Análisis Forense y Respuesta a Incidentes

Proyecto Final de Ciberseguridad - 4Geeks Academy

Riccardo Barbieri

Marzo 2025

Estructura del Proyecto

Fase 1: Análisis Forense - Identificación y Recolección de Evidencias

Fase 2: Detección y Corrección de Vulnerabilidades Adicionales

Fase 3: Plan de Respuesta a Incidentes y Sistema de Gestión de Seguridad

Objetivos del Proyecto

Contenido:

Identificar vulnerabilidades críticas en infraestructura

Documentar evidencias forenses de compromiso

Explotar y corregir vulnerabilidades detectadas

Desarrollar un plan integral de respuesta a incidentes

Implementar un Sistema de Gestión de Seguridad basado en ISO27001

Análisis Forense

Contenido:

Metodología sistemática de identificación de evidencias

Análisis de logs y configuraciones de servicios críticos

Examen de procesos y permisos de archivos

Análisis de red y servicios expuestos

Documentación detallada de hallazgos

Vulnerabilidades Críticas

Contenido:

Configuración SSH insegura (PermitRootLogin yes)

FTP configurado de forma insegura (acceso anónimo)

Directorios web listables (Options Indexes)

Permisos incorrectos en wp-config.php

Puertos innecesarios abiertos

Configuración insegura de base de datos

Detección de Vulnerabilidades Adicionales

Contenido:

Metodología PTES/OWASP para evaluación de seguridad

Escaneo de puertos y servicios

Análisis de configuraciones

Pruebas de penetración controladas

Explotación: FTP Anónimo

Contenido:

Vector de ataque: Acceso anónimo con capacidad de escritura

Carga de payload malicioso (reverse shell) vía FTP

Ejecución remota de código (RCE)

Establecimiento de persistencia

CVSS: 9.8 (Crítico)

Escalación de Privilegios

Contenido:

Vulnerabilidad en kernel Linux 4.15.x

Enumeración de binarios SUID

Explotación de permisos excesivos

Obtención de acceso como root

CVSS: 9.8 (Crítico)

Correcciones Implementadas

Contenido:

Desactivación de acceso FTP anónimo

Actualización del kernel a versión segura

Corrección de permisos restrictivos para wp-config.php

Desactivación de listado de directorios web

Configuración de firewall con reglas estrictas

Cambio de credenciales de base de datos

Plan de Respuesta a Incidentes

Contenido:

Procedimientos detallados por tipo de incidente

Roles y responsabilidades definidos

Fases de respuesta: Detección, Contención, Erradicación, Recuperación

Comunicación durante incidentes

Métricas y documentación post-incidente

Procedimientos por Tipo de Incidente

Contenido:

Denegación de Servicio (DoS/DDoS)

Fugas de Información

Malware y Ransomware

Acceso No Autorizado

Uso Indebido de Recursos

Estrategias específicas para cada tipo

Sistema de Gestión de Seguridad (ISMS)

Contenido:

Marco ISO 27001 implementado

Ciclo PDCA (Plan-Do-Check-Act)

Gestión y clasificación de activos

Evaluación y tratamiento de riesgos

Políticas y controles de seguridad

Mejora continua

Controles de Seguridad Implementados

Contenido:

Controles organ zativos (roles, responsabilidades)

Controles técnicos (cifrado, autenticación, firewalls)

Controles físicos (seguridad de instalaciones)

Controles de personal (formación, concienciación)

Controles de recuperación (backups, continuidad)

Protección de Datos Sensibles

Contenido:

Estrategia DLP (Data Loss Prevention)

Clasificación de datos académicos y administrativos

Controles para datos en reposo, en movimiento y en uso

Automatización de protección con implementación gradual

Monitorización continua

Lecciones Aprendidas

Contenido:

Importancia de la configuración segura de servicios

Valor de mantener sistemas actualizados

Necesidad del principio de mínimo privilegio

Defensa en profundidad como estrategia esencial

Monitorización proactiva para detección temprana

Recomendaciones Futuras

Contenido:

Implementar programa de parcheado automático

Realizar pruebas de penetración periódicas

Desarrollar programa de concienciación en seguridad

Implementar monitorización avanzada (SIEM/SOC)

Adoptar framework NIST CSF o ISO 27001 completo

Impacto en el Negocio

Contenido:

Protección de datos sensibles de estudiantes y academia

Cumplimiento con requisitos legales y regulatorios

Reducción de riesgos operacionales y financieros

Mejora de la confianza de estudiantes y colaboradores

Posicionamiento como referente en seguridad educativa

Conclusiones

Contenido:

Sistema comprometido a través de múltiples vulnerabilidades

Vector de ataque completo: acceso, ejecución, escalación

Implementación exitosa de correcciones técnicas

Desarrollo de estructura organizativa para gestión de seguridad

Transformación hacia una cultura de seguridad proactiva