ELECTIVA INFORMÁTICA FORENSE
PARCIAL 2

8 de Julio de 2019

CASO DE HACKING

- **Escenario**

El 20 de septiembre de 2004, una computadora portátil Dell CPi, serie # VLQLW, fue encontrada abandonada junto con una tarjeta PCMCIA inalámbrica y una antena 802.11b casera externa. Se sospecha que esta computadora se utilizó para fines de piratería, aunque no puede vincularse a un sospechoso de piratería, G = r = e = g S = c = h = a = r = d = t. (Los signos de igual son solo para evitar que los rastreadores web indexen este nombre; no hay signos de igual en los archivos de imagen). Schardt también recibe el apodo en línea de "Mr. El mal "y algunos de sus asociados han dicho que estacionaría su vehículo dentro del rango de puntos de acceso inalámbrico (como Starbucks y otros puntos de acceso de T-Mobile) donde luego interceptaría el tráfico de Internet, intentando obtener números de tarjetas de crédito, nombres de usuario y contraseñas.

Encuentre cualquier software de piratería, evidencia de su uso y cualquier dato que pueda haber sido generado. Intente vincular la computadora con el sospechoso, G = r = e = g S = c = h = a = r = d = t.

- **Lea esto antes de empezar**

La imagen del disco ha sido dividida en 8 archivos que debe descargar de aquí y verificar su hash:

	DESCARGAR
1	http://tiny.cc/7xue9y
2	http://tiny.cc/kave9y
3	http://tiny.cc/bcve9y
4	http://tiny.cc/pdve9y
5	http://tiny.cc/leve9y
6	http://tiny.cc/qgve9y
7	http://tiny.cc/aive9y
8	http://tiny.cc/2kve9y

```
MacBook-Pro-de-Relis:Downloads samador$ md5 SCHARDT.00*
MD5 (SCHARDT.001) = 28a9b613d6eefe8a0515ef0a675bdebd
MD5 (SCHARDT.002) = c7227e7eea82d218663257397679a7c4
MD5 (SCHARDT.003) = ebba35acd7b8aa85a5a7c13f3dd733d2
MD5 (SCHARDT.004) = 669b6636dcb4783fd5509c4710856c59
MD5 (SCHARDT.005) = c46e5760e3821522ee81e675422025bb
MD5 (SCHARDT.006) = 99511901da2dea772005b5d0d764e750
MD5 (SCHARDT.007) = 99511901da2dea772005b5d0d764e750
MD5 (SCHARDT.008) = 8194a79a5356df79883ae2dc7415929f
```

Luego de desacargar los 8 archivos y verificar su hash, debe unirlos y verificar de nuevo el hash de la siguiente forma:

```
MacBook-Pro-de-Relis:Downloads samador$ cat SCHARDT.001 >> SCHARDT.img
MacBook-Pro-de-Relis:Downloads samador$ cat SCHARDT.002 >> SCHARDT.img
MacBook-Pro-de-Relis:Downloads samador$ cat SCHARDT.003 >> SCHARDT.img
MacBook-Pro-de-Relis:Downloads samador$ cat SCHARDT.004 >> SCHARDT.img
MacBook-Pro-de-Relis:Downloads samador$ cat SCHARDT.005 >> SCHARDT.img
MacBook-Pro-de-Relis:Downloads samador$ cat SCHARDT.006 >> SCHARDT.img
MacBook-Pro-de-Relis:Downloads samador$ cat SCHARDT.007 >> SCHARDT.img
MacBook-Pro-de-Relis:Downloads samador$ cat SCHARDT.008 >> SCHARDT.img
MacBook-Pro-de-Relis:Downloads samador$ md5 SCHARDT.img
MD5 (SCHARDT.img) = aee4fcd9301c03b3b054623ca261959a
```

Su análisis forense (Con fotografías de pantallazos) debe resolver las siguientes preguntas:

1. ¿Cuál es el hash de la imagen? ¿Coincide el hash de adquisición y verificación?
2. ¿Cuál sistema operativo fue usado en la computadora?
3. ¿Cuál fue la fecha de instalación?
4. ¿Cuál es la configuración de la zona horaria?
5. ¿Quién es el propietario registrado?
6. ¿Cuál es el nombre de la cuenta de la computadora?

ELECTIVA INFORMÁTICA FORENSE
PARCIAL 2

8 de Julio de 2019

7. ¿Cuál es el nombre de dominio principal?
8. ¿Cuándo fue la última fecha / hora de apagado de la computadora grabada?
9. ¿Cuántas cuentas se registran (número total)?
10. ¿Cuál es el nombre de cuenta del usuario que usa principalmente la computadora?
11. ¿Quién fue el último usuario que inició sesión en la computadora?
12. Una búsqueda del nombre de "Greg Schardt" revela múltiples visitas. Uno de estos demuestra que Greg Schardt es el Sr. Evil y también es el administrador de esta computadora. ¿Qué archivo es? ¿Con qué programa de software se relaciona este archivo?
13. Enumera las tarjetas de red usadas por esta computadora
14. Este mismo archivo informa la dirección IP y la dirección MAC de la computadora. ¿Qué son?
15. Se puede usar una búsqueda en Internet del nombre / modelo del proveedor de tarjetas NIC por dirección MAC para averiguar qué interfaz de red se utilizó. En la respuesta anterior, los primeros 3 caracteres hexadecimales de la dirección MAC informan al vendedor de la tarjeta. ¿Qué tarjeta NIC se utilizó durante la instalación y configuración de LOOK @ LAN?
16. Encuentra 6 programas instalados que pueden usarse para hackear.
17. ¿Cuál es la dirección de correo electrónico SMTP para Mr. Evil?
18. ¿Cuáles son los ajustes de NNTP (servidor de noticias) para Mr. Evil?
19. ¿Qué dos programas instalados muestran esta información?
20. ¿Enumera 5 grupos de noticias a los que se ha suscrito el Sr. Evil?
21. Se instaló un popular programa IRC (Internet Relay Chat) llamado MIRC. ¿Cuál es la configuración del usuario que se mostró cuando el usuario estaba en línea y en un canal de chat?
22. Este programa IRC tiene la capacidad de registrar sesiones de chat. Enumera 3 canales de IRC a los que accedió el usuario de esta computadora.
23. También se encontró que se instaló Ethereal, un popular programa de "olfateo" que se puede usar para interceptar paquetes de Internet por cable e inalámbricos. Cuando los paquetes TCP se recopilan y vuelven a ensamblar, el directorio de guardado predeterminado es ese directorio users \ My Documents. ¿Cuál es el nombre del archivo que contiene los datos interceptados?
24. Ver el archivo en formato de texto revela mucha información sobre quién y qué fue interceptado. ¿Qué tipo de computadora inalámbrica fue la víctima (persona a la que se grabó su navegación por Internet)?
25. ¿A qué sitios web accedía la víctima?
26. Busque la dirección de correo electrónico principal de los usuarios principales. ¿Qué es?
27. Yahoo mail, un popular servicio de correo electrónico basado en la web, guarda copias del correo electrónico con el nombre de archivo.
28. ¿Cuántos archivos ejecutables hay en la papelera de reciclaje?
29. ¿Son estos archivos realmente eliminados?
30. ¿Cuántos archivos realmente se informan para ser eliminados por el sistema de archivos?
31. Realice una comprobación de antivirus. ¿Hay algún virus en la computadora?

ELECTIVA INFORMÁTICA FORENSE
PARCIAL 2

8 de Julio de 2019

En equipos de 3 integrantes máximo debe realizar el análisis forense.

Debe entregar 2 informes:

- El primero debe ser escrito e informando todas las herramientas que utilizó, además de acompañar este informe con las fotografías de los comandos usados y cómo logró dar respuesta a las preguntas. (**Enviarlo al correo samador@unicauca.edu.co a más tardar el domingo 14 de Julio a las 23:59:59**).
- El segundo informe debe ser un video que muestre paso a paso desde el planteamiento del escenario y cada una de las preguntas formuladas. (El video no debe superar los 40 minutos). (**Subirlo a la nube (Youtube, Vimeo, DailyMotion, etc) y enviarme solo el enlace a más tardar el domingo 14 de Julio a las 23:59:59**).

Referencia adicional sobre *convertir imagenes vmdk, raw, qcow2, vdi y vpc con qemu-img* http://tiny.cc/8t8e9y y poder virtualizarlas con un gestor de máquinas virtuales.