LABORATORIO 3

JERRY RIVERA SANCHEZ

CIBERSEGURIDAD

TALENTO TECH

VALLEDUPAR - CESAR

2025

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

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

Evidencia que Debe Buscarse:

- **Correos Electrónicos Sospechosos:**
    - Remitentes desconocidos o con direcciones similares a las oficiales (spoofing).
    - Enlaces que redirigen a sitios web fraudulentos (verificar URLs).
    - Archivos adjuntos sospechosos (.exe, .zip, .doc con macros o scripts).
- **Logs del Sistema:**
    - Si el usuario hizo clic en un enlace o descargó un archivo, analizar los registros de los clics y de las descargas.
    - Comportamiento del sistema que se active poco después de la interacción (por ejemplo, comportamiento inusual en el antivirus o un aumento en el tráfico de red).
- **Testimonios del Usuario:**
    - ¿El usuario recuerda haber recibido un correo inusual?
    - ¿El correo solicitaba datos sensibles o pedía hacer clic en enlaces para "verificar" cuentas?

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 de correo entrante:**
  - Registros de correos electrónicos recibidos, incluyendo remitente, asunto, direcciones de IP, encabezados (headers), etc.
  - Verificar si el correo tiene características sospechosas: por ejemplo, direcciones de remitente falsificadas (spoofing), encabezados mal formados, o mensajes con links que redirigen a sitios no oficiales.
- **Logs de actividades de usuario:**
  - Verificación de correos electrónicos que los usuarios hayan recibido y abierto (debe correlacionarse con las posibles infecciones).
  - Acciones de los usuarios: ¿han hecho clic en enlaces sospechosos? ¿Han descargado archivos adjuntos?
- **Antivirus/Antispam logs:**
  - Si el correo fue marcado como spam o identificado como phishing, debería haber una entrada en los registros del sistema antispam.
  - Revisión de patrones de detección por firmas de malware o enlaces maliciosos.
- **Autenticación y Accesos:**
  - Revisión de inicios de sesión en los servidores de correo electrónico (si un atacante accedió a una cuenta, quedará registrada).
  - Revisar IPs desconocidas o ubicaciones atípicas desde donde se accedió.

2.2 Análisis de la Actividad Maliciosa:

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

Una vez que se han recolectado los logs, el siguiente paso es realizar un análisis para buscar **patrones inusuales** o indicadores de compromiso (IoC) que puedan ayudar a identificar las actividades maliciosas. Aquí te doy algunos puntos clave para cada tipo de log:

a. Análisis en los Logs de Servidores de Correo Electrónico:

- **Análisis de la fuente del correo (Remitente):**
    - Verificar si el dominio del remitente coincide con el dominio legítimo de la empresa o servicio. Si es un **spoofing** (suplantación de identidad), la dirección de correo del remitente parecerá legítima pero tendrá pequeños errores, como cambios en un carácter.
- **Verificación de enlaces y URLs:**
    - En los encabezados del correo, buscar cualquier URL sospechosa. Puedes usar herramientas de análisis de URL (p. ej., VirusTotal) para comprobar si las URLs están relacionadas con sitios fraudulentos.
    - Si el correo contiene enlaces que llevan a páginas de inicio de sesión, buscar si estas URLs no coinciden con las oficiales de la empresa.

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.

- **Aislamiento Inmediato del Sistema Comprometido:**
  - **Desconectar** el sistema afectado de la red para evitar que el atacante siga propagándose o exfiltrando datos. Esto puede incluir desconectar la máquina afectada físicamente o aislarla a través de firewalls o controles de red.
  - Si el sistema comprometido es un servidor de correo electrónico, un **firewall** o un **IDS/IPS** puede ser configurado para bloquear las comunicaciones con direcciones IP externas sospechosas.
- **Revisión de Registros (Logs):**
  - **Analizar los logs** de los sistemas afectados para detectar qué ocurrió y cómo se comprometió el sistema (por ejemplo, si el atacante logró acceder tras un clic en un correo de phishing).
  - Revisa los logs de acceso, los de actividad del sistema, los de antivirus/antimalware, etc.
- **Detección de Actividad Anómala:**
  - Si el sistema está infectado con **malware** (por ejemplo, un troyano, keylogger, o software de control remoto), debes ejecutar un **análisis completo del sistema** utilizando herramientas de antivirus/malwares actualizados.
  - Verifica si los archivos del sistema se han alterado, si hay procesos desconocidos ejecutándose o si los permisos de las cuentas han cambiado.

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

Una vez que los sistemas comprometidos han sido aislados y estás comenzando a investigar el ataque, es importante evaluar los efectos que el compromiso ha tenido sobre los tres pilares fundamentales de la seguridad de la información:

1. **Impacto en la Disponibilidad de los Datos:**
    - **¿El sistema afectado se ha vuelto inaccesible o ha estado caído?** Si el atacante cifró archivos o bloqueó el acceso al sistema (por ejemplo, con ransomware o algún tipo de malware), esto afecta la **disponibilidad**.
    - **Revisión de interrupciones de servicios**: Verificar si el sistema comprometido proporcionaba servicios a otros usuarios (p. ej., servidores de correo, bases de datos). Si el sistema es crítico, ¿ha afectado la operación normal de la empresa?
2. **Impacto en la Integridad de los Datos:**
    - **¿Se han modificado, alterado o destruido datos?** Un ataque de phishing puede permitir que el atacante obtenga acceso a datos confidenciales o sistemas de gestión de bases de datos. Si se han modificado datos, es importante evaluar si se puede restaurar la versión anterior de esos datos.
    - **Comprobación de integridad de los archivos y registros**: Si el atacante utilizó el acceso para alterar archivos del sistema o bases de datos, debes realizar una auditoría completa para verificar la integridad de los datos.
3. **Impacto en la Confidencialidad de los Datos:**
    - **¿Se ha filtrado información sensible?** Si el atacante obtuvo acceso a datos personales, financieros o cualquier tipo de información confidencial, es crítico evaluar el alcance de la **violación de la confidencialidad**.
        - Revisa si el atacante pudo haber exfiltrado datos a través de canales de comunicación (como correo electrónico, servidores externos, etc.).

4.1 Medidas de Contención Inmediatas:

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

Una vez identificado el incidente y aislado el sistema comprometido, es fundamental tomar medidas inmediatas para contener la amenaza y evitar que se propague a otros sistemas:

- **Desconectar sistemas comprometidos:** Inmediatamente aislar de la red los dispositivos afectados para evitar propagación, robo de datos o instalación de software malicioso adicional.
- **Bloqueo de comunicaciones salientes y entradas sospechosas:** Configurar firewalls para bloquear conexiones desde y hacia direcciones IP sospechosas o dominios maliciosos identificados durante el análisis.
- **Revocar credenciales comprometidas:** Si hay indicios de que credenciales fueron robadas, deshabilitar cuentas afectadas, forzar el cambio de contraseñas y monitorear intentos de acceso no autorizados.
- **Desactivar enlaces maliciosos y correos electrónicos:** Si se identificó un correo de phishing como vector, eliminarlo de todas las bandejas de entrada a través del servidor de correo, y advertir a los usuarios que no lo abran.

4.2 Plan de Recuperación:

Actividad: Desarrollar un plan para restaurar los sistemas afectados y volver a la

La fase de recuperación debe centrarse en restaurar los sistemas afectados a su estado seguro, asegurando la continuidad del negocio y minimizando la pérdida de datos:

- **Restaurar desde copias de seguridad seguras:** Verificar y restaurar los sistemas comprometidos desde backups previos al incidente. Asegurarse de que las copias de seguridad no estén comprometidas.
- **Verificación post-restauración:** Luego de restaurar, ejecutar herramientas de análisis para asegurarse de que no quedan rastros del malware ni puertas traseras.
- **Reinstalación de sistemas críticos (si es necesario):** En caso de compromisos graves, realizar una reinstalación completa del sistema operativo y las aplicaciones en los equipos afectados.
- **Actualizar sistemas y parches de seguridad:** Aplicar todos los parches necesarios a los sistemas restaurados para cerrar las vulnerabilidades explotadas.
- **Pruebas de funcionamiento:** Validar que todos los sistemas restaurados funcionen correctamente y de manera segura antes de volver a ponerlos en producción.
- **Reincorporación a la red:** Una vez validados, reincorporar los sistemas a la red bajo un entorno controlado.

4.3 Comunicación:

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

Una comunicación efectiva es vital durante un incidente de seguridad. Debe dirigirse a varios públicos según la gravedad y naturaleza del ataque:

- **Equipo de respuesta a incidentes (CSIRT):** Mantenerlos informados en tiempo real sobre la evolución del incidente.
- **Alta dirección:** Proveer informes periódicos del impacto, acciones tomadas, y los riesgos actuales para apoyar en la toma de decisiones estratégicas.
- **Usuarios internos:** Notificar sobre el incidente, instrucciones específicas (por ejemplo, cambio de contraseñas, no abrir ciertos correos), y medidas adoptadas.
- **Departamentos legales y cumplimiento:** Si hay implicaciones legales o regulatorias (p. ej., filtración de datos personales), el equipo legal debe ser notificado para activar el protocolo correspondiente.
- **Clientes o terceros afectados:** En caso de violación de datos sensibles, puede ser necesario comunicar a los clientes afectados y a las autoridades de protección de datos (según la legislación aplicable, como el Habeas Data o el GDPR en otros países).