Reporte de incidente

16/07/2025

4Geeks Academy

INDICE

4Geeks Academy

RESUMEN

SE ENCONTRARON LOS SIGUIENTES PROBLEMAS

Configuraciones Peligrosas

Incluyen permisos excesivos, servicios innecesarios habilitados y falta de cifrado. Son vulnerabilidades "de baja dificultad" frecuentemente explotadas por scripts automatizados.

Falta de Monitoreo

La ausencia de registros detallados y alertas tempranas permite que ataques pasen desapercibidos durante meses (promedio: 287 días según IBM).

Debilidades en Autenticación

Mecanismos de verificación de identidad insuficientes, principal vector en el 80% de brechas relacionadas con hacking (Verizon DBIR 2023).

Exposición de Datos

Configuraciones que revelan información sensible directa o indirectamente, violando principios de "need-to-know".

FTP CON ACCESO ANÓNIMO HABILITADO

FTP con acceso anónimo habilitado

- **Servicio de transferencia de archivos que no requiere credenciales, permitiendo la descarga/upload de archivos sin restricciones.**

```
debian@debian:~$ sudo systemctl list-units --type=service | grep -i ftp
  vsftpd.service                       loaded active running vsftpd FTP server
debian@debian:~$ sudo grep -i "anonymous_enable" /etc/vsftpd.conf
anonymous_enable=YES
debian@debian:~$
```

4Geeks Academy

ACCESO ROOT REMOTO EN MARIADB

- Configuración que permite conexiones administrativas desde cualquier red externa, facilitando el control completo de las bases de datos por atacantes.

```
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 ]

Performing filesystem checks
```

4Geeks Academy

POLÍTICA DE CONTRASEÑAS DÉBILES

- Configuración que permite conexiones administrativas desde cualquier red externa, facilitando el control completo de las bases de datos por atacantes.

```
MariaDB [(none)]> SHOW GRANTS FOR 'user'@'localhost';
+-------------------------------------------------------------------------------------------------------------------
------------------------------+
| Grants for user@localhost
                              |
+-------------------------------------------------------------------------------------------------------------------
------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO `user`@`localhost` IDENTIFIED BY PASSWORD '*2470C0C06DEE42FD1618BB99005ADCA
2EC9D1E19' WITH GRANT OPTION |
+------------------------------+-------------------------------------------------------------------------------------
------------------------------+
1 row in set (0.001 sec)
```

4Geeks Academy

PERMISOS GLOBALES (777) EN WP-CONFIG.PHP

- Archivo crítico de WordPress con permisos de escritura/lectura para todos los usuarios del sistema, permitiendo su modificación por procesos maliciosos.

```
debian@debian:/var/www/html$ ls -l wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30  2024 wp-config.php
```

4Geeks Academy

LISTADO DE DIRECTORIOS WEB ACTIVADO

- Configuración del servidor web que muestra el contenido de carpetas cuando no hay archivo índice, exponiendo estructura de directorios y archivos sensibles.

```
debian@debian:/$ curl -I http://localhost/wp-content/
HTTP/1.1 200 OK
Date: Tue, 15 Jul 2025 18:19:51 GMT
Server: Apache/2.4.62 (Debian)
Content-Type: text/html; charset=UTF-8
```

4Geeks Academy

PLAN DE RESPUESTA

Estructura Organizacional del Equipo de Respuesta

Un equipo de respuesta efectivo requiere una estructura escalonada con roles y responsabilidades claramente definidos. La estructura propuesta sigue el modelo NIST SP 800-61 y se compone de tres niveles de actuación:

Procedimientos de Contención Avanzada

La contención debe ser progresiva para balancear impacto operacional con efectividad:

4Geeks Academy

SISTEMA DE GESTION DE SEGURIDAD

Marco de Implementación

Configuraciones que revelan información sensible directa o indirectamente, violando principios de "need-to-know".

Controles Clave Explicados

La ausencia de registros detallados y alertas tempranas permite que ataques pasen desapercibidos durante meses (promedio: 287 días según IBM).

Modelo de Gobernanza

Mecanismos de verificación de identidad insuficientes, principal vector en el 80% de brechas relacionadas con hacking (Verizon DBIR 2023).

GRACIAS

4Geeks
Academy