INSTITUTO NACIONAL DE CIBERSEGURIDAD

ANÁLISIS FORENSE DIGITAL

Unidad 6 – Obtención de información en Linux

universidad de león

MINISTERIO DE DEFENSA

SAPROMIL

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

INDICE

1. Ficheros de configuración del usuario. History.
2. Ficheros de configuración del sistema.
3. Logs más interesantes según distribución.
4. Obtención de información en live. Scripts de incident response.
5. Análisis de memoria RAM en Linux. Volatility.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

universidad de león
MINISTERIO DE DEFENSA
SAPROMIL
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

1. Ficheros de configuración del usuario. History.

❑Introducción

- ✓ La metodología vista hasta el momento se aplica igualmente en cuanto a triage live de la máquina o adquisición en frío.
- ✓ Los sistemas Linux son más sencillos en cuanto a dónde encontrar información y el formato en el que esta se encuentra, habitualmente en texto.
- ✓ Siguen una estructura estándar de directorios y la información habitualmente está almacenada en texto, de modo que no necesitamos una herramienta para cada artifact, como sucede en Windows.
- ✓ Con sencillas herramientas de búsqueda y procesamiento de texto podemos obtener los resultados requeridos en el análisis.

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

1. Ficheros de configuración del usuario. History.

❑Comandos imprescindibles en el análisis de una máquina Linux

- ✓ Un mínimo manejo de la consola de Linux es necesario para encontrar información en los ficheros de logs.
- ✓ Hay una serie de comandos imprescindibles, cuyo conocimiento nos permitirá encontrar lo que buscamos de una forma eficiente:
- ✓ grep: nos permite la búsqueda de cadenas en un fichero o en lo que enviemos como entrada.
  - ✓ -v para excluir la cadena indicada
  - ✓ -i para obviar mayúsculas/minúsculas
  - ✓ -c cuenta las ocurrencias en vez de mostrar las líneas
  - ✓ -H nos devuelve el nombre del archivo en el que se encuentra la coincidencia

```
grep cadena_a_encontrar donde_buscarla o comando | grep cadena_a_encontrar
```

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

1. Ficheros de configuración del usuario. History.

❑Comandos imprescindibles en el análisis de una máquina Linux (ii)

- ✓find: nos permite buscar ficheros en el sistema de ficheros. Es una herramienta muy potente y que tiene muchos modificadores. Nos vamos a centrar en los básicos y en los de tiempo
  - ✓ -name para indicar el nombre de archivo. Con –iname no distingue entre mayúsculas/minúsculas
  - ✓ -type para indicar el tipo de fichero, f, b, d, l o c.
  - ✓ -not para excluir una cadena en el nombre de los ficheros buscados
  - ✓ -ctime –atime o –mtime -n, ficheros creados, accedidos o modificados en los n días anteriores
  - ✓ -cmin, -amin o mmin –n, ficheros creados, accedidos o modificados en los n minutos anteriores

```
find donde_buscar criterios_de_busqueda
```

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

1. Ficheros de configuración del usuario. History.

❑Comandos imprescindibles en el análisis de una máquina Linux (iii)

- ✓ ls: herramienta para listar el contenido de un directorio, con opciones interesantes para la ordenación y filtrado.
  - ✓ -a muestra ficheros ocultos
  - ✓ -t los ordena por fecha de modificación, interesante para los logs.
- ✓ tail/head: permite ver las últimas/primeras 10 líneas de un fichero.
- ✓ more/less: permite paginar la salida por pantalla de un fichero de texto.

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

1. Ficheros de configuración del usuario. History.

❑Directorios de interés según FHS

FHS, Filesystem Hierarchy Standard, es el estándar de nomenclatura de directorios para sistemas NIX.

Según este estándar, la información de interés forense se encuentra en:

✓ /etc	Directorio dónde se encuentran los ficheros de configuración del sistema.
✓ /var/log	Directorio dónde se encuentran los logs del sistema
✓ /root	Directorio home del usuario root
✓ /home/"usuario"	Directorio home del usuario "usuario"

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

1. Ficheros de configuración del usuario. History.

❑Ficheros de información del usuario

- ✓En el directorio home de cada usuario, hay una serie de ficheros y subdirectorios ocultos, comienzan por ., que almacenan información de la actividad de usuario.
- ✓El más relevante es .bash_history, que almacena los comandos introducidos por consola por el usuario. Es un fichero de texto, aunque el comando history nos permite opciones avanzadas sobre él.
- ✓Tenemos la caché de múltiples programas en el directorio .cache
- ✓También podemos encontrar los comandos introducidos en la consola de mysql en mysql_history
- ✓Y los artifacts de navegación en el directorio .mozilla/firefox/xxxxxx.default.

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

2. Ficheros de configuración del sistema.

❑El directorio /etc

✓Todas las configuraciones se almacenan en este directorio, en ficheros en formato de texto. Como ejemplo:

Fichero	Contenido
/etc/passwd	Usuarios del sistema.
/etc/shadow	Hashes de passwords.
/etc/group	Grupos del sistema
/etc/resolv.conf	Servidores DNS/etc
/etc/fstab	Sistemas de archivos montados al arranque
/etc/sudoers	Politica de uso de sudo
/etc/crontab	Tareas programadas a nivel sistema

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

2. Ficheros de configuración del sistema.

❑El directorio /etc (ii)

- ✓ Adicionalmente encontramos, en subdirectorios de etc, las configuraciones de otros servicios, como SSH, logrotate, pam, network, hhtpd o systemd.
- ✓ Por ello, siempre que hagamos una adquisición de un sistema Linux, nos llevaremos la carpeta /etc.
- ✓ El contenido de /etc puede variar entre distribuciones, aunque siempre contendrá la configuración.

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

3. Logs más interesantes según distribución.

❑Ficheros de log

- ✓El servicio encargado de generar logs es rsyslog o syslog-ng. Su configuración se encuentra en /etc/rsyslog.conf
- ✓Los logs rotan, es decir, se van generando ficheros según los criterios indicados al servicio logrotate, /etc/logrotate.conf. El resultado es que encontraremos varios ficheros de log para una misma aplicación, de los cuales uno será el corriente y el resto, logs anteriores.
- ✓Los logs “rotados” aparecen con un . Y un número secuencial o comprimidos.

```
Jul 30 08:32:27 KaliLinux org.gnome.Terminal.desktop[1347]: # watch_fast: "/org/gno
me/terminal/legacy/" (establishing: 0, active: 0)
```

Ejemplo de log de un sistema Linux

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

3. Logs más interesantes según distribución.

❑Ficheros de log del sistema

- ✓ Todos en la ruta /var/log
- ✓ `messages:` fichero de log de propósito general, donde encontraremos información genérica del sistema.
- ✓ `auth.log`: registros de autenticación, de servicios o interactivas.
- ✓ `kern.log`: mensajes del kernel de Linux. También podemos usar comando `dmesg`. Aquí veremos drivers y mensajes de estado del SO.
- ✓ `btmp` y `wtmp`: ficheros binarios con información sobre las sesiones. Los consultamos con los comandos `lastb`, intentos de accesos fallidos, y `last` para los intentos de acceso válidos.

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

3. Logs más interesantes según distribución.

❑Ficheros de log del sistema (ii)

✓ `/var/run/utmp`: log binario que mantiene registro de los usuarios actuales en el sistema. Lo consultamos con los comandos `who` o `w`.

```
root@KaliLinux:/var/log# who
root     :1           2020-07-30 08:32 (:1)
root@KaliLinux:/var/log# w
 10:04:17 up  1:32,  1 user,  load average: 0,00, 0,00, 0,00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     :1       :1               08:32   ?xdm?  19.96s  0.01s /usr/libexec/gdm-x
root@KaliLinux:/var/log# S
```

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

3. Logs más interesantes según distribución.

❑Ficheros de log de aplicación

- ✓ Habitualmente haremos forense de máquinas Linux que son servidores.
- ✓ Entre los servicios más habituales, podemos encontrar servidores web, servidores de BBDD y servicios de seguridad tipo firewall, UTM, VPN, etc…
- ✓ Estos servicios dejan sus propios logs en un directorio con el nombre del servicio, en la ruta /var/log/”servicio”, p.e. /var/log/apache2.
- ✓ Del servicio apache son interesantes los logs:
  - ✓ access.log: registros de las peticiones (get) procesadas.
  - ✓ error.log: registro de las peticiones erróneas.
- ✓ Del servicio mysql (MariaDB) son interesantes los logs:
  - ✓ error.log: registra los intentos de inicio de sesión erróneos, entre otros.

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

3. Logs más interesantes según distribución.

❑Linux logs en Systemd - Journald

- ✓ En distribuciones basadas en Systemd, todas desde hace ya unos años, el servicio encargado de generar logs es journald.
- ✓ Journald centraliza todos los logs, no siendo necesario syslog y no generando, de forma predeterminada, los distintos ficheros de log que se generaban históricamente.
- ✓ El programa para control y acceso a la información del Daemon es journalctl, del que debemos disponer de unas mínimas nociones para poder extraer información de interés forense.
- ✓ Journald almacena la información en /var/log/journal/Machine-ID
- ✓ Machine-ID es un identificador único que se crea en el primer arranque y se almacena /etc/machine-id.
- ✓ Los logs son binarios, pero tenemos la facilidad de verlos con cualquier journalctl, no es necesario que sea el de la misma máquina: `journalctl –file <filename>`

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

3. Logs más interesantes según distribución.

❑Journald – parámetros y opciones indispensables

- ✓ Para un fichero externo, `--header` nos describe las características del fichero de log y `--verify` comprobamos la integridad del fichero.
- ✓ Para filtrado de logs por tiempo, flags –S, since, y –U, until, `journalctl --directory ./evidence -S 2020-11-01 -U 2020-11-03`
- ✓ Con el parámetro `–f`, hacemos seguimiento en tiempo real, similar a `tail –f`.
- ✓ Si sólo nos interesan los logs del boot actual, usamos `–b`. Si del anterior, `-b -1.`
- ✓ Con `journalctl --utc,` nos muestra la información en hora UTC+0.
- ✓ Con `_UID=XX` o `_PID=XXXX` podemos filtrar por proceso o identificador de usuario.

Actividad: visitar y poner en práctica… *https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs-es*

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

4. Obtención de información en live. Scripts de incident response.

❑Adquisición mediante Shell scripts

- ✓La adquisición en sistemas Linux se hace con scripts de Shell, que nos permiten recopilar la información necesaria.
- ✓En general, es común que sobre Linux tengamos servidores, y cada uno puede tener una función distinta, por lo que la información a llevarnos puede variar.
- ✓Tenemos distintos scripts disponibles para tomarlos como punto de partida, aunque es necesario personalizarlos para la máquina de la que queremos adquirir.

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

4. Obtención de información en live. Scripts de incident response.

❑Scripts de automatización- Ejemplos

➢ https://github.com/WithSecureLabs/LinuxCatScale

Es un potente Script, del fabricante Fsecure, que hace una recopilación general y agrupa la información para poder ser tratada con búsquedas desde Elasticsearch.

➢ https://www.securizame.com/lintriage/

Lintriage es una herramienta de código abierto desarrollada por Securízame, diseñada específicamente para la extracción de artefactos forenses desde sistemas Linux vivos. Es la “hermana” de la útil Wintriage, por lo que puede ser una buena idea usar ambas herramientas para adquisición live..

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

5. Análisis de memoria RAM en Linux. Volatility.

❑Adquisición de memoria en Linux

✓ Linux presenta una dificultad mayor en la adquisición y análisis de memoria que Linux.

Para la adquisición, tenemos dos posibilidades:

✓ Como **primera opción**, debemos de volcarla con Lime, un módulo Linux, compilado para el Kernel de la máquina que queremos adquirir. Una vez adquirida, el análisis es lo mismo que lo visto para Windows con Volatility. https://github.com/504ensicsLabs/LiME

✓ Una vez instalado el módulo, crea un fichero con el volcado de memoria que puede ser analizado con Volatility siempre que dispongamos del perfil adecuado para el kernel adquirido.

✓ Como **segunda opción** tenemos AVML de Microsoft, que permite adquirir la memoria con un ejecutable genérico, sin tener que compilarlo para el kernel de interés. https://github.com/microsoft/avml

✓ Es útil cuando no está habilitada la opción “kernel_lockdown” del kernel.

UNIDAD 6 – OBTENCIÓN DE INFORMACIÓN EN LINUX

5. Análisis de memoria RAM en Linux. Volatility.

❑Análisis de memoria en Linux

- ✓ Ambos volcados, con Lime o con AVML, pueden ser analizados con Volatility.
- ✓ Disponemos de dos versiones de Volatility, la 2.x, con la que necesitamos disponer de un perfil específico para el kernel de origen de la evidencia de memoria.
- ✓ Podemos crearlo o localizarlo en repositorios no oficiales: https://github.com/volatilityfoundation/profiles/tree/master/Linux
- ✓ En el caso de volatility 3, es capaz de generar los “symbols tables” para analizar distintos volcados de memoria.
- ✓ Es decisión del analista elegir una u otra versión.

FIN UNIDAD

Unidad 6
OBTENCIÓN D EINFORMACIÓN EN LINUX

universidad de león
MINISTERIO DE DEFENSA
SAPROMIL
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD