LABORATORIO 3 INCIDENTE CRITICO

Phishing

Paso 1: Identificar el Vector de Ataque Inicial

1.1 Revisión de Indicadores Iniciales

Actividad:
Reunir la siguiente información para detectar signos tempranos del incidente:

- Quejas de usuarios sobre correos sospechosos.
- Reportes de accesos no autorizados.
- Fallas o comportamiento anómalo en sistemas específicos (por ejemplo, ralentización, bloqueos).
- Detección de archivos adjuntos no esperados.
- Notificaciones automáticas de antivirus o sistemas EDR.

Posibles vectores de ataque:

- **Phishing** (email malicioso con enlace o archivo adjunto).

1.2 Evaluación de la Evidencia

Actividad:
Recolectar evidencia que apunte al vector de ataque más probable.

Si el phishing es identificado:

- Analizar encabezados de correos electrónicos sospechosos.
- Revisar los enlaces y archivos adjuntos.
- Confirmar si hubo usuarios que hicieron clic o ejecutaron archivos.

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

2.1 Recolección de Logs

Actividad:
Recolectar los siguientes registros:

Logs del servidor de correo electrónico:

- Trazabilidad del correo recibido (IP de origen, remitente, asunto).
- Usuarios que abrieron o hicieron clic en el correo.

Logs del sistema de bases de datos:

- Accesos inusuales o desde cuentas no autorizadas.
- Consultas masivas o fuera de horario.

Logs de seguridad (SIEM / Antivirus / EDR):

- Alertas de ejecución de archivos sospechosos.
- Instalación de software no autorizado.
- Comportamientos anómalos (por ejemplo, conexiones externas).

2.2 Análisis de la Actividad Maliciosa

Actividad:
Buscar patrones inusuales:

- Accesos desde direcciones IP extranjeras.
- Elevación de privilegios.
- Creación de nuevas cuentas.

Herramientas de análisis sugeridas:

- Herramientas nativas de logs (Event Viewer en Windows, journalctl en Linux).

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

3.1 Identificación de Sistemas Comprometidos

Actividad:

- Verificar equipos donde se abrió el correo malicioso.
- Revisar conexiones laterales desde esos sistemas.
- Aislar dispositivos sospechosos de estar comprometidos.

Acciones clave:

- Revisar si el malware se propagó por la red.
- Usar herramientas de monitoreo para detectar comportamiento lateral.

3.2 Evaluación del Impacto

Actividad: Evaluar el impacto del ataque en:

- **Disponibilidad:**
  ¿Hubo interrupción de servicios?

  ¿El ataque afectó la operatividad?

- **Integridad:**
  ¿Se alteraron datos?

  ¿Hay registros modificados o eliminados?

- **Confidencialidad:**
  ¿Se accedió o filtró información sensible?

Paso 4: Proponer Medidas de Contención Inmediatas

4.1 Medidas de Contención Inmediatas

Actividad:

- **Desconectar sistemas comprometidos** de la red.
- **Actualizar sistemas** vulnerables o con software desactualizado.
- **Cambiar credenciales** de usuarios afectados y administrativos.

Otras medidas:

- Aplicar bloqueos en firewall.
- Eliminar persistencias del atacante.

4.2 Plan de Recuperación

Actividad: Desarrollar plan para restaurar la operación normal:

- **Restauración desde copias de seguridad** verificadas y limpias.
- **Monitoreo y validación** post-recuperación para asegurar ausencia de amenazas.

Evaluación Post-Incidente

4.3 Comunicación

Actividad:
Informar adecuadamente sobre el incidente a:

- **Internamente:**
  A equipos de TI, ciberseguridad, dirección y usuarios afectados.
- **Externamente :**
  Autoridades regulatorias (ej. en caso de fuga de datos) y clientes.

Transparencia:

- Documentar todo el proceso.
- Comunicar acciones realizadas y lecciones aprendidas.