**Paso 1: Identificar el Vector de Ataque Inicial**

**1.1 Revisión de Indicadores Iniciales**

**Actividad:**  
Para identificar los primeros signos de un incidente de seguridad, debemos prestar atención a:

* Mensajes extraños en correos electrónicos (asuntos sospechosos, remitentes desconocidos, archivos adjuntos inesperados).
* Fallos inusuales en sistemas específicos (reinicios constantes, lentitud repentina, comportamientos extraños).
* Alertas del antivirus o sistema de detección de intrusos.

**Posibles vectores de ataque:**

| **Vector** | **Señales Comunes** |
| --- | --- |
| Phishing | Correos falsos con enlaces a sitios fraudulentos o adjuntos maliciosos |
| Explotación de vulnerabilidad | Fallos sin razón aparente en servicios conocidos (por ejemplo, Apache, MySQL) |
| Acceso no autorizado | Inicios de sesión desde ubicaciones extrañas o fuera de horario |

**1.2 Evaluación de la Evidencia**

**Actividad:**

* **Si se identifica phishing:** Revisar el contenido del correo, verificar enlaces maliciosos, analizar los encabezados del email para rastrear su origen.
* **Si hay una vulnerabilidad sospechosa:** Revisar versiones de software, identificar servicios sin parches de seguridad, analizar CVEs (Common Vulnerabilities and Exposures).

**Resultado Esperado:**  
Ejemplo: *“Se detectó un correo electrónico de phishing con un archivo adjunto tipo .exe. El usuario lo abrió y, posteriormente, el sistema presentó una conexión saliente inusual a un servidor externo.”*

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

**2.1 Recolección de Logs**

**Actividad:**

* **Servidor de correo electrónico:** Revisar logs de envío/recepción. Buscar intentos de suplantación o correos sospechosos.
* **Base de datos:** Consultar logs de acceso (por ejemplo, intentos de acceso fuera de horario o desde IP desconocidas).
* **Seguridad del sistema:** Verificar alertas del firewall, antivirus, y sistemas IDS/IPS.

**2.2 Análisis de la Actividad Maliciosa**

**Actividad:**  
Buscar patrones anómalos:

* Múltiples intentos fallidos de inicio de sesión.
* Conexiones a IPs no habituales.
* Transferencia masiva de datos.

**Herramientas sugeridas:**

* **Wireshark:** Captura de paquetes.
* **Splunk / ELK Stack:** Análisis de logs.
* **Fail2Ban:** Detección de ataques de fuerza bruta.

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

**3.1 Identificación de Sistemas Comprometidos**

**Actividad:**

* Revisar si el malware se ha propagado a equipos conectados en red.
* Analizar si hubo acceso a servidores críticos o bases de datos sensibles.

**3.2 Evaluación del Impacto**

**Actividad:**  
Evaluar con base en:

* **Disponibilidad:** ¿Se interrumpió algún servicio?
* **Integridad:** ¿Hubo modificación o eliminación de archivos?
* **Confidencialidad:** ¿Se accedió o exfiltró información sensible?

**Ejemplo :**  
*“El sistema de contabilidad fue afectado. Se alteraron registros financieros, y se detectó un intento de acceso a la base de datos de clientes.”*

**Paso 4: Proponer Medidas de Contención Inmediatas**

**4.1 Medidas de Contención**

**Actividad:**

* Desconectar los sistemas infectados de la red.
* Cambiar contraseñas de todos los usuarios.
* Aplicar actualizaciones pendientes de software.

**4.2 Plan de Recuperación**

**Actividad:**

* Restaurar datos desde respaldos verificados.
* Asegurar que los sistemas estén limpios antes de volver a conectar.
* Monitorear en tiempo real para detectar reactivaciones del ataque.

**4.3 Comunicación**

**Actividad:**

* Informar al equipo de TI, gerencia y usuarios afectados.
* Documentar los hechos y acciones tomadas.
* En casos críticos, comunicar a entidades externas (por ejemplo, CERT nacional).

**Transparencia:**  
Proveer detalles sobre qué ocurrió, qué medidas se tomaron y qué acciones seguirán.

**Lista de Verificación Final**

* Revisión de conceptos en Academia Cisco
* Análisis de logs y vectores de ataque
* Mejorar las políticas de uso de redes
* Mayor monitoreo
* Propuesta de medidas de contención
* Plan de recuperación redactado
* Informe final en PDF para subir a la tarea