	Informe de análisis de vulnerabilidades, explotación y resultados del reto Steel Mountain.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	07/05/2024	xx/xx/2023	1.0	MQ-HM- GAME ZONE.	RESTRINGIDO

Informe de análisis de vulnerabilidades, explotación y resultados del reto Eternal.

N.- MQ-HM- GAME ZONE

Generado por:

Hacker Mentor, Ing. David Tafolla Recinos

Especialista de Ciberseguridad, Seguridad de la Información

Fecha de creación:
17.05.2024

Índice

Contenido

1. Resumen Ejecutivo

Este informe documenta las vulnerabilidades descubiertas durante una prueba de penetración de la máquina virtual "GameZone" de TryHackMe. Se identificaron varias debilidades significativas, incluyendo una vulnerabilidad de inyección SQL y configuraciones incorrectas de permisos que permitieron la escalada de privilegios. Las recomendaciones proporcionadas tienen como objetivo mitigar estos riesgos y fortalecer la seguridad del sistema.

2. Alcance

El alcance de esta evaluación incluyó:

- **Servicios Web:** Evaluación de la aplicación web alojada en "GameZone".
- **Configuraciones del Sistema:** Revisión de permisos y configuraciones de archivos críticos.
- **Servicios de Red:** Escaneo y enumeración de puertos y servicios accesibles.
- No se realizaron pruebas de denegación de servicio ni ataques destructivos.

3. Metodología

3.1 Reconocimiento

Puertos abiertos descubiertos por nmap:

```
┌──(hmstudent㉿kali)-[~/Clases_Pentesting/GameZone/Nmap]
└─$ sudo nmap -sS --min-rate 800 -p- --open -n -v -Pn 10.10.218.199 -oG allpo
rts
[sudo] password for hmstudent:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan tim
es may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-16 20:16 EDT
Initiating SYN Stealth Scan at 20:16
Scanning 10.10.218.199 [65535 ports]
Discovered open port 80/tcp on 10.10.218.199
Discovered open port 22/tcp on 10.10.218.199
SYN Stealth Scan Timing: About 44.97% done; ETC: 20:18 (0:00:38 remaining)
Completed SYN Stealth Scan at 20:17, 54.67s elapsed (65535 total ports)
Nmap scan report for 10.10.218.199
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 54.77 seconds
           Raw packets sent: 68121 (2.997MB) | Rcvd: 68030 (2.721MB)
```

Puertos encontrados

Versiones de puertos abiertos:

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu L
inux; protocol 2.0)
| ssh-hostkey:
|   2048 61ea89f1d4a7dca550f76d89c3af0b03 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFJTi0lKi0G+v4eFQU+P+CBodBOruOQC+3C/n
Xv0JVeR7yDWH6iRsFsevDofWcq05MZBr/CDPCnluhZzM1psx+5bp1Eiv3ecO0PF1QjhAzsPwUcmFS
G1zAg+S757M+RFeRs0Jw0WMev8N6aR3uBZQSDPwBHGps+mZZZRcsssckJGQCZ4Qg/6PVFIwNGx9Uo
ftdMFyfNMU/TDZmoatzo/FNEJOhbR38dF/xw9s/HRhugrUsLdNHyBxYShcY3B0Y2eLjnnuUWhYPmL
ZqgHuHr+eKnb1Ae3MB5lJTfZf3OmWaqcDVI3wpvQK7ACC9S8nxL3vYLyzxlvucEZHM9ILBI7Ov
|   256 b37d72461ed341b66a911516c94aa5fa (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKA
U0Orx0zOb8C4AtiV+Q1z2yj1DKw5Z2TA2UTS9Ee1AYJcMtM62+f7vGCgoTNN3eFj3lTvktOt+nMYs
ipuCxdY=
|   256 536709dcfffb3a3efbfecfd86d4127ab (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL6LScmHgHeP2OMerYFiDsNPqgqFbsL+GsyehB7
6kldy
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Game Zone
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Versión de Openssh

Versión de servicio http

Conversión del .xml a .html:

Online Hosts

10.10.218.199

Ports

Port	Protocol	State Reason	Service	Product	Version	Extra Info
22	tcp	open syn-ack	ssh	OpenSSH	7.2p2 Ubuntu 4ubuntu2.7	Ubuntu Linux; protocol 2.0

cpe:/a:openbsd:openssh:7.2p2

ssh-hostkey

```
2048 61ea89f1d4a7dca550f76d89c3af0b03 (RSA)
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFJTi0lKi0G+v4eFQU+P+CBodBOruOQC+3C/nXv0JVeR7yDWH6iRsFsevDofWcq05MZBr/CDPCnluhZzM1psx+5bp1Eiv3ecO0PF1QjhAzsPwUcmFSG1zAg+S757M+RFeRs0Jw0WMev8N6aR3uBZQSDPwBHGps+mZZZRcsssckJGQCZ4Qg/
6PVFIwNGx9UoftdMFyfNMU/TDZmoatzo/FNEJOhbR38dF/xw9s/HRhugrUsLdNHyBxYShcY3B0Y2eLjnnuUWhYPmLZqgHuHr+eKnb1Ae3MB5lJTfZf3OmWaqcDVI3wpvQK7ACC9S8nxL3vYLyzxlvucEZHM9ILBI7Ov
256 b37d72461ed341b66a911516c94aa5fa (ECDSA)
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKAU0Orx0zOb8C4AtiV+Q1z2yj1DKw5Z2TA2UTS9Ee1AYJcMtM62+f7vGCgoTNN3eFj3lTvktOt+nMYsipuCxdY=
256 536709dcfffb3a3efbfecfd86d4127ab (ED25519)
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL6LScmHgHeP2OMerYFiDsNPqgqFbsL+GsyehB76kldy
```

80	tcp	open syn-ack	http	Apache httpd	2.4.18	(Ubuntu)

cpe:/a:apache:http_server:2.4.18

http-cookie-flags

```
/:
  PHPSESSID:
    httponly flag not set
```

http-title

```
Game Zone
```

IP, Puertos Sistema operativo

IP	10.10.218.199 10.10.211.15 10.10.146.91 (Cambio por que se acabó el tiempo de uso)
Sistema Operativo	Linux Ubuntu 2.7
Puertos/Servicios	22 -SSH 80 – HTTP

3.2 Análisis de vulnerabilidades/debilidades

Escaneo de vulnerabilidades con nmap:

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu L
inux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.2p2:
|       PRION:CVE-2016-8858     7.8     https://vulners.com/prion/PRION:CVE-2
016-8858
|       PRION:CVE-2016-6515     7.8     https://vulners.com/prion/PRION:CVE-2
016-6515
|       PACKETSTORM:140070      7.8     https://vulners.com/packetstorm/PACKE
TSTORM:140070   *EXPLOIT*
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulne
rs.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 *EXPLOIT*
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888  *
EXPLOIT*
|       CVE-2016-8858   7.8     https://vulners.com/cve/CVE-2016-8858
|       CVE-2016-6515   7.8     https://vulners.com/cve/CVE-2016-6515
|       1337DAY-ID-26494        7.8     https://vulners.com/zdt/1337DAY-ID-26
494     *EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPL
OIT*
```

Posibles vulnerabilidades del servicio ssh

```
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| vulners:
|   cpe:/a:apache:http_server:2.4.18:
|       PACKETSTORM:176334      7.5     https://vulners.com/packetstorm/PACKE
TSTORM:176334   *EXPLOIT*
|       PACKETSTORM:171631      7.5     https://vulners.com/packetstorm/PACKE
TSTORM:171631   *EXPLOIT*
|       OSV:BIT-APACHE-2023-25690       7.5     https://vulners.com/osv/OSV:B
IT-APACHE-2023-25690
|       OSV:BIT-APACHE-2022-31813       7.5     https://vulners.com/osv/OSV:B
IT-APACHE-2022-31813
|       OSV:BIT-APACHE-2022-23943       7.5     https://vulners.com/osv/OSV:B
IT-APACHE-2022-23943
|       OSV:BIT-APACHE-2022-22720       7.5     https://vulners.com/osv/OSV:B
IT-APACHE-2022-22720
|       OSV:BIT-APACHE-2021-44790       7.5     https://vulners.com/osv/OSV:B
```

Posibles vulnerabilidades del servicio http

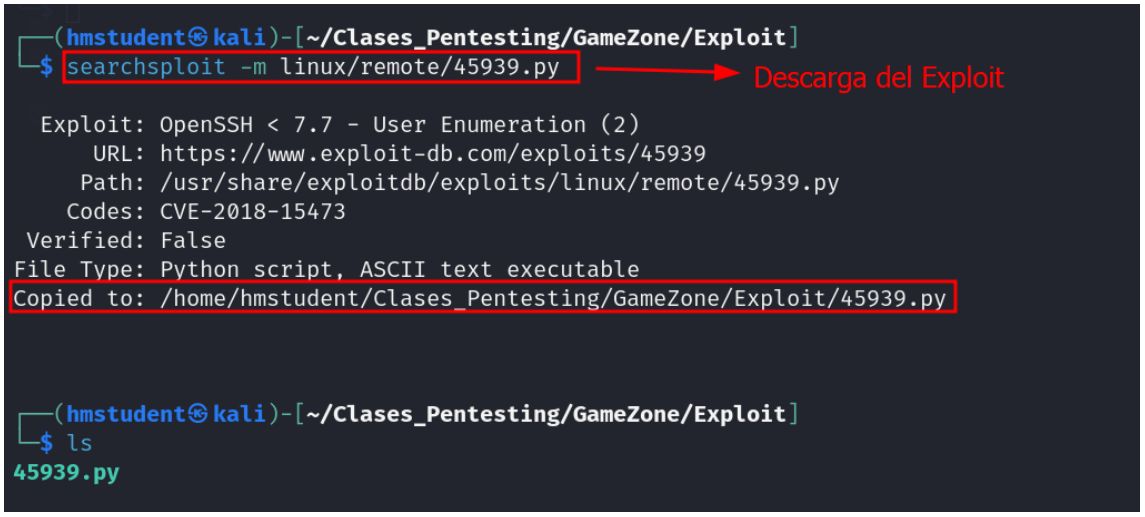
Enumeración de usuario por openssh por searchsploit (45939.py):

1. Búsqueda de exploit en searchsploit:

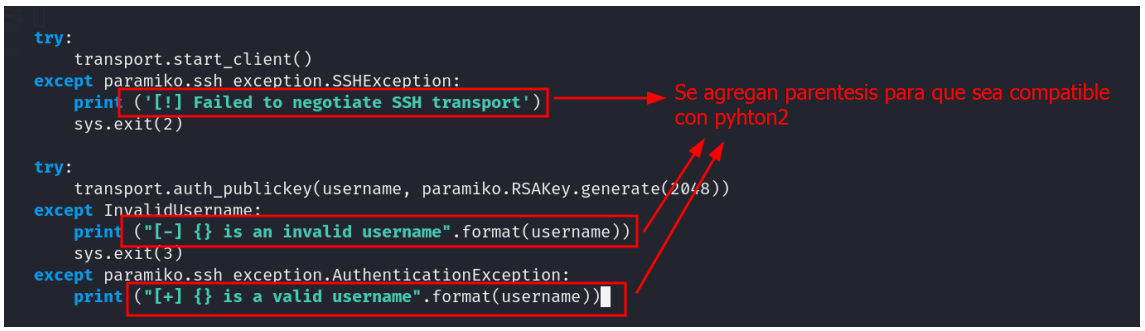
```
┌──(hmstudent㉿kali)-[~/Clases_Pentesting/GameZone/Exploit]
└─$ searchsploit openssh 7.2
------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration                                      | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                | linux/remote/45210.py
OpenSSH 7.2 - Denial of Service                                               | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection                       | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration                                          | linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                      | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                          | linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration                                         | linux/remote/40113.txt
------------------------------------------------------------------------------ ---------------------------
Shellcodes: No Results
```

Posible exploit

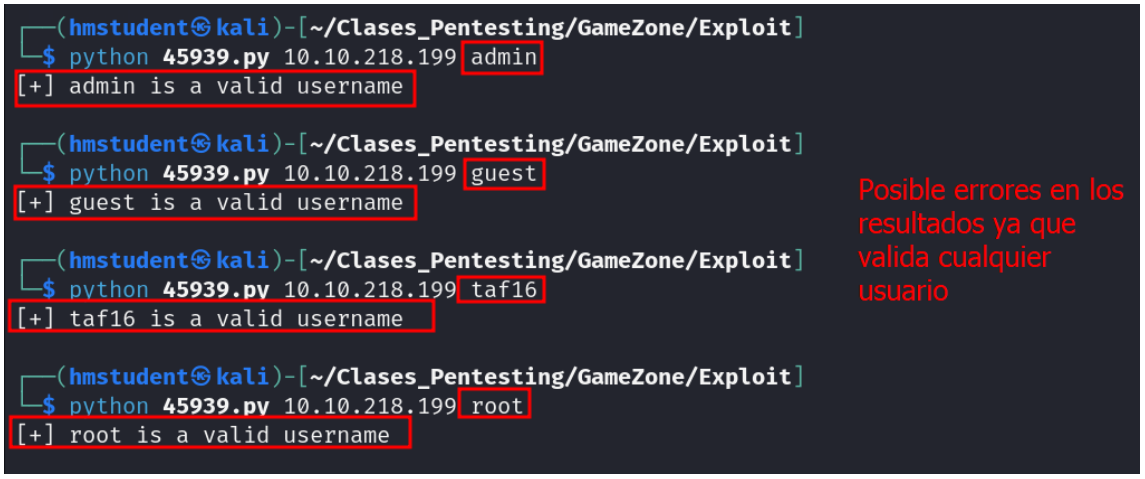
2. Descarga del exploit:



3. Modificación del exploit en Python para su ejecución:

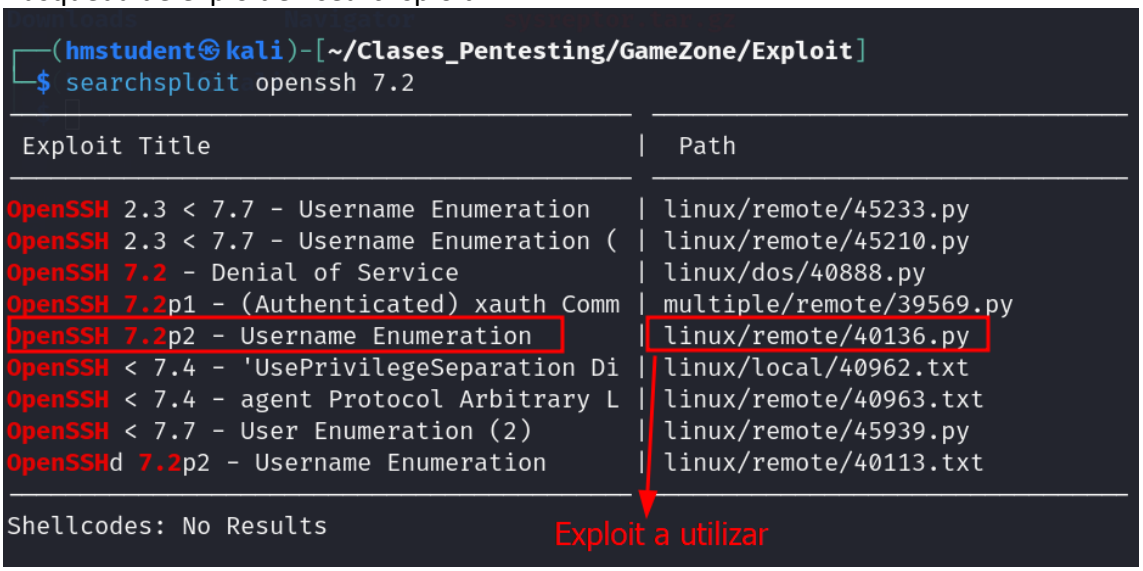


4. Ejecución del exploit:

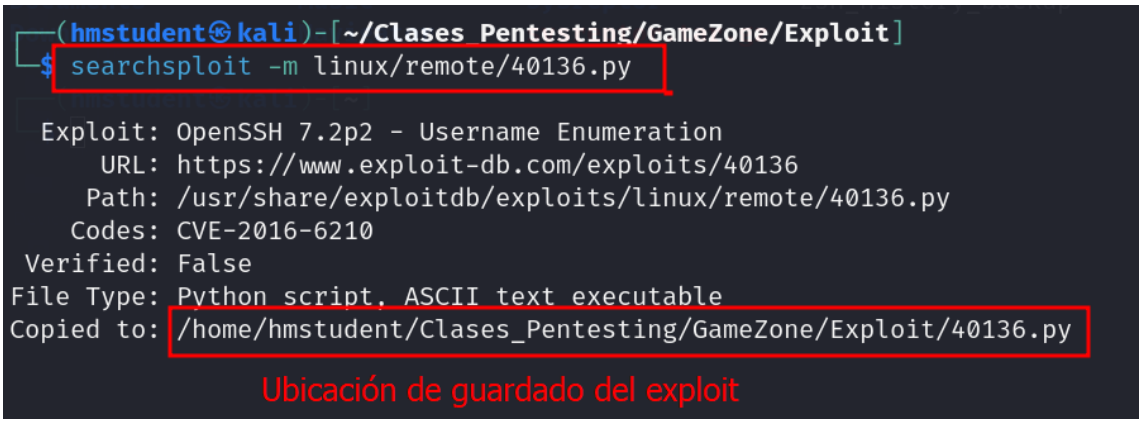


Enumeración de usuario por openssh por searchsploit (40136.py):

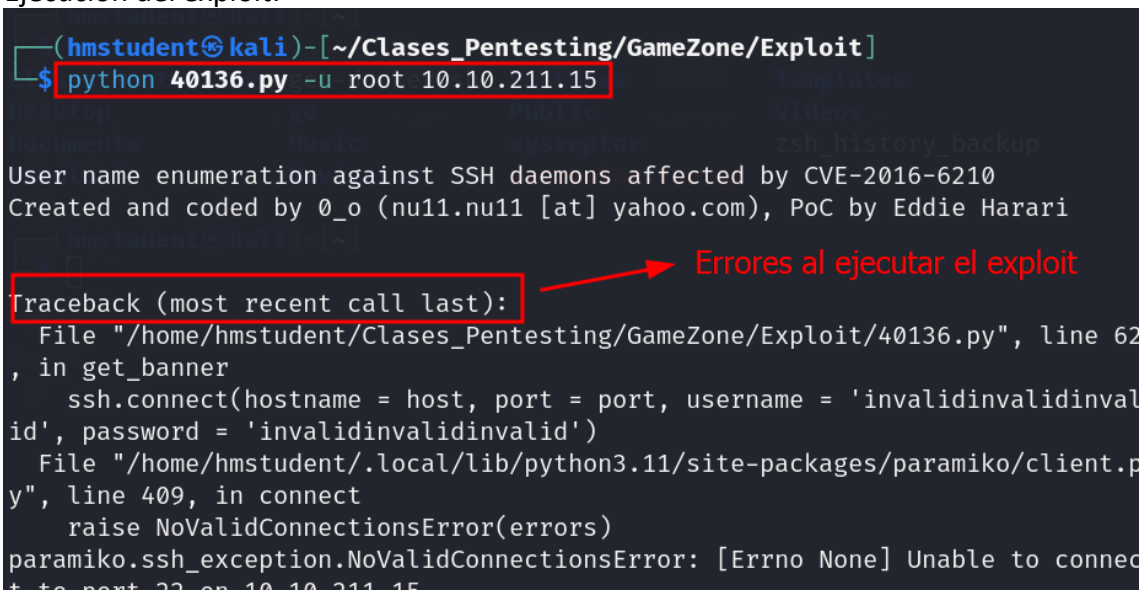
1. Búsqueda de exploit en searchsploit:



2. Descarga del exploit:



3. Ejecución del exploit:



4. Prueba Manual de conexión ssh (Puerto cerrado)

```
┌──(hmstudent㉿kali)-[~/Clases_Pentesting/GameZone/Exploit]
└─$ ssh root@10.10.211.15
ssh: connect to host 10.10.211.15 port 22: Connection refused
```

Error al conectarse al puerto

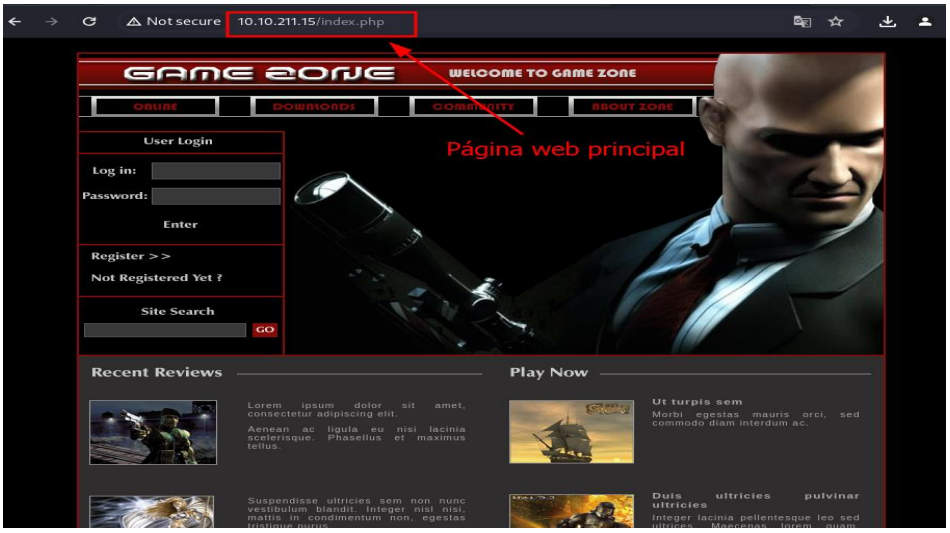
Fuzzing de la página web:

1. Wfuzz:

```
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.211.15/FUZZ
Total requests: 4614

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000012:   403        11 L     32 W       296 Ch      ".htaccess"
000000011:   403        11 L     32 W       291 Ch      ".hta"
000000001:   200        110 L    319 W      4502 Ch     "http://10.1
                                                        0.211.15/"
000000013:   403        11 L     32 W       296 Ch      ".htpasswd"

000002021:   200        110 L    319 W      4502 Ch     "index.php"
000003588:   403        11 L     32 W       300 Ch      "server-stat
                                                        us"

Total time: 0
Processed Requests: 4614
Filtered Requests: 4608
Requests/sec.: 0
```

Páginas encontradas

Index.php:

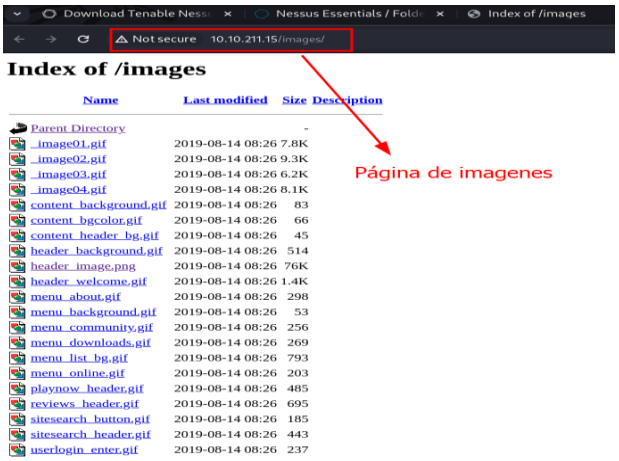


2. Gobuster:

```
┌──(hmstudent㉿kali)-[~/GameZone/Exploit]
└─$ gobuster dir -u http://10.10.211.15/ -t 20 -w /usr/share/wordlists/dirb/b
ig.txt -x .php .html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.211.15/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 296]
/.htpasswd            (Status: 403) [Size: 296]
/.htaccess.php        (Status: 403) [Size: 300]
/.htpasswd.php        (Status: 403) [Size: 300]
/images               (Status: 301) [Size: 313] [--> http://10.10.211.15/imag
es/]
/index.php            (Status: 200) [Size: 4502]
/portal.php           (Status: 302) [Size: 0] [--> index.php]
/server-status        (Status: 403) [Size: 300]
Progress: 40938 / 40940 (100.00%)
===============================================================
```

Páginas encontradas

Directorio de las imágenes:



Información de la página por whatweb:

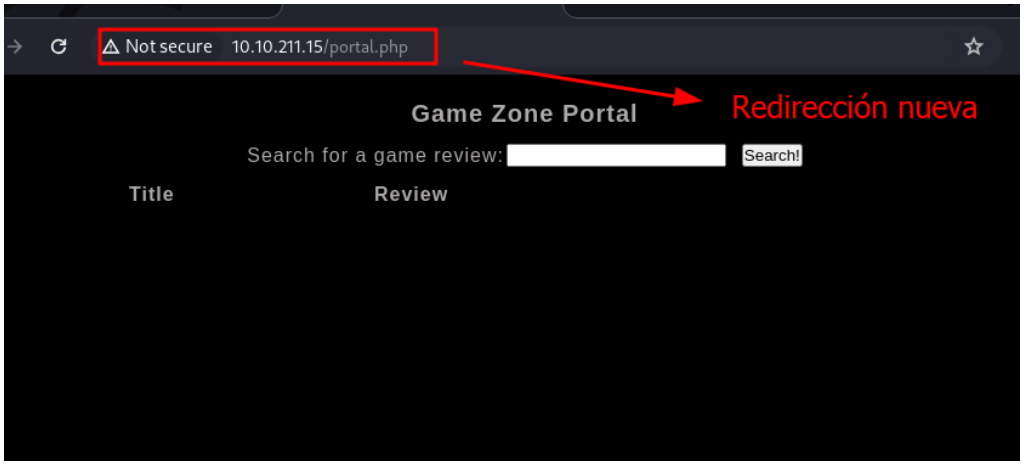
```
┌──(hmstudent㉿kali)-[~]
└─$ whatweb http://10.10.211.15/ -v
WhatWeb report for http://10.10.211.15/
Status    : 200 OK
Title     : Game Zone
IP        : 10.10.211.15
Country   : RESERVED, ZZ

Summary   : Apache[2.4.18], Cookies[PHPSESSID], HTTPServer[Ubuntu Linux][Apac
he/2.4.18 (Ubuntu)], PasswordField[password]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.18 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : PHPSESSID

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : Apache/2.4.18 (Ubuntu) (from server string)

[ PasswordField ]
        find password fields
```

Comando

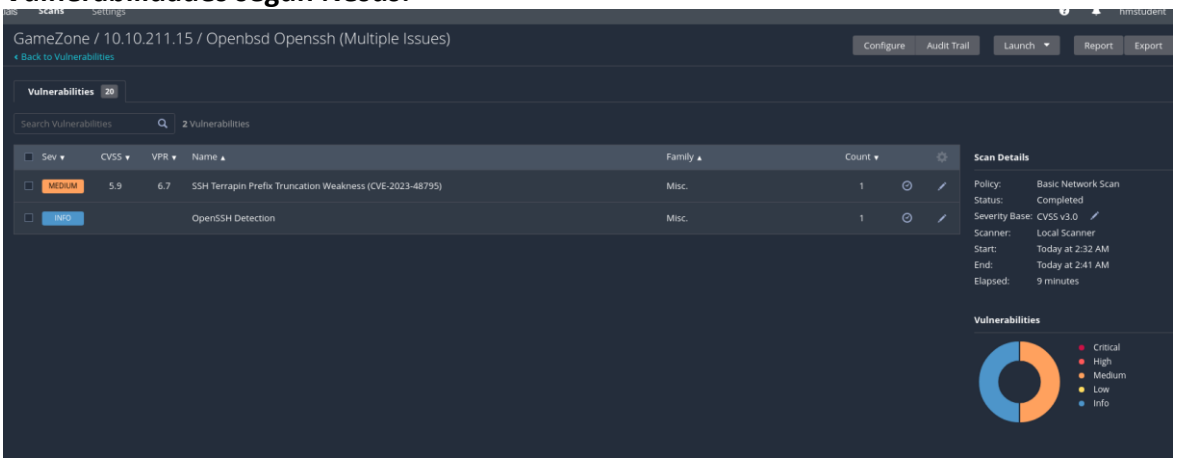
Inyeccción SQL para acceder al panel de página:

1. Colocar ' or 1=1 -- - en el “Log in” para el acceso a la plataforma:

2. Acceso a la página



Vulnerabilidades según Nesus:



Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

Puerto	Vulnerabilidad
22	Enumeración de usuarios
80	SQL Injection
80	Ver directorios mediante Fuzzing (Directory listing)

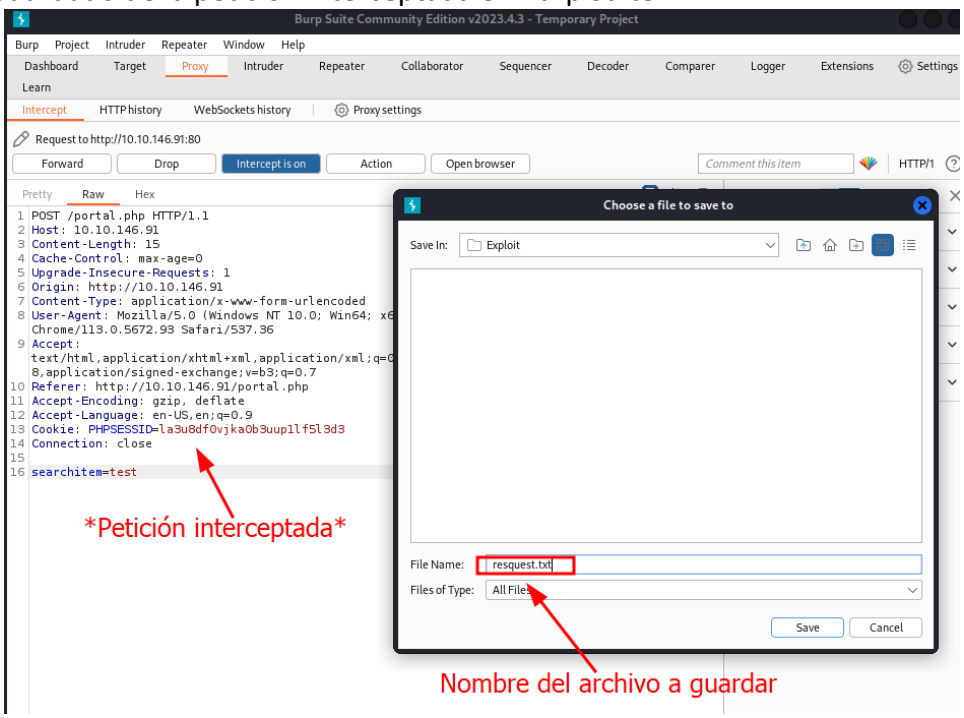
3.3 Explotación

Proceso manual/ automatizado.

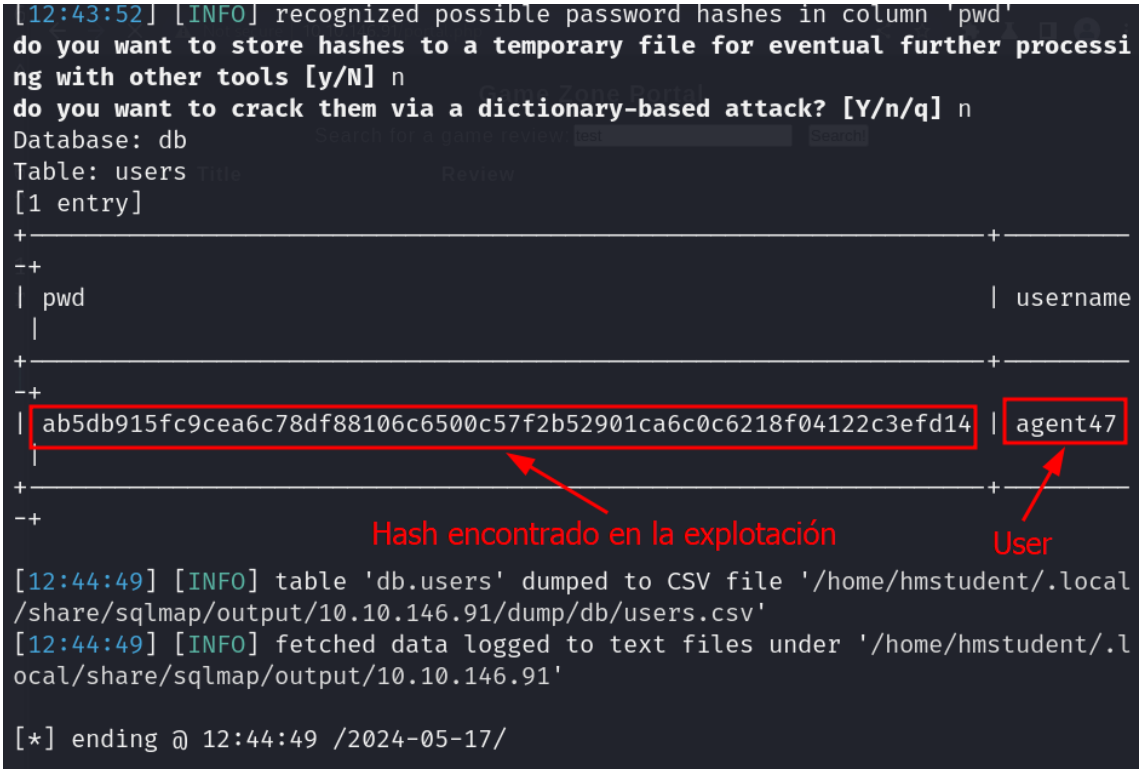
Automatizado

Explotación mediante SQLMap

1. Guardado de la petición interceptada en Burp Suite:



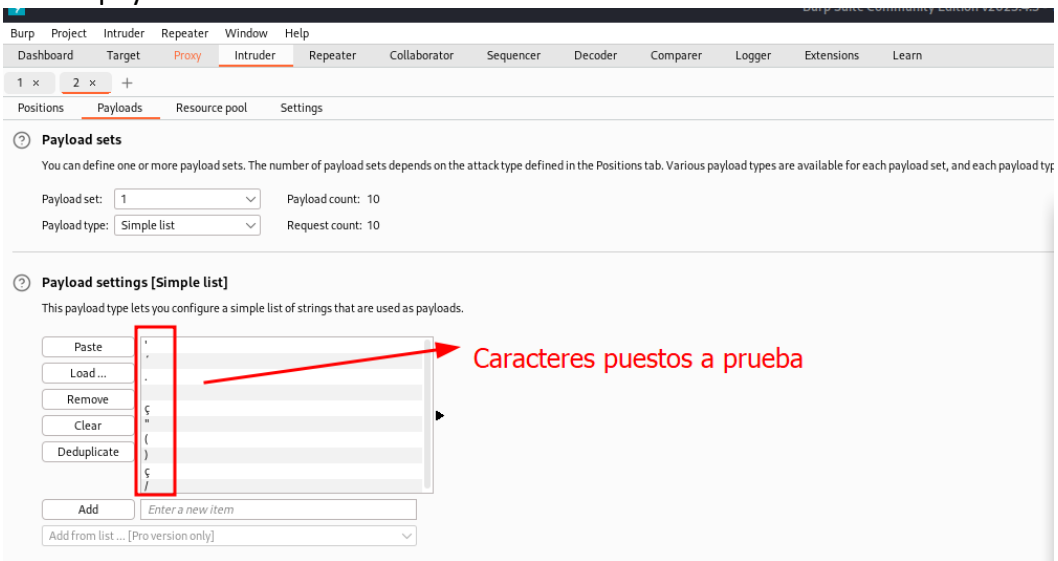
2. Explotación mediante SQLMap



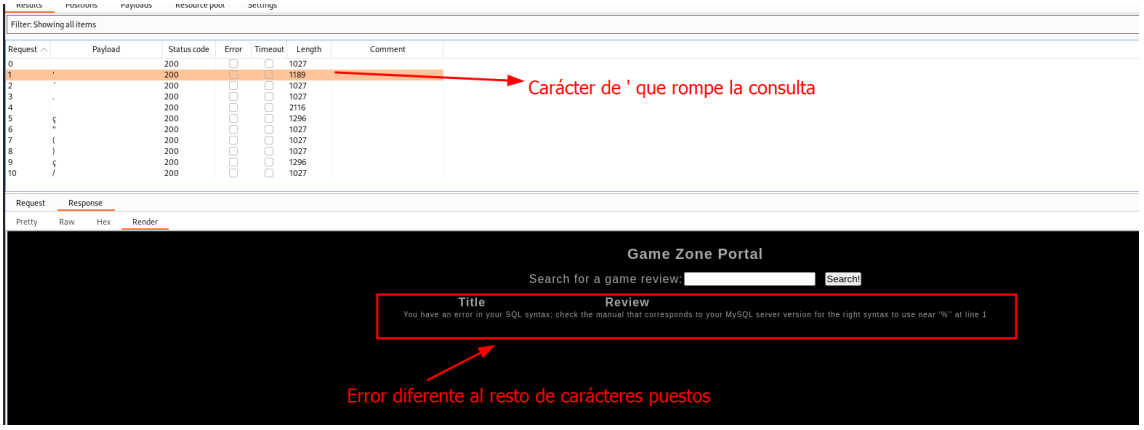
Manual

Explotación mediante inyección sql con Burp Suite:

3. Búsqueda de caracteres que rompan con consulta sql mediante la creación de un payload:

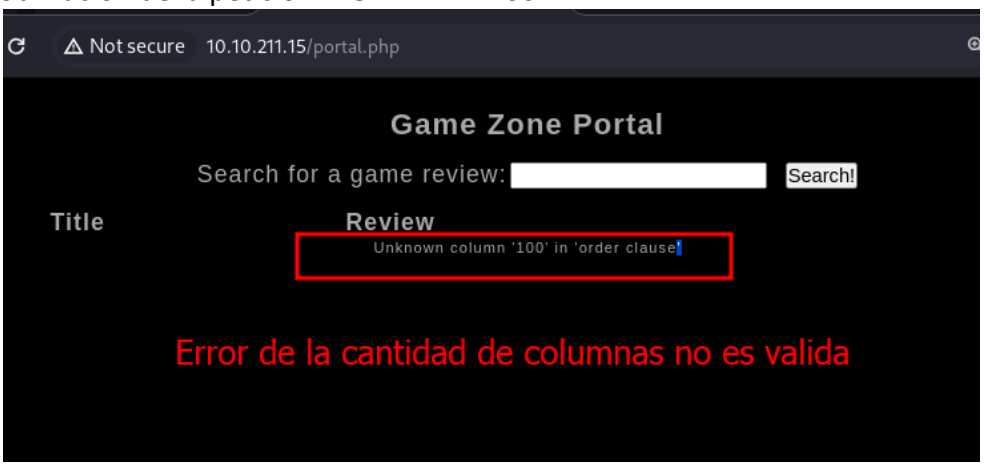


4. Localización de carácter especial que cumple la función de romper la consulta:

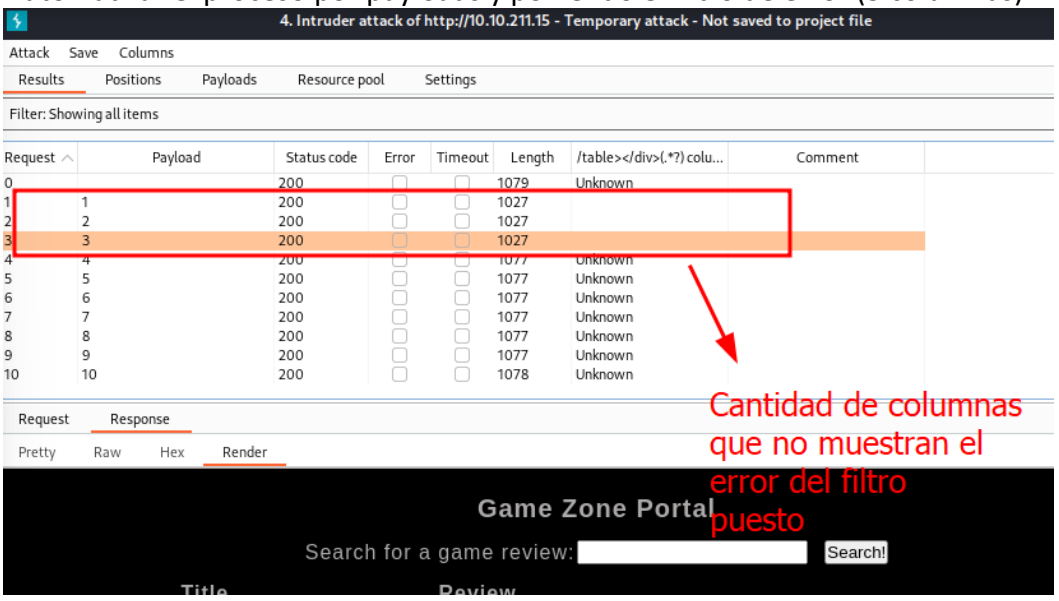


5. Saber la cantidad de columnas que hay en la BD:

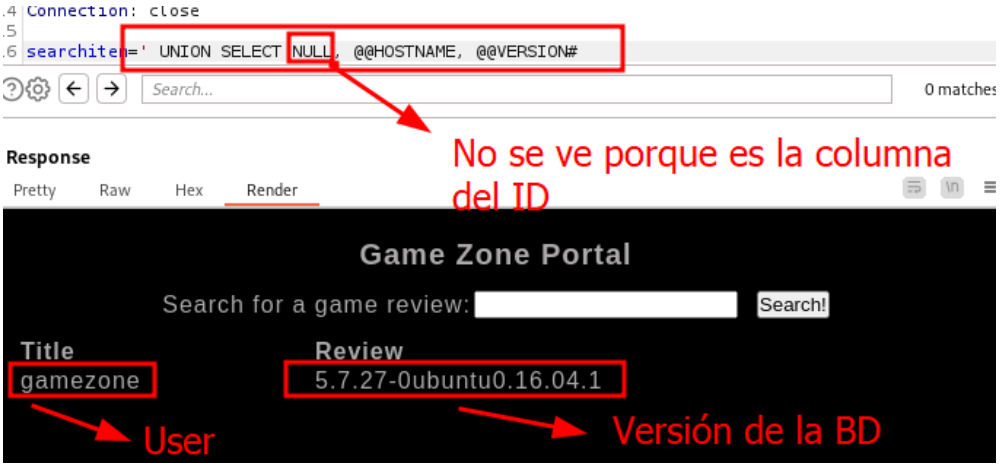
- Utilización de la petición "' ORDER BY 100#"



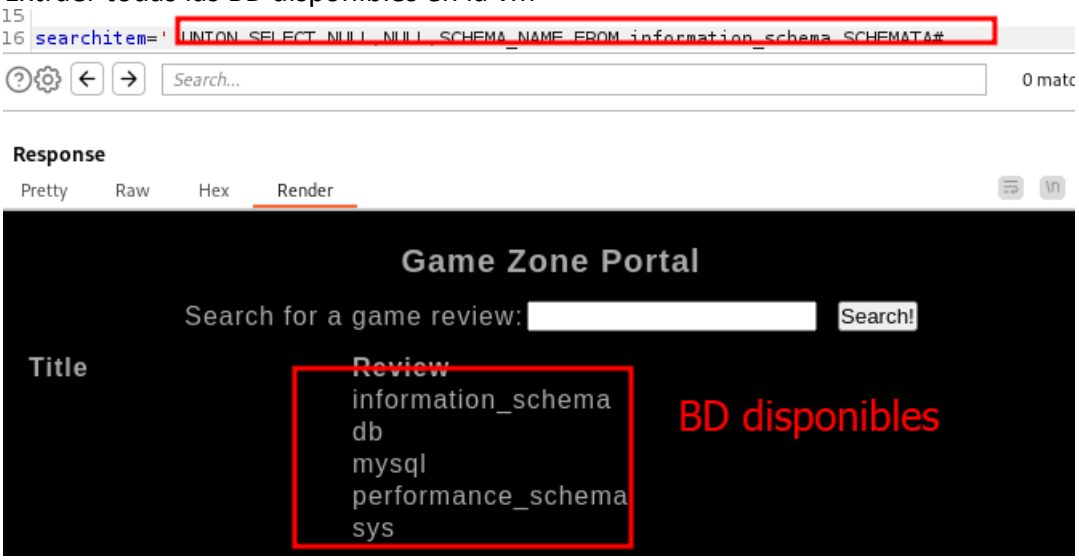
- Automatizar el proceso por payloads y poniendo el filtro de error (3 columnas):



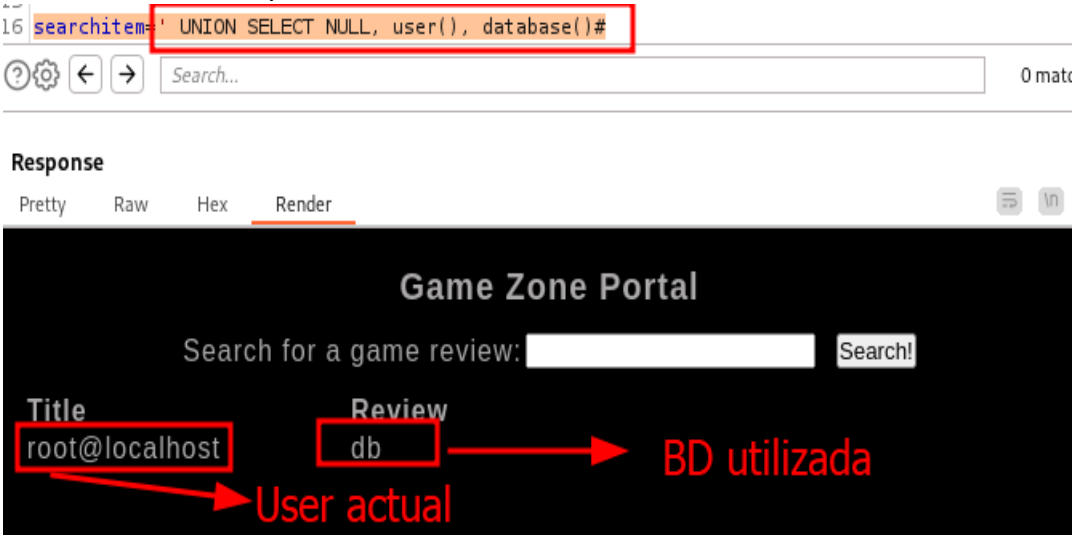
6. Saber la versión de la BD que tiene corriendo y el usuario:



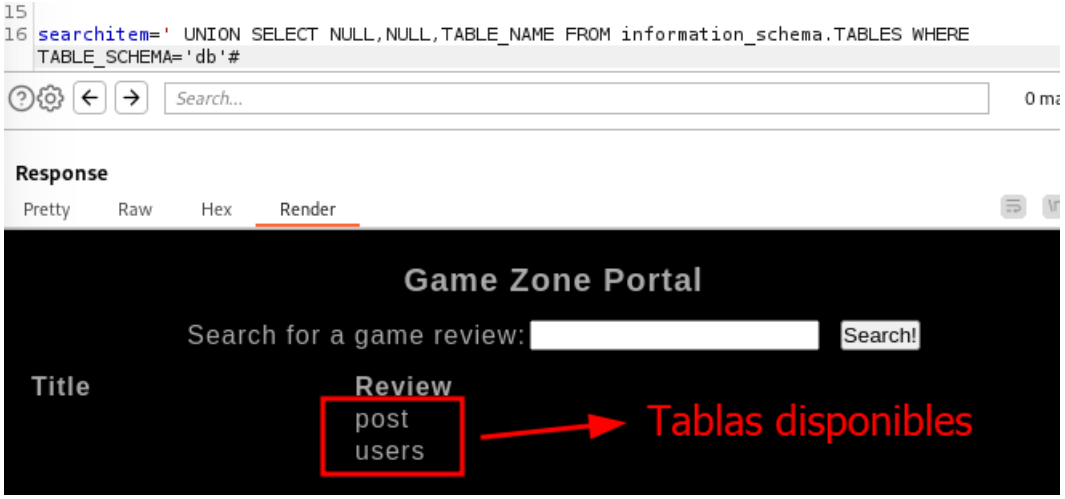
7. Extraer todas las BD disponibles en la vm



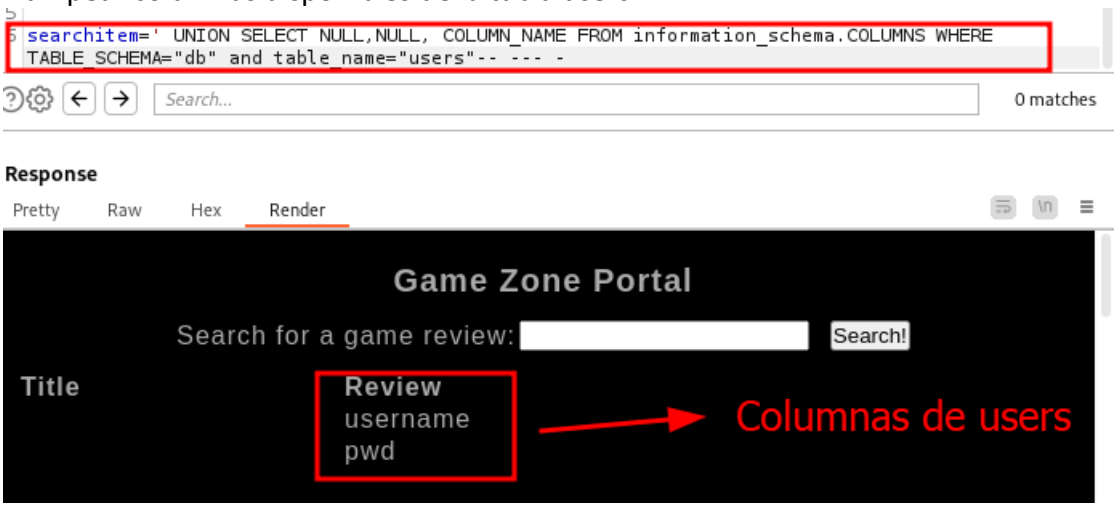
8. Ver BD utilizada y usuario actual:



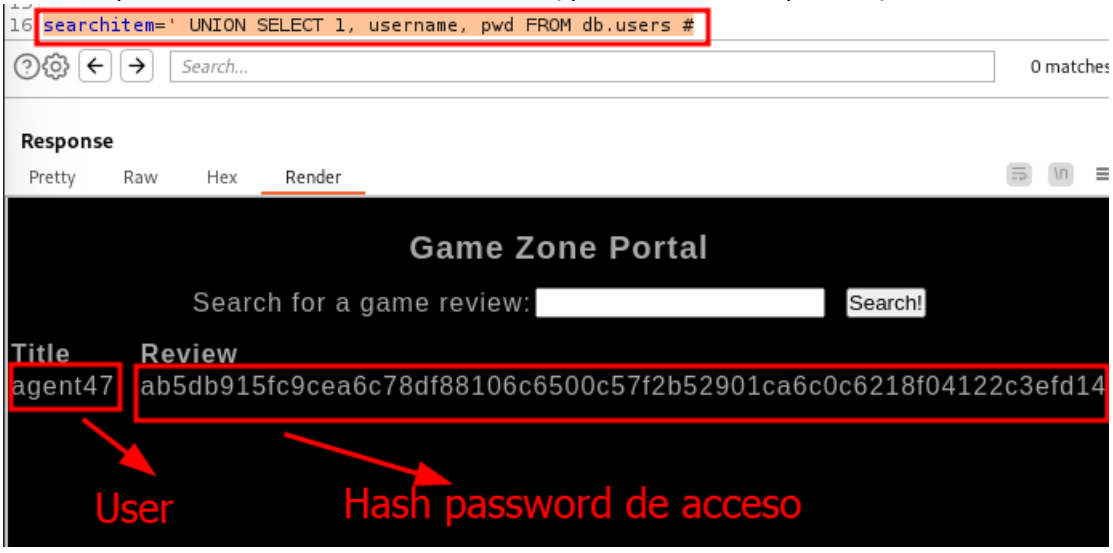
9. Enumera las tablas de la base db:



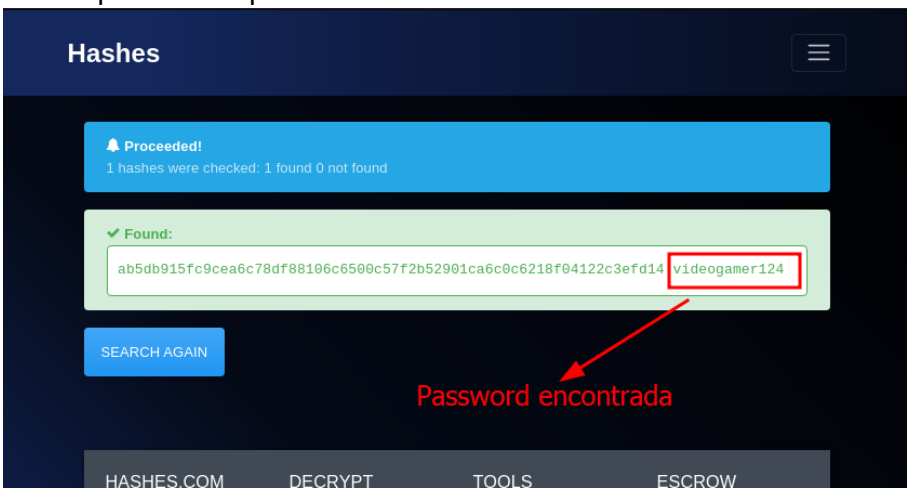
10. Dumpear columnas disponibles de la tabla users:



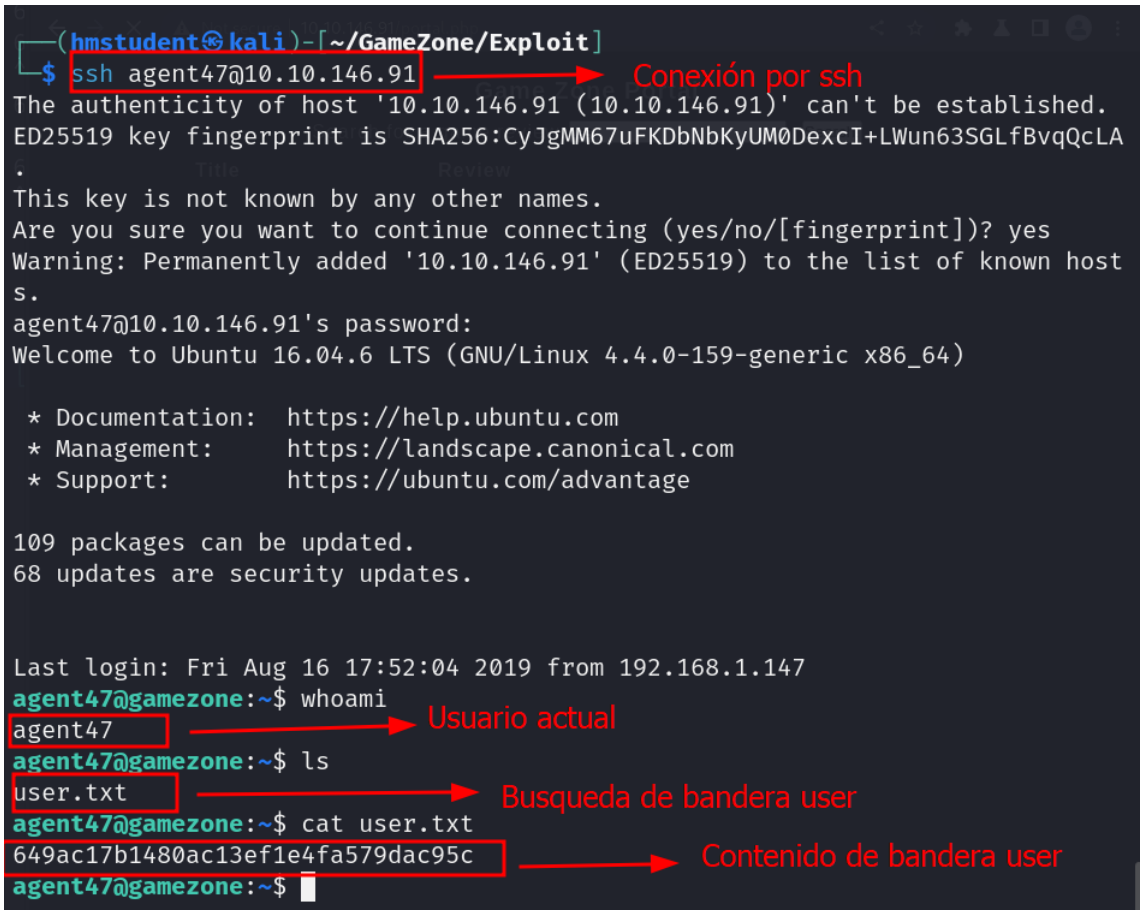
11. Búsqueda de datos de acceso de la bd(para conectarse por ssh):



12. Desencriptación del password online:



Acceso mediante ssh con la contraseña descifrada y búsqueda de bandera user:



Exponer servicios con túneles SSH inversos

1. Ver puertos abiertos desde la sesión de agent47:

```
agent47@gamezone:~$ netstat -lnt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

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

tcp6       0      0 :::80                   :::*                    LISTEN

tcp6       0      0 :::22                   :::*                    LISTEN
```

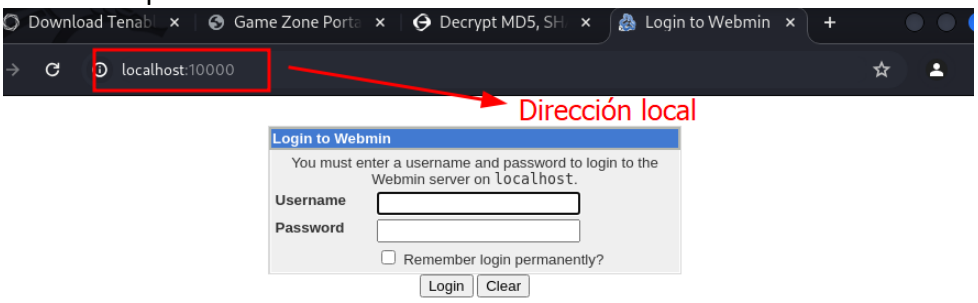
2. Apuntado del puerto 10000 de la maquina victima en mi maquina local (local port forwarding):

```
┌──(hmstudent㉿kali)-[~/GameZone/Exploit]
└─$ ssh -L 10000:localhost:10000 agent47@10.10.146.91
agent47@10.10.146.91's password:
Permission denied, please try again.
agent47@10.10.146.91'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.
```

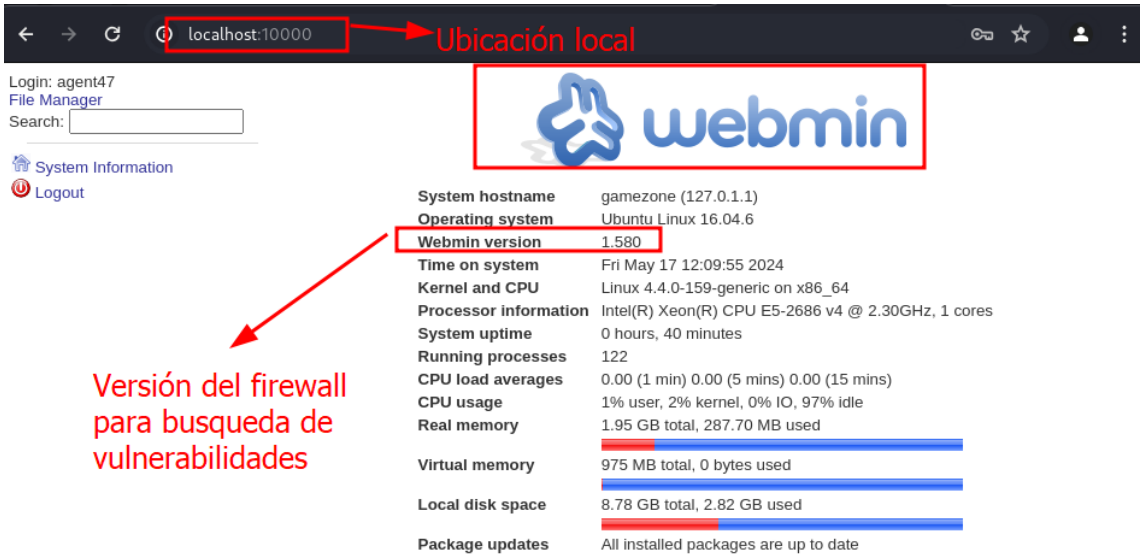
Creación del puente

3. Acceder localmente al puerto para ver el firewall y versión que tiene:

- Acceso al puerto 10000:

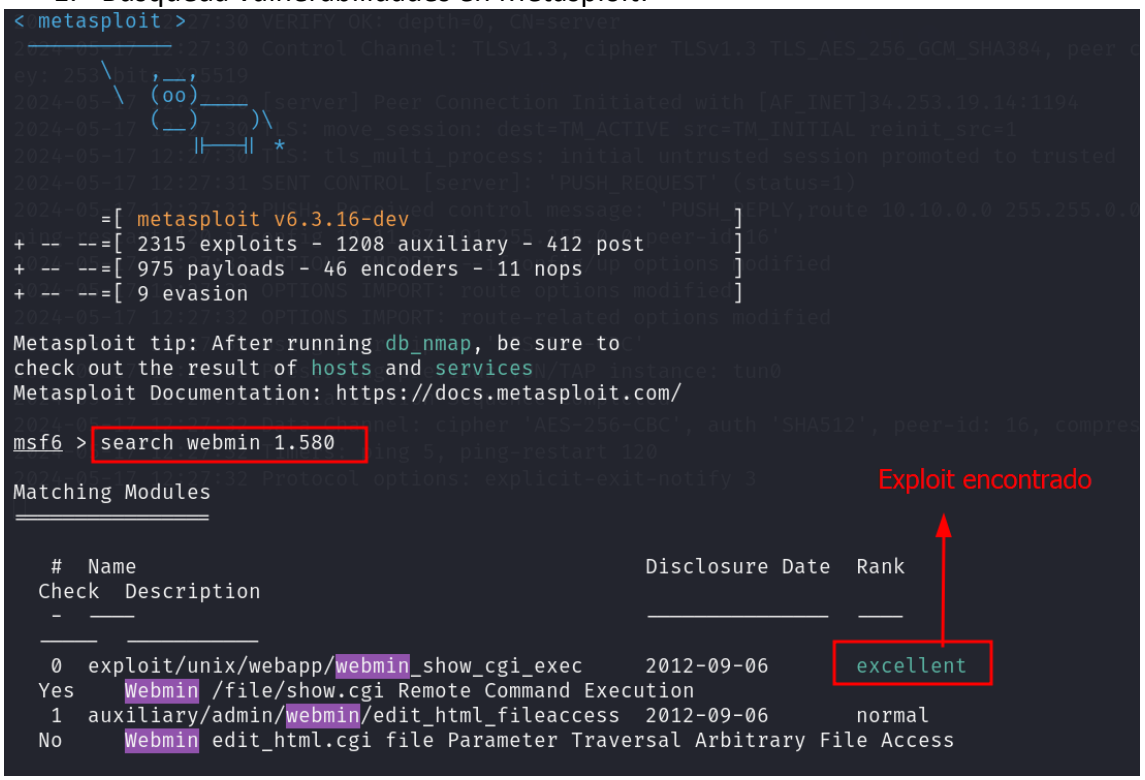


- Iniciado sesión con los datos anteriormente encontrados:

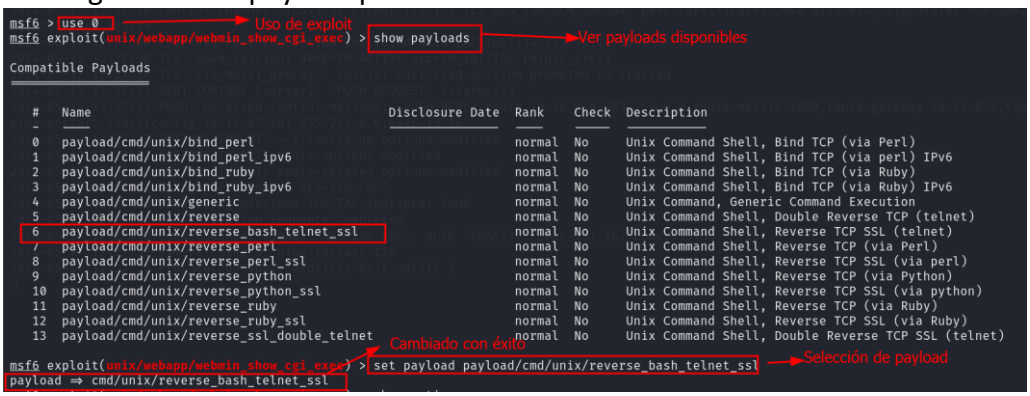


Escalado de privilegios de admin mediante vulnerabilidad

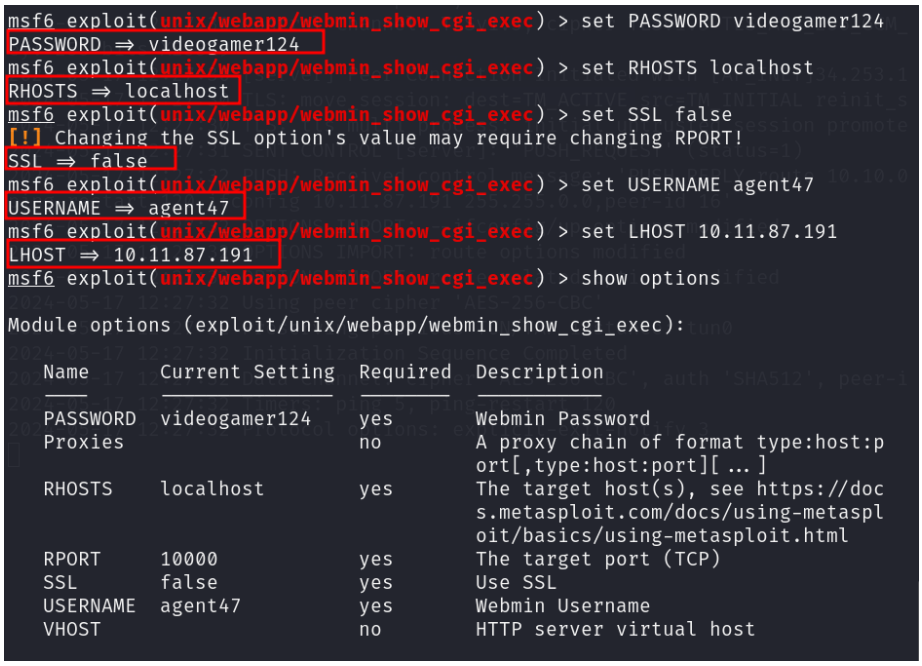
1. Búsqueda vulnerabilidades en Metasploit:



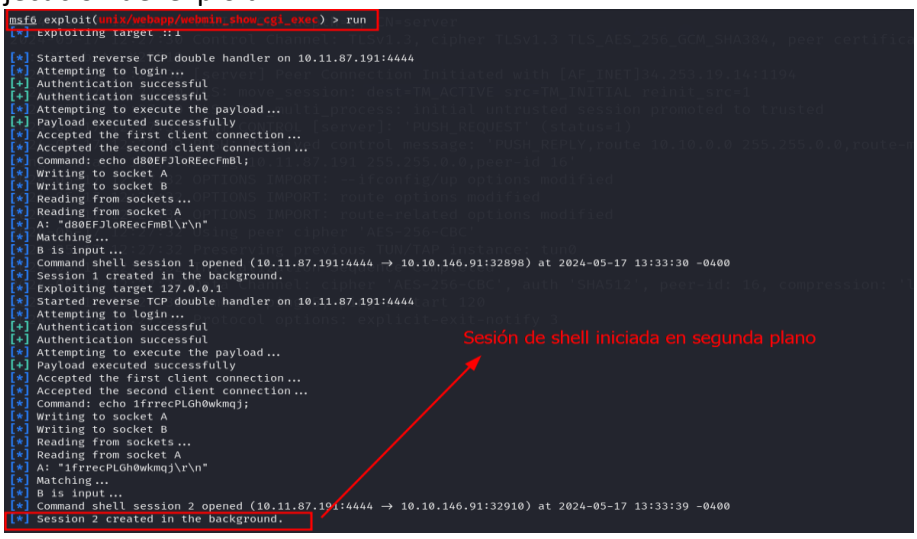
2. Configuración de payload para reverse shell



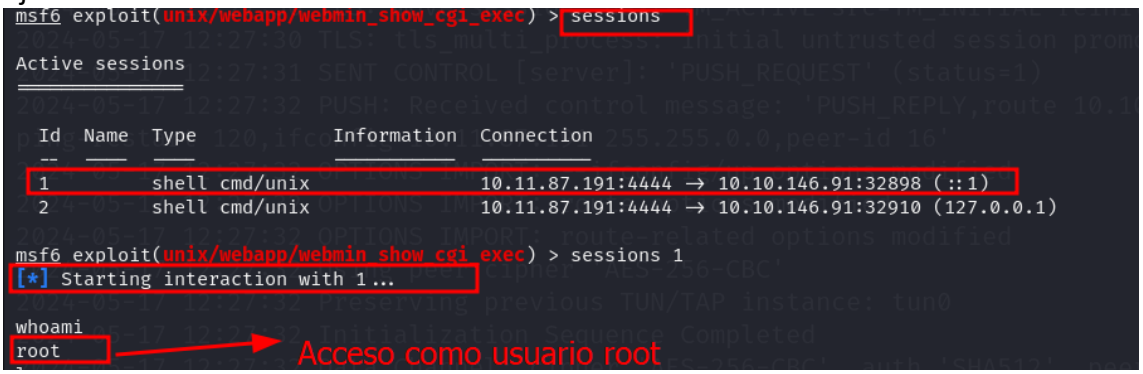
3. Configuración de parámetros del exploit:



4. Ejecución del exploit:



5. Ejecución de sesión root:



6. Búsqueda de la bandera root:

4. Escalación de privilegios si/no

Si: Método de escalada

5. Banderas

Bandera1	649ac17b1480ac13ef1e4fa579dac95c
Bandera2	a4b945830144bdd71908d12d902adeee

6. Herramientas usadas

Nmap	Para ver puertos y versiones
Gobuster	Para ver ficheros disponibles
Metasploit	Para buscar vulnerabilidades por versión
Whatweb	Para ver la tecnología de la página
hashes.com	Para desencriptar hash
Comandos sql	Para romper la petición e inyectar comandos
Burp Suite	Para interceptar petición a la página y automatizar pruebas de sqli

7. EXTRA Opcional

Herramientas usadas

Nesus	Para ver vulnerabilidades

FFuF	Para ver ficheros disponibles
SQLMap	Automatizar inyección sql

Técnicas:
Sql inyection: Para poder acceder a información del sistema mediante la web con conexión a la BD
Local port forwarding: Para acceder a puerto de la vm de manera local (Hacer puente)
Reverse Shell: Para acceder como administrador mediante exploit

8. Hallazgos

8.1 Inyección SQL

Descripción	Se encontró una vulnerabilidad de inyección SQL en la página de inicio de sesión de la aplicación web.
Impacto	Permite a un atacante acceder a la base de datos subyacente, exponiendo información sensible como credenciales de usuarios.
Evidencia	Al ingresar ' OR '1'='1' -- en el campo de contraseña, se obtuvo acceso a la cuenta administrativa.
Recomendación	Implementar consultas preparadas y procedimientos almacenados para prevenir la inyección SQL.
Prioridad	Alta

8.2 Configuración Incorrecta de Permisos

Descripción	Archivos sensibles como /etc/passwd y /etc/shadow tenían permisos incorrectos que permitían su edición por usuarios no privilegiados.
Impacto	Un usuario sin privilegios pudo escalar a nivel root modificando archivos críticos del sistema.
Evidencia	Un usuario común pudo editar el archivo /etc/passwd para añadir una cuenta con privilegios de root.
Recomendación	Revisar y aplicar los permisos mínimos

	necesarios a archivos sensibles.
Prioridad	Alta

8.3 Explotación de Servicios Web

Descripción	Archivos sensibles como /etc/passwd y /etc/shadow tenían permisos incorrectos que permitían su edición por usuarios no privilegiados.
Impacto	La exposición de estos directorios podría permitir la filtración de información sensible y proporcionar vectores adicionales para ataques.
Evidencia	La exploración con Gobuster mostró varios directorios accesibles sin autenticación.
Recomendación	Proteger directorios sensibles con autenticación y restringir el acceso a archivos innecesarios.
Prioridad	Media

8.4 Falta de actualizaciones de seguridad

Descripción	Varios servicios y aplicaciones no estaban actualizados, dejando el sistema vulnerable a exploits conocidos.
Impacto	Exposición a vulnerabilidades conocidas que podrían ser explotadas por atacantes.
Evidencia	El escaneo reveló versiones antiguas de Apache y PHP con vulnerabilidades conocidas.
Recomendación	Establecer un proceso de actualización regular para todos los componentes del sistema.
Prioridad	Media

9. Recomendaciones Detalladas

- **Corregir Vulnerabilidades:** Implementar parches para la inyección SQL y asegurar configuraciones de permisos correctas.

- **Monitoreo y Actualización:** Establecer un sistema de monitoreo continuo y mantener todos los software actualizados.

- **Seguridad de Contraseñas:** Usar contraseñas fuertes y únicas, y almacenar credenciales de manera segura.

- **Auditorías Regulares:** Realizar auditorías de seguridad periódicas para identificar y mitigar nuevas vulnerabilidades.

10. Conclusión

La evaluación de la VM "GameZone" reveló varias vulnerabilidades críticas que deben ser abordadas de inmediato para proteger el sistema. Implementar las recomendaciones ayudará a mitigar los riesgos identificados y fortalecerá la seguridad general del entorno. Es crucial mantener un enfoque proactivo en la gestión de la seguridad para prevenir futuros incidentes.