Ex. No. 5	**Password Cracking**
Date of Exercise	13/09/23

Aim:

To crack/identify a Password using any tool.

Description:

Password cracking is a prominent activity for a hacktivist, password cracking can be done in terminals or in tools which may or may not have GUI. There are quite a few famous tools available as an open source which can be installed for most of the platforms. Some of the famous tools are discussed below:

I. John the Ripper

II. Air crack-ng

III. Cain and Abel

IV. Ophcrack

I. John the Ripper- is free and Open Source software, distributed primarily in source code form.

There is a professional option also available as a paid feature. John the Ripper is used to detect weak passwords for brute forcing. The tool has number ways to crack a password from dictionary attack to brute forcing. The tool relies on word list for any kind of dictionary and brute force attack.

Aircrack-ng- is a powerful wi-fi password cracking tool that can crack WEP or WPA passwords. It can analyse wireless encrypted packets then tries to crack passwords using its cracking algorithm.

It also uses FMS attack as well as other useful attack techniques.

Air crack-ng is a complete suite of tools to assess Wi-Fi network security.

It focuses on different areas of Wi-Fi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools
- Attacking: Replay attacks, DE authentication, fake access points and others via packet injection
- Testing: Checking Wi-Fi cards and driver capabilities (capture and injection)
- Cracking: WEP and WPA PSK (WPA 1 and 2)

Cain and Abel- is a popular password cracking tool which can handle variety of task. The tool is only available for windows platform. It can be a sniffing tool in a network and can handle operations like cracking encrypted password using dictionary attack, recording VoIP conversations, brute force attacks, crypt analysis attack, revealing password boxes, uncovering cached passwords, decoding scrambled passwords, analyse routing protocol .

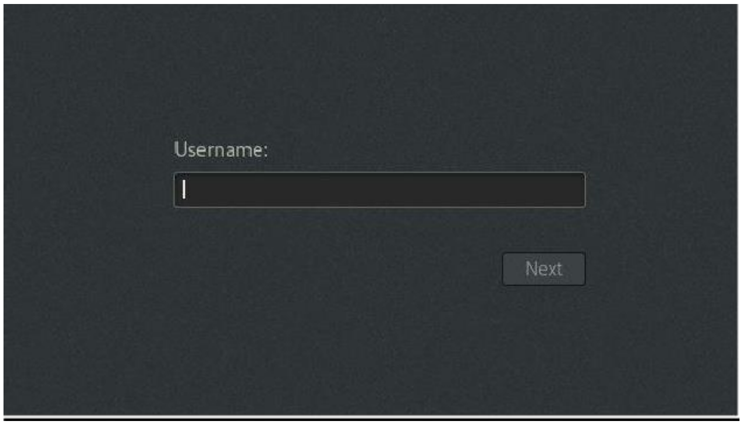
This tool does not exploit any vulnerability, it only covers security weakness of protocols to grab passwords. This was developed for network administrators, security professionals and penetration testers.

Ophcrack- is a free Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms.

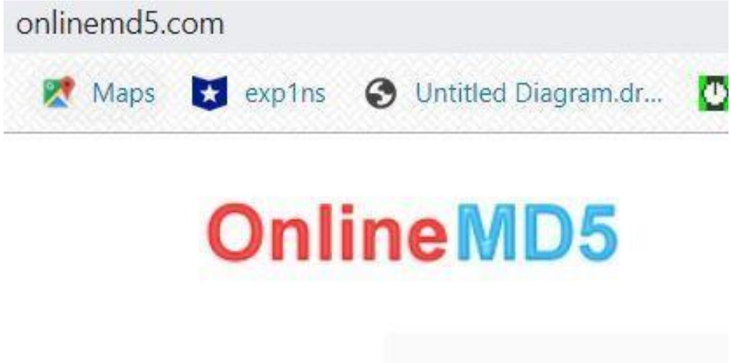
Implementation Steps:

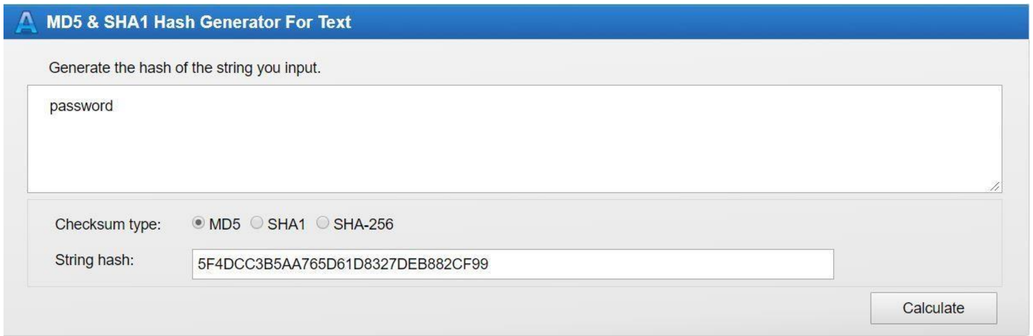
Output:

Step 1. Login into Kali



Step 2. Open a browser and search for an MD5 Hash calculator online





MD5 & SHA1 Hash Generator For Text

Generate the hash of the string you input.

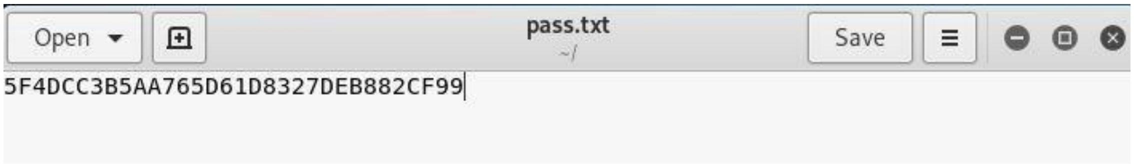
password

Checksum type: ● MD5 ○ SHA1 ○ SHA-256

String hash: 5F4DCC3B5AA765D61D8327DEB882CF99

Step 3. Enter a password and generate the MD5 hash in which ever website you are using.

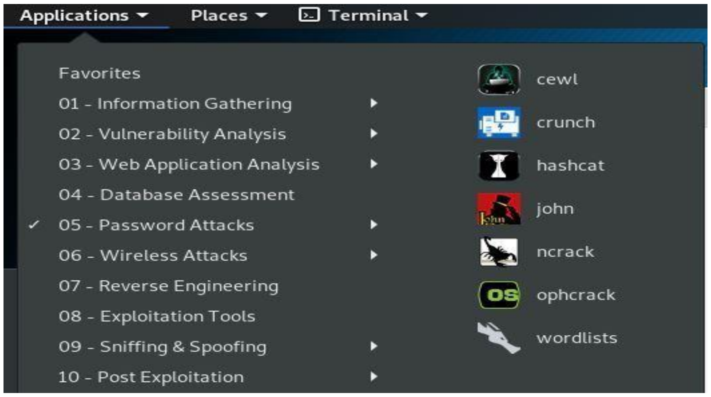
Step 4. Copy and paste the MD5 hash into a test file on your Kali Machine and save the text file



pass.txt
~/

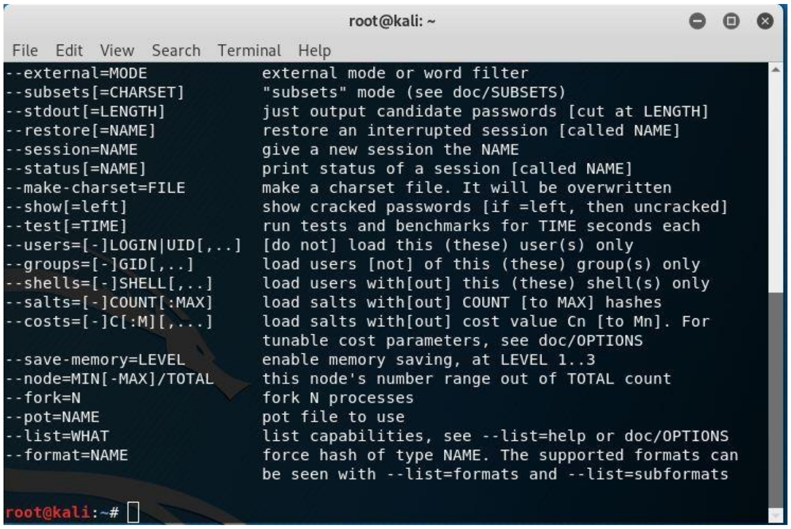
```
5F4DCC3B5AA765D61D8327DEB882CF99
```

with as pass.txt



Step 5. Open the John the Ripper Application window.

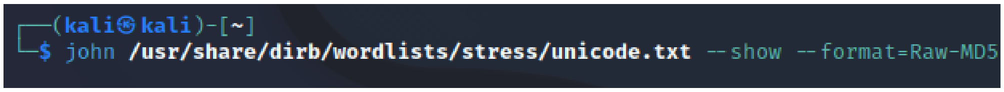
Step 6. A terminal window will launch, showing you different commands for the application.



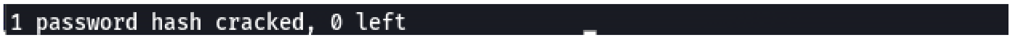
```
--external=MODE            external mode or word filter
--subsets[=CHARSET]        "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session [called NAME]
--make-charset=FILE        make a charset file. It will be overwritten
--show[=left]              show cracked passwords [if =left, then uncracked]
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]  [do not] load this (these) user(s) only
--groups=[-]GID[,..]       load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]     load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]     load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,...]     load salts with[out] cost value Cn [to Mn]. For
                           tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL     this node's number range out of TOTAL count
--fork=N                   fork N processes
--pot=NAME                 pot file to use
--list=WHAT                list capabilities, see --list=help or doc/OPTIONS
--format=NAME              force hash of type NAME. The supported formats can
                           be seen with --list=formats and --list=subformats

root@kali:~#
```

Step 7. To locate the location of the installed wordlist, rockyou.txt, the following command should be executed.

Step 8. To obtain the password from hash using dictionary brute forcing, use the following command.



```
┌──(kali㉿kali)-[~]
└─$ john /usr/share/dirb/wordlists/stress/unicode.txt --show --format=Raw-MD5
```



```
1 password hash cracked, 0 left
```

Result:

Password is cracked successfully using the available open-source tools in Kali Linux.