PROYECTO FINAL

Fase 1: Corrección de un Hackeo

Análisis forense, identificación de vulnerabilidades explotadas, y bloqueo efectivo del exploit para contener la amenaza.

Fase 2: Nueva Vulnerabilidad

Escaneo del sistema en busca de una vulnerabilidad adicional, explotación controlada, escalado de privilegios, corrección y documentación del proceso.

Fase 3: Plan de Respuesta y Certificación

Diseño de un plan de respuesta a incidentes (NIST), desarrollo de SGSI (ISO 27001) y medidas de prevención de pérdida de datos (DLP).

Vulnerabilidades

Puerto 80 WEB

Vulnerable. WordPress con permisos inseguros y directorios expuestos.

Puerto 22 SSH

Riesgo Alto. Configuración muy debil.

Puerto 21 FTP

Protocolo inseguro y sin uso. Completamente incesario

Identificación de la brecha en archivos importantes .php

```
drwxr-xr-x  3 root     root      4096 Sep 30  2024 ..
-rwxrwxrwx  1 www-data www-data   523 Sep 30  2024 .htaccess
-rwxrwxrwx  1 www-data www-data 10701 Sep 30  2024 index.html
-rwxrwxrwx  1 www-data www-data   405 Feb  6  2020 index.php
-rwxrwxrwx  1 www-data www-data 19915 Dec 31  2023 license.txt
-rwxrwxrwx  1 www-data www-data  7409 Jun 18  2024 readme.html
-rwxrwxrwx  1 www-data www-data  7387 Feb 13  2024 wp-activate.php
drwxrwxrwx  9 www-data www-data  4096 Sep 10  2024 wp-admin
-rwxrwxrwx  1 www-data www-data   351 Feb  6  2020 wp-blog-header.php
-rwxrwxrwx  1 www-data www-data  2323 Jun 14  2023 wp-comments-post.php
-rwxrwxrwx  1 www-data www-data  3017 Sep 30  2024 wp-config.php
drwxrwxrwx  5 www-data www-data  4096 Oct  8  2024 wp-content
-rwxrwxrwx  1 www-data www-data  5638 May 30  2023 wp-cron.php
drwxrwxrwx 30 www-data www-data 12288 Sep 10  2024 wp-includes
-rwxrwxrwx  1 www-data www-data  2502 Nov 26  2022 wp-links-opml.php
-rwxrwxrwx  1 www-data www-data  3937 Mar 11  2024 wp-load.php
-rwxrwxrwx  1 www-data www-data 51238 May 28  2024 wp-login.php
-rwxrwxrwx  1 www-data www-data  8525 Sep 16  2023 wp-mail.php
-rwxrwxrwx  1 www-data www-data 28774 Jul  9  2024 wp-settings.php
-rwxrwxrwx  1 www-data www-data 34385 Jun 19  2023 wp-signup.php
-rwxrwxrwx  1 www-data www-data  4885 Jun 22  2023 wp-trackback.php
-rwxrwxrwx  1 www-data www-data  3246 Mar  2  2024 xmlrpc.php
```

Hallazgo

Permisos de lectura, escritura y ejecución en todo el directorio web.

Significado

Escritura para cualquier persona que entre en el directorio

Impacto

Cualquier atacante puede subir y ejecutar malware sin necesidad de contraseña.

Acceso desde IP Desconocida.

```
-- Boot a10a791769204440c8e08594d6547449b --
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 systemd[1]: 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 b986fb6c4cd1419ab698ae8aba591bd8 --
```

Posible Acceso malintencionado por el SSH desde una IP desconocida y un puerto arbitrario.

Correcion de las vulnerabilidades.

```
sudo systemctl stop cups

sudo systemctl disable cups
```

Eliminamos el servicio del puerto 631

```
sudo systemctl stop vsftpd
sudo systemctl disable vsftpd
```

Eliminamos el servicio FTP puerto 21

```
sudo find /var/www/html/ -type d -exec chmod 755 {} \;

sudo chmod 600 /var/www/html/wp-config.php

sudo find /var/www/html/ -type f -exec chmod 644 {} \;
```

Corregimos el problema de seguridad de la carpeta /html, haciendo unas faciles modificaciones.

Correcion de las vulnerabilidades 2.

```
debian@debian:~$ sudo -l
Matching Defaults entries for debian on debian:
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User debian may run the following commands on debian:
    (ALL : ALL) ALL
debian@debian:~$
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
debian  ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute
%sudo   ALL=(ALL:ALL) ALL
```

Borrar la linea debian, evitamos que se pueda acceder como "root" el usuairo debian.

FASE 2.Análisis de Vulnerabilidades

Servicio	Versión	ID	Impacto	Análisis
OpenSSH	9.2p1	CVE-2024-6387	Crítico	Conocida como "RegreSSHion". Permite ejecución remota de código (RCE).
VSFTPD	3.0.3	CVE-2021-30047	Alto	Permite denegación de servicio (DoS).

Explotación de Nueva Vulnerabilidad

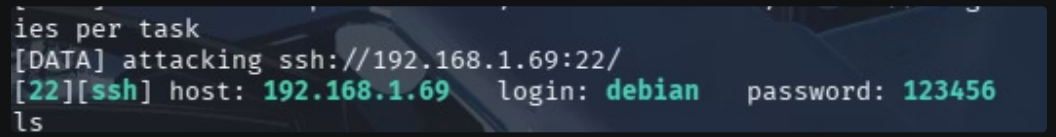
Ataque de Fuerza Bruta - Hydra

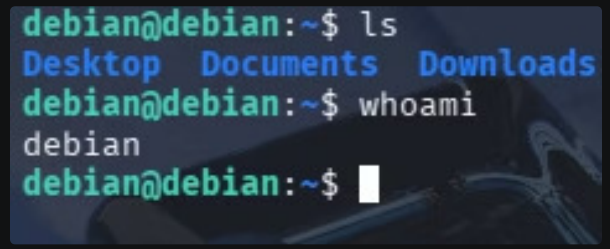
Escenario

- Atacante: Kali Linux
- Objetivo: Puerto 22 SSH del servidor Debian

Resultado

- Se halló la contraseña rapidamente
- Credencial comprometida: **debian / 123456**
- Impacto: Acceso remoto completo sin necesidad de exploit complejo





Solución: Persistencia de Logs

Problema

- Los logs solo estaban en memoria (journald)
- Riesgo: Si el atacante reinicia el servidor, se borran las evidencias forenses

Solución → rsyslog

- Instalación del servicio para persistir eventos en disco
- Ruta crítica creada: /var/log/auth.log

Beneficio Clave: Permite que herramientas de defensa como Fail2Ban lean los ataques en tiempo real.

Monitorización en Tiempo Real

Defensa con Fail2Ban y Bloqueo de IPs

Política jail.local

- Intentos: 3 intentos fallidos
- Ban time: 1 minuto (pruebas) / Permanente (Producción)
- Acción: iptables-allports (Bloqueo total de la IP)

Efecto Inmediato

- Detección en tiempo real en auth.log
- La IP atacante es rechazada
- El ataque se detiene automáticamente sin intervención humana

FASE 3:Plan de Respuesta

Detección

- EDR conectados a SIEM para visibilidad centralizada.
- Sistemas IDS/IPS para identificar y prevenir intrusiones.
- Monitoreo continuo 24/7 de la infraestructura crítica.

Contención

- Identificación rápida y aislamiento de equipos comprometidos.
- Realización de adquisición "en caliente" para preservar evidencia forense.

Eliminación

- Erradicación de componentes maliciosos y tareas programadas.
- Cambio forzado de todas las contraseñas afectadas.

Recuperación

- Restauración de sistemas a partir de copias de seguridad limpias y verificadas.
- Verificación exhaustiva del correcto funcionamiento y seguridad del sistema.

Protección de Datos y Continuidad

Estrategias implementadas para prevenir la pérdida de información y asegurar la recuperación efectiva del sistema ante cualquier incidente.

Prevención de Pérdida de Datos (DLP)

- **Datos en Reposo:** Aplicación de cifrado de credenciales y establecimiento de permisos restrictivos en archivos críticos.
- **Datos en Tránsito:** Uso exclusivo de canales cifrados como SSH/SFTP para transferencias. Eliminación completa del uso de FTP por ser inseguro.

Política de Respaldos (Backups)

- **Frecuencia:** Copia diaria de la base de datos y respaldos semanales para todos los ficheros web.
- **Método:** Tareas de respaldo automatizadas mediante scripts de cron para asegurar consistencia y regularidad.
- **Almacenamiento:** Al menos una copia de seguridad debe residir fuera del servidor principal, ofreciendo una protección robusta contra amenazas como el ransomware.