Dilan Aragón

Laboratorio 3 Ciberseguridad

Paso 1

1. ¿Qué ataque recibiste?
   /R. Virus Troyano
2. ¿Por qué?
   /R. El archivo virus parecía un instalador legitimo debido a que tenia el antivirus desactivado por acciones anteriores, este programa paso por desapercibido y el equipo empezó a mostrar ventanas emergentes de CMD.
3. ¿Qué harías?
   /R. Activar el antivirus y hacer un escaneo completo de sistema de manera rigurosa o restaurar el equipo a su copia de seguridad anterior.

Paso 2

1. ¿Cuáles Pueden ser los logs de los sistemas afectados que se deben revisar? (servidores de correo electrónico, bases de datos, terminales).
   /R.
   Servidores de correo electrónico:
   Logs de envío y recepción de correos: Para buscar correos sospechosos que puedan haber contenido el troyano o ejecutando comandos maliciosos.

   Bases de datos:
   Logs de acceso: Para identificar accesos no autorizados a la base de datos o intentos de explotación.

   Terminales:
   Logs del antivirus: Para verificar si el troyano fue detectado, bloqueado o pasó desapercibido

2. ¿Qué análisis se deben realizar en los logs para buscar patrones inusuales?
   /R.
   Revisar intentos de acceso no autorizados: Buscar múltiples intentos fallidos de inicio desde ubicaciones geográficas inusuales.

   Comportamientos anómalos en el tráfico de red: Detectar conexiones inusuales que podrían estar relacionadas con la exfiltración de datos.
   Actividades sospechosas de archivos: Verificar si hay programas ejecutándose de manera inesperada.

3. ¿Qué herramientas de análisis se podrían utilizar los logs?
   /R.
   - Visor De eventos de Windows
   - WireShark
   - Splunk

Paso 3

1. ¿Qué se debe realizar cuando se identifica los sistemas comprometidos?
   /R.
   - **Contener la amenaza:** Si el ataque es un troyano, procedería a eliminar el código infectado utilizando herramientas antivirus o de eliminación de malware.

   - **Restaurar desde copias de seguridad**: Restauraría los sistemas comprometidos desde copias de seguridad limpias y no infectadas.

   - **Realizar un análisis forense:** Revisaría las evidencias de los sistemas comprometidos para entender cómo se produjo el ataque.

2. ¿Qué se debe tener en cuenta para evaluar el impacto en la disponibilidad, integridad y confidencialidad de los datos?
   /R.
   - **Disponibilidad:** Determinar si los sistemas comprometidos están fuera de servicio o si la red está afectada. Esto puede incluir la caída de servidores, denegación de servicio (DoS), o bloqueos en la comunicación.

   - **Integridad**: Comprobar si los datos han sido alterados, corrompidos o eliminados. Si los atacantes han tenido acceso a bases de datos o archivos sensibles, puede haber manipulado la información.

   - **Confidencialidad**: Determinar si los atacantes han robado o comprometido datos sensibles, como credenciales de acceso, información personal, financiera o confidencial.

Paso 4

1. ¿Qué plan Desarrollarías restaurar los sistemas afectados y volver a la operación normal?

/R.
Empezaría con el **aislamiento inmediato** de los sistemas comprometidos para evitar la propagación del ataque, seguido de un **análisis forense** exhaustivo para identificar la naturaleza de la intrusión, **conservar evidencia** y determinar los sistemas afectados. después, se elimina la amenaza mediante **herramientas antivirus**, aplicando **parches de seguridad** y cerrando vectores de ataque, como contraseñas débiles, los sistemas se restauran desde **copias de seguridad**, asegurando la aplicación de actualizaciones y configuraciones de seguridad.

2. Determina a quién se le debe informar sobre la situación, las medidas tomadas, y las siguientes etapas.
    - Transparencia: que se debe realizar

/R.
A la **alta dirección** sobre el impacto y medidas de restauración, luego al **equipo de TI y seguridad**, Después me dirijo **usuarios afectados** con detalles de recuperación, más tarde a **clientes y proveedores** si están impactados, a **agencias regulatorias** y, por último, a los **medios de comunicación** si el programa es “Famoso”.