Laboratorio: El Incidente Crítico

Sesión #3

Duración: 2 horas

Objetivos del Laboratorio

1. Identificar el vector de ataque inicial (ej. 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.

Materiales Necesarios

- GitHub como repositorio.
- Academia Cisco.
- Computador.
- Acceso a internet.

Paso 1: Identificar el Vector de Ataque Inicial

1.1 Revisión de Indicadores Iniciales

- Actividad:
  Se recopilará información de alertas o comportamientos anómalos, como:
  - Correos electrónicos sospechosos.
  - Fallos o lentitud en servicios críticos.
  - Accesos inusuales en horarios no laborales.
  - Usuarios que reportan acciones que no han realizado.
- Posibles Vectores:
  - Phishing: Correos con enlaces o adjuntos maliciosos.
  - Explotación de vulnerabilidad: Uso de software desactualizado.
  - Acceso no autorizado: Inicio de sesión desde direcciones IP inusuales.

1.2 Evaluación de la Evidencia

- Actividad:
  - Si se identifica phishing: Buscar el correo, el enlace, IP de origen y si fue abierto.
  - Si hay sospecha de vulnerabilidad: Revisar parches de seguridad faltantes.
  - Analizar credenciales usadas para accesos no comunes.

Resultado Esperado:
Establecer el vector inicial del ataque, por ejemplo:
"Phishing con archivo adjunto malicioso que permitió la instalación de un backdoor."

Paso 2: Analizar los Logs del Sistema para Encontrar Evidencias

2.1 Recolección de Logs

- Actividad:
  - Logs del Servidor de Correo Electrónico: Buscar envíos y accesos inusuales.
  - Logs del Sistema de Bases de Datos: Accesos fuera del horario habitual.
  - Logs de Seguridad: Alertas de firewall, antivirus, intentos fallidos de inicio de sesión.

2.2 Análisis de la Actividad Maliciosa

- Actividad:
  Identificar patrones:
  - Repetición de accesos desde misma IP.
  - Uso de comandos no comunes.
  - Usuarios accediendo a recursos que no les corresponden.
- Herramientas de Análisis:
  - SIEM (Splunk, Graylog)
  - Wireshark
  - Logwatch
  - Sysinternals (Windows)

Paso 3: Determinar el Alcance del Compromiso

3.1 Identificación de Sistemas Comprometidos

- Actividad:
  - Evaluar interconexiones del sistema afectado.
  - Determinar si otros servidores o estaciones de trabajo fueron atacados.

3.2 Evaluación del Impacto

- Actividad:
  Evaluar los siguientes aspectos:
  - Disponibilidad: Servicios caídos o degradados.
  - Integridad: Datos modificados o eliminados.
  - Confidencialidad: Exposición de datos sensibles.

Resultado Esperado:
Lista de sistemas afectados, datos comprometidos y servicios interrumpidos.

Paso 4: Proponer Medidas de Contención Inmediatas

4.1 Medidas de Contención

- Actividad:
  - Desconectar sistemas afectados de la red.
  - Aplicar actualizaciones críticas.
  - Cambiar credenciales y forzar cierre de sesión.

4.2 Plan de Recuperación

- Actividad:
  - Restaurar sistemas desde copias de seguridad limpias.
  - Monitorear la infraestructura para asegurar que no quede rastro del atacante.
  - Realizar una evaluación post-incidente para mejorar procesos.

4.3 Comunicación

- Actividad:
  - Informar al equipo de TI, usuarios afectados y, si aplica, a la alta dirección.
  - Documentar las acciones tomadas con transparencia.
  - Proveer una cronología del incidente.

Lista de Verificación Final

- [x] Revisar en la Academia Cisco los conceptos clave del incidente.
- [x] Documentar cada actividad realizada.
- [x] Subir el informe en PDF al apartado de tarea.