LABORATORIO 3

CIBERSEGURIDAD

FABIAN ANDRES BENJUMEA

UNIVERSIDAD POPULAR DEL CESAR

VALLEDUPAR

2025

Actividad: que información reunirías para identificar los primeros signos del incidente (mensajes extraños, fallos en sistemas específicos).

Recibí un ataque de phishing

Mensajes Sospechosos (Emails, SMS, Mensajería Interna)

- Copia del mensaje recibido (cabecera incluida si es email).
- Dirección del remitente (ver si imita una oficial).
- Asunto del mensaje.
- Enlaces incluidos (sin hacer clic, solo inspeccionarlos).
- Archivos adjuntos.
- Hora y fecha de recepción.

Comportamiento Anómalo del Sistema o Usuario

- Reportes de usuarios que hicieron clic en enlaces o descargaron archivos.
- Cambios en configuraciones de cuentas (como contraseñas o correo de recuperación).
- Fallos al iniciar sesión o accesos desde ubicaciones inusuales.
- Aparición de pop-ups o redirecciones extrañas en navegadores.
- Alertas de antivirus o sistemas de seguridad.

Análisis Técnico (si es posible)

- Registro de eventos del servidor de correo (log de entrega, IP del remitente).
- Rastreo de enlaces sospechosos (ver si redirigen a sitios de phishing conocidos).
- Detección de tráfico inusual hacia dominios desconocidos.
- Hash de archivos adjuntos para análisis en sandbox o antivirus.

Testimonios y Reportes de Usuarios

- ¿Quién recibió el mensaje?
- ¿Qué acción realizaron (clic, descarga, ingreso de credenciales)?
- ¿Notaron algo inusual tras la interacción?

Sistemas Afectados o Comprometidos

- Cuentas que reportaron actividad no autorizada.
- Servicios o sistemas donde hubo fallos justo después del mensaje.
- Pérdida de acceso o bloqueo de usuarios.

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

¿Qué se debe buscar si se confirma que fue phishing?

1. Información del Correo/Mensaje Sospechoso

- **Cabeceras completas del correo electrónico**
  Permiten rastrear IPs de origen, servidores usados, posibles redirecciones.
- **Remitente del mensaje**
  Comparar si el dominio está falsificado (ej. soporte@micros0ft.com).
- **Contenido del mensaje**
  Ver si contiene amenazas, urgencia, errores gramaticales o llamados a la acción inusuales.
- **Archivos adjuntos o enlaces**
  Analizar qué tipo de archivo es (.zip, .exe, .doc con macros), o a qué URL dirige.
- **Firma digital o indicadores de autenticidad falsificados o ausentes**

2. Datos sobre los Enlaces o Archivos Adjuntos

- **URL destino**
  Usar herramientas como VirusTotal, URLScan, o sandbox para analizar.
- **Dominios utilizados en el phishing**
  Son nuevos, similares a dominios legítimos o con registros WHOIS sospechosos.
- **Hashes de los archivos adjuntos**
  Para detección en motores antivirus y correlación con campañas conocidas.

3. Comportamiento de los Usuarios Involucrados

- ¿Alguien **hizo clic en el enlace**? ¿Ingresó credenciales?
- ¿Se descargó algún archivo?

- ¿Hubo alguna acción tras la interacción (cambio de contraseña, movimientos sospechosos)?

4. Rastreo en Sistemas y Logs

- **Logs del servidor de correo**
  Para confirmar envío y recepción del mensaje.
- **Logs de acceso a cuentas**
  Horarios, IPs inusuales, cambios en las sesiones.
- **Alertas del antivirus o EDR**
  Si detectaron comportamientos anómalos tras abrir el mensaje.

5. Indicadores de Compromiso (IoCs)

- Direcciones IP sospechosas.
- Dominios/URLs usados en el ataque.
- Hashes de archivos adjuntos.
- Scripts, malware, troyanos asociados.

6. Usuarios Afectados o Vulnerables

- Nombres de usuarios que recibieron o interactuaron con el phishing.
- Roles críticos que puedan amplificar el riesgo (TI, finanzas, dirección).
- Cuentas con acceso privilegiado que fueron potencialmente comprometidas.

Herramientas útiles para análisis

- **VirusTotal** (archivos y enlaces)
- **URLScan.io** (análisis de sitios)
- **WHOIS** (información de dominio)
- **MxToolbox** (cabeceras de correo y reputación)

- **Outlook Headers Analyzer** (extrae y analiza cabeceras de email)

Actividad: Describir cuales pueden ser los logs de los sistemas afectados que se deben revisar (servidores de correo electrónico, bases de datos, terminales). - Logs del Servidor de Correo Electrónico: Que se debe buscar.

Logs del Servidor de Correo Electrónico – ¿Qué revisar?

Tipos de Logs que pueden estar disponibles:

- Logs de envío y recepción (Mail Transfer Logs)
- Logs de autenticación (SMTP/IMAP/POP)
- Logs de filtro antispam/antivirus
- Logs de reglas de transporte o reglas personalizadas
- Logs de auditoría de buzón (si están habilitados)

¿Qué se debe buscar en estos logs?

- Detalles del Mensaje de Phishing
- Fecha y hora de recepción del correo sospechoso.
- Dirección IP del servidor remitente (¿es sospechosa o lista negra?).
- Dominio del remitente (¿es legítimo o falsificado?).
- Nombre del remitente visible vs dirección real.
- Asunto del mensaje, para facilitar el rastreo de copias similares.

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

Herramientas de Análisis: Que herramientas de análisis se podrían utilizar para los logs

Análisis de Logs para Buscar Patrones Inusuales

Análisis de Logs de Correo Electrónico

- Accesos desde IPs desconocidas o países no habituales.
- Altos volúmenes de mensajes salientes (indicio de un botnet o cuenta comprometida).
- Reenvíos masivos de correos dentro de la organización.
- Cambios en las reglas del servidor de correo (ej. reenvíos automáticos a direcciones externas).
- No coincidencias en los encabezados de los correos (ej. SPF, DKIM, DMARC).
- Errores de autenticación repetidos desde IPs fuera de la región normal de operación.

Actividad: que se debe realizar cuando se identifica los sistemas comprometidos.
Revisa los sistemas interconectados: Evalúa el impacto en la infraestructura crítica: 3.2 Evaluación del Impacto:

Cuando se identifica que los sistemas están comprometidos debido a un ataque de phishing (o cualquier otro tipo de ataque cibernético), es crucial seguir un protocolo adecuado para mitigar el daño, aislar los sistemas comprometidos y evaluar el impacto en la infraestructura crítica de la organización.

Pasos a seguir cuando se identifican sistemas comprometidos:

1. Aislar los Sistemas Comprometidos

- **Desconectar de la red**: Si se confirma que un sistema está comprometido, se debe aislarlo inmediatamente de la red para evitar que el atacante pueda moverse lateralmente o exfiltrar datos.

- **Deshabilitar cuentas comprometidas**: Cambiar contraseñas, suspender cuentas de usuario afectadas y deshabilitar accesos remotos o VPNs comprometidos.
- **Desactivar servicios vulnerables**: Si el ataque ha explotado vulnerabilidades específicas en ciertos servicios o aplicaciones, es recomendable desactivarlos hasta que se pueda realizar un análisis de seguridad completo.

2. Evaluar el Impacto en la Infraestructura Crítica

La infraestructura crítica es cualquier componente esencial que mantiene el funcionamiento de la organización. Esto incluye:

- **Servidores** (bases de datos, aplicaciones críticas, servidores web).
- **Redes** (firewalls, switches, routers).
- **Sistemas de control** (SCADA, industrial, IoT).
- **Plataformas de comunicación** (email, intranet).
- **Sistemas de almacenamiento de datos** (archivos, backups).

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

Disponibilidad

La **disponibilidad** se refiere a que los datos y los sistemas estén **accesibles** y **funcionales** cuando se necesiten. Un ataque puede comprometer la disponibilidad de diferentes formas, como la **denegación de servicio** (DoS), el **secuestro de datos**, o la **destrucción de recursos**.

¿Qué se debe evaluar para la disponibilidad?

- **Interrupción de servicios**: ¿Se ha producido una caída en los sistemas críticos (servidores, aplicaciones, bases de datos)? Si es así, ¿qué tan graves son las interrupciones y cuánto tiempo han durado?
- **Rendimiento degradado**: ¿Los sistemas están funcionando de manera más lenta de lo habitual debido a la sobrecarga del sistema o al tráfico malicioso generado por el ataque?

Integridad

La integridad se refiere a que los datos sean exactos, completos y no hayan sido alterados de manera no autorizada. Un atacante podría alterar la integridad de los datos, ya sea modificando, eliminando o corrompiendo información clave.

¿Qué se debe evaluar para la integridad?

- **Modificación de datos**: ¿Existen indicios de que los datos han sido **manipulados**? Por ejemplo, si un atacante ha cambiado registros en bases de datos (como información financiera o personal), o si se ha utilizado software malicioso para modificar archivos.
- **Pérdida de datos**: ¿Se han **eliminado** o **corrompido** datos debido al ataque? Esto podría incluir archivos de clientes, registros financieros o datos de transacciones.

Confidencialidad

La confidencialidad se refiere a que los datos solo sean accesibles para aquellas personas o sistemas autorizados. Los ataques de phishing pueden comprometer la confidencialidad mediante el robo de credenciales, acceso no autorizado o exfiltración de información confidencial.

¿Qué se debe evaluar para la confidencialidad?

- **Acceso no autorizado a datos sensibles**: ¿El atacante ha conseguido acceder a información confidencial (por ejemplo, contraseñas, datos personales, registros financieros, secretos comerciales)?
- **Exfiltración de datos**: ¿Se ha producido una fuga de información hacia destinos no autorizados (servidores externos, cuentas de email) o se han comprometido sistemas de almacenamiento?

Resultado Esperado:

- Identificar **qué datos sensibles han sido comprometidos**, cómo se exfiltraron (por ejemplo, correos electrónicos, credenciales de acceso) y cuántos usuarios se vieron afectados.

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

Desconectar sistemas comprometidos

Una de las primeras acciones críticas que debes realizar es aislar y desconectar cualquier sistema que haya sido comprometido para evitar que el atacante pueda propagar el ataque a otros sistemas o exfiltrar más datos.

Acciones Específicas:

- **Desconectar de la red**: Desconecta inmediatamente los sistemas comprometidos de la red corporativa (mediante el desconectar físicamente los cables de red o desactivar las interfaces de red).
- **Desactivar conexiones remotas**: Si los atacantes han obtenido acceso a través de VPN o escritorio remoto, desactiva todos los accesos remotos a estos sistemas comprometidos para evitar que sigan controlándolos.

Actualización de Sistemas

Después de identificar el ataque, es fundamental asegurarse de que los sistemas estén actualizados y protegidos contra posibles vectores de ataque similares, como las vulnerabilidades de zero-day que pudieron haber sido explotadas.

Acciones Específicas:

- **Aplicar parches de seguridad**: Asegúrate de que todos los sistemas afectados, así como los que podrían estar en riesgo, tengan parches de seguridad aplicados, especialmente en sistemas operativos y aplicaciones críticas.
- **Sistema operativo**: Asegúrate de que tanto servidores como estaciones de trabajo estén actualizados con los últimos parches de seguridad.

Cambio de Credenciales

El cambio de credenciales es una medida crítica para prevenir que los atacantes sigan utilizando las cuentas comprometidas. Especialmente cuando se han obtenido credenciales válidas como resultado de un ataque de phishing, cambiar contraseñas y habilitar medidas de autenticación adicionales es esencial.

Acciones Específicas:

- **Cambio inmediato de contraseñas**:
    - Cambia las contraseñas de todas las cuentas de usuario que se sospeche han sido comprometidas.
    - Cambia las contraseñas de administración y credenciales de servicio que se pudieran haber visto comprometidas, como las que permiten el acceso remoto o la administración de sistemas críticos.

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

Restauración desde Copias de Seguridad

Objetivo: Recuperar los sistemas comprometidos utilizando las copias de seguridad (backups) más recientes y verificadas, asegurando la integridad y disponibilidad de los datos, y minimizando el impacto operativo.

Pasos a seguir:

1. Verificar la integridad de las copias de seguridad:
2. Restaurar sistemas críticos:
3. Comprobar la consistencia de los datos:
4. Reconfigurar sistemas afectados:
5. Realizar una prueba de funcionamiento:

Monitoreo y Validación

Objetivo: Garantizar que los sistemas restaurados estén funcionando correctamente y monitorear el entorno para detectar cualquier posible signo de actividad maliciosa o compromisos adicionales.

Pasos a seguir:

1. Monitoreo intensivo post-restauración:
2. Verificación de la integridad de los sistemas restaurados:
3. Validación del acceso y las credenciales:
4. Reactivar servicios y aplicaciones:

5. Verificar la restauración de la conectividad:

Evaluación Post-Incidente

Objetivo: Evaluar el impacto del ataque, comprender las lecciones aprendidas y tomar medidas para fortalecer la infraestructura y prevenir futuros incidentes.

Pasos a seguir:

1. Análisis de la causa raíz:
2. Evaluación del impacto:
3. Revisión de las políticas y procedimientos de seguridad:
4. Mejoras en la infraestructura de seguridad:
5. Capacitación y concientización del personal:
6. Comunicación y reportes: