# ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

# CENTRO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA

# ANÁLISIS CON HERRAMIENTAS FORENSES (LINUX)

Audie Estrella Ponce [(1)]; José Pincay Mero [(2)]
Facultad de Ingeniería Electricidad y Computación
Escuela Superior Politécnica del Litoral
Campus Gustavo Galindo Velasco, Km. 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil - Ecuador
auespo_10@hotmail.com [(1);] josapinc@espol.edu.ec [(2)]
Febrero del 2012 – Febrero del 2013
Guayaquil – Ecuador

Directora de Tesis Ing. Karina Astudillo, mail karina.astudillo@elixircorp.biz

## Resumen

*La presente tesis consiste en examinar cuatro archivos que fueron extraídos de una computadora con sistema operativo Linux que fue víctima de un ataque de seguridad, el sistema operativo que utilizamos para realizar el análisis fue Backtrack Linux versión 5.*
*Se llevó a cabo un análisis de computación forense a los archivos que se nos proporcionaron; con la finalidad de poder determinar su implicación en el ataque de seguridad realizado al equipo antes descrito. El concepto de computación forense está adquiriendo una gran importancia debido al aumento del valor de la información y al uso que se le da a esta. Además de las constantes intrusiones que han ocurrido en los sistemas informáticos, que han derivado en el robo de información sensible y pérdidas cuantiosas de muchas empresas a nivel mundial.*
*Esta prueba o esta evidencia contenida en las computadoras pueden ser obtenidas desde correos electrónicos, fotografías u otros documentos. Más importante aún es que esta evidencia, dependiendo del caso, puede ser frecuentemente recuperada de una computadora sospechosa, inclusive si el dueño o usuario de esta máquina borró la información, desfragmentó el disco o inclusive si lo formateó.*

***Palabras claves:*** *Análisis de Computación Forense, Backtrack Versión 5, Evidencia, Robo de Información.*

## Abstract

*This work consists in the examination of four files that were removed from a computer running Linux that was the victim of a security attack, the operating system used for analysis was Backtrack Linux version 5. It has been conducted a forensic analysis of the computer files that were provided, in order to determine their involvement in the attack described above. The concept of computer forensics is becoming very important due to the increase of the value of information and its use.*
*Furthermore, the constant intrusions that have occurred in computer systems have led to the theft of sensitive information and significant losses for many companies worldwide, the evidence contained in computers, can be obtained from emails, photos or any other kind of documents. Even more important is that this evidence may be frequently recovered from a suspect computer, even if the owner or user of this machine deleted the information, defragmented or formatted the disk.*

***Keywords:*** *Computer Forensic Analysis, Backtrack Linux Version 5, Evidence, Information Theft.*

# 1. Introducción

La computación forense es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Es importante mencionar, que en una infraestructura informática se puede analizar cualquier dispositivo que posea una memoria, por lo que se puede analizar los siguientes dispositivos:

- ✓ Disco duro de una computadora o servidor.
- ✓ Logs de seguridad.
- ✓ Credenciales de autentificación.
- ✓ Teléfono móvil o celular.
- ✓ Agendas electrónicas (PDA).
- ✓ Dispositivos de GPS.
- ✓ Impresora.
- ✓ Memoria USB.

Existen varios usos de la informática forense entre los que tenemos:

- ✓ Prosecución Criminal: Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
- ✓ Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, etc.
- ✓ Investigación de Seguros: La evidencia encontrada en computadores puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
- ✓ Temas Corporativos: Puede ser recolectada información en casos de apropiación de información confidencial, propietaria o espionaje industrial.
- ✓ Mantenimiento de la ley: Puede ser usada en la búsqueda inicial de órdenes judiciales.

El proceso de análisis forense a un equipo informático se describe a continuación

- ✓ Identificación: Se identifica o detecta el evento.
- ✓ Preservación: Se conserva la cadena de custodia y documentación.
- ✓ Recolección: Se recupera los datos y se recoge la evidencia.
- ✓ Examinación: Se realiza el seguimiento y extracción de datos ocultos.
- ✓ Análisis: Se realiza el estudio de la evidencia.
- ✓ Presentación: Se elabora el reporte de la Investigación.
- ✓ Decisión.

# 2. Metodología

.

La metodología de la computación forense se la puede resumir en cuatro pasos.

- ✓ Identificar qué dispositivo puede contener evidencia, reconociendo la frágil naturaleza de los datos digitales.
- ✓ Preservar la evidencia contra daños accidentales o intencionales, usualmente esto se realiza efectuando una copia o imagen espejada del medio analizado.
- ✓ Analizar la imagen copia de la original, buscando la evidencia o información necesaria.
- ✓ Terminada la investigación se debe realizar el reporte de hallazgos a la persona indicada para tomar decisiones.

# 3. Desarrollo de la Investigación

Para el análisis del caso se nos proporcionó cuatro archivos los cuales fueron extraídos de una computadora con sistema operativo Linux

Los archivos entregados fueron los siguientes

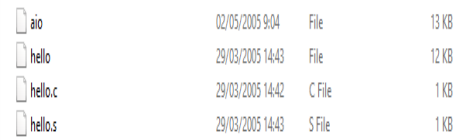


**Figura 1 Evidencia Obtenida**

En la Figura 1 se nos detalla los nombres de los archivos entregados los cuales se analizarán para poder determinar su implicación en el ataque de seguridad realizado al equipo antes descrito.

Antes de comenzar con el análisis de los archivos lo primero que aseguraremos es la integridad de estos, el primer archivo que analizamos es el hello.c y nos ayudamos de los siguientes comandos:

- ✓ Md5sum.
- ✓ File.
- ✓ Strings.

Con los cuales no se encontró información relevante para nuestro análisis.

El siguiente archivo que analizamos es el hello, para lo cual utilizamos los siguientes comandos.

- ✓ Md5sum.
- ✓ File.
- ✓ Strings.
- ✓ Hexdump –C.
- ✓ Nm.
- ✓ Ldd.
- ✓ Readelf --file –headers.
- ✓ Readelf --section –headers.
- ✓ Readelf --program – headers.
- ✓ Readelf --symbols.
- ✓ Readelf --hexdump.
- ✓ Objdump --disassemble.
- ✓ Strace.
- ✓ Gnu debugger.

Con estos comandos pudimos analizar el contenido, estructura y cabeceras del archivo, los cuales usamos como plantilla para poder realizar comparaciones con el archivo aio.

Una vez analizados estos archivos, continuamos con el aio; para lo cual utilizamos los mismos comandos con los cuales analizamos el archivo hello donde encontramos que el aio (all in one) es un backdoor que puede ser ejecutado de las siguientes maneras:

- ✓ Servidor HTTPD.
- ✓ Backdoor ICMP.
- ✓ Backdoor Shell.
- ✓ Socket Transmisor.
- ✓ Shell HTTP.
- ✓ Bind root shell.

Con los comandos utilizados se pudo determinar que este archivo está escrito en lenguaje ensamblador, al revisar su contenido no se pudo obtener ninguna información de relevancia o importancia.

## 4. Conclusiones

Según lo analizado e investigado el código malicioso se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños, este se denomina en informática como un troyano, los troyanos pueden realizar diferentes tareas, pero en la mayoría de los casos crean una puerta trasera que permite la administración remota a un usuario no autorizado.

Un troyano no es un virus informático, aun cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus consiste en su finalidad, para que un programa sea un troyano sólo tiene que acceder y controlar la máquina victima sin ser advertido.

Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

Se puede utilizar un código malicioso ya existente y modificarlo para hacerlo menos vulnerable a los diferentes sistemas de seguridad de la red, mínimos cambios en un código malicioso pueden hacer que ya no sea reconocido como malicioso por un programa antivirus, es por esta razón que existen tantas variantes de virus, gusanos y otros códigos maliciosos.

El atacante puede hacer uso de los diferentes puertos utilizados y así comprometer la seguridad e integridad de los datos de la red.

Un atacante que intente o consiga tener control sobre nuestro ordenador necesita tener a su disposición una puerta abierta en nuestro ordenador para poder comunicarse, es decir, un puerto de comunicaciones.

Los códigos maliciosos pueden tener múltiples objetivos como extenderse por la computadora, otras computadoras en una red o por Internet, robar información y claves, eliminar archivos e incluso formatear el disco duro o mostrar publicidad no deseada.

## 5. Recomendaciones

Una medida básica de seguridad es conocer qué puertos están abiertos y por qué están abiertos, hay que analizarlos dependiendo de los servicios que utilice la empresa porque de no ser así puede representar una potencial falla de seguridad.

Desde el punto de vista de seguridad, es recomendable permitir el acceso sólo a los servicios que sean imprescindibles, dado que cualquier servicio expuesto a Internet es un punto de acceso potencial para intrusos.

Debería implementarse soluciones Anti-x, estas son herramientas para la detección y eliminación de amenazas de tipo spam, virus o malware, que se encuentran en el tráfico de la red o en el correo.

Con respecto a la seguridad de la red es la implementación de HIPS o sistema de prevención contra intrusos, es un sistema que monitorea cada actividad que realiza un programa y notifica al usuario lo que está pasando para que este tome acción, permitiendo o bloqueando la acción. Adicional los HIPS incluyen sistemas de consultas de comunidad en las notificaciones a los usuarios, estos sistemas intentan ayudar al usuario a seleccionar la mejor opción de bloquear o continuar en base a las respuestas de otros usuarios. En otras palabras, cada vez que un usuario bloquea o permite el acceso a un programa, el HIPS almacena esta información en una base de datos central y la comparte con la comunidad de usuarios de ese HIPS.

Otra medida de seguridad que se debería tomar en cuenta es la implementación de un firewall que normalmente se utiliza para evitar que usuarios no autorizados no puedan tener acceso a la red interna.

Es muy importante que se creen cuentas de usuarios con los permisos estrictamente necesarios para las tareas que se vayan a realizar y de esta manera poder minimizar las posibilidades de que un troyano pueda ejecutarse con permisos de administrador.

En las políticas de seguridad establecidas se debe incluir la aplicación de actualizaciones periódicas de seguridad o parches, para esto lo más indicado sería tener un servidor de actualizaciones central para evitar que todas las PC's clientes de la red se conecten a Internet a tratar de actualizar.

Estos equipos clientes deberían actualizar sus sistemas a través del Servidor Central que es el único que podría conectarse a Internet para bajar todas las actualizaciones de los equipos de red.

Cuando haya la necesidad de instalar algún programa es muy importante considerar que para prevenir posibles troyanos hay que asegurarse antes de la instalación de un paquete de verificar su checksum MD5 y su firma PGP. El MD5 comprueba la integridad y no alteración del paquete, y la firma PGP la autenticidad de su autor.

Mantener un servidor activo de logs en la red es muy importante para poder monitorear toda la actividad que se genera en los equipos de comunicación; esto nos ayudaría para saber si las actividades programadas se cumplieron correctamente o para determinar en qué actividad un servidor dio error y colapsó o hubo algún movimiento sospechoso.

## 6. Referencias


[1] Interpol, Ciberdelincuencia, http://www.interpol.int/es/Criminalidad/Delincuencia-inform%C3%A1tica/Ciberdelincuencia, fecha de consulta agosto 2012.

[2] El universo, Estadísticas delitos informáticos, http://www.eluniverso.com/2012/06/29/1/1356/bancos-deben-tener-seguros-contra-delitos-informaticos.html, fecha de consulta agosto 2012.

[3] El tiempo, Computación forense, http://www.eltiempo.com/tecnologia/actualidad/ARTICULO-WEB-NEW_NOTA_INTERIOR-9644346.html, fecha de consulta agosto 2012.

[4] Ramos Alejandro, Historia de la computación forense, http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html, fecha de consulta agosto 2012.

[5] Zuccardi Giovanny, Objetivos de la Computación forense, http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf, fecha de consulta agosto 2012.

[6] Ardita Julio, Metodología de la computación forense, http://www-2.dc.uba.ar/materias/crip/docs/ardita01.pdf, fecha de consulta agosto 2012.

[7] Gutiérrez David, Usos de la Computación forense, http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf, fecha de consulta agosto 2012.

[8] Wikipedia, Proceso de análisis forense, http://es.wikipedia.org/wiki/C%C3%B3mputo_forense, fecha de consulta agosto 2012.

[9] Wikipedia, Herramientas para el análisis forense, http://es.wikipedia.org/wiki/C%C3%B3mputo_forense, fecha de consulta agosto 2012.