MODULO 3 – Capítulo 6

Ejercicio – antivirus: comparativa

Realizar una comparativa de antivirus para evaluar su capacidad de detección de amenazas, como el keylogger Spyrix, requiere un enfoque metódico y preciso. A continuación, te proporciono un procedimiento paso a paso para llevar a cabo esta evaluación en máquinas virtuales Windows 11:

Preparativos iniciales

1. **Configura las máquinas virtuales:**
    - Crea varias máquinas virtuales con Windows 11 instalado.
    - Asegúrate de que cada máquina tenga acceso a internet para actualizar los antivirus y realizar las pruebas.
    - Configura un punto de restauración o instantánea (snapshot) antes de instalar cualquier software malicioso.
2. **Descarga e instala los antivirus gratuitos:**
    - Descarga las versiones gratuitas más recientes de:
        - Avast
        - AVG
        - NOD32 (ESET)
        - Malwarebytes
        - Avira
        - ClamWin
        - Norton
        - Kaspersky
    - Instala cada uno en una máquina virtual diferente.
3. **Actualiza los antivirus:**
    - Antes de comenzar las pruebas, asegúrate de que todos los antivirus estén completamente actualizados con las últimas bases de datos de firmas.
4. **Obtén una copia del archivo malicioso (Spyrix Keylogger):**
    - Descarga una versión legítima del Spyrix Keylogger desde una fuente confiable (por ejemplo, sitios web de malware para pruebas, como VirusShare o Malware Bazaar).
    - Guarda el archivo en un lugar seguro fuera de las máquinas virtuales.
5. **Crea un entorno controlado:**
    - Desactiva temporalmente la conexión a internet en las máquinas virtuales durante las pruebas para evitar que el malware se comunique con servidores externos.

- Utiliza herramientas como Wireshark o Procmon para monitorear el comportamiento del sistema si es necesario.

Procedimiento paso a paso

Paso 1: Preparación de la prueba

1. Restaura la instantánea (snapshot) de la máquina virtual para garantizar condiciones iniciales consistentes.
2. Verifica que el antivirus esté activo y funcionando correctamente.
3. Documenta el estado inicial del sistema (por ejemplo, archivos en disco, procesos en ejecución).

Paso 2: Introducción del archivo malicioso

1. Copia el archivo Spyrix Keylogger al escritorio de la máquina virtual.
2. Observa si el antivirus detecta automáticamente el archivo al ser copiado.
    - Si lo detecta, registra el mensaje de advertencia y la acción tomada (cuarentena, eliminación, etc.).
    - Si no lo detecta, continúa con el siguiente paso.

Paso 3: Ejecución del archivo malicioso

1. Intenta ejecutar el archivo Spyrix Keylogger manualmente.
2. Observa si el antivirus bloquea la ejecución.
    - Si lo bloquea, registra el mensaje de advertencia y la acción tomada.
    - Si permite la ejecución, documenta este fallo.

Paso 4: Escaneo manual

1. Realiza un escaneo completo del sistema utilizando el antivirus instalado.
2. Verifica si el archivo Spyrix Keylogger es detectado durante el escaneo.
    - Si es detectado, registra el tiempo de detección y la acción tomada.
    - Si no es detectado, documenta este resultado.

Paso 5: Comprobación del comportamiento del malware

1. Si el archivo malicioso no fue detectado ni bloqueado:
    - Verifica si el malware ha logrado instalar servicios o componentes adicionales en el sistema.
    - Usa herramientas como `Task Manager` o `Autoruns` para identificar nuevos procesos o entradas en el registro del sistema.

Paso 6: Repetición con otros antivirus

1. Repite los pasos anteriores en cada máquina virtual con un antivirus diferente.
2. Documenta los resultados obtenidos para cada producto.

Documentación de resultados

Para cada antivirus, registra los siguientes puntos:

- ¿Fue detectado el archivo Spyrix Keylogger al ser copiado?
- ¿Fue bloqueada la ejecución del archivo malicioso?
- ¿Fue detectado durante el escaneo manual?
- ¿Qué acciones tomó el antivirus (cuarentena, eliminación, etc.)?
- ¿Hubo algún impacto en el rendimiento del sistema durante las pruebas?

Consideraciones finales

1. **Cumplimiento ético:**
    - No uses malware en sistemas reales o fuera de un entorno controlado.
    - Asegúrate de cumplir con las leyes y regulaciones locales relacionadas con el uso de software malicioso.
2. **Limitaciones de las versiones gratuitas:**
    - Ten en cuenta que las versiones gratuitas de algunos antivirus pueden tener menos funcionalidades avanzadas que las versiones de pago.
3. **Interpretación de resultados:**
    - Evalúa no solo la capacidad de detección, sino también el impacto en el rendimiento del sistema y la facilidad de uso del software.