```
.ds LF D. Brezinski, T. Killalea
.ds RF FORMFEED[Pág. %]
.ds CF Mejores prácticas actuales
.ds LH RFC 3227
.ds RH Febrero 2002
.ds CH Recolección y archivo de evidencias
.pl 10.0i
.po 0
.ll 7.2i
.lt 7.2i
.nr LL 7.2i
.nr LT 7.2i
.hy 0
.ad l
.in 0
```

Network Working Group D. Brezinski
Request for Comments: 3227 In-Q-Tel
BCP: 55 T. Killalea
Category: Best Current Practice neart.org
February 2002

PAUTAS PARA LA RECOLECCION Y ARCHIVO DE EVIDENCIA

Status de este Memo

Este documento especifica las mejores prácticas corrientes de Internet para la comunidad de Internet y la discusión de pedido y sugerencias para los mejoramientos. La distribución de este Memo no es limitada.

Anuncio de derecho de autor

Resumen

Un "Incidente de seguridad" como se define en el "Glosario de Seguridad de Internet", RFC 2828, es un evento de seguridad de sistemas importante, en el cual la política de seguridad del sistema no se obedece o no se cumple. El propósito de este documento es proveer a los administradores de un sistema de pautas sobre la recolección y archivo de evidencia importante para dicho incidente de seguridad.

Si la recolección de evidencia se realiza correctamente, es mucho mas útil para la detección del atacante, y representa una oportunidad mucho mayor de ser admitida en el hecho de un procedimiento.

Tabla de contenido

1.Introducción

Un "incidente de seguridad" como se define en RFC 2828, es un evento de seguridad de sistemas importante, en el cual la política de seguridad del sistema no se cumple o no se obedece. El propósito de este documento es proveer a los administradores de un sistema pautas sobre la recolección y archivo de reevidencia importante para dicho incidente de seguridad. No es nuestra intención insistir en que todos los administradores del sistema estrictamente deben seguir estas pautas cada vez que tienen un incidente de seguridad, queremos proveer un guía sobre que deberíamos hacer si ellos eligen recolectar y proteger la informaron relacionada a un intruso.

Dicha recolección representa un esfuerzo considerable por parte del administrador del sistema. En los últimos años se han realizado grandes progresos para acelerar la reinstalación del Sistema Operativo y facilitar la reversión de un sistema a un estado "conocido" haciendo de este modo, la "Opción fácil" aun mas atractiva. Mientras tanto, poco se ha realizado para suministrar formas fáciles para archivar la evidencia (la opción difícil). Además las capacidades de memoria y de disco en aumento y el uso más difundido de cautela y de tácticas de cubrir huellas por parte de los atacantes han exacerbado el problema.

Si la recolección de evidencia se realiza correctamente, es mucho mas útil para aprehender al atacante y representa una oportunidad mucho mayor en ser admitida como hecho en un juicio.

Deberías utilizar esta pautas como una base para formular tus procedimientos de recolección de evidencia de sitio y deberías incorporar tus procedimientos de sitio en una documentación de manejo de incidente. Las pautas en este documento pueden no ser apropiadas en todas las jurisdicciones. Una vez que hayas formulado tus procedimiento de recolección de evidencia de sitio, deberías tener la aplicación de la ley para tu jurisdicción confirmando que son adecuados.

1Convenciones utilizadas en este documento

Las palabras claves "requerido", "debe", "no debe", "debería", "no debería" y

puede de este documento deben ser interpretadas como se describe en "Palabras claves para usar en RFC's para indicar niveles de requerimiento".

2.Principios directrices durante la recolección de evidencia
Adherir a la política de seguridad de sitio y comprometer al personal de aplicación de la ley y manejo de incidente apropiados.
Capturar la imagen tan exacta del sistema como sea posible.
Conservar notas detalladas. Estas deberían incluir fechas y horarios. Si es posible generar un copia automática. (por ejemplo, sobre los sistema Unix, se puede utilizar el programa "Script", sin embargo, el archivo output que se genera no debería ser para medios, es decir parte de la evidencia). Las notas y las impresiones deberían ser firmadas y fechadas.
Notar la diferencia entre el sistema real y el UTC. Para cada marca de tiempo provista, indicar si se utiliza UTC y hora local.
Estar preparado para testificar (tal vez años mas tarde) trazando todas las acciones que tomaste y en que momentos. Las notas detalladas serán vitales.
Minimizar los cambios a los datos a medida que los van recolectando. Esto no esta limitado a los cambios de contenido, tu deberías evitar la actualización de archivos o tiempos de acceso de directorio.
Borrar caminos externos para cambiar.
Cuando te enfrentes a una elección entre recolección y análisis, tu debería hacer la recolección primeo y el análisis después.
Aunque escasamente necesita establecerse, tus procedimiento debería ser implementable. Como con cualquier aspecto de un política de respuesta a un incidente, los procedimiento deberían ser evaluados para asegurar la viabilidad, particularmente en una crisis, Si es posible los procedimientos debería ser automatizados por razones de velocidad y precisión. Ser metódicos.
Para cada dispositivo, debería adoptarse un enfoque metódico que siga las directivas establecidas de tu procedimiento de recolección. La velocidad será a menudo critica, por eso donde exista un numero de dispositivos que requieran examen puede ser apropiado extender el trabajo entre tu equipo para recolectar la evidencia en paralelo. Sin embargo, en una recolección de sistema simple debería realizarse paso por paso.
Proceder desde lo volátil a lo menos volátil (ver orden de volatilidad abajo)
Deberías hacer una copia a nivel de bit de los medios del sistema. Si deseas hacer un análisis forense, deberías hacer una copia a nivel de bit de tu copia de evidencia para tal fin, ya que tu análisis alterará casi seguramente el tiempos de acceso de los archivo. Evitar hacer forensics sobre la copia de evidencia.

2.1 Orden de volatilidad
Cuando recolectes la evidencia deberías proceder desde los volátil a lo menos volátil. Aquí hay un ejemplo de orden de volatilidad para un sistema típico.
Registros, Cache.
Tabla de ruta. ARP Cache, Tabla de Proceso, Núcleo de estadísticas, memoria-Sistema de Archivo temporarios
Disco
Datos de monitoreo y log's remotos que es relevante al sistema en cuestión
Configuración física, topología de red.
Medio de Archivos.

2.2 Cosas para evitar
Es demasiado fácil destruir la evidencia, aún desapercibidamente.
No cerrar hasta que hayas completado la recolección de evidencia.

```
Se puede perder mucha evidencia y el atacante puede haber alterado los
startup/shutdown scripts/services para destruir evidencia.
No confíes  en los programas sobre el sistema. Conduce tu evidencia reuniendo
programas a partir de medios protegidos apropiadamente (ver abajo)
No ejecutes programas que modifiquen el tiempo de acceso de los archivos sobre el
sistema (por ejemplo: "tar" o "xcopy")
Cuando elimines los caminos externos para el cambio, observa que simplemente
desconectando o filtrando desde la red puede accionar "deadman switches" que
detectan cuanto están fuera de la red y limpian la evidencia.

2.3 Consideraciones privadas
Respetar las reglas de privacidad y las directivas de tu compañía y de tu
jurisdicción legal. En particular, asegúrate de que ninguna información
recolectada junto con la evidencia que estás buscando está disponible a cualquiera
que normalmente no tuviera acceso a esta información. Esto incluye acceso a
archivos log (que pueden revelar modelos de comportamiento del usuario) así como
también archivos de datos personales.
No te entrometas en la privacidad de la gente sin una justificación convincente.
En particular, no recolectes información de áreas a las que tu normalmente no
tienes porque acceder (tales como almacenamiento de archivos personal) al menos
que tengas indicios suficientes de que existe un incidente real.
Asegúrate de que tengas el apoyo de los procedimientos establecidos de tu compañía
en seguir los pasos que tú haces para recolectar la evidencia de un incidente.

2.4 consideraciones Legales
La Evidencia de computadora necesita ser:
Admisible: debe estar de acuerdo con ciertas reglas legales antes de ser puesta
ante una corte.
Auténtica: Debe ser posible ligar positivamente el material de evidencia al
incidente.
Completa: Debe contar la historia completa y n solamente una perspectiva
particular.
Confiable: No debe existir nada acerca de cómo la evidencia fue recolectada y
posteriormente manejada que ponga en duda acerca de su autenticidad y veracidad.
Creíble: Debe ser fácilmente creíble y comprensible por una corte.


3.El procedimiento de recolección
Tus procedimientos de recolección deberían ser tan detallados como sea posible.
Como es el caso con tus procedimientos de manejo de incidente global, deberían ser
inequívocos y deberían minimizar la cantidad de toma de decisiones que se
necesitan durante el proceso de recolección.

3.1 Transparencia
Los métodos utilizados para recolectar evidencia deberían ser transparentes y
reproducibles. Deberías estar preparado para reproducir exactamente los métodos
que utilizaste, y tener aquellos métodos examinados por expertos independientes.

3.2. Pasos de la recolección
Donde está la evidencia? Enumerar que sistemas estuvieron involucrados en el
incidente y a partir de que evidencia serán recolectados.
Establecer , de ser posible, lo que es relevante y admisible. Cuando estés en
duda, era en la recolección en demasía mas que recolectar lo suficiente.
Para cada sistema, obtener el orden de volatilidad relevante.
```

Quitar caminos externos para el cambio.
Siguiendo el orden de volatilidad, recolectar la evidencia con herramientas como se discutirá en la sección 5
Registrarla extensión del desplazamiento del reloj del Sistema.
Preguntar que mas puede ser evidencia mientras trabajas a través de los pasos de recolección.
Documenta cada paso.
No olvidarse de la gente involucrada. Tomar notas de quien estuvo allí, y que estuvieron haciendo, que observaron y como reaccionaron. Donde sea factible deberías considerar sumas de control que se generan y la firma criptográfica de la evidencia recolectada, ya que esto puede hacer mas fácil la preservación de una cadena fuerte de evidencia. Al hacer esto tu no debes alterar la evidencia.

4.El procedimiento del Archivo
La evidencia debe estar estrictamente asegurada. Además, la cadena de custodia necesita estar claramente documentada.

4.1 Cadena de Custodia
Deberías ser capaz de describir claramente cómo se encontró la evidencia, como se manejó y todo lo que le pasó a ella.
Lo que sigue necesita ser documentado:
Donde, Cuando y por quien fue descubierta y recolectada la evidencia.
Donde, Cuando y por quien fue manejada o examinada la evidencia.
Quien tuvo la custodia de la evidencia, durante que período, Como fue almacenada?
Cuando la evidencia cambió de custodia, cuando y como ocurrió la transferencia (incluir números de shipping, etc.)

4.2 Donde y como archivar
si es posible usar comúnmente medios (mas que algunos medios de almacenamiento obscuros) para archivar.
El acceso a la evidencia debería estar extremadamente restringido, y debería estar claramente documentado. Debería ser posible detectar acceso no autorizado.

5.Herramientas que necesitarás
Deberías tener los programas que necesitas para realizar la recolección de evidencia y análisis forense en medios de solo lectura (por Ej. Un CD)
Deberías tener preparado un ser de herramientas para cada uno de los sistemas operativos que manejes antes de tener que usarlo.
Tu test de herramientas debería incluir lo siguiente:
Un programa para procesos de examen (por Ej. "ps")
Programas para estado de sistemas de examen (por Ej. "showrev", "ifconfig", "netsat", "arp").
Un programa para hacer copias bit-a-bit (por Ej. "dd", "SafeBack").
Programas para generar sumas de control y Firmas (por Ej. "shalsum", a cheksum-enabled "dd", "safeBack", "pgp").
Programas para generar imágenes esenciales y para examinarlas (por Ej. "goore", "gdb").
Escritura/manuscritos la recolección de evidencia automatizada (por Ej. The Coroner's toolkit (FAR 1999)

Los programas en tu ser de herramientas deberían estar estáticamente unidos y no debería requerir el uso de cualquier biblioteca, solo aquellas de medios de solo

lectura. Aun entonces, ya que rootkits modernos pueden ser instalados a trabes de módulos kernel cargables, deberías considerar que tus herramientas no podrían darte una imagen completa del sistema.

Deberías estar preparado para testificar acerca de la autenticidad y la seguridad de las herramientas que usas.

6.Referencias

[FAR 1999] Farmer, D. y W Vwnwma "Computer Forensics Analysis Class Hadouts"
[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, September 1997.

[RFC2350] Brownlee, N. and E. Guttman, "Expectations for Computer Security Incident Response", FYI 8, RFC 2350, June 1998.

RFC2828] Shirey, R., "Internet Security Glossary", FYI 36, RFC 2828, May 2000.

7.Reconocimientos

Reconocemos con gratitud los comentarios constructivos recibidos de Herald Alvestrand, Byron Collie, Barbara Fraser, Gordon Lennox, Andrew Rees, Steve Romin y Floyd Short.

8.Consideraciones de Seguridad

Este documento completo discute temas de Seguridad

9.Direcciones de los Autores

Dominique Brezinski In-Q-Tel
1000 Wilson Blvd., Ste. 2900 Arlington, VA 22209 USA
EMail: dbrezinski@In-Q-Tel.org

Tom Killalea Lisi/n na Bro/n Be/al A/tha na Muice
Co. Mhaigh Eo IRELAND Phone: +1 206 266-2196
EMail: tomk@neart.org

10.Enunciados de Derecho de Autor

```
ES" base y la Sociedad de Internet y la Fuerza de Ingeniería de Internet rechaza
todas las garantías, expresas o implicadas, pero no limitada a ninguna garantía
que el uso de la información aquí provista no violará ningún derecho o ninguna
garantía implicada de comerciabilidad o conveniencia para un propósito particular.
Reconocimiento
Fondos para la Función RFC Editor se proveen actualmente por la Sociedad Internet.
```