LABORATORIO #3
CASO #3: Introducción a la Ciberseguridad
EL INCIDENTE CRÍTICO

PRESENTADO POR:

NAYIBE ESTHER ALTAMAR SERRANO

EJECUTOR TÉCNICO
JUAN SUÁREZ

MENTOR
ELISEO RODRÍGUEZ

CIBERSEGURIDAD – NIVEL BÁSICO

TALENTO TECH - UNIVERSIDAD LIBRE

JUNIO - 2025

EL INCIDENTE CRÍTICO

OBJETIVOS DEL LABORATORIO

1. Identificar el vector de ataque inicial (e.g., phishing, explotación de vulnerabilidad).

2. Analizar los logs del sistema para encontrar evidencias de actividad maliciosa.

3. Determinar el alcance del compromiso y los sistemas afectados.

4. Proponer medidas de contención y recuperación

Estructura del Laboratorio

Paso 1: Identificar el Vector de Ataque Inicial

1.1 Revisión de Indicadores Iniciales:

• **Actividad:** que información reunirías para identificar los primeros signos del incidente (mensajes extraños, fallos en sistemas específicos).

• Posibles vectores:

Phishing

Explotación de Vulnerabilidad

Acceso NO Autorizado 1 Evaluación de la Evidencia:

• **Actividad:** Establecer cuál es la información que se puede recolectar y permita identificar el vector de ataque más probable.

Si el phishing es identificado Que se debe buscar.

Si una vulnerabilidad es sospechosa: Que se debe identificar.

Resultados Esperados

• Establecer parámetros que permitan la identificación del vector de ataque inicial (por ejemplo, phishing con un archivo adjunto malicioso).

Paso 2: Analizar los Logs del Sistema para Encontrar Evidencias de Actividad Maliciosa

2.1 Recolección de Logs:

● **Actividad:** Describir cuales pueden ser los logs de los sistemas afectados que se deben revisar (servidores de correo electrónico, bases de datos, terminales).

Logs del Servidor de Correo Electrónico Que se debe buscar.

Logs del Sistema de Bases de Datos: Que se debería identificar.

Logs de Seguridad: Que se debe revisar de cualquier alerta.

2.2 Análisis de la Actividad Maliciosa:

● **Actividad:** Que análisis se debe realizar en los logs para buscar patrones inusuales.

● **Herramientas de Análisis:** Que herramientas de análisis se podrían utilizar para los logs

Paso 3: Determinar el Alcance del Compromiso y los Sistemas Afectados

3.1 Identificación de Sistemas Comprometidos:

● **Actividad:** que se debe realizar cuando se identifica los sistemas comprometidos.

Revisa los sistemas interconectados:

Evalúa el impacto en la infraestructura crítica: 3.2 Evaluación del Impacto

● **Actividad:** que se debe tener en cuenta para evaluar el impacto en la disponibilidad, integridad y confidencialidad de los datos.

Disponibilidad

Integridad:

Confidencialidad

Resultados Esperados

Paso 4: Proponer Medidas de Contención Inmediatas:

4.1 Medidas de Contención Inmediatas:

● **Actividad:** qué medidas se pueden implementar para detener el ataque y prevenir una mayor propagación.

Desconectar sistemas comprometidos:

Actualización de Sistemas:

Cambio de Credenciales:

4.2 Plan de Recuperación:

● **Actividad:** Desarrollar un plan para restaurar los sistemas afectados y volver a la operación normal.

Restauración desde Copia de Seguridad:

Monitoreo y Validación: Evaluación Pots-Incidente

4.3 Comunicación

· **Actividad:** Determinar a quién se le debe informar sobre la situación, las medidas tomadas, y las siguientes etapas.

Transparencia: que se debe realizar

Lista de Verificación

Ejemplo 1. Revisar en la academia cisco los conceptos.

2. Subir un documento pdf al apartado de tarea con las actividades realizadas

EL INCIDENTE CRÍTICO – LABORATORIO DE CIBERSEGURIDAD

Objetivos del Laboratorio

1. Identificar el vector de ataque inicial (por ejemplo, phishing o explotación de vulnerabilidad).
2. Analizar los registros (logs) del sistema para encontrar evidencia de actividad maliciosa.
3. Determinar el alcance del compromiso y los sistemas afectados.
4. Proponer medidas de contención y recuperación ante el incidente.

Paso 1: Identificar el Vector de Ataque Inicial

1.1 Revisión de Indicadores Iniciales:

Actividad:

- **Reunir información de señales sospechosas:**
  - Reportes de usuarios sobre mensajes extraños.
  - Fallos en servicios (inaccesibilidad de sistemas, errores en aplicaciones).
  - Alertas del sistema antivirus o firewall.
  - Intentos fallidos de acceso.

Posibles vectores:

- **Phishing:** Correos electrónicos sospechosos con enlaces o archivos adjuntos maliciosos.
- **Explotación de vulnerabilidades:** Software desactualizado con fallos de seguridad conocidos.
- **Acceso no autorizado:** Inicios de sesión desde ubicaciones inusuales.

1.2 Evaluación de la Evidencia:

Actividad:

- **Si se sospecha de phishing**, buscar:
  - Correos con archivos .exe, .docm, .zip sospechosos.
  - Enlaces que redirigen a sitios falsos.
  - Usuarios que abrieron o descargaron contenido malicioso.

- **Si se sospecha de vulnerabilidad**, identificar:
    - Software desactualizado o sin parches.
    - Explotación registrada en logs de seguridad.
    - Cambios no autorizados en configuraciones del sistema.

Resultado esperado:

- Identificar claramente el vector de ataque inicial (ej.: *phishing con archivo malicioso .zip*).

Paso 2: Analizar los Logs del Sistema

2.1 Recolección de Logs:

Actividad:
Revisar los siguientes registros:

- **Logs del servidor de correo electrónico**:
    - Envío y recepción de correos sospechosos.
    - Archivos adjuntos abiertos por usuarios.
    - Intentos de autenticación fallida.
- **Logs del sistema de bases de datos**:
    - Accesos inusuales a datos sensibles.
    - Consultas ejecutadas por usuarios no autorizados.
- **Logs de seguridad**:
    - Alertas de antivirus/IDS.
    - Escalamiento de privilegios.
    - Accesos desde IPs o regiones anómalas.

2.2 Análisis de Actividad Maliciosa:

Actividad:

- Buscar patrones inusuales: múltiples intentos fallidos, accesos fuera del horario laboral, ejecución de scripts desconocidos.

Herramientas recomendadas:

- **Splunk**, **Kibana**, **ELK Stack**, **Wireshark**, **Syslog Viewer**.

Paso 3: Determinar el Alcance del Compromiso

3.1 Identificación de Sistemas Comprometidos:

Actividad:

- Revisar equipos conectados a la misma red del sistema afectado.
- Escanear dispositivos con herramientas de detección de malware (Ej.: Malwarebytes, Nessus).
- Aislar los sistemas infectados para evitar propagación.

3.2 Evaluación del Impacto:

Actividad:
Evaluar en base a los principios de seguridad CIA:

- **Disponibilidad**: ¿Se interrumpió algún servicio?
- **Integridad**: ¿Se modificaron datos?
- **Confidencialidad**: ¿Se expuso información sensible?

Resultado esperado:

- Mapa de los sistemas comprometidos y estimación del nivel de daño.

Paso 4: Contención y Recuperación

4.1 Medidas de Contención Inmediatas:

Actividad:

- Desconectar los sistemas comprometidos de la red.
- Cambiar credenciales afectadas (usuarios y administradores).
- Aplicar parches y actualizaciones a software vulnerable.
- Revocar accesos temporales o sospechosos.

4.2 Plan de Recuperación:

Actividad:

- Restaurar sistemas desde **copias de seguridad confiables**.
- Ejecutar análisis de seguridad post-restauración.
- Validar integridad de datos recuperados.
- Aumentar la monitorización en tiempo real.

4.3 Comunicación y Evaluación Post-Incidente:

Actividad:

- Informar a:
    - Usuarios afectados.
    - Alta dirección.
    - Equipo de TI.
    - Autoridades pertinentes (si es legalmente obligatorio).

Transparencia:

- Documentar y comunicar el incidente, acciones tomadas, lecciones aprendidas y plan de prevención futuro.

Conclusión del Laboratorio

Este laboratorio permite aplicar los conceptos fundamentales de ciberseguridad para responder eficazmente a un incidente real. A través de la identificación del vector de ataque, análisis de logs, evaluación de impacto y propuesta de medidas de contención y recuperación, se fortalece la capacidad de detección y respuesta ante ciberataques. Además, se destaca la importancia de la confidencialidad, integridad y disponibilidad (CIA) como pilares para mantener la seguridad de los sistemas y la información.