Date: 15/02/2025

Lab Practical 10:

Perform password cracking concept using brute forec too; L0phtCrack and john the ripper.

John the ripper:

John the Ripper is a popular password cracking tool that can be used to perform brute-force attacks using different encryption technologies and helpful wordlists. It's often what pen-testers and ethical hackers use to find the true passwords behind hashes.

- **Set format of hash:**

  John –format=<name>

  Some populare format is **SHA1,SHA32,SHA256,SHA512,MD1,MD3,MD5,NTLM** etc.

- **Crack zip password :**

  1. Created a zip with password encrypted and convert it into hash.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ zip2john secrate_file.zip  > sec.hash
ver 1.0 efh 5455 efh 7875 secrate_file.zip/Secret.txt PKZIP Encr: 2b chk, TS_chk, cmplen=39, decmplen=27, crc=44909741 ts=1416 cs=1416 type=0
```

  2. **Get the wordlist file from rockyou.txt.gz**

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cat rockyou.txt
123456
12345
123456789
password
loveyou
```

  3. **Crack Zip file**

  Select wordlist file and hash file

  Cracked password is 12121212

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt sec.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
12121212         (secrate_file.zip/Secret.txt)
1g 0:00:00:00 DONE (2025-02-11 02:25) 16.66g/s 68266p/s 68266c/s 68266C/s 123456..oooooo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Date: 15/02/2025

- **Crack Password of User in linux**
  1. **Find Shadow file and Password file in linux**
     Path: sudo cat /etc/passwd
     sudo cat /etc/shadow

     password file: The /etc/passwd file is a plain-text database housing fundamental user information. Each line in the file represents a user account and is divided into fields separated by colons

     shadow file: For heightened security, critical user authentication information, particularly hashed passwords, resides in the /etc/shadow file, accessible exclusively to privileged users.

     Unshadow Both file to get hash:

```
┌──(kali㉿kali)-[~]
└─$ sudo unshadow /etc/passwd /etc/shadow
[sudo] password for kali:
root:*:0:0:root:/root:/usr/bin/zsh
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
```

  2. Take a hash and store into new file:

```
  GNU nano 8.3                    new.txt *
root:$6$riekpK4m$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfbneE
bo0wSijW1GQussvJSk8X1M56kzgGj8f7DFN1h4dy1
:0:0:root:/root:/bin/bash
```

  3. Crack the hash password:

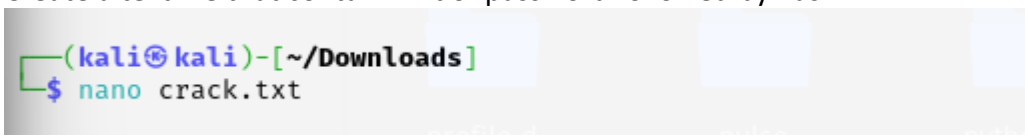
```
┌──(kali㉿kali)-[~/Downloads]
└─$ john --wordlist=rockyou.txt new.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128
SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mercedes         (root)
1g 0:00:00:00 DONE (2025-02-15 12:35) 2.941g/s 376.4p/s 376.4c/s 3
76.4C/s 123456..555555
Use the "--show" option to display all of the cracked passwords re
liably
Session completed.
```

Date: 15/02/2025

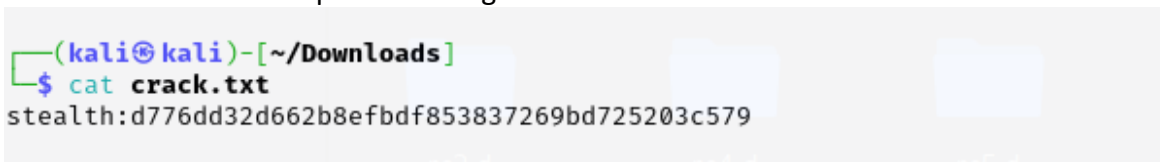
- **Crack Password using single mode**:

  In single-crack mode, John takes a string and generates variations of that string in order to generate a set of passwords.

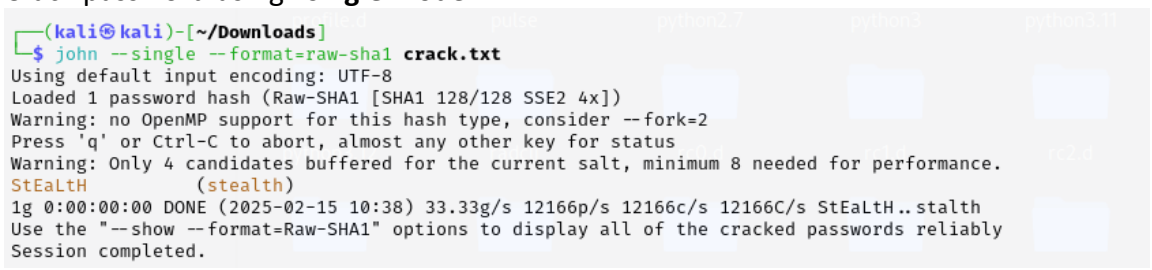
  1. Create a text file that contain hint of password followed by hash



  2. Here cracker know that password might be stealth:



  3. Crack password using **–single** mode:



  4. Use –show option to show password

Date: 15/02/2025

Hydar:

Hydra is a fast and flexible password-cracking tool that supports numerous protocols, including SSH, FTP, HTTP, and more. Its versatility makes it an indispensable asset for security professionals seeking to assess the strength of passwords and identify vulnerabilities in systems. With Hydra, users can perform brute-force attacks by systematically attempting different combinations of usernames and passwords until the correct credentials are discovered.

- **Crack password of login Web page**

1. Get the URL of login page, here we used DVWA login page:

2. **Crack password :**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ hydra http-get://127.0.0.1/DVWA -l admin -P rockyou.txt -V -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these *** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-16 02:00:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1/p:14344400), ~
896525 tries per task
[DATA] attacking http-get://127.0.0.1:80/DVWA
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456" - 1 of 14344400 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "12345" - 2 of 14344400 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456789" - 3 of 14344400 [child 2] (0/0
)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 4 of 14344400 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "iloveyou" - 5 of 14344400 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "monkey" - 14 of 14344400 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "lovely" - 15 of 14344400 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "jessica" - 16 of 14344400 [child 15] (0/0
)
[80][http-get] host: 127.0.0.1   login: admin   password: 12345
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-16 02:00:37
```

Date: 15/02/2025

- **[Option] -l:** it is used to specify user, in over case we already known that user is admin If we don't know the user than use **-L and specify user wordlist**
- **[Option] -P:** it is used to specify password wordlist, if you already known what is password use -p and specify the password
- **[Option] -V:** used for verbose mode, where it will show the login+pass combination for each attempt.
- **[Option] -f:** it is used to stop trying combination when valid user and password found
- **[Option] -t**: it specify the task, how many request/combination can apply at once, it is used when there is firewall, we can decrease the number of attempts do at a time so the firewall can't detect unusual activity.