Victor Daniel Torres Solano – Laboratorio 3

1.1.

- Mensajes raros en el correo o en pantalla (por ejemplo, errores que nunca habían salido).
- Usuarios que dicen que no pueden entrar o que ven cosas diferentes.
- Programas que se cierran solos o que funcionan lento.
- Cambios en archivos sin explicación (como archivos que desaparecen o se modifican solos).
- Sesiones abiertas con usuarios que no deberían estar conectados.

1.2.

Si se sospecha de phishing, ¿qué se debe buscar?

- Correos raros con enlaces sospechosos o archivos adjuntos.
- Quejas de usuarios que recibieron mensajes pidiendo datos personales o contraseñas.
- Cuentas comprometidas, es decir, que alguien entró sin permiso después de que el usuario hizo clic en algo.
- Registros (*logs*) que muestren que se abrió un enlace o se inició sesión desde una IP extraña.
- Cambios en la contraseña sin que el usuario los haya hecho.

Si se sospecha de una *vulnerabilidad*, ¿qué se debe identificar?

- Versiones de software sin actualizar o con errores conocidos.
- Servicios abiertos al internet que no deberían estar accesibles.
- Errores en los registros del sistema, como intentos de acceso repetidos.
- Programas que se comportan raro o que no deberían estar corriendo.
- Accesos sospechosos a funciones que solo usan los administradores.

2.1.

Logs del servidor de correo electrónico: ¿Qué se debe buscar?

- Correos salientes sospechosos desde cuentas internas (puede ser una señal de cuenta robada).
- Errores de entrega inusuales (como correos rechazados por spam).
- Inicios de sesión raros en las cuentas de correo (por ejemplo, desde otros países o a horas inusuales).
- Enlaces o archivos enviados a varios usuarios (posible phishing).

Logs del sistema de bases de datos: ¿Qué se debería identificar?

- Consultas extrañas o pesadas, como intentos de sacar todos los datos de una tabla.
- Cambios en los datos hechos por usuarios que no deberían tener permiso.
- Intentos fallidos de conexión (alguien podría estar tratando de adivinar contraseñas).
- Accesos desde IPs desconocidas.

Logs de seguridad (de cualquier sistema): ¿Qué se debe revisar?

- Alertas de antivirus o firewall (por ejemplo, archivos bloqueados o conexiones bloqueadas).
- Intentos de acceso fallidos repetidos (alguien tratando de entrar sin permiso).
- Cambios en configuraciones del sistema o cuentas de usuario.
- Archivos ejecutados que normalmente no se usan.

2.2.

¿Qué se debe analizar en los logs para encontrar actividad rara?

- Muchos intentos fallidos de acceso (alguien tratando de adivinar contraseñas).
- Inicios de sesión en horarios raros (por ejemplo, de madrugada).
- Accesos desde lugares desconocidos o países lejanos.
- Cambios en archivos o configuraciones que no fueron autorizados.
- Usuarios nuevos que no deberían existir o que tienen muchos permisos.
- Programas o comandos que se ejecutaron y no son comunes en el sistema.
- Repetición de acciones sospechosas (por ejemplo, muchas búsquedas en la base de datos).

¿Qué herramientas se pueden usar para revisar los logs?

- **Event Viewer (Visor de eventos)**: viene con Windows, sirve para revisar errores y accesos.
- **Syslog:** sistema de registro en servidores Linux.
- **Wireshark:** analiza el tráfico de red, útil si crees que los datos están saliendo sin permiso.
- **Splunk**: herramienta para buscar y analizar grandes cantidades de logs.
- **ELK Stack (Elasticsearch, Logstash, Kibana):** sistema para juntar, buscar y ver logs con gráficos.
- **Logwatch o GoAccess:** generan reportes simples en servidores Linux.
- **Notepad++ o Excel**: si los logs están en texto, puedes abrirlos ahí para buscar cosas raras.

3.1.

¿Qué se debe hacer cuando se detectan sistemas comprometidos?

Revisar los sistemas interconectados

- Ver si el sistema afectado se comunica con otros sistemas (como servidores, bases de datos o computadoras de la red).
- Revisar si esos otros sistemas también muestran señales raras o están en riesgo.
- Cortar temporalmente la conexión si es necesario, para evitar que el ataque se propague.

Evaluar el impacto en la infraestructura crítica

- **Ver si el ataque afectó partes importantes como:**
    - Servidores principales
    - Sistemas de respaldo
    - Sistemas que controlan accesos o servicios clave
- **Preguntarse:**
    - ¿El ataque puede detener el trabajo de la empresa?
    - ¿Se perdió información importante?
    - ¿Está en riesgo la seguridad de los usuarios o clientes?

¿Qué se debe tener en cuenta para evaluar el impacto en...

Disponibilidad

- Ver si los sistemas están funcionando o si se cayeron.
- Comprobar si los usuarios pueden acceder a los datos o servicios.
- Revisar si hubo interrupciones, cuánto tiempo duraron y cuántos usuarios afectó.

Integridad

- Ver si los datos fueron cambiados, eliminados o corrompidos sin permiso.
- Comparar los datos actuales con respaldos o registros anteriores.
- Comprobar si los resultados del sistema son confiables.

Confidencialidad

- Revisar si se robaron o expusieron datos privados o sensibles.
- Identificar si hubo accesos no autorizados a información confidencial.
- Evaluar si hubo filtraciones de información, como datos personales o contraseñas.

Resultado Esperado:

- Saber qué tan grave es el daño y en qué áreas (disponibilidad, integridad, confidencialidad).
- Poder decidir qué se repara primero y cómo se comunica el incidente.
- Tener una idea clara para hacer mejoras y evitar que pase de nuevo.

4.1.

Medidas de Contención Inmediatas

Desconectar sistemas comprometidos

- Separar de la red cualquier computadora o servidor que esté afectado.
- Esto evita que el ataque se propague a otros sistemas conectados.
- También ayuda a analizar el sistema sin que el atacante siga teniendo acceso.

Actualización de sistemas

- Instalar parches de seguridad y actualizaciones pendientes del sistema operativo y programas.
- Esto cierra las puertas por donde el atacante pudo haber entrado.
- Asegurarse de que todo el software esté actualizado para evitar más vulnerabilidades.

Cambio de credenciales

- Cambiar contraseñas de los usuarios afectados, especialmente los que tengan permisos altos.
- Obligar a todos los usuarios a actualizar sus claves, por precaución.
- Revisar si hay cuentas falsas o nuevas creadas por el atacante.

4.2.

Restauración desde Copias de Seguridad

- Verificar que las copias de seguridad sean recientes y no estén comprometidas.
- Restaurar los sistemas afectados usando estas copias para devolver los datos y configuraciones a su estado previo al ataque.
- Asegurarse de que los datos restaurados sean correctos y no estén alterados.

Monitoreo y Validación

- Vigilar los sistemas de cerca después de la restauración para asegurarse de que no haya nuevas señales de ataque.
- Validar que todo funcione correctamente (redes, bases de datos, aplicaciones).
- Revisar logs y alertas de seguridad para ver si hay actividad sospechosa.

Evaluación Post-Incidente

- Hacer una revisión completa de todo lo ocurrido: cómo empezó el ataque, qué impacto tuvo y cómo se resolvió.
- Evaluar si el plan de respuesta fue efectivo y qué se puede mejorar.
- Actualizar las medidas de seguridad para evitar que el incidente se repita.

4.3.

¿A quién se le debe informar sobre la situación?

- A los líderes de la empresa o responsables: Para que tomen decisiones y asignen recursos si es necesario.
- A los usuarios afectados: Informarles si sus datos o cuentas están comprometidos.
- A los equipos de seguridad y técnicos: Para que sigan trabajando en la resolución del problema.
- A las autoridades, si es necesario: Si el ataque afecta a datos personales o es un incidente grave, puede que haya que notificarlo a organismos oficiales.
- A los clientes o proveedores: Si el incidente afecta la entrega de servicios o productos.

¿Qué se debe realizar?

- Ser honesto y claro sobre lo que ocurrió. Explicar qué se sabe hasta el momento y lo que se está haciendo para solucionar el problema.
- Evitar dar información incorrecta o incompleta que pueda generar más confusión o preocupación.
- Mantener informadas a las partes interesadas durante todo el proceso de recuperación.
- Asegurarse de que los mensajes sean coherentes y claros para que no haya malentendidos.