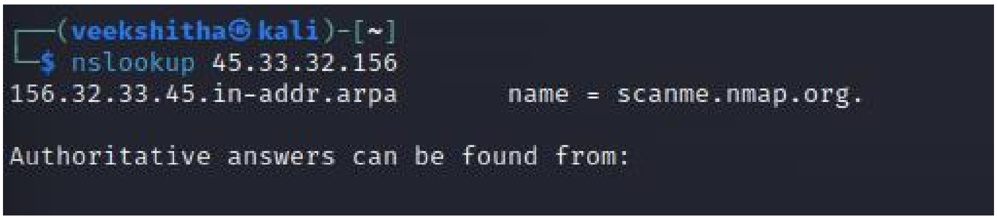
```
┌──(veekshitha㉿kali)-[~]
└─$ dnsrecon -d reddit.com
[*] std: Performing General Enumeration against: reddit.com...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to reddit.map.fastly.net
[!] It is resolving to 199.232.105.140
[!] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for reddit.com
[*]      SOA ns-557.awsdns-05.net 205.251.194.45
[*]      SOA ns-557.awsdns-05.net 2600:9000:5302:2d00::1
[*]      NS ns-378.awsdns-47.com 205.251.193.122
[*]      NS ns-378.awsdns-47.com 2600:9000:5301:7a00::1
[*]      NS ns-557.awsdns-05.net 205.251.194.45
[*]      NS ns-557.awsdns-05.net 2600:9000:5302:2d00::1
[*]      NS ns-1029.awsdns-00.org 205.251.196.5
[*]      NS ns-1029.awsdns-00.org 2600:9000:5304:500::1
[*]      NS ns-1887.awsdns-43.co.uk 205.251.199.95
[*]      NS ns-1887.awsdns-43.co.uk 2600:9000:5307:5f00::1
[*]      A reddit.com 151.101.65.140
[*]      A reddit.com 151.101.193.140
[*]      A reddit.com 151.101.129.140
[*]      A reddit.com 151.101.1.140
[*]      TXT _dmarc.reddit.com v=DMARC1; p=reject; rua=mailto:dmarc-report@reddit.com; ruf=mailto:dmarc-failures@re
ddit.com; fo=1
[*] Enumerating SRV Records
[-] No SRV Records Found for reddit.com
```

NMAP :



```
┌──(veekshitha㉿kali)-[~]
└─$ nslookup scanme.nmap.org
Server:         49.205.171.194
Address:        49.205.171.194#53

Non-authoritative answer:
Name:   scanme.nmap.org
Address: 45.33.32.156
Name:   scanme.nmap.org
Address: 2600:3c01::f03c:91ff:fe18:bb2f
```

Vice versa



```
┌──(veekshitha㉿kali)-[~]
└─$ nslookup 45.33.32.156
156.32.33.45.in-addr.arpa       name = scanme.nmap.org.

Authoritative answers can be found from:
```

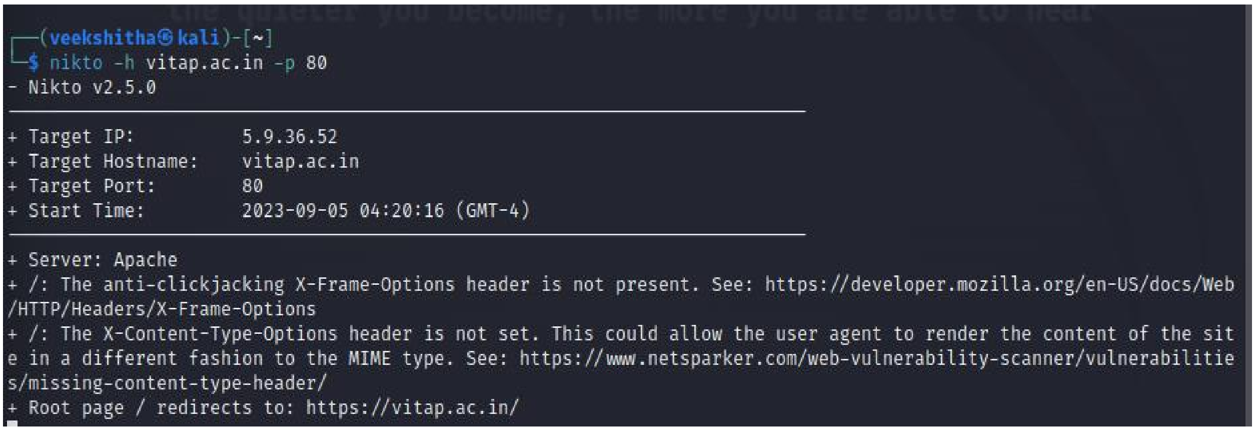
Information gathering in Kali Linux is a crucial phase in the field of cybersecurity, particularly for penetration testing, ethical hacking, and security assessments. The goal of information gathering is to gather as much relevant information as possible about the target to understand its infrastructure, vulnerabilities, and potential attack vectors.

2. Vulnerability Analysis :

It involves the systematic process of identifying and assessing vulnerabilities in a system, network, or application to determine its security weaknesses. The goal of vulnerability analysis is to proactively discover and address vulnerabilities before malicious actors can exploit them.

Tool - **Nikto :**

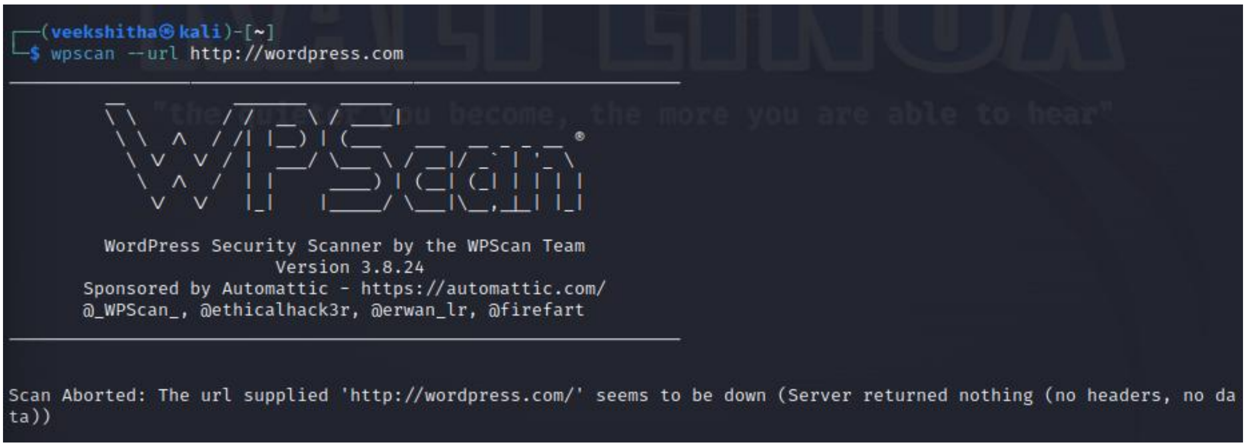
Nikto is one of the tools available in Kali Linux that specializes in web server and web application vulnerability scanning.



```
┌──(veekshitha㉿kali)-[~]
└─$ nikto -h vitap.ac.in -p 80
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          5.9.36.52
+ Target Hostname:    vitap.ac.in
+ Target Port:        80
+ Start Time:         2023-09-05 04:20:16 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web
/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ Root page / redirects to: https://vitap.ac.in/
```

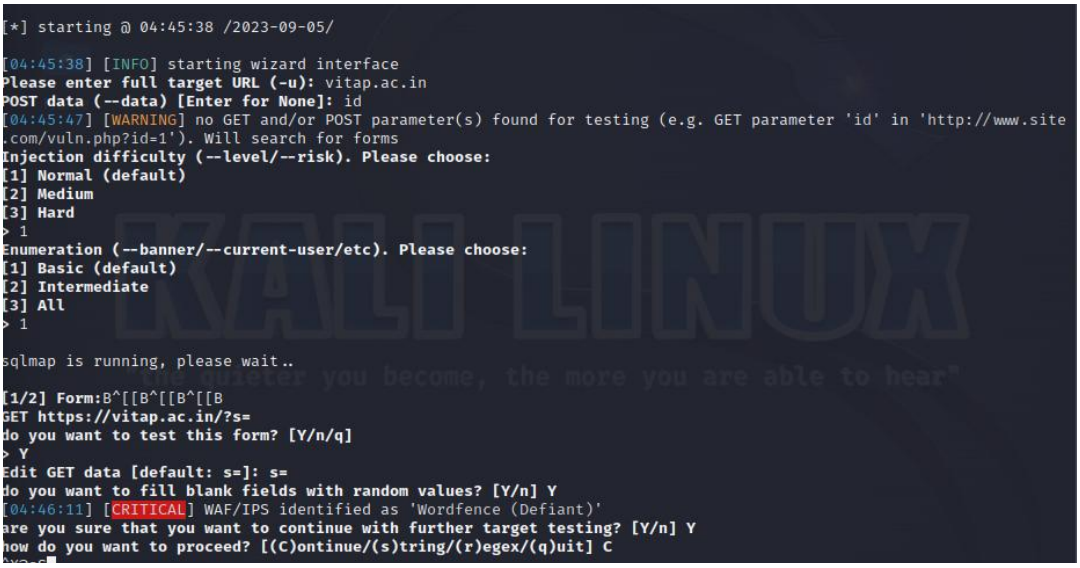
3. Web Application Analysis :

Tool - wpscan :



```
┌──(veekshitha㉿kali)-[~]
└─$ wpscan --url http://wordpress.com
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.24
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________


Scan Aborted: The url supplied 'http://wordpress.com/' seems to be down (Server returned nothing (no headers, no da
ta))
```

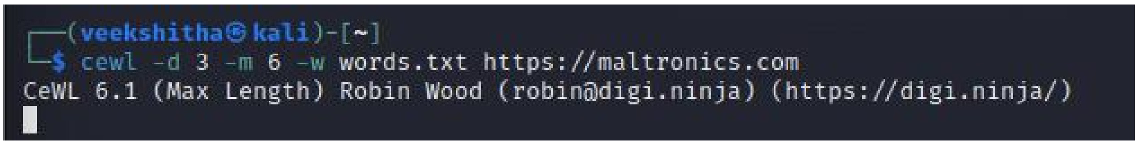
4. DataBase Assesment :



```
[*] starting @ 04:45:38 /2023-09-05/

[04:45:38] [INFO] starting wizard interface
Please enter full target URL (-u): vitap.ac.in
POST data (--data) [Enter for None]: id
[04:45:47] [WARNING] no GET and/or POST parameter(s) found for testing (e.g. GET parameter 'id' in 'http://www.site
.com/vuln.php?id=1'). Will search for forms
Injection difficulty (--level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard
> 1
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 1

sqlmap is running, please wait..

[1/2] Form:B^[[B^[[B^[[B
GET https://vitap.ac.in/?s=
do you want to test this form? [Y/n/q]
> Y
Edit GET data [default: s=]: s=
do you want to fill blank fields with random values? [Y/n] Y
[04:46:11] [CRITICAL] WAF/IPS identified as 'Wordfence (Defiant)'
are you sure that you want to continue with further target testing? [Y/n] Y
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] C
```

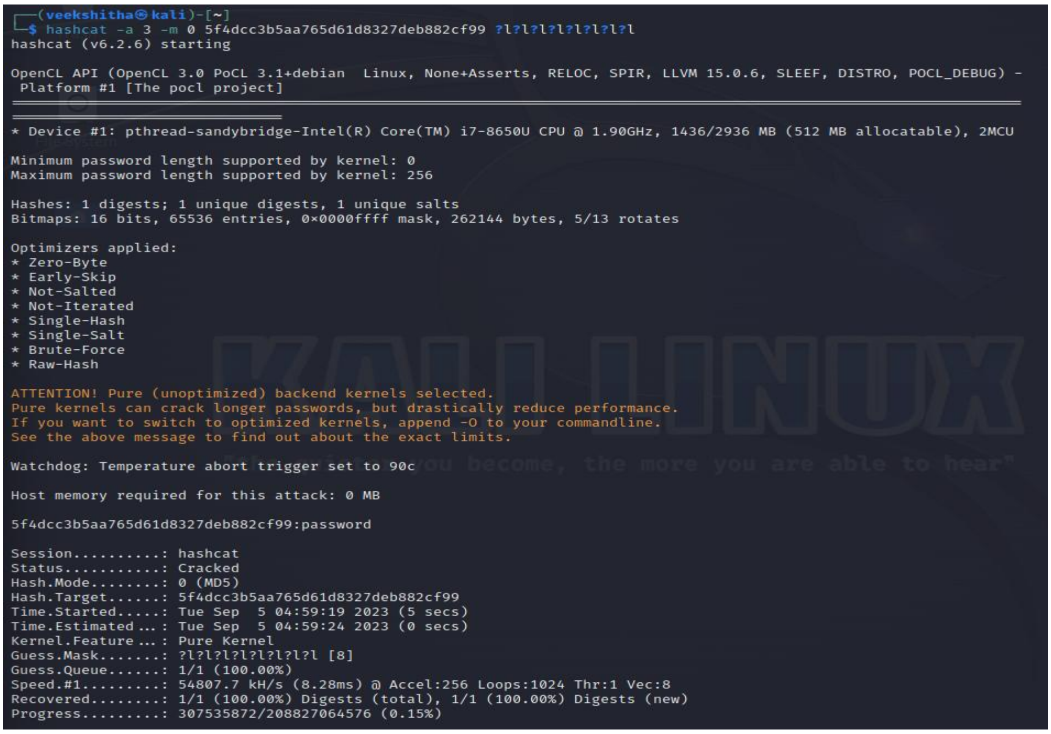
5. Password attacks

Cwel :



```
┌──(veekshitha㉿kali)-[~]
└─$ cewl -d 3 -m 6 -w words.txt https://maltronics.com
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

Hashcat :



```
┌──(veekshitha㉿kali)-[~]
└─$ hashcat -a 3 -m 0 5f4dcc3b5aa765d61d8327deb882cf99 ?l?l?l?l?l?l?l?l
hashcat (v6.2.6) starting

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-Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz, 1436/2936 MB (512 MB allocatable), 2MCU

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

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Brute-Force
* 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: 0 MB

5f4dcc3b5aa765d61d8327deb882cf99:password

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 5f4dcc3b5aa765d61d8327deb882cf99
Time.Started.....: Tue Sep  5 04:59:19 2023 (5 secs)
Time.Estimated ...: Tue Sep  5 04:59:24 2023 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Mask.......: ?l?l?l?l?l?l?l?l [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 54807.7 kH/s (8.28ms) @ Accel:256 Loops:1024 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 307535872/208827064576 (0.15%)
```

6.**Wireless attacks:** These tools are used to attack wireless networks. They can be used to crack wireless passwords, inject malicious code into wireless traffic, and even take control of wireless access points. Some of the most popular wireless attack tools in Kali Linux include Aircrack-ng, Kismet, and Reaver.

7. **Reverse engineering:** These tools are used to decompile and analyze software. This can be used to identify vulnerabilities in the software's code, as well as to develop exploits for those vulnerabilities. Some of the most popular reverse engineering tools in Kali Linux include Ghidra, IDA Pro, and Radare2.

8**. Exploitation tools:** These tools are used to exploit vulnerabilities in a target system or network. They can be used to gain unauthorized access to the system, install malware, or disrupt operations. Some of the most popular exploitation tools in Kali Linux include Metasploit Framework, BeEF, and SET.

9. **Sniffing and spoofing:** These tools are used to capture and analyze network traffic. This can be used to identify sensitive information being transmitted over the network, as well as to launch man-in-the-middle attacks. Some of the most popular sniffing and spoofing tools in Kali Linux include Wireshark, tcpdump, and ettercap.

10.**Post exploitation:** These tools are used to maintain and control access to a compromised system or network. They can be used to install backdoors, steal data, and launch further attacks. Some of the most popular post exploitation tools in Kali Linux include Meterpreter, Cobalt Strike, and Powershell Empire.

11.**Forensics:** These tools are used to collect and analyze digital evidence. This evidence can be used to investigate security incidents, as well as to prosecute criminals. Some of the most popular forensics tools in Kali Linux include The Sleuth Kit, Autopsy, and EnCase.