



## PROYECTO FINAL

### FASE 1: Reconocimiento y recolección de evidencias

**OBJETIVO:** Llevar a cabo un análisis forense para bloquear el exploit, corregir la vulnerabilidad y evitar que el atacante escale.

Se encontró un archivo **README.TXT** donde dentro del directorio **/var/log** y se observó lo siguiente:

```
1 You are looking for the traditional text log files in /var/log, and they are
2 gone?
3
4 Here's an explanation on what's going on:
5
6 You are running a systemd-based OS where traditional syslog has been replaced
7 with the Journal. The journal stores the same (and more) information as classic
8 syslog. To make use of the journal and access the collected log data simply
9 invoke "journalctl", which will output the logs in the identical text-based
10 format the syslog files in /var/log used to be. For further details, please
11 refer to journalctl(1).
12
13 Alternatively, consider installing one of the traditional syslog
14 implementations available for your distribution, which will generate the
15 classic log files for you. Syslog implementations such as syslog-ng or rsyslog
16 may be installed side-by-side with the journal and will continue to function
17 the way they always did.
18
19 Thank you!
20|
21 Further reading:
22     man:journalctl(1)
23     man:systemd-journald.service(8)
24     man:journald.conf(5)
25     https://0pointer.de/blog/projects/the-journal.html
```

se utilizó comando Journalctl -u ssh y se detectó que el 08/10/2024 el usuario malicioso se conectó a través del servicio SSH (PUERTO 22) con IP 192.168.0.134 PUERTO 45623 SSH2

```
Oct 08 16:48:02 debian sshd[555]: Server listening on 0.0.0.0 port 22.
Oct 08 16:48:02 debian sshd[555]: Server listening on :: port 22.
Oct 08 16:48:02 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:28:37 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 08 17:28:38 debian sshd[550]: Server listening on 0.0.0.0 port 22.
Oct 08 17:28:38 debian sshd[550]: Server listening on :: port 22.
Oct 08 17:28:38 debian sshd[550]: Started ssh.service - OpenBSD Secure Shell server.
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:40:59 debian sshd[1650]: pam_env(sshd:session): deprecated reading of user environment enabled
-- Boot ae175a3b4a684a8b8d98a103e055d944 --
Mar 21 14:35:17 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Mar 21 14:35:17 debian sshd[591]: Server listening on 0.0.0.0 port 22.
Mar 21 14:35:17 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Mar 21 14:35:17 debian sshd[591]: Server listening on :: port 22.
Mar 21 15:06:05 debian systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
Mar 21 15:06:05 debian sshd[591]: Received signal 15; terminating.
Mar 21 15:06:05 debian systemd[1]: ssh.service: Deactivated successfully.
Mar 21 15:06:05 debian systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
-- Boot 832cd6f8b91a44679e04447421a06be4 --
Mar 21 15:06:15 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Mar 21 15:06:15 debian sshd[568]: Server listening on 0.0.0.0 port 22.
Mar 21 15:06:15 debian sshd[568]: Server listening on :: port 22.
Mar 21 15:06:15 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
-- Root 921f573203c117h5285e76r127e9e087 --
```

Se utilizó el siguiente comando para un escaneo completo de Malwares y Rootkits con el programa rkhunter

/usr/bin/lwp-request	[ Warning ]
/usr/bin/bsd-mailx	[ OK ]
/usr/bin/dash	[ OK ]
/usr/bin/x86_64-linux-gnu-size	[ OK ]
/usr/bin/x86_64-linux-gnu-strings	[ OK ]
/usr/bin/inetutils-telnet	[ OK ]
/usr/bin/which.debianutils	[ OK ]
/usr/lib/systemd/systemd	[ OK ]

Performing malware checks

Checking running processes for suspicious files	[ None found ]
Checking for login backdoors	[ None found ]
Checking for sniffer log files	[ None found ]
Checking for suspicious directories	[ None found ]
Checking for suspicious (large) shared memory segments	[ Warning ]
Checking for Apache backdoor	[ Not found ]

```
Performing system configuration file checks
  Checking for an SSH configuration file [ Found ]
  Checking if SSH root access is allowed [ Warning ]
  Checking if SSH protocol v1 is allowed [ Not set ]
  Checking for other suspicious configuration settings [ None found ]
  Checking for a running system logging daemon [ Found ]
  Checking for a system logging configuration file [ Found ]
```

```
System checks summary
=====
```

```
File properties checks...
```

```
  Files checked: 144
  Suspect files: 1
```

```
Rootkit checks...
```

```
  Rootkits checked : 497
  Possible rootkits: 7
```

```
Applications checks...
```

```
  All checks skipped
```

```
The system checks took: 1 minute and 7 seconds
```

```
All results have been written to the log file: /var/log/rkhunter.log
```

```
One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

## IDENTIFICACION DE ARCHIVOS Y PROCESOS SOSPECHOSOS

Se utilizo comando ps aux --sort=-%cpu | head -10 para ejecutar los procesos con los siguientes resultados:

```
debian@debian:/$ ps aux --sort=-%cpu | head -10
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
debian    2136  2.5  4.7 484496 94712 ?        S1   13:40   4:47 /usr/bin/python3 /usr/bin/orca
root     1629  1.2 10.9 539672 219628 tty7    Ssl+ 13:40   2:21 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/lightdm/root/
:0 -nolisten tcp vt7 -novtswitch
debian    2367  0.8  1.0 730636 20844 ?        Ssl  13:40   1:36 /usr/bin/speech-dispatcher --spawn --communication-method unix
_socket --socket-path /run/user/1000/speech-dispatcher/speechd.sock --port 6560
debian    1877  0.6  1.6 1703280 34036 ?        S<sl 13:40   1:15 /usr/bin/pulseaudio --daemonize=no --log-target=journal
debian    2066  0.4  4.8 1012604 98624 ?        S1   13:40   0:52 /usr/bin/caja
debian    2832  0.4  2.5 691140 52032 ?        S1   13:45   0:45 mate-terminal
debian    1961  0.2  0.1 282896 2280 ?        S1   13:40   0:30 /usr/bin/VBoxClient --draganddrop
debian    1990  0.1  0.5 15216 10872 ?        S    13:40   0:17 /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2
/accessibility.conf --nofork --print-address 11 --address=unix:path=/run/user/1000/at-spi/bus_0
debian    2315  0.1  0.6 108996 12568 ?        S1   13:40   0:13 /usr/lib/speech-dispatcher-modules/sd_espeak-ng /etc/speech-di
spatcher/modules/espeak-ng.conf
```

Se puede observar que el uso del procesador y la memoria ram sobre todo ha requerido mas que los otros procesos en ejecución por lo tanto lo hace sospechoso de que el usuario malicioso lo haya utilizado.

```
debian@debian:/$ sudo lsof -i -n -P
[sudo] password for debian:
COMMAND      PID      USER      FD  TYPE DEVICE SIZE/OFF NODE NAME
avahi-dae    506      avahi     12u  IPv4  15241      0t0  UDP *:5353
avahi-dae    506      avahi     13u  IPv6  15242      0t0  UDP *:5353
avahi-dae    506      avahi     14u  IPv4  15243      0t0  UDP *:41924
avahi-dae    506      avahi     15u  IPv6  15244      0t0  UDP *:38433
NetworkMa    521      root      26u  IPv4  66654      0t0  UDP 10.0.2.11:68->10.0.2.3:67
vsftpd      565      root      3u   IPv6  15421      0t0  TCP  *:21 (LISTEN)
sshd        586      root      3u   IPv4  15511      0t0  TCP  *:22 (LISTEN)
sshd        586      root      4u   IPv6  15524      0t0  TCP  *:22 (LISTEN)
apache2     651      root      4u   IPv6  15566      0t0  TCP  *:80 (LISTEN)
mariadb     660      mysql     17u  IPv4  15647      0t0  TCP 127.0.0.1:3306 (LISTEN)
apache2    11091     www-data   4u   IPv6  15566      0t0  TCP  *:80 (LISTEN)
cupsd       11093     root      6u   IPv6  65507      0t0  TCP  [::1]:631 (LISTEN)
cupsd       11093     root      7u   IPv4  65508      0t0  TCP 127.0.0.1:631 (LISTEN)
apache2     11131     www-data   4u   IPv6  15566      0t0  TCP  *:80 (LISTEN)
apache2     11132     www-data   4u   IPv6  15566      0t0  TCP  *:80 (LISTEN)
apache2     11133     www-data   4u   IPv6  15566      0t0  TCP  *:80 (LISTEN)
apache2     11134     www-data   4u   IPv6  15566      0t0  TCP  *:80 (LISTEN)
exim4      13253  Debian-exim  4u   IPv4  78733      0t0  TCP 127.0.0.1:25 (LISTEN)
exim4      13253  Debian-exim  5u   IPv6  78734      0t0  TCP  [::1]:25 (LISTEN)
```

Para archivos recientemente modificados se utilizó el siguiente comando:  
**sudo find / -type f -mtime -2 2>/dev/null**

```
\var/log/wtmp
\var/log/apache2/error.log.1
\var/log/apache2/error.log
\var/log/apache2/error.log.2.gz
\var/log/boot.log
\var/log/Xorg.0.log
\var/log/alternatives.log
\var/log/fontconfig.log
\var/log/lightdm/seat0-greeter.log.old
\var/log/lightdm/lightdm.log
\var/log/lightdm/seat0-greeter.log
\var/log/lightdm/x-0.log.old
\var/log/lightdm/lightdm.log.old
\var/log/lightdm/x-0.log
\var/log/exim4/mainlog
\var/log/vboxadd-uninstall.log
\var/log/vboxadd-setup.log.3
\var/log/apt/eipp.log.xz
\var/log/apt/history.log
\var/log/apt/term.log
\var/log/btmp
\var/log/boot.log.1
\var/log/irkhunter.log
\var/log/Xorg.0.log.old
\var/log/journal/41b6de202c3f48fd4a490411748aaaff/system.journal
\var/log/journal/41b6de202c3f48fd4a490411748aaaff/system@000631313a12166b-f766d3f1a4484f89.journal~
\var/log/journal/41b6de202c3f48fd4a490411748aaaff/user-1000@0006313118cb4412-90689cbf1876f180.journal~
\var/log/journal/41b6de202c3f48fd4a490411748aaaff/system@0006313117afe67c-1e2d233646f28969.journal~
\var/log/journal/41b6de202c3f48fd4a490411748aaaff/system@00063130ecb9e2ed-96f158a769053858.journal~
\var/log/journal/41b6de202c3f48fd4a490411748aaaff/user-1000.journal
```

```
/var/log/cups/access_log.1
/var/log/cups/access_log
/var/log/cups/access_log.2.gz
/var/log/cups/error_log
/var/log/vboxadd-setup.log
/var/log/vboxadd-install.log
/var/log/vboxadd-setup.log.2
/var/log/dpkg.log
/var/log/vboxadd-setup.log.4
/var/log/vboxadd-setup.log.1
```

## LISTADO DE PUERTOS ABIERTOS

```
debian@debian:/$ sudo netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 127.0.0.1:3306          0.0.0.0:*
tcp      0      0 127.0.0.1:25          0.0.0.0:*
tcp      0      0 0.0.0.0:22          0.0.0.0:*
tcp      0      0 127.0.0.1:631          0.0.0.0:*
tcp6     0      0 ::1:25                ::*:*
tcp6     0      0 ::22                 ::*:*
tcp6     0      0 ::21                 ::*:*
tcp6     0      0 ::1:631              ::*:*
tcp6     0      0 ::80                 ::*:*
udp      0      0 0.0.0.0:5353          0.0.0.0:*
udp      0      0 0.0.0.0:41924         0.0.0.0:*
udp6     0      0 ::5353              ::*:*
udp6     0      0 ::38433             ::*:*
```

## CORRECCION Y REFUERZO DE SEGURIDAD

Se modifco la configuración de SSH (/etc/ssh/sshd\_config)

con nano denegando el permiso RootLogin:

```
#RekeyLimit default none
# Logging
#SyslogFacility AUTH
#LogLevel INFO
# Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#PubkeyAuthentication yes
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
```

Luego reiniciamos el servicio con el siguiente comando:

sudo systemctl restart sshd.

Se implementaron reglas estrictas en UFW:

```
sudo ufw default deny incoming
```

```
sudo ufw allow OpenSSH
```

```
sudo ufw enable
```

```
debian@debian:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

```
debian@debian:~$ sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
```

```
debian@debian:~$ sudo ufw enable
Firewall is active and enabled on system startup
debian@debian:~$
```

Por ultimo se realizo cambio de contraseñas y claves de acceso:

```
root@debian:/home/debian# sudo cat /etc/passwd | grep usuario
root@debian:/home/debian# sudo useradd -m usuario
root@debian:/home/debian# sudo chmod 640 /etc/shadow
sudo chown root:shadow /etc/shadow
root@debian:/home/debian# sudo passwd usuario
New password:
Retype new password:
passwd: password updated successfully
root@debian:/home/debian#
```

**CONTRASEÑA CAMBIADA: 4geeks123**

Se verifico con el siguiente comando `sudo cat /etc/vsftpd.conf | grep -v '^#'` que el servidor FTP estaba vulnerable.

```
debian@debian:/etc/ssh$ sudo cat /etc/vsftpd.conf | grep -v "^#"
[sudo] password for debian:
listen=NO
listen_ipv6=YES
anonymous_enable=YES
local_enable=YES
write_enable=YES
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
```

Se modifico el archivo cambiando los valores en anonymous\_enable=NO y en ssl\_enable=NO

luego se guardo dicha configuración y se reinició el servicio con comando sudo systemctl restart vsftpd:

#### PERMISOS EN WP-CONFIG.PHP

```
debian@debian:/$ sudo ls -l /var/www/html/wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 12:02 /var/www/html/wp-config.php
debian@debian:/$ sudo chmod 600 /var/www/html/wp-config.php
debian@debian:/$ sudo ls -l /var/www/html/wp-config.php
-rw----- 1 www-data www-data 3017 Sep 30 12:02 /var/www/html/wp-config.php
```

#### Hallazgos:

- Se hallaron procesos desconocidos corriendo bajo root.
- Se encontraron archivos sospechosos en /var/log

### Informe de Medidas Tomadas y Recomendaciones

#### Resumen de Acciones Realizadas

- Se identificó acceso no autorizado a través de SSH.
- Se eliminaron procesos maliciosos y archivos sospechosos.

- Se bloquearon puertos utilizados por el atacante y también los que fueran innecesarios que estén abiertos
- Se reforzó la seguridad de SSH y el firewall con failban2
- Se realizaron cambios de contraseñas y se actualizaron paquetes.

## Recomendaciones para Prevenir Futuros Ataques

- Implementar autenticación de doble factor (2FA) para SSH.
- Configurar monitoreo activo con herramientas como fail2ban y auditd.
- Realizar auditorías de seguridad periódicas.
- Usar listas blancas para accesos a SSH.
- Mantener el sistema actualizado y aplicar parches de seguridad de inmediato.

**Estado Actual: Seguridad reforzada, sistema estable.**

## Verificación de la configuración de MySQL

```
Database changed
MariaDB [mysql]> SELECT user, host, authentication_string FROM mysql.user;
+-----+-----+-----+
| User      | Host      | authentication_string |
+-----+-----+-----+
| mariadb.sys | localhost |                   |
| root       | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| mysql      | localhost | invalid             |
| wordpressuser | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| user       | localhost | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+-----+-----+-----+
```

## Análisis de Usuarios y Contraseñas en MySQL (MariaDB)

En la consulta realizada, los siguientes usuarios tienen contraseñas almacenadas como **hashes** en la. Para determinar si una contraseña es débil en la columna `authentication_string`. Para determinar si una contraseña es débil, podemos comparar los hashes con bases de datos conocidas de contraseñas vulnerables.

### 1. Identificación de Contraseñas Débiles

Algunos hashes son comunes y corresponden a contraseñas débiles en bases de datos filtradas. Analizamos los usuarios:

- **Débil →root(**  
\*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9)  
● **Débil**, que es extremadamente insegura→ Este hash corresponde a la contraseña "123456", que es extremadamente insegura.
- **wordpressuser(**  
\*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9)  
● **Débil** → Usa el mismo hash que , por lo que su contraseña también es insegura→ Usa el mismo hash que root, por lo que su contraseña también es "123456".
- **user(** \*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19)  
● **Débil** → Este hash corresponde a , otra contraseña extremadamente insegura→ Este hash corresponde a "password", otra contraseña extremadamente insegura.
- **mysql→ "invalid"**  
⚠ **Possiblemente corrupto o no configurado correctamente** . Esto puede significar que este usuario no tiene una contraseña establecida correctamente y puede representar un riesgo.
- **mariadb.sys**  
○ **Sin información de autenticación** . Este usuario del sistema no debería usarse para autenticación normal.

## 2. Soluciones y Buenas Prácticas

Para fortalecer la seguridad, sigue estas recomendaciones:

### 2.1. Actualizar las contraseñas a valores seguros

Genera contraseñas seguras (mínimo 12 caracteres, combinando letras, números y símbolos) y cambia las credenciales:

```
ALTER USER 'root'@'localhost' IDENTIFIED BY 'S3gur@P4ssw0rd!';
ALTER USER 'wordpressuser'@'localhost' IDENTIFIED BY 'WpS3gura!2024';
ALTER USER 'user'@'localhost' IDENTIFIED BY 'Us3r_F0rt!fied';
```

Si el usuario mysql no se usa, eliminarlo:

```
DROP USER 'mysql'@'localhost';
```

## 2.2. Implementar Políticas de Contraseñas Seguras

Habilita el **complemento de validación de contraseñas** en MariaDB:

```
INSTALL PLUGIN validate_password SONAME 'validate_password.so';
```

**Configure la política para exigir contraseñas segura:**

```
SET GLOBAL validate_password_policy = STRONG;
```

## 2.3. Restringir Accesos No Necesarios

- **Limitar accesos remotos** : Si root no necesita acceso externo, asegúrese de que solo pueda autenticarse localmente:

```
UPDATE mysql.user SET host='localhost' WHERE user='root';  
FLUSH PRIVILEGES;
```

- **Eliminar usuarios innecesarios o no utilizados** :

```
DROP USER 'mariadb.sys'@'localhost';
```

## CONCLUSION

**Los usuarios root, wordpressuser y user tienen contraseñas extremadamente débiles y deben cambiarse de inmediato.** Además, se recomienda eliminar usuarios no necesarios y aplicar restricciones de acceso para fortalecer la seguridad de MySQL.

## **FASE 2: Detectar y corregir una vulnerabilidad diferente**

Informe de Explotación y Corrección de Vulnerabilidad

### **1. Objetivo**

El objetivo de este ejercicio es escanear un sistema Debian, detectar una vulnerabilidad distinta a la explotada anteriormente, explotarla y aplicar medidas correctivas para mitigar el riesgo.

## 2. Escaneo del Sistema

Se realizó un escaneo completo del sistema objetivo con Nmap para identificar servicios y vulnerabilidades potenciales.

### Comandos ejecutados:

```
nmap -sV -p- -O 10.0.2.11
```

```
(kali㉿KaliUltimate)-[~]
└─$ nmap -sV -p- -O 10.0.2.11 -oN escaneo_completo.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 11:38 CEST
Nmap scan report for 10.0.2.11
Host is up (0.00045s latency).

Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh          OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.62 ((Debian))
8834/tcp  open  ssl/nessus-xmlrpc?
MAC Address: 08:00:27:EE:95:3F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
nmap -p- -sC -sV -O --script=vulners,vuln 10.0.2.11
```

### 🔍 ¿Qué hace este comando?

- **-sV**: Detecta versiones de servicios.
- **-p-**: Escanea todos los puertos (0-65535).
- **-O**: Intenta identificar el sistema operativo.

Este escaneo es exhaustivo, ya que analiza todos los puertos y obtiene la versión de cada servicio identificado, además de intentar identificar el sistema operativo.

### Resultado del Escaneo:

- **Puertos abiertos:**
  - 21/tcp (ftp) - Servicio: vsftpd 3.0.3
  - 22/tcp (ssh) - Servicio: OpenSSH 9.2p1 (Debian)
  - 80/tcp (http) - Servicio: Apache httpd 2.4.62 (Debian)

- 8834/tcp (ssl/nessus-xmlrpc?) - Servicio desconocido, posiblemente relacionado con Nessus.
- **Sistema Operativo detectado:**
  - Específicamente: Linux 2.6.62

### 3. Identificación de Vulnerabilidad

El servicio Apache detectado ejecuta la versión 2.4.18, la cual permite **Directory Listing** en el directorio /uploads.

**Comando de verificación:**

```
nikto -h http://10.0.2.11
nmap --script http-vuln* -p 80 10.0.2.11
```

**Resultado del escaneo con Nikto:**

- Identificación de archivos expuestos o peligrosos.
- Detecta métodos HTTP permitidos.
- Detección de versiones inseguras o desactualizadas del servidor web.
- Identificación de configuraciones inseguras como Directory Listing.

Nikto detectó que **Apache HTTPD 2.4.62** presenta vulnerabilidades de configuración relacionadas con:

- **Directory Listing activado.**
- **Archivos expuestos potencialmente sensibles.**

**Vulnerabilidad Detectada:**

- **Directory Listing activado:** Permite visualizar el contenido de /var/www/html/uploads/ sin restricciones.

### 4. Explotación de la Vulnerabilidad

Acceso directo al contenido del directorio desde un navegador:

<http://10.0.2.11/uploads/>

## Proyecto Final

Sat, 29 Mar 2025 14:55:26 EDT

**TABLE OF CONTENTS****Vulnerabilities by Host**

- 10.0.2.11

**Vulnerabilities by Host**[Collapse All](#) | [Expand All](#)**10.0.2.11**

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
CRITICAL	9.8	9.4	0.4447	208700	Debian dsa-5788 : firefox-esr - security update

\* indicates the v3.0 score was not available;  
the v2.0 score is shown

[Hide](#)

Esto permite la descarga de archivos confidenciales sin restricciones.

## 5. Corrección de la Vulnerabilidad

Se editó el archivo de configuración de Apache para deshabilitar el Directory Listing y se actualizó la versión del Navegador Firefox, se cerraron puertos innecesarios.



```
(kali㉿Kaliultimate)-[~]
$ nmap -p- -T4 10.0.2.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-02 18:58 CEST
Nmap scan report for 10.0.2.11
Host is up (0.00035s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed  ssh
MAC Address: 08:00:27:EE:95:3F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 90.24 seconds

(kali㉿Kaliultimate)-[~]
$ nmap -p- -sC -sV -O --script=vulners,vuln 10.0.2.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-02 19:02 CEST
Nmap scan report for 10.0.2.11
Host is up (0.00047s latency).
The connection to 10.0.2.11 is taking too long to respond.
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed  ssh
MAC Address: 08:00:27:EE:95:3F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running: Linux 2.6.X, VMware ESX Server 3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.11 cpe:/o:vmware:esx:3.0:2
OS details: Linux 2.6.11, Linux 2.6.18, Linux 2.6.20.6, Linux 2.6.23, Linux 2.6.39, VMware ESX Server 3.0.2
Network Distance: 1 hop
Try Again
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 120.37 seconds
```

## Directorio web Listable:

```
GNU nano 7.2          /etc/apache2/apache2.conf *
<Directory />
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

<Directory /usr/share>
    AllowOverride None
    Options Indexes FollowSymLinks
    Require all granted
</Directory>

<Directory /var/www/>
    Options -Indexes
    AllowOverride None
    Require all granted
</Directory>

#<Directory /srv/>
#    Options Indexes FollowSymLinks
```

## Configuración aplicada:

```
<Directory /var/www/html/
    Options -Indexes
    AllowOverride All
</Directory>
```

## Reinicio del servicio Apache:

```
sudo systemctl restart apache2
```

```
lebian@debian:~$ sudo nano /etc/apache2/apache2.conf
[sudo] password for debian:
lebian@debian:~$ sudo systemctl restart apache2
lebian@debian:~$
```

## Detencion de procesos:

Active Internet connections (only servers)					
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8834	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN
tcp6	0	0	::1:25	:::*	LISTEN
tcp6	0	0	:::8834	:::*	LISTEN
tcp6	0	0	:::21	:::*	LISTEN
tcp6	0	0	::1:631	:::*	LISTEN
udp	0	0	0.0.0.0:5353	0.0.0.0:*	
udp	0	0	0.0.0.0:40605	0.0.0.0:*	
udp6	0	0	:::60532	:::*	
udp6	0	0	:::5353	:::*	

```
debian@debian:~$ sudo systemctl stop mariadb
debian@debian:~$ sudo systemctl stop exim4
debian@debian:~$ sudo systemctl stop cups
debian@debian:~$ sudo systemctl stop vsftpd
debian@debian:~$ sudo systemctl stop nessusd
```

## 6. Conclusión

El sistema presentaba un problema de configuración en Apache que permitía el listado de archivos de un directorio sin protección. Se corrigió mediante la edición de la configuración de Apache, deshabilitando el listado de índices mediante la opción Options -Indexes.

## FASE 3: Plan de respuesta de incidentes y certificación

### Plan de Respuesta a Incidentes Basado en NIST SP 800-61

#### 1. Identificación del Incidente

- **Monitoreo y Detección:** Se utilizan herramientas como fail2ban, auditd y rkhunter para detectar actividades sospechosas.

- **Evidencia del Ataque:**
  - Se identificó un acceso no autorizado por SSH en el puerto 22 desde la IP 192.168.0.134.
  - Procesos sospechosos con alto consumo de CPU detectados con ps aux.
  - Puertos abiertos identificados con nmap.
  - Modificaciones en archivos recientes usando find.

## 2. Contención del Incidente

- **Medidas Inmediatas:**
  - Bloquear la IP atacante con ufw.
  - Deshabilitar acceso root en SSH (/etc/ssh/sshd\_config).
  - Reiniciar servicios afectados (systemctl restart sshd).
  - Cambiar credenciales de acceso (ejemplo: 4geeks123).
- **Restricción de Servicios:**
  - Implementar reglas estrictas de firewall (ufw deny incoming).
  - Deshabilitar Anonymous FTP (anonymous\_enable=NO).
  - Bloquear listado de directorios en Apache (Options -Indexes).

## 3. Erradicación del Incidente

- **Eliminación de archivos sospechosos en /var/log.**
- **Revisión de configuraciones de seguridad en FTP y Apache.**
- **Eliminación de procesos maliciosos identificados.**
- **Actualización de paquetes y parches de seguridad.**

## 4. Recuperación

- **Restauración del sistema:** Verificar la integridad del sistema y restaurar desde un respaldo si es necesario.
- **Verificación de logs** con journalctl para asegurar que no hay más actividad sospechosa.
- **Pruebas de Seguridad** con Nikto y Nmap para verificar correcciones.

## 5. Prevención de Futuros Incidentes

- Implementar autenticación de doble factor (2FA) en SSH.
- Establecer monitoreo activo con herramientas como fail2ban.
- Auditorías de seguridad periódicas.
- Aplicar actualizaciones y parches de seguridad inmediatamente.

# Sistema de Gestión de Seguridad de la Información (SGSI) - ISO 27001

## 1. Análisis de Riesgos

- Identificación de activos críticos como el servidor comprometido.
- Evaluación de amenazas y vulnerabilidades.
- Definición de niveles de impacto y probabilidad de riesgo.

## 2. Definición de Políticas de Seguridad

- **Política de acceso:** Restricción de accesos innecesarios.
- **Política de contraseñas:** Uso de claves seguras y cambios periódicos.
- **Política de respaldo:** Implementación de copias de seguridad automáticas.

## 3. Implementación de Controles de Seguridad

- **Control de Acceso:**
  - Uso de ufw y fail2ban para restringir accesos sospechosos.
  - Configuración de permisos adecuados en wp-config.php.
- **Cifrado de Datos:**
  - Implementación de SSL/TLS en servicios web.
  - Cifrado de archivos sensibles.
- **Monitoreo y Registro:**
  - Uso de auditd para registrar accesos y modificaciones.
  - Configuración de alertas en logs del sistema.

## 4. Plan de Acción y Mejora Continua

- Evaluación de incidentes pasados para fortalecer la seguridad.
- Capacitación al equipo en mejores prácticas de ciberseguridad.
- Simulación de ataques para evaluar la efectividad de las medidas tomadas.

Con estas estrategias, la seguridad del sistema se refuerza, minimizando el riesgo de futuros ataques y asegurando el cumplimiento de la norma ISO 27001.

