# Informe del Incidente de Seguridad

**Servidor Crítico – 4Geeks Academy**

## 1. Introducción

El presente informe documenta en detalle el incidente de seguridad que afectó al servidor crítico de 4Geeks Academy. Se detalla la detección del incidente, las técnicas de análisis forense empleadas, las evidencias recabadas, la línea de tiempo de eventos, el impacto en el sistema y las acciones correctivas implementadas para mitigar la amenaza. El objetivo es proporcionar una base sólida para comprender el suceso, aprender de la experiencia y reforzar la postura de seguridad del entorno.

## 2. Resumen Ejecutivo

El incidente se detectó tras la identificación de patrones inusuales en los logs de autenticación, específicamente en el archivo /var/log/auth.log, donde se observaron múltiples intentos fallidos y accesos no autorizados vía SSH. Posteriormente, se detectaron evidencias de acceso indebido a servicios FTP y configuraciones vulnerables en archivos críticos (por ejemplo, wp-config.php). Se constató que el atacante aprovechó contraseñas débiles y configuraciones erróneas para escalar privilegios y establecer backdoors en el sistema. La respuesta inmediata incluyó la contención del incidente, análisis forense, eliminación de accesos maliciosos y fortalecimiento de las configuraciones de seguridad.

## 3. Descripción del Incidente

### 3.1 Contexto y Origen

**Fecha y Hora de Detección:**  
El incidente fue detectado el 24 de febrero de 2025 a las 09:00 hrs, cuando se observaron anomalías en los logs del sistema.

**Vectores de Ataque Identificados:**

* + **Acceso SSH:** Se observaron múltiples intentos de autenticación fallida, seguidos de accesos exitosos utilizando credenciales débiles.
  + **Servicio FTP:** Configuración errónea que permitía accesos anónimos y la transferencia no cifrada de archivos.
  + **Exposición de Archivos Críticos:** Permisos inapropiados en wp-config.php y directorios web listables, facilitando el acceso a información sensible.

### 3.2 Modus Operandi del Atacante

El atacante aprovechó vulnerabilidades conocidas en la configuración del servidor:

* Utilizó ataques de fuerza bruta y credenciales comprometidas para obtener acceso SSH.
* Explotó la configuración insegura del FTP para transferir archivos maliciosos y establecer mecanismos de persistencia.
* Modificó permisos y creó backdoors, permitiendo el acceso remoto posterior al incidente.
* Ocultó rastros en los logs mediante técnicas de borrado o manipulación, dificultando inicialmente la correlación de eventos.

## 4. Metodología de Análisis Forense

Para el análisis del incidente se emplearon diversas herramientas y técnicas forenses:

* **Recopilación de Evidencias:**  
  Se extrajeron y analizaron logs del sistema, principalmente /var/log/auth.log, utilizando comandos como grep para identificar patrones sospechosos.
* **Análisis de Procesos y Archivos:**  
  Se utilizaron comandos como ps, ls y find para detectar procesos inusuales, archivos modificados y posibles backdoors.
* **Detección de Malware y Rootkits:**  
  Se ejecutó chkrootkit para identificar la presencia de software malicioso y se realizaron análisis complementarios con Lynis.
* **Escaneo de Vulnerabilidades:**  
  Herramientas como **Nmap**, **Nikto** y **OpenVAS** permitieron identificar servicios expuestos y configuraciones erróneas en la red y en el servidor.
* **Monitoreo y Captura de Tráfico:**  
  Se empleó **Wireshark** para analizar el tráfico de red y detectar actividades sospechosas o inusuales asociadas al incidente.
* **Registro de Eventos:**  
  Se documentó la línea de tiempo completa del ataque, recopilando datos de todas las herramientas y fuentes de evidencia disponibles.

## 5. Línea de Tiempo del Incidente

**[T0 – Inicio del Ataque y Primeras Pruebas]:**  
Se realizaron las primeras pruebas de detección el 24 de febrero de 2025 a las 09:00 hrs, cuando se observaron intentos de acceso SSH no autorizados en el log /var/log/auth.log.

**[T1 – Acceso y Establecimiento de Persistencia]:**  
Una vez obtenidas credenciales válidas, el atacante estableció conexiones SSH, creó usuarios fraudulentos y modificó permisos en archivos críticos, como wp-config.php.

**[T2 – Explotación del Servicio FTP]:**  
Aprovechando la configuración errónea del FTP, se realizaron transferencias de archivos maliciosos y se dejó evidencia de un posible backdoor en el sistema.

**[T3 – Manipulación de Logs y Escalada de Privilegios]:**  
Se detectaron intentos de borrar o modificar entradas en los logs, junto con la apertura de puertos no autorizados para mantener la persistencia y facilitar el acceso remoto.

**[T4 – Detección y Respuesta Inmediata]:**  
Tras la correlación de evidencias por el equipo de seguridad, se procedió a la contención del incidente: se detuvieron servicios comprometidos, se eliminaron usuarios maliciosos y se reforzaron las configuraciones.

## 6. Evidencias Recabadas

### 6.1 Logs y Registros

**SSH:**  
Los registros de /var/log/auth.log mostraron intentos de acceso repetitivos, con patrones de éxito tras múltiples fallos, evidenciando un ataque de fuerza bruta.

**FTP:**  
Se encontraron registros de conexiones anónimas y transferencias de archivos inusuales en el log del servicio FTP, lo que confirmó la explotación de la configuración insegura.

### 6.2 Archivos y Configuraciones Modificados

**Archivos Críticos:**  
Se identificó la modificación de wp-config.php, con cambios en los permisos que permitieron el acceso no autorizado a credenciales de base de datos.

**Backdoors y Scripts Maliciosos:**  
Se detectaron scripts y archivos no reconocidos en directorios del sistema, que fueron eliminados durante la fase de contención.

### 6.3 Análisis de Tráfico de Red

* **Wireshark:**  
  El análisis de tráfico reveló comunicaciones anómalas hacia IPs externas, lo que confirmó el envío y recepción de datos no autorizados, probablemente para la exfiltración de información.

### 6.4 Escaneos de Vulnerabilidades

* **Nmap, OpenVAS y Nikto:**  
  Estos escaneos ayudaron a identificar puertos abiertos innecesarios, configuraciones erróneas y otros vectores potenciales que fueron explotados por el atacante.

## 7. Impacto y Alcance del Incidente

### 7.1 Impacto en el Sistema

* **Compromiso de Credenciales:**  
  La utilización de contraseñas débiles permitió el acceso no autorizado a servicios críticos (SSH, FTP, MySQL).
* **Exposición de Información Sensible:**  
  La configuración inadecuada de archivos críticos y directorios permitió la exposición de datos y credenciales de acceso.
* **Persistencia del Atacante:**  
  La creación de backdoors y la manipulación de logs complicaron la detección inicial y posibilitaron una presencia prolongada en el sistema.

### 7.2 Alcance del Ataque

* **Servicios Afectados:**  
  El ataque se extendió a múltiples servicios, incluyendo SSH, FTP y el servidor web, evidenciando un ataque multifacético.
* **Potencial Exfiltración de Datos:**  
  Se detectaron comunicaciones hacia servidores externos, lo que sugiere que pudo haberse exfiltrado información sensible antes de la contención.

## 8. Acciones Inmediatas y Correctivas

### 8.1 Contención y Mitigación Inmediata

* **Detención de Servicios Comprometidos:**  
  Se procedió a detener temporalmente los servicios afectados (SSH, FTP) mediante systemctl para evitar la propagación del ataque.
* **Eliminación de Accesos Maliciosos:**  
  Se borraron usuarios fraudulentos y se eliminaron scripts y archivos no autorizados.
* **Refuerzo de Configuraciones:**  
  Se ajustaron los permisos de archivos críticos (wp-config.php), se reconfiguraron servicios y se cerraron puertos no esenciales mediante ajustes en el firewall.

### 8.2 Medidas Correctivas Posteriores

* **Actualización de Credenciales:**  
  Se actualizó la configuración de contraseñas, implementando autenticación basada en claves para SSH y fortaleciendo las contraseñas en MySQL.
* **Reconfiguración de Servicios:**  
  Se mejoró la seguridad del servicio FTP deshabilitando accesos anónimos y se reforzó la configuración del servidor web para evitar la indexación de directorios.
* **Monitoreo y Auditoría:**  
  Se implementaron herramientas como Fail2ban, Wireshark y OpenVAS para un monitoreo continuo, además de establecer auditorías periódicas con Lynis y Nikto.
* **Plan de Respuesta y SGSI:**  
  Se actualizó el plan de respuesta a incidentes y se implementó un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO 27001 para asegurar la continuidad y resiliencia del entorno.

## 9. Lecciones Aprendidas y Recomendaciones

### 9.1 Lecciones Aprendidas

* **Importancia de las Configuraciones Seguras:**  
  La debilidad en la configuración de servicios críticos (SSH, FTP y permisos de archivos) facilitó el acceso no autorizado.
* **Detección Temprana:**  
  La correlación y análisis de logs es vital para detectar patrones de ataque a tiempo y responder de forma oportuna.
* **Monitoreo Continuo:**  
  Un sistema de monitoreo robusto (integrando herramientas como Fail2ban, Wireshark y auditorías periódicas con Lynis) es esencial para identificar actividades anómalas.

### 9.2 Recomendaciones

* **Fortalecer Credenciales y Autenticación:**  
  Adoptar políticas de contraseñas robustas y utilizar métodos de autenticación multifactor para todos los accesos.
* **Revisar y Actualizar Configuraciones:**  
  Revisar periódicamente las configuraciones de servicios críticos y aplicar mejores prácticas de seguridad.
* **Implementar Controles de Acceso y Permisos:**  
  Limitar estrictamente los permisos en archivos sensibles y asegurar que solo usuarios autorizados tengan acceso a recursos críticos.
* **Realizar Pruebas y Simulacros:**  
  Ejecutar simulacros de incidentes y pruebas de penetración periódicas para evaluar la efectividad de las medidas implementadas.
* **Capacitación Continua:**  
  Entrenar al personal en técnicas de respuesta a incidentes y en las mejores prácticas de ciberseguridad para mejorar la resiliencia organizacional.

## 10. Conclusiones

El incidente evidenció una combinación de vulnerabilidades de configuración y debilidades en la gestión de credenciales que permitieron el acceso no autorizado y la persistencia del atacante en el sistema. La respuesta coordinada, basada en técnicas de análisis forense y el uso de un amplio arsenal de herramientas (entre ellas grep, chkrootkit, Nmap, Lynis, Nikto, Wireshark, Fail2ban y OpenVAS), permitió contener el incidente y minimizar el impacto. La experiencia destaca la necesidad de reforzar las políticas de seguridad, implementar controles de acceso rigurosos y mantener una vigilancia continua sobre el entorno.

La implementación de un plan de respuesta a incidentes robusto y la certificación del SGSI conforme a ISO 27001 se presentan como pilares fundamentales para evitar la recurrencia de incidentes similares y garantizar la integridad y confidencialidad de los sistemas críticos.