Saul Hernandez Castilla

CASO ESCENARIO:

Un servidor de bases de datos muestra fallos inusuales y pérdida de registros.

PARTE 1: IDENTIFICAR EL VECTOR DE ATAQUE INICIAL

EXPLOTACION DE VULNARIBILIDAD

- Sistemas desactualizados sin parches de seguridad.
- Logs de explotación de servicios.
- Registros de ejecución de comandos no autorizados.

RESULTADO ESPERADO: Determinar que el vector inicial fue la explotación de una vulnerabilidad en el servidor.

PARTE 2: RECOLECCION DE LOGS

Logs del Sistema de Bases de Datos

- Consultas inusuales o complejas: Como UNION SELECT, que pueden indicar intentos de inyección SQL.
- Accesos fuera de horario o por usuarios no habituales.
- Errores de autenticación: Intentos fallidos que podrían indicar escaneo de credenciales.

Logs de Seguridad (Sistema Operativo, Firewall, Antivirus, etc.)

- Alertas de antivirus/antimalware: Identificación de archivos maliciosos detectados.
- Eventos de inicio de sesión fallidos o inusuales.
- Cambios en permisos de archivos o cuentas.

Análisis de la Actividad Maliciosa

- **Qué análisis realizar**:
    - Correlacionar momentos de caída del servidor con accesos anómalos.
    - Identificar qué usuario o servicio fue explotado.
    - Revisar creación de usuarios administrativos no autorizados.
- **Herramientas de análisis**:
    - SIEM (Wazuh, AlienVault).
    - Osquery para auditar sistemas.
    - Vulnerability Scanners (Nessus, OpenVAS) para confirmar vulnerabilidades

PARTE 3: DETERMINAR EL ALCANCE DEL COMPROMISO Y LOS SISTEMAS AFECTADAS

Actividad: ¿Qué se debe realizar al identificar los sistemas comprometidos?

- **Aislar el sistema afectado:**
    - Desconectarlo de la red para evitar que el ataque se propague. **(Impacto 4.8)**
    - Desactivar accesos remotos temporalmente. **(Impacto 4.4)**
- **Preservar la evidencia:**
    - No apagar el sistema de inmediato. **(Impacto 3.2)**
    - Realizar una copia forense de los discos y de la memoria.**(Impacto 4.4)**
- **Analizar logs y comportamientos:**
    - Revisar registros recientes, procesos activos, usuarios conectados, cambios no autorizados. **(Impacto 4.5)**

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

Disponibilidad

- ¿Se interrumpieron servicios clave?
- ¿Cuánto tiempo han estado inactivos?
- ¿Cuál fue el alcance del tiempo de inactividad?
- **Ejemplo de resultado esperado:** Servicio restaurado en menos de 1 hora, sin pérdida de funcionalidad permanente.

Integridad

- ¿Se alteraron datos o configuraciones?
- ¿Hay archivos modificados sin autorización?
- ¿Se borró información sensible o registros importantes?
- **Resultado esperado:** Detección de cambios ilegítimos y recuperación desde respaldo confiable.

Confidencialidad

- ¿Se accedió a información sensible (usuarios, claves, datos personales, financieros)?
- ¿Se ha producido una posible fuga de datos?
- ¿Se han detectado transferencias de información a destinos no autorizados?

Resultado esperado: Confirmación de que no hubo fuga o, si la hubo, dimensionar el alcance y notificar según ley.

PARTE 4: PROPONER MEDIDAS DE CONTENCIÓN INMEDIATAS

Actividad: ¿Qué medidas se pueden implementar para detener el ataque y prevenir una mayor propagación?

Desconectar sistemas comprometidos

- Aislar de la red cualquier equipo afectado.
- Bloquear puertos y conexiones activas sospechosas.
- Detener servicios críticos si están siendo utilizados por el atacante.

Actualización de sistemas

- Aplicar parches de seguridad pendientes en todos los sistemas.
- Verificar que el software esté actualizado y sin vulnerabilidades conocidas.
- Reforzar configuraciones seguras.

Cambio de credenciales

- Cambiar contraseñas de usuarios con acceso a los sistemas afectados.
- Forzar la revocación de sesiones activas.
- Establecer autenticación multifactor si es posible.

Saul Hernandez Castilla

PLAN DE RECUPERACIÓN

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

Restauración desde copias de seguridad

- Verificar la integridad de las copias antes de restaurar.
- Restaurar únicamente desde puntos anteriores al incidente.
- Documentar el proceso de restauración.

Monitoreo y validación

- Supervisar los sistemas restaurados para detectar nuevas actividades anómalas.
- Validar que los datos y configuraciones sean correctos.
- Realizar pruebas de funcionamiento de los servicios críticos.

Evaluación post-incidente

- Documentar cronológicamente lo sucedido.
- Realizar un análisis de causa raíz.
- Evaluar el tiempo de respuesta, efectividad de las acciones y mejoras necesarias.

Comunicación

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

Transparencia: ¿Qué se debe realizar?

- Informar con claridad y prontitud a las partes interesadas (usuarios, directivos, TI, legales).
- Explicar qué ocurrió, qué se hizo para mitigarlo, y qué medidas se tomarán a futuro.
- Comunicar a entidades regulatorias si la ley lo exige (por fuga de datos, por ejemplo).
- Mantener actualizada a la dirección sobre el estado de la recuperación.