Plan de Respuesta a Incidentes y Certificación

Resumen Ejecutivo

Durante las fases de pentesting, se identificaron varias vulnerabilidades críticas en el sistema, incluyendo:

- **Acceso root permitido en SSH:** Configuración insegura que permite el acceso directo como root mediante SSH.
- **Servicios innecesarios expuestos:** Servicios como Apache, FTP y CUPS están expuestos y podrían ser explotados.
- **Vulnerabilidades en Apache:** Posibilidad de ataques de denegación de servicio (DoS) y enumeración de directorios.

Se propone un Plan de Respuesta a Incidentes basado en el marco del NIST SP 800-61, que incluye la identificación, contención, erradicación y recuperación de incidentes. Además, se recomienda la implementación de un SGSI conforme a ISO 27001 para gestionar de manera sistemática la seguridad de la información.

Plan de respuesta a incidentes basado en NIST SP 800-61

Alcance y objetivos

El presente plan de respuesta a incidentes se enfoca en la gestión y mitigación de incidentes de seguridad relacionados con la máquina previamente comprometida (Debian con IP 192.168.1.139).

Su objetivo principal es establecer procedimientos claros y eficaces para la detección, contención, erradicación y recuperación de incidentes de seguridad informática, garantizando la continuidad operativa y la integridad de los datos.

1. **Preparación:**

Creación de un Equipo de Respuesta ante Incidentes (CSIRT)

- **Composición del equipo:** Integrado por personal de seguridad de la información, administradores de sistemas, desarrolladores y responsables de cumplimiento normativo.
- **Recursos:** Herramientas de monitoreo de seguridad, soluciones SIEM, IDS/IPS y respaldo de sistemas.
- **Responsabilidades:** Identificación y respuesta ante incidentes, implementación de soluciones y prevención de futuros ataques.

Configuración de Herramientas y Tecnologías

- **Herramientas de monitoreo:** SIEM para la recopilación y análisis de logs.

- **Protección de endpoints:** Antivirus, EDR y firewalls.
- **Sistemas de respaldo:** Implementación de copias de seguridad diarias con pruebas de restauración periódicas.
- **Cifrado de datos sensibles:** Aplicación de cifrado AES-256 en bases de datos y almacenamiento.

Políticas y procedimientos

- **Políticas de acceso:** Autenticación multifactor (MFA) para accesos críticos.
- **Procedimientos de escalamiento:** Plan de acción en caso de incidentes críticos.
- **Capacitación y concienciación:** Formación del personal en buenas prácticas de seguridad.

Formación de equipo y partes interesadas

- **Capacitación del CSIRT:** Entrenamiento continuo en respuesta a incidentes y análisis forense.
- **Sensibilización del personal:** Programas educativos sobre ciberseguridad para toda la organización.
- **Coordinación con terceros:** Definición de protocolos de comunicación con proveedores y entidades regulatorias.

2. **Detección y Análisis**

Pruebas

- Simulación de ataques controlados (red teaming y blue teaming).
- Análisis de vulnerabilidades periódico con herramientas como Nmap, OpenVAS y Nessus.

Análisis de incidentes

- Revisión de logs para identificar patrones de ataque.
- Análisis forense de sistemas comprometidos.

3. **Priorización**

- **Críticos:** Respuesta en menos de 3 horas.
- **Medios:** Respuesta en 12-24 horas.
- **Bajos:** Resolución planificada según impacto.

4. **Contención, Erradicación y Recuperación**

Contención

- Aislamiento de sistemas comprometidos.
- Bloqueo de IPs maliciosas y control de acceso segmentado.

Erradicación

- Eliminación de malware y restauración de configuraciones seguras.
- Actualización de sistemas y aplicaciones vulnerables.

Recuperación

- Restauración de sistemas desde respaldos seguros.
- Verificación de integridad post-recuperación.

5. Mecanismos de Protección de Datos

Respaldos periódicos:

- Realizar copias de seguridad diarias y almacenarlas en ubicaciones seguras.

Cifrado de datos sensibles:

- Implementar cifrado AES-256 para datos en reposo y TLS 1.2 para datos en tránsito.

Controles de acceso estrictos:

- Implementar autenticación multifactor (MFA) y el principio de mínimo privilegio.

6. Post-Incidente

Mejora continua

- Evaluación de incidentes pasados y refinamiento de estrategias.
- Implementación de nuevos controles de seguridad según amenazas emergentes.

Mantenimiento

- Revisiones periódicas del plan de respuesta.
- Simulaciones de incidentes para validación de procesos.

Implementación del SGSI conforme a ISO 27001

Análisis de Riesgos

- Identificación de activos críticos y amenazas.
- Evaluación del impacto y probabilidad de incidentes:
    - **Riesgo Inherente**: Evaluación antes de aplicar controles.
    - **Riesgo Actual**: Impacto tras medidas de mitigación.
    - **Riesgo Residual**: Riesgo restante tras implementación completa.

*Ver anexo: Documento Excel adjunto "AARR_Proyecto Final_DMR"

Definición de Políticas de Seguridad

- Establecimiento de normas para la gestión segura de la información.
- Creación de directrices sobre el acceso y manejo de datos sensibles.

Planes de Acción

- Desarrollo de estrategias para proteger la información crítica.
- Implementación de medidas de control como segmentación de red y monitoreo activo.

Controles Aplicados (ISO 27002)

1. Control de Acceso

- **Restricción de SSH y MFA**
    - **Código 9.1.2 (Acceso a redes y servicios de red):** Solo se proporciona acceso autorizado a usuarios específicos.
    - **Código 9.2.2 (Provisión de acceso de usuario):** Implementación de un procedimiento formal para asignar o revocar accesos.
    - **Código 9.2.3 (Gestión de privilegios de acceso):** Restricción y control del uso de privilegios de acceso.
    - **Código 9.2.4 (Gestión de información secreta de autenticación):** Control formal del proceso de autenticación.
    - **Código 9.2.5 (Revisión de derechos de acceso):** Verificación periódica de accesos concedidos.
    - **Código 9.3.1 (Uso de información secreta de autenticación):** Implementación de buenas prácticas en la gestión de credenciales.

- **Código 9.4.3 (Sistema de gestión de contraseñas):** Uso de sistemas que garanticen contraseñas seguras y robustas.
- **Código 9.4.4 (Uso de utilidades con privilegios del sistema):** Restricción y control estricto del uso de herramientas con privilegios elevados.

2. Criptografía

- **Protección de Información Sensible**
  - **Código 10.1.2 (Gestión de claves):** Desarrollo e implementación de políticas sobre el ciclo de vida de claves de cifrado.

3. Gestión de Activos

- **Inventario de dispositivos**
  - **Código 8.1.1 (Inventario de activos):** Identificación y mantenimiento de un inventario actualizado de activos de información.

4. Gestión de Incidentes de Seguridad de la Información

- **Procesos documentados de respuesta**
  - **Código 16.1.1 (Responsabilidades y procedimientos):** Definición clara de roles y procedimientos de gestión de incidentes.
  - **Código 16.1.2 (Notificación de eventos de seguridad):** Establecimiento de canales de notificación rápida de incidentes.
  - **Código 16.1.3 (Notificación de puntos débiles de seguridad):** Proceso formalizado para que empleados y terceros reporten vulnerabilidades.
  - **Código 16.1.4 (Evaluación y decisión sobre eventos de seguridad):** Determinación de si los eventos de seguridad son incidentes reales.
  - **Código 16.1.5 (Respuesta a incidentes de seguridad):** Aplicación de procedimientos documentados en la respuesta a incidentes.
  - **Código 16.1.6 (Aprendizaje de incidentes de seguridad):** Uso del análisis de incidentes para mejorar la seguridad y prevenir futuros problemas.
  - **Código 16.1.7 (Recopilación de evidencias):** Implementación de procedimientos de recopilación y preservación de evidencias en incidentes de seguridad.

5. Seguridad en Operaciones

- **Monitoreo y auditoría continua**
    - **Código 12.3.1 (Copias de seguridad de la información):** Implementación de backups regulares con verificación periódica.
    - **Código 12.4.1 (Registro de eventos):** Captura, protección y revisión de logs de actividad y eventos de seguridad.
    - **Código 12.6.1 (Gestión de vulnerabilidades técnicas):** Evaluación de vulnerabilidades y adopción de medidas correctivas.
    - **Código 12.7.1 (Controles de auditoría de sistemas de información):** Planificación y ejecución de auditorías sin afectar procesos críticos.

6. Seguridad en Comunicaciones

- **Segregación de redes y controles de red**
    - **Código 13.1.1 (Controles de red):** Gestión y control de redes para proteger la información.
    - **Código 13.1.3 (Segregación en redes):** Separación de servicios, usuarios y sistemas en distintas redes para minimizar riesgos.

7. Adquisición, Desarrollo y Mantenimiento de Sistemas

- **Seguridad en el ciclo de vida del software**
    - **Código 14.2.3 (Revisión técnica de aplicaciones tras cambios en sistemas operativos):** Evaluación de impactos en seguridad antes de implementar cambios.
    - **Código 14.2.4 (Restricciones a los cambios en paquetes de software):** Control riguroso sobre modificaciones en software.
    - **Código 14.2.5 (Principios de ingeniería de sistemas seguros):** Aplicación de principios de seguridad en el desarrollo de sistemas.

8. Cumplimiento

- **Verificación y auditoría periódica**
    - **Código 18.2.3 (Comprobación del cumplimiento técnico):** Revisión regular para garantizar conformidad con las políticas de seguridad.

*Ver anexo: Documento Excel adjunto “AARR_Proyecto Final_DMR”