UD1 – Adopción de pautas de seguridad informática

Tarea 3: John The Ripper

Transmisión de Fulcrum.

Hemos conseguido acceder al disco duro de uno de los ordenadores imperiales. Debes acceder a dicho disco para intentar obtener los usuarios y contraseñas de dicho disco para obtener toda la información posible.
No obstante, hay un pequeño problema. Hemos ocultado la ubicación del disco dentro de un fichero de KeePass, pero no recordamos la contraseña.
Deberás crackear la contraseña del fichero fulcrum.kdbx para poder acceder a dicho archivo y consultar la ubicación del disco.
Una vez tengas el disco, deberás extraer todos los usuarios y contraseñas.

No te preocupes, no estás solo, a continuación te dejaremos unos enlaces y unos pasos que te pueden servir de ayuda.

Léelo todo y, al final, encontrarás todo lo que necesitamos que hagas.

Que la Fuerza te acompañe!

Algunos enlaces de ayuda:

- OVA Máquina virtual Kali – En las ISOs de http://tic.ieslasenia.org
- Guest Additions para Kali (VBox) - https://www.kali.org/docs/virtualization/install-virtualbox-guest-additions/
- Web John The Ripper - https://www.openwall.com/john/
- Ayuda John - https://charlesreid1.com/wiki/John_the_Ripper
- Guía John - https://www.hackingarticles.in/beginner-guide-john-the-ripper-part-1/
- Modos de funcionamiento John- https://www.openwall.com/john/doc/MODES.shtml
- Wordlits gratis en diferentes idiomas - https://mirrors.edge.kernel.org/openwall/wordlists/
- Conseguir clave de KeePass con Hashcat - https://www.rubydevices.com.au/blog/how-to-hack-keepass
- Conceptos básicos de John - https://thehackerway.com/2011/05/19/conceptos-basicos-sobre-tecnicas-de-crackeo-con-john-the-ripper/
- Uso práctico de John - https://thehackerway.com/2011/05/20/uso-practico-de-john-the-ripper/

Para poner teclado español al abrir una consola de Kali: `setxkbmap es`

Primer paso: "Cómo obtener password del archivo Keepass"

- Descarga el archivo KeePass "`fulcrum.kdbx`" de Aules.
- Crea una máquina virtual con la OVA de Kali Linux. Esta distribución trae un montón de herramientas de hacking. Copia en la máquina Kali el archivo Keepass para trabajar.
- Los archivos cifrados y protegidos con contraseña como archivos comprimidos, pdf o del keepass contienen dentro el hash de la contraseña. Extrae el hash de la contraseña del archivo con las utilidades de John The Ripper que ya vienen instaladas en Kali Linux (https://www.openwall.com/john/) y ponle tu nombre al archivo resultado.
- Edita el archivo para ver el contenido y borra el nombre del archivo de delante del texto. Tienes que borrar lo que hay delante de $keepass$ (esto último indica que el hash es del programa Keepass). Si no, no va a funcionar.
- Busca el código del tipo de hash para poder ponerlo cuando busques en el archivo (en este caso, Keepass). Puedes ver los tipos con `hashcat -h` (y filtrar la salida por palabra clave con el pedido grep)
- Ahora utiliza el código encontrado para ejecutar el comando (sustituye los nombres por los que has puesto tú en el archivo de hash y en el de diccionario). Usa el diccionario `rockyou.txt`. Los diccionarios preinstalados en Kali se encuentran en /usr/share/wordlists y quizás se encuentran comprimidos y antes debas descomprimirlos.
- Mientras se ejecuta, puedes ver por dónde va pulsando `[s]tatus`.
- Si lo encuentra (puede tardar hasta 1 día o más, déjalo trabajar), puedes ver el resultado añadiendo al comando anterior `--show` (verás el password detrás del hash).
- Comprueba con el programa Keepass que puedes abrir el archivo cifrado de passwords con el que ha encontrado John.

Segundo paso: "Cómo extraer el almacén de contraseñas del equipo sospechoso"

- Crea una máquina virtual (victima-tunombre) para tratar de arrancar el disco duro encontrado. Podrás comprobar que existe un sistema operativo instalado. Trata de iniciar sesión. Puesto que el sistema controla la autenticación, no podrás acceder al sistema sin saber la contraseña.
- Tratamos de obtener el archivo de passwords. Añade la imagen del disco sospechosa a la máquina virtual de Kali Linux. Tienes que añadirlo a la controladora SATA en los parámetros de la máquina virtual. Habrá que detener antes la máquina.
  NOTA: Se podría hacer todo con una Kali Live, montando la imagen ISO de Kali en la máquina virtual "victima" para iniciar Kali Live sin instalar nada. Así simularíamos que estamos poniendo un pendrive en la máquina para arrancar una distro live. Hazlo como prefieras.
- Una vez iniciado Kali, accede al disco de la máquina a vulnerar por extraer los archivos de passwords (`/etc/passwd y /etc/shadow`).
- Para ver los dispositivos disponibles podemos hacer (si es necesario): `fdisk -l`

- Ahora copiaremos los archivos de passwords (`/etc/passwd y /etc/shadow`) en un directorio diferente para no dañar el disco original de la víctima (por ejemplo en `/home/kali/trabajo`). Es necesario trabajar en un directorio temporal fuera del disco de la víctima.
- Ya podemos hacer el proceso de búsqueda de passwords con John_the_Ripper.
- Convierte el archivo shadow en un archivo estándar de contraseñas con el comando `unshadow`.
- Ejecuta John the Ripper con el archivo obtenido. En una primera aproximación que tarda poco tiempo, hacemos "John" en modo Single. Se aplican reglas básicas como poner el nombre de usuario y datos personales que aparecen en el archivo de passwords como si fueran el password.
  `# john --single passwords-nombre`
  NOTA: Si john parece colgado (está generando contraseñas) puedes pulsar una tecla para que informe por dónde va. Puedes detener la búsqueda de passwords (CTRL+C) y si vuelves más adelante, continuará donde lo habías dejado.
  NOTA: Para ver qué passwords se han encontrado, utiliza el parámetro `--show`

Crack de passwords con reglas

- Ahora ejecutamos a John con un diccionario sencillo de 500 passwords (wordlist) y le decimos que genere variaciones de estas contraseñas (rules). Busca y descarga el archivo o utiliza el que lleva Kali:
  `# john --wordlist=/usr/share/wordlists/500-worst-passwords.txt --rules passwords-nombre`
- Ahora ejecutamos a John con una lista mucho más completa (más lento). Atacaremos con la wordlist "rockyou.txt":
  `# john --wordlist=/usr/share/wordlists/rockyou.txt --rules passwords-nombre`

Crack de passwords incremental

- `# john --wordlist=/usr/share/wordlists/rockyou.txt --rules passwords-nombre`
- Si no tenemos ningún diccionario a mano o no nos quedan passwords por obtener, podemos utilizar el modo incremental de John indicando qué caracteres debe utilizar (en este caso del ejemplo "alpha", que indica sólo caracteres alfabéticos) . Prueba otras combinaciones.

  `# john --incremental:alpha passwords-nombre`

Necesitamos que hagas lo siguiente:

1. Documenta todo el proceso y realiza capturas de la salida de los comandos, en modo texto si es posible.

2. Obtén la contraseña del archivo KeePass "fulcrum.kdbx" para saber cómo descargar la imagen de

disco. Recuerda calcular el hash de los archivos (compara con los valores que le damos a los archivos con extensión sha256 para asegurar que el archivo no se ha corrompido).
3. Da todos los pasos para "robar" los archivos de passwords del disco víctima y extraer las contraseñas.

4. Al final de la tarea debemos haber obtenido TODAS las contraseñas. Escribe en una tabla los nombres de los usuarios seguidos de su contraseña.

5. Inicia sesión con un usuario que permita trabajar como root. Si puede ser con el propio usuario root, mejor