Análisis Forense y Respuesta a Incidentes

Proyecto Final de Ciberseguridad - 4Geeks Academy

Riccardo Barbieri

Objetivos del Proyecto

El proyecto se estructuró en tres fases complementarias e interconectadas.

Comenzamos con un Análisis Forense e Identificación de Vulnerabilidades, seguido por la Detección y Explotación de Vulnerabilidades Adicionales, y finalizamos con la Implementación de un Sistema de Gestión de Seguridad.

Aplicamos metodologías estándar de la industria como ISO 27001.

Análisis Forense

Durante la primera fase identificamos múltiples vulnerabilidades críticas en el servidor.

Encontramos SSH con acceso directo root habilitado, servicio FTP anónimo con permisos de escritura, directorios web listables por configuración insegura de Apache, archivos de configuración como wp-config.php con permisos incorrectos, credenciales de bases de datos compartidas entre usuarios, y puertos innecesarios expuestos.

Vulnerabilidades Críticas

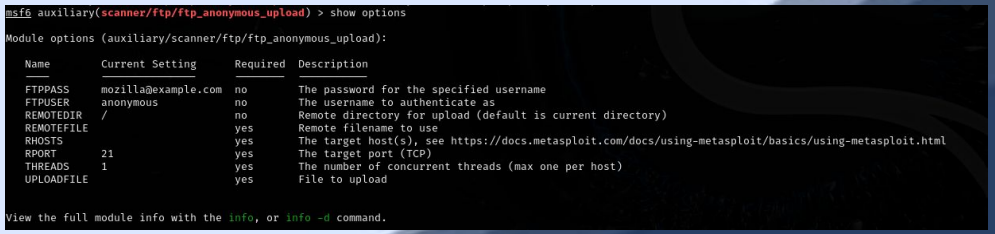
El análisis de logs reveló evidencias claras de compromiso previo en el sistema. La configuración SSH era especialmente vulnerable porque tenía habilitado PermitRootLogin yes, permitiendo acceso directo como administrador.

Además, la autenticación por contraseña estaba activada en lugar de usar únicamente claves públicas. Estos ajustes inseguros facilitan ataques de fuerza bruta y acceso no autorizado. Identificamos también múltiples sesiones sospechosas.

Detección de Vulnerabilidades Adicionales

Para la segunda fase realizamos un escaneo exhaustivo que reveló un servicio FTP activo ejecutando vsftpd 3.0.3.

Verificamos el acceso anónimo utilizando tanto cliente FTP estándar como módulos de Metasploit, confirmando que permitía no solo lectura sino también escritura. Adicionalmente identificamos que el sistema ejecutaba un kernel Linux 4.15.x con vulnerabilidades conocidas. Esta configuración con CVSS de 9.8, de nivel crítico.



Explotación: FTP Anónimo

Procedimos a demostrar el impacto creando una reverse shell con msfvenom compatible con Linux x64.

Cargamos exitosamente este payload al directorio /upload aprovechando el acceso FTP anónimo. Configuramos un listener netcat en nuestra máquina para recibir la conexión en el puerto 4444. Al ejecutar el payload conseguimos una shell remota con los privilegios del usuario que ejecuta el servicio FTP. Realizamos enumeración del sistema identificando binarios SUID y vulnerabilidades adicionales.

Escalación de Privilegios

Explotamos una vulnerabilidad en el kernel Linux 4.15.x (gestión incorrecta de privilegios).

Esta vulnerabilidad nos permitió escalar privilegios y obtener acceso completo como usuario root.

Con este nivel de acceso logramos control total del sistema con capacidad para leer o modificar cualquier archivo, instalar backdoors persistentes que sobrevivan reinicios, y potencialmente comprometer otros sistemas conectados a la misma red.

Correcciones Implementadas

Implementamos medidas correctivas para todas las vulnerabilidades detectadas.

Desactivamos completamente el acceso FTP anónimo modificando la configuración de vsftpd. Actualizamos el kernel a una versión superior a 5.0 para corregir las vulnerabilidades de escalación.

Aplicamos permisos restrictivos (chmod 640) a archivos sensibles como wp-config.php. Configuramos un firewall con reglas específicas, desactivamos el listado de directorios en Apache y renovamos todas las credenciales.

Plan de Respuesta a Incidentes

Desarrollamos un plan integral de respuesta a incidentes con procedimientos específicos para diferentes escenarios como denegación de servicio y fugas de información.

Definimos claramente roles y responsabilidades para cada fase: detección, contención, erradicación y recuperación. Creamos plantillas de comunicación adaptadas a distintos tipos de incidentes.

Implementamos sistemas de monitorización continua.

Sistema de Gestión de Seguridad

Implementamos un Sistema de Gestión de Seguridad basado en ISO 27001 adaptado al contexto educativo de 4Geeks Academy. Definimos un alcance preciso que incluye la infraestructura crítica, datos académicos e información personal.

Desarrollamos una política de clasificación de activos con cuatro niveles de sensibilidad. Establecimos un proceso de evaluación de riesgos que considera tanto probabilidad como impacto. Seleccionamos controles específicos basados en los resultados de la evaluación e implementamos un ciclo de mejora continua.

Protección de Datos Sensibles

Desarrollamos una estrategia DLP (Data Loss Prevention) específicamente diseñada para proteger datos académicos sensibles.

Implementamos controles para datos en reposo mediante cifrado y gestión de permisos granular. Aseguramos los datos en tránsito utilizando TLS y canales seguros de comunicación.

Configuramos sistemas de monitorización para detectar comportamientos anómalos y potenciales fugas. Implementamos clasificación automática de datos y planificamos un despliegue gradual en cuatro fases para minimizar el impacto operativo.

Lecciones Aprendidas

Este proyecto nos permitió confirmar la importancia crítica de las configuraciones seguras por defecto, ya que la mayoría de vulnerabilidades se originaron en configuraciones incorrectas. Verificamos la necesidad de mantener actualizados los sistemas, especialmente componentes críticos como el kernel.

Confirmamos el valor del principio de mínimo privilegio y la implementación de defensa en profundidad con múltiples capas de protección. Comprobamos que la seguridad debe entenderse como un proceso continuo que requiere monitorización activa y mejora constante.

Conclusiones

El proyecto demostró un vector de ataque completo que incluye acceso inicial, explotación y escalación de privilegios hasta obtener control total. Implementamos correcciones efectivas para todas las vulnerabilidades identificadas y desarrollamos un marco organizativo para la gestión de seguridad a largo plazo.

La postura de seguridad de 4Geeks Academy ha mejorado significativamente, estableciendo una base sólida para un programa de seguridad continuo que protege integralmente los activos críticos de la institución académica y la información sensible de estudiantes y personal.