Laboratorio 3

Paso 1: ataque hipotético (identificar el Vector de Ataque Inicial):

Identificación de los primeros signos del incidente

Información que reunir:

- **Mensajes o correos electrónicos sospechosos recibidos recientemente**
  - Asunto, remitente, contenido, enlaces o archivos adjuntos.
- **Fallos en sistemas específicos:**
  - Inicios de sesión inusuales o desde ubicaciones geográficas no comunes.
  - Bloqueos, ralentizaciones o errores inesperados en aplicaciones críticas.
  - Alertas del antivirus o EDR (Endpoint Detection & Response).
- **Cambios no autorizados en configuraciones o archivos:**
  - Scripts desconocidos ejecutándose en segundo plano.
  - Archivos modificados recientemente sin justificación.
- **Actividad de red anómala:**
  - Conexiones salientes a direcciones IP inusuales.
  - Transferencias de datos masivas fuera del horario habitual.

Recolección de información para identificar el vector de ataque (Phishing)

Fuentes de información:

- **Logs de correos electrónicos:**
  - Revisar encabezados de correos, enlaces incluidos, nombre del archivo adjunto.
- **Análisis de archivos adjuntos:**
  - Hash MD5/SHA1, firmas, comportamiento en entorno sandbox.
- **Usuarios afectados:**
  - ¿Quién abrió el correo? ¿Quién descargó o ejecutó el archivo?
- **Historial de navegación y clics en enlaces:**
  - Registrar URLs visitadas desde correos sospechosos.
- **Capturas o transcripciones de mensajes (correo, chat):**
  - Textos engañosos que suplantan identidad de bancos, RRHH, soporte técnico, etc.

Si el phishing es identificado: ¿Qué se debe buscar?

Parámetros clave:

- **Remitente falsificado o similar a uno legítimo (spoofing):**
  - ej. soporte@micros0ft.com en vez de support@microsoft.com.
- **Presión emocional o urgencia en el mensaje:**
  - "Tu cuenta será bloqueada en 24 horas..."
- **Solicitudes de ingreso de credenciales o descarga de archivos.**
- **Archivos adjuntos comunes usados en phishing:**
  - `.docm`, `.xlsm`, `.zip`, `.exe`, con nombres como `Factura_12345.docm`
- **Ejecución de macros maliciosas o scripts de PowerShell.**
- **Redirección a páginas falsas (phishing web):**
  - Clon de sitios legítimos con formularios falsos de login.

Resultado esperado: Parámetros para identificar el vector inicial

Parámetro	Descripción
Tipo de correo	Phishing con archivo adjunto o enlace
Formato del adjunto	`.zip`, `.docm`, `.exe`, etc.
Actividad del usuario	Apertura del archivo, habilitación de macros, clic en enlaces
Indicadores en sistemas	Infecciones detectadas, ejecución de scripts desconocidos
Logs de red	Comunicación con dominio/IP sospechoso tras la apertura del archivo
Identificación de malware	Hash del archivo, análisis de comportamiento, familia de malware asociada
Usuario objetivo o víctima	¿Fue un ataque dirigido? ¿Phishing masivo?

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

Recolección de Logs: ¿Qué revisar en cada sistema?

Logs del Servidor de Correo Electrónico

Objetivo: Detectar correos de phishing o actividad inusual relacionada con los mismos.

¿Qué buscar?

- **Correos con archivos adjuntos o enlaces sospechosos.**
- **Remitentes falsificados (spoofing) o inusuales.**
- **Tiempos de recepción fuera del horario laboral.**
- **Usuarios que hicieron clic en enlaces o descargaron archivos.**
- **Errores de autenticación (SMTP/IMAP).**
- **Alta frecuencia de envío de un mismo dominio (posible spam).**
- **Mensajes marcados como spam o rechazados por filtros.**

Ejemplo de log (Postfix, Exchange, etc.):

```
Jan 12 10:23:14 mailserver postfix/smtpd[10123]: connect from
unknown[203.0.113.55]
```

Logs del Sistema de Bases de Datos (DBMS)

Objetivo: Verificar accesos no autorizados o extracción de datos.

¿Qué se debería identificar?

- **Consultas inusuales o masivas (SELECT * ... WHERE 1=1).**
- **Accesos fuera del horario habitual.**
- **Errores de autenticación (login fallidos).**
- **Usuarios accediendo a tablas que normalmente no usan.**
- **Cambios o eliminaciones masivas de registros.**
- **Creación de nuevos usuarios sin justificación.**

Ejemplo de log (MySQL):

```
Access denied for user 'admin'@'10.0.0.5' (using password: YES)
```

Logs de Seguridad (SIEM, SO, firewall, endpoint, etc.)

Objetivo: Identificar alertas de comportamiento malicioso.

¿Qué se debe revisar?

- **Alertas de antivirus o EDR (malware detectado).**
- **Ejecutables desconocidos iniciados por el usuario.**

- **Conexiones a IPs o dominios sospechosos.**
- **Instalación de software no autorizado.**
- **Escalamiento de privilegios o modificación de permisos.**
- **Cambios en archivos de sistema.**
- **Tareas programadas nuevas o scripts ejecutados sin justificación.**

Ejemplo de log (Windows Event Viewer):

```
Security Event ID 4625 - An account failed to log on.
```

Análisis de la Actividad Maliciosa

¿Qué patrones buscar?

- **Frecuencia anormal de accesos en corto tiempo.**
- **Mismo usuario accediendo desde múltiples IPs geográficamente distantes.**
- **Usuarios con permisos bajos accediendo a recursos restringidos.**
- **Mismo archivo ejecutado en múltiples terminales.**
- **Transacciones o comandos repetitivos (indicador de automatización).**
- **Secuencia temporal sospechosa (por ejemplo: login + modificación + logout rápida).**

Herramientas de Análisis Recomendadas

Análisis de Logs (Manual y Automatizado)

- **Splunk**: Análisis de grandes volúmenes de logs, alertas y correlación de eventos.
- **ELK Stack (Elasticsearch, Logstash, Kibana)**: Visualización y análisis centralizado de logs.
- **Graylog**: Alternativa ligera a ELK para centralizar y buscar en logs.
- **Wireshark**: Si se sospecha exfiltración de datos o conexiones extrañas.
- **OSSEC / Wazuh**: Detección de intrusos en logs en tiempo real.
- **PowerShell (Windows)** o **Grep/Awk (Linux)** para análisis puntual.

Resultado Esperado:

Una correlación de eventos extraídos de distintos logs que:

- Confirme el ingreso inicial (por ejemplo, apertura de un correo con adjunto malicioso).
- Identifique al usuario afectado y sus acciones posteriores.
- Permita trazar el movimiento lateral o ejecución del malware.
- Proporcione evidencia para aplicar medidas correctivas y preventivas.

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

Identificación de Sistemas Comprometidos

¿Qué se debe realizar al identificar sistemas comprometidos?

Paso 1: Aislar los sistemas afectados

- Desconectar de la red los equipos comprometidos para evitar propagación.
- Preservar los datos para análisis forense (no reiniciar ni formatear aún).

Revisa los sistemas interconectados:

- Verifica si hay conexiones desde/hacia el sistema comprometido.
    - **¿Qué otros dispositivos se comunicaron con él recientemente?**
- Evalúa si hay **movimiento lateral** del atacante (por ejemplo, uso de credenciales robadas).
- Revisa logs de red, RDP, SMB, VPN y otros servicios compartidos.

Evalúa el impacto en la infraestructura crítica:

- ¿Afecta sistemas clave como controladores de dominio, servidores de archivos, bases de datos, correo electrónico, etc.?
- ¿Se interrumpieron servicios esenciales del negocio?
- ¿Se puso en riesgo la seguridad de las copias de respaldo?

Evaluación del Impacto

¿Qué tener en cuenta para evaluar el impacto en la triada CIA?

Disponibilidad:

- ¿Los sistemas afectados están caídos, lentos o inaccesibles?
- ¿Se perdió acceso a servicios esenciales (por ejemplo, correo, ERP, sitio web)?
- ¿Se alteraron cronogramas o se detuvieron procesos críticos?
- ¿Se activó algún ransomware o DoS?

Integridad:

- ¿Se modificaron archivos sin autorización?
- ¿Se alteraron bases de datos o registros de sistema?
- ¿Hay pérdida de precisión o confiabilidad de la información?
- ¿Hay cambios en configuraciones, scripts o políticas de acceso?

Confidencialidad:

- ¿Se exfiltraron datos sensibles (clientes, empleados, finanzas)?
- ¿Se accedió a información clasificada o confidencial sin autorización?
- ¿Se detectaron conexiones a sitios de Command & Control (C2)?
- ¿Se filtraron contraseñas, tokens o llaves privadas?

Resultado Esperado:

Un informe claro que:

- Enumere todos los **sistemas comprometidos** y los **sistemas interconectados potencialmente afectados**.
- Determine si hay impacto en **la operación (disponibilidad), los datos (integridad)** o **la privacidad (confidencialidad)**.
- Clasifique el impacto en bajo / medio / alto riesgo, basado en el análisis de los sistemas y datos afectados.
- Sirva como base para las decisiones de contención, recuperación y comunicación interna y externa.

Paso 4: Proponer Medidas de Contención Inmediatas

Medidas de Contención Inmediatas

Actividad: Medidas para detener el ataque y prevenir propagación

Desconectar sistemas comprometidos:

- Aislar de la red cualquier equipo afectado (WiFi, Ethernet, VPN).
- Suspender sesiones activas sospechosas.
- Usar firewalls para bloquear tráfico malicioso.

Actualización de Sistemas:

- Aplicar parches de seguridad a SO, aplicaciones y firmware.
- Actualizar definiciones de antivirus/EDR.
- Reinstalar software si fue modificado o comprometido.

Cambio de Credenciales:

- Obligar a cambiar contraseñas en cuentas comprometidas o sospechosas.
- Revocar tokens/API keys que pudieron haber sido expuestos.
- Revisar grupos de permisos en cuentas con privilegios elevados.

4.2 Plan de Recuperación

Actividad: Restaurar sistemas afectados y volver a operación normal

Restauración desde Copias de Seguridad:

- Verificar integridad de las copias antes de restaurar.
- Restaurar solo desde backups **previos al incidente**.
- Validar la restauración en un entorno controlado antes de poner en producción.

Monitoreo y Validación:

- Habilitar monitoreo continuo en sistemas restaurados.
- Implementar alertas sobre comportamiento anómalo.

- Analizar tráfico de red, actividad de usuarios y registros del sistema.

Evaluación Post-Incidente:

- Realizar una reunión de cierre (post-mortem) para documentar:
    - Vector de ataque.
    - Tiempo de detección y contención.
    - Medidas tomadas y tiempos de respuesta.
    - Lecciones aprendidas y mejoras al plan de respuesta a incidentes.

4.3 Comunicación

Actividad: A quién informar y qué comunicar

Grupos clave:

- **Internamente:**
    - Equipo de TI / Ciberseguridad.
    - Gerencia / Dirección.
    - Usuarios afectados.
- **Externamente (si aplica):**
    - Clientes.
    - Proveedores.
    - Entidades regulatorias.
    - CERT nacional o sectorial.

Transparencia – ¿Qué se debe realizar?

- Comunicar hechos, no suposiciones.
- Explicar las medidas de contención y recuperación.
- Informar qué datos pudieron verse comprometidos.
- Detallar los pasos a seguir (cambios de contraseña, revisión de sistemas, etc.).
- Mantener actualizaciones periódicas mientras se resuelve el incidente.

Lista de Verificación (Ejemplo para Entrega Académica)

1. Revisar los conceptos en **Cisco Academy** (ciberseguridad, respuesta a incidentes, etc.).
2. Documentar todas las actividades realizadas en formato **PDF**:
    a. Análisis de logs.
    b. Determinación del alcance.
    c. Medidas de contención y recuperación.
    d. Comunicación y evaluación post-incidente.
3. Subir el documento al **apartado de tarea** en la plataforma indicada.
4. Incluir capturas, evidencias o simulaciones si fueron realizadas.