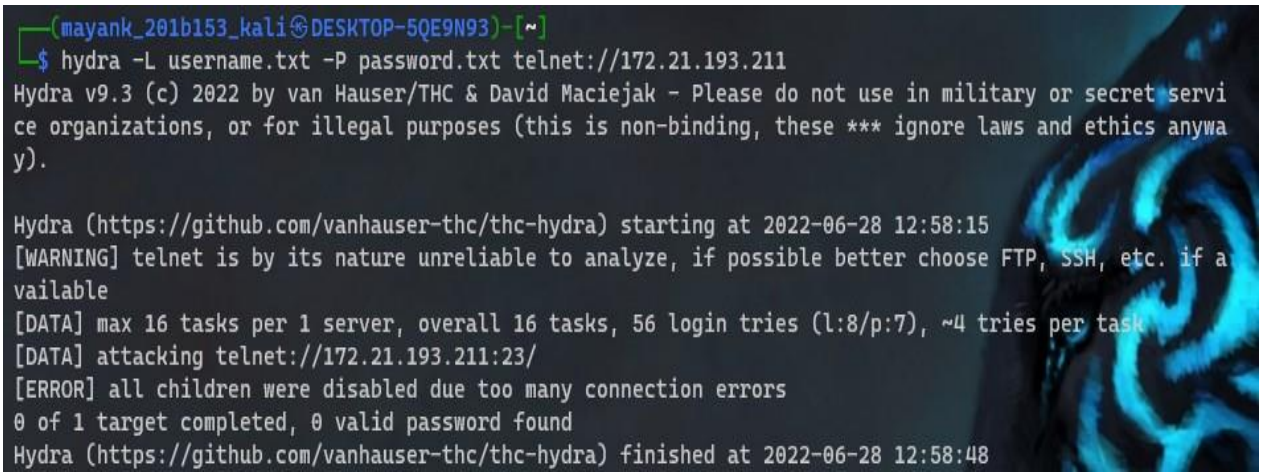
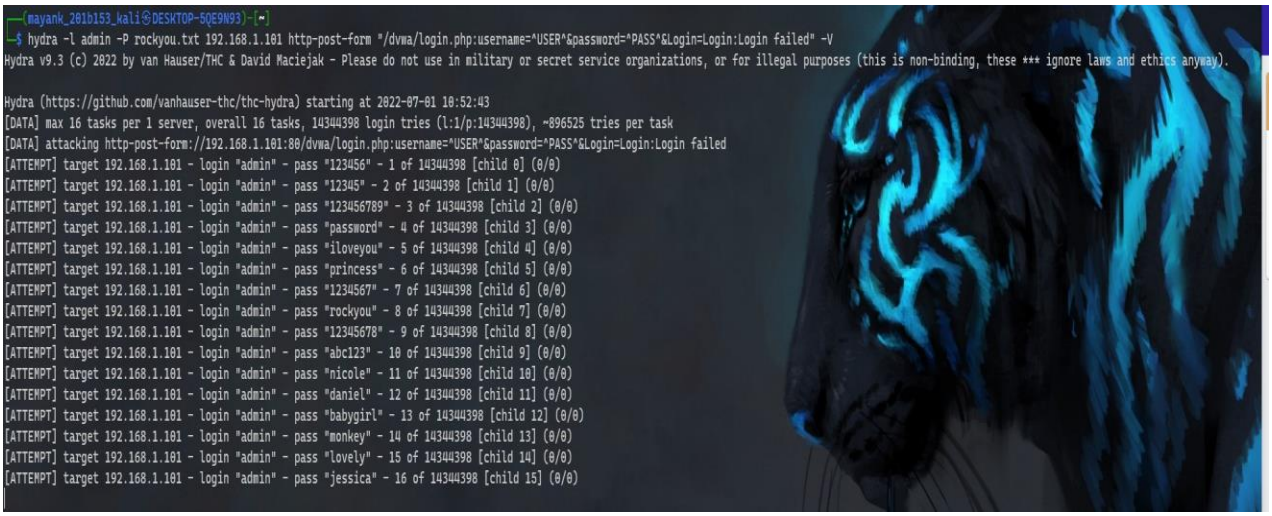
Internship Project System Hacking:

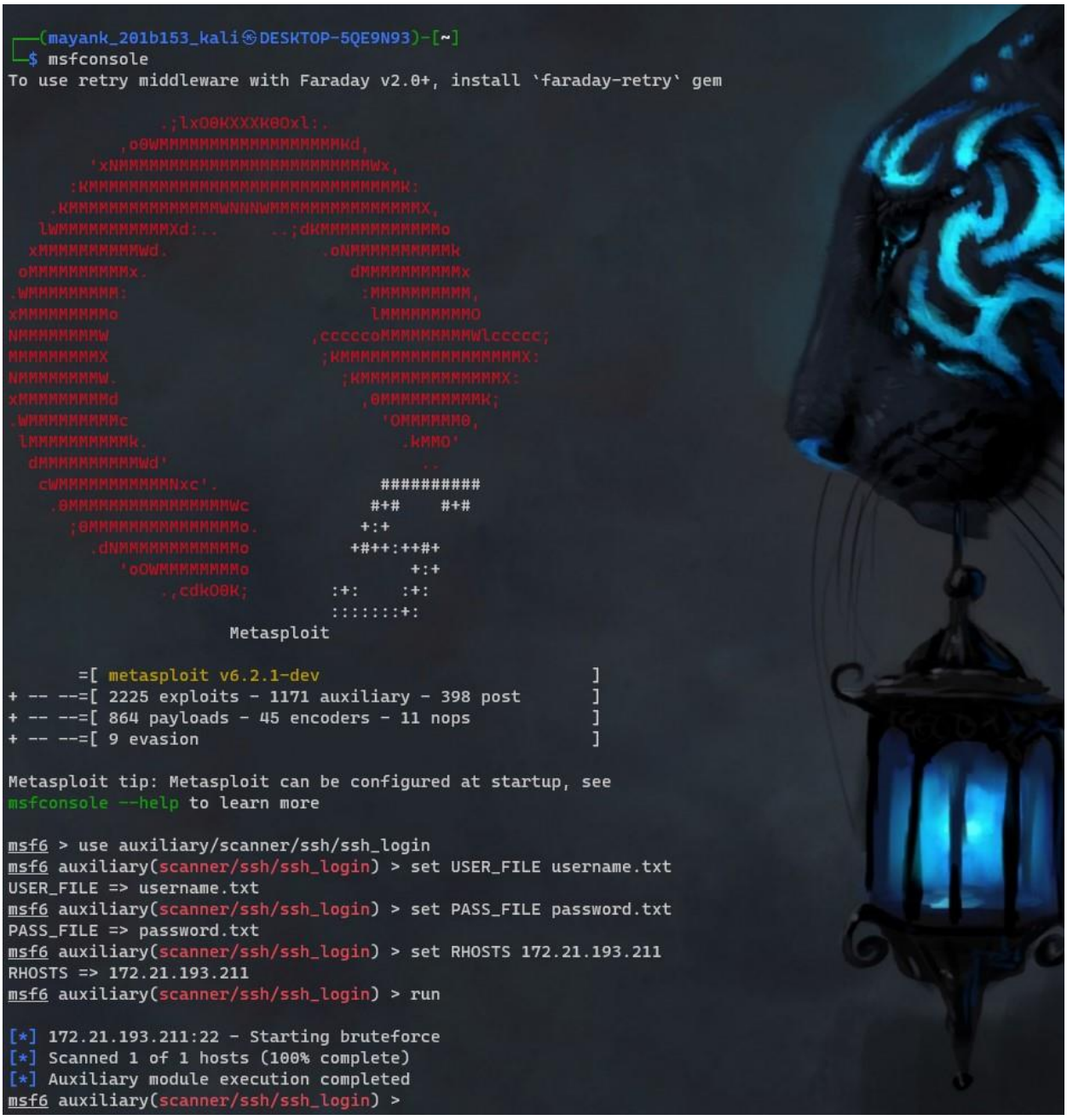
By- Mayank Singh Tomar (tomarm698@gmail.com)

1. HYDRA





2. Auxiliary Module

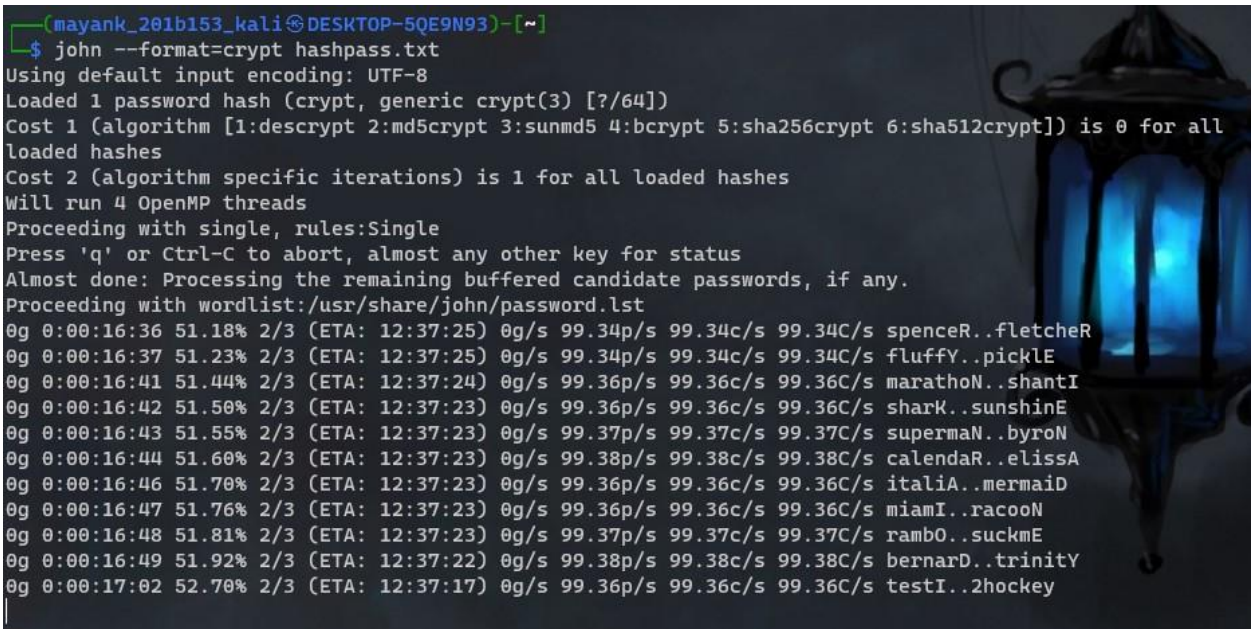


3. NSE scripts

```
┌──(mayank_201b153_kali㉿DESKTOP-5QE9N93)-[~]
└─$ cd /usr/share/nmap/scripts

┌──(mayank_201b153_kali㉿DESKTOP-5QE9N93)-[/usr/share/nmap/scripts]
└─$ ls -l | grep ssh
-rw-r--r-- 1 root root  5391 Jan 18 20:24 ssh2-enum-algos.nse
-rw-r--r-- 1 root root  1200 Jan 18 20:24 ssh-auth-methods.nse
-rw-r--r-- 1 root root  3045 Jan 18 20:24 ssh-brute.nse
-rw-r--r-- 1 root root 16036 Jan 18 20:24 ssh-hostkey.nse
-rw-r--r-- 1 root root  5948 Jan 18 20:24 ssh-publickey-acceptance.nse
-rw-r--r-- 1 root root  3781 Jan 18 20:24 ssh-run.nse
-rw-r--r-- 1 root root  1423 Jan 18 20:24 sshv1.nse

┌──(mayank_201b153_kali㉿DESKTOP-5QE9N93)-[/usr/share/nmap/scripts]
└─$ nmap --script ssh-brute.nse -p 22 172.17.0.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 12:31 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 5.20 seconds

┌──(mayank_201b153_kali㉿DESKTOP-5QE9N93)-[/usr/share/nmap/scripts]
└─$ nmap --script ssh-brute.nse -p 22 192.168.29.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 12:32 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.89 seconds

┌──(mayank_201b153_kali㉿DESKTOP-5QE9N93)-[/usr/share/nmap/scripts]
└─$ nmap -Pn --script ssh-brute.nse -p 22 192.168.29.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 12:32 IST
Nmap scan report for 192.168.29.40
Host is up.

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 16.56 seconds
```

```
┌──(mayank_201b153_kali㉿DESKTOP-5QE9N93)-[/usr/share/nmap/scripts]
└─$ sudo nmap -Pn --script ssh-brute.nse -p 22 172.17.0.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 11:15 IST
Nmap scan report for 172.17.0.2
Host is up.

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 15.43 seconds
```

4. John the ripper



5. Password generating using CRUNCH