PRÁCTICA 4: ADQUISICIÓN DE EVIDENCIAS EN MÁQUINA ENCENDIDA.

A) Imaginemos que nos encontramos con un equipo encendido que ejecuta un sistema operativo Windows. Ante esta tesitura pueden ocurrir varias posibilidades: 1) Que el equipo sea un servidor y cientos e incluso miles de usuarios requieren de los servicios que ofrecen; 2) Que no tengamos mucha información sobre la configuración del equipo, así que no sabemos si su disco duro está cifrado y por tanto si lo apagamos es posible que no seamos capaces de volver a arrancarlo, perdiendo la posibilidad de extraer evidencias digitales del mismo.

   Ante estas situaciones podemos extraer un c**lonado del disco duro o también una imagen completa** como hicimos anteriormente en la práctica 2 mediante el uso del comando DD para windows (http://www.chrysocome.net/dd)

   Tal y como estudiamos en los apartados 2.31 y 2.5.5 del tema 2, también existe la posibilidad de realizar **adquisiciones de evidencias parciales** se actuará siguiendo los procedimientos indicados en las adquisiciones de dispositivos encendidos. En este caso será necesaria la identificación de la parte de interés para el análisis, carpetas, archivos o bases de datos sobre las que va a versar el posterior estudio.

   Vamos a entrenar como hacer un clonado de disco en caliente, es decir, sin apagar el equipo, donde estudiaremos qué posibilidades nos ofrece el software: clonado de disco completo y/o imagen completa y adquisición de evidencias parciales.

B) Idem que en el apartado anterior, pero con el sistema operativo cifrado.

Objetivos principales de la práctica 4)

- **Recopilación de pruebas en caliente (clonado/imagen de disco completo e imagen parcial) ante situaciones donde bien no se puede apagar el equipo o existe la posibilidad de no poder volver a arrancar el equipo si se apaga:**

Se pide:

A)

- Crear una máquina virtual con Windows 7 32 bits versión Ultimate con las siguientes características:
  - 2 GB de RAM
  - Una unidad de disco (C) duro de 10 GB
  - Segunda unidad de disco duro (D) de 20 GB donde realizar las imágenes.
- Descargar la utilidad DD para windows desde http://www.chrysocome.net/dd
- Descargar la utilidad FTK Imager Lite desde aquí
- Estudiar las posibilidades de realizar imágenes del disco completo (en caliente) que ofrece DD. Realizar una imagen completa del disco de 10GB en un fichero en el volumen D.
- Estudiar las posibilidades de realizar una extracción parcial del directorio “C:\Users” mediante la herramienta FTK Imager Lite.

B) Cifrar el sistema de ficheros de la máquina del apartado anterior y repetir las operaciones de extracción de evidencia digitales tanto completas como parciales.

ANEXO: Cifrado del sistema de archivos con Bitlocker

1. ¿Qué es el Cifrado de unidad BitLocker?

El Cifrado de unidad BitLocker es una característica de seguridad integral del sistema operativo Windows 7 que ayuda a proteger los datos almacenados en unidades de datos fijas y extraíbles y en la unidad del sistema operativo. BitLocker protege de "ataques sin conexión", que son aquéllos que se realizan deshabilitando o evitando el sistema operativo instalado, o bien, quitando físicamente el disco duro para atacar los datos por separado. En el caso de las unidades de datos fijas y extraíbles, BitLocker ayuda a garantizar que los usuarios pueden leer y escribir datos en la unidad solo cuando cuentan con la contraseña correspondiente, con credenciales de tarjeta inteligente o cuando usan la unidad de datos en un equipo protegido con BitLocker que tenga las claves adecuadas. Si en su organización hay equipos que ejecuten versiones anteriores de Windows, se puede usar el Lector de BitLocker To Go™ para permitir a esos equipos leer las unidades extraíbles protegidas con BitLocker.

La protección de BitLocker en unidades del sistema operativo admite la autenticación de dos factores mediante el uso del Módulo de plataforma segura (TPM) junto con un número de identificación personal (PIN) o clave de inicio, así como la autenticación de un solo factor mediante el almacenamiento de una clave en una unidad flash USB o mediante el uso solo del TPM. El uso de BitLocker con un TPM proporciona una mayor protección a los datos y ayuda a garantizar la integridad del componente de arranque inicial. Esta opción requiere que el equipo disponga de un microchip de TPM y una BIOS compatibles. Un TPM compatible se define como la versión 1.2 del TPM. Una BIOS compatible debe admitir el TPM y la raíz estática de Trust Measurement, tal y como define Trusted Computing Group. Para obtener más información acerca de las especificaciones del TPM, visite la sección sobre dichas especificaciones del sitio web de Trusted Computing Group (en inglés) (http://go.microsoft.com/fwlink/?LinkId=72757).

El TPM interactúa con la protección de la unidad del sistema operativo de BitLocker para ayudar a proporcionar protección al inicio del sistema. El usuario no puede apreciar esto y el inicio de sesión de usuario no cambia. Sin embargo, si la información de inicio varía, BitLocker pasará al modo de recuperación y se necesitará una contraseña o clave de recuperación para volver a tener acceso a los datos.

2. Requisitos del Cifrado de unidad BitLocker

Los requisitos de hardware y software para BitLocker son los siguientes:

- Un equipo que ejecute Windows 7 Enterprise, Windows 7 Ultimate o Windows Server 2008 R2.
- Un equipo que cumpla los requisitos mínimos de Windows 7 o Windows Server 2008 R2.
- Se recomienda disponer de un microchip de TMP, versión 1.2, activado para su uso con BitLocker en unidades del sistema operativo para la validación de componentes de arranque iniciales y el almacenamiento de la clave maestra de BitLocker. Si el equipo no tiene un TPM, es posible usar una unidad flash USB para almacenar la clave de BitLocker.
- Una BIOS compatible con Trusted Computing Group (TCG) para su uso con BitLocker en las unidades del sistema operativo.

· Una configuración de BIOS para iniciar primero desde el disco duro, no desde la unidad USB o de CD.

3. Activar Bitlocker en la unidad del S.O.

1. Haga clic en **Inicio**, **Panel de control**, **Sistema y seguridad** y, a continuación, en **Cifrado de unidad BitLocker**.

2. Haga clic en **Activar BitLocker** para la unidad del sistema operativo. BitLocker examinará el equipo a fin de asegurarse de que cumple con los requisitos del sistema de BitLocker. Si el equipo cumple con los requisitos, BitLocker le informará los próximos pasos que deben realizarse para activar BitLocker, tales como la preparación de la unidad, la activación del TPM y el cifrado de la unidad.

Si cuenta con una sola partición para la unidad del sistema operativo, BitLocker preparará la unidad; para ello, reducirá el tamaño de la unidad del sistema operativo y creará una nueva partición del sistema para usarla para los archivos del sistema que se necesitan para iniciar o recuperar el sistema operativo y que no se pueden cifrar. Esta unidad no tendrá una letra de unidad para evitar que se almacenen archivos de datos en esta unidad sin darse cuenta. Una vez que la unidad está preparada, debe reiniciarse el equipo.

Si el TPM no está inicializado, el asistente para la configuración de BitLocker le indica que debe quitar las unidades USB, los CDs o los DVDs del equipo y reiniciar el equipo para iniciar el proceso de activación del TPM. Se le solicitará que habilite el TPM antes de que arranque el sistema operativo o, en algunos casos, deberá navegar a las opciones BIOS y habilitar el TPM manualmente. Este comportamiento depende del BIOS del equipo. Después de confirmar que desea que el TPM esté habilitado, el sistema operativo se iniciará y aparecerá el indicador de progreso **Inicializando el hardware de seguridad de TPM**.

Podrá usar BitLocker aunque su equipo no tenga un TPM, pero se usará el método de autenticación **Clave de inicio solamente**. Toda la información necesaria de la clave de cifrado se almacena en una unidad flash USB que el usuario debe insertar en el equipo durante el inicio. La clave almacenada en dicha unidad desbloquea el equipo. Se recomienda el uso de un TPM, ya que ayuda a proteger frente a ataques contra el proceso de inicio crítico del equipo. Con el método **Clave de inicio solamente** sólo se cifra la unidad; no se validan los componentes de la primera fase de arranque ni las alteraciones del hardware. Para usar este método, el equipo debe admitir la lectura de dispositivos USB en el entorno anterior al arranque y se debe habilitar este método de autenticación; para ello, active la casilla **Permitir BitLocker sin un TPM compatible** en la configuración de directiva de grupo **Requerir autenticación adicional al iniciar**, que se encuentra en la siguiente ubicación del Editor de directivas de grupo local: **Configuración del equipo\Plantillas administrativas\Componentes de Windows\Cifrado de unidad BitLocker\Unidades del sistema operativo**.

3. Una vez que se inicializa el TPM, el asistente para la configuración de BitLocker le solicita que elija cómo desea almacenar la clave de recuperación. Puede elegir entre las opciones siguientes:

- **Guardar la clave de recuperación en una unidad flash USB**. Guarda la clave de recuperación en una unidad flash USB.
- **Guardar la clave de recuperación en un archivo**. Guarda la clave de recuperación en una unidad de red o en otra ubicación.
- **Imprimir la clave de recuperación**. Imprime la clave de recuperación.

Use una o varias de estas opciones para conservar la clave de recuperación. Para cada opción que seleccione, siga los pasos del asistente para establecer la ubicación para guardar o imprimir la clave de recuperación. Cuando haya terminado de guardar la clave de recuperación, haga clic en **Siguiente**.

Importante

La clave de recuperación es necesaria cuando una unidad de datos fija protegida con BitLocker configurada para desbloqueo automático se traslada a otro equipo, o si la contraseña o la tarjeta inteligente asociadas con el desbloqueo de la unidad fija o extraíble no están disponibles, como puede suceder cuando se olvida la contraseña o se pierde la tarjeta inteligente. Necesitará la clave de recuperación para desbloquear los datos cifrados en la unidad si BitLocker cambia a un estado de bloqueo. Esta clave de recuperación es única para esta unidad en particular. No se puede usar para recuperar datos cifrados de ninguna otra unidad protegida con BitLocker.

Para lograr la máxima seguridad, debería almacenar las claves de recuperación lejos de las unidades con las que están asociadas.

4. El asistente para la configuración de BitLocker le pregunta si está listo para cifrar la unidad. Confirme que la casilla **Ejecutar la comprobación del sistema de BitLocker** está activada y, a continuación, haga clic en **Continuar**.

5. Confirme que desea reiniciar el equipo al hacer clic en **Reiniciar ahora**. El equipo se reinicia y BitLocker comprueba si el equipo cumple con los requisitos de BitLocker y está preparado para el cifrado. Si no lo está, al iniciar sesión aparecerá un mensaje de error que alerta sobre el problema.

6. Si está preparado para el cifrado, aparecerá la barra de estado **Cifrar**, que muestra el progreso de cifrado de la unidad. Puede supervisar el estado de finalización en curso del cifrado de la unidad de disco, si mueve el puntero del mouse sobre el icono **Cifrado de unidad BitLocker** en el área de notificación, en el extremo derecho de la barra de tareas. El cifrado de la unidad puede tardar unos minutos. Puede usar su equipo durante el cifrado, pero el rendimiento será menor. Cuando el cifrado se haya completado, aparecerá un mensaje de finalización.