Reporte de incidentes

Fuga de Información

Tipo de Documento:	Guía
Fecha de Publicación:	03 de diciembre de 2015
Clasificación:	Acceso Libre

Presentado a:	Público General
Autores:	Alan Rodríguez
Versión:	1.2
Estado:	Final

CONTROL DE VERSIÓN

PREPARADO POR: Alan Rodríguez

APROBADO POR: Silvia Batista

FECHA DE INICIO: 18 de junio de 2015

ESTADO DEL DOCUMENTO: Final

HISTORIA DE CAMBIOS:

Fecha	Cambios	Autores	Versión
18/junio/2015	Borrador inicial	Alan Rodríguez	0.1
13/julio/2015	Cambios en redacción	Silvia Batista, Alan Rodríguez	1.0
03/diciembre/2015	Adaptación a formato	Alan Rodríguez	1.1
26/enero/2016	Ediciones	Mario Góngora, Alan Rodríguez	1.2

Contenido

1. Objetivos

1.1. Objetivo general

Documento de guía rápida de referencia para la recolección de información que sirva de evidencia a compartir con el *CSIRT Panamá* para el análisis en caso de incidentes informáticos en el Estado Panameño.

1.2. Objetivo específico

Ofrecer algunos comandos en sistemas *Linux* y *Windows* para la obtención de información que sirva de evidencia en el análisis de incidentes relacionados con la fuga de información.

2. Guía de recolección de evidencia

Reportando fuga de información

Importante: **recolectar la evidencia** a compartir con el equipo *CSIRT Panamá* **antes de realizar algún cambio interno.**

Comprimir los archivos con la contraseña: Evidencia-CSIRT

Agregar en archivo comprimido y **cifrado con la llave pública del *CSIRT Panamá***:

- ✓ En caso de tener protección contra denegación de servicio, *WAF* (*Web Application Firewall*); Sistema de Detección/Prevención de Intrusos (*IDS/IPS*) y/o cortafuegos, enviar registros de actividad al menos dos días antes del descubrimiento del incidente y dos días después (si aplica el caso).

Tiempo de actividad del servidor

Comando *Linux*	Comando equivalente *Windows*
$ uptime > uptime_Institución	C:\Windows\system32>net statistics server > stat_Institución

Centro Nacional de Respuesta a Incidentes Informáticos - CSIRT Panamá | Autoridad Nacional para la Innovación Gubernamental | Edificio Balboa 757, Corregimiento Ancón, Ciudad de Panamá | Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

Últimas conexiones internas al servidor

Comando *Linux*	Comandos equivalentes *Windows*
$ last > last_Institución	C:\Windows\system32>net user username | findstr /B /C:"Last logon" > net_user
	C:\Windows\system32>net user administrator | findstr /B /C:"Last logon" > net_user
	C:\Windows\system32>net user Administrador | findstr /B /C:"Ultima sesión iniciada" > net_user

Nota importante en entorno *Windows*: el comando arroja resultados solo cuando los nombres de usuario, dominio y cadena a buscar están escritas en el idioma que utiliza el sistema. También es importante acotar que el comando es sensible a mayúsculas.

Conexiones al servidor al momento de recolectar la evidencia

Comando *Linux*	Comandos equivalentes *Windows*
$ who > who_Institución	C:\Windows\system32>net session > net_session_Institución

Cantidad de usuarios actualmente creados por el administrador (revisar archivos de configuración)

Comando *Linux*	Comandos equivalentes *Windows*
# cut -d: -f1 /etc/passwd > users_Institución	C:\Windows\system32>net session > net_session_Institución
# cut -d: -f1 /etc/shadow > shadow_Institución	

En caso de fuga de información (publicación no autorizada de contenido) enviar la siguiente información:

- Dirección *URL* del sitio donde se encuentra publicada la información no autorizada.
- Captura de pantalla de la publicación no autorizada y guardar como archivo *.png*.
- Archivos de configuración de servidor *web* (si aplica)
  - *robots.txt,* módulos activos y usados con respectivas versiones
  - En *Linux: apache.conf, apache2.conf, httpd.conf, ngnix.conf.*
  - En *Windows: RootWeb.config, ApplicationHost.config*
- Archivos de contenido *web* (directorio del contenido de la página *web*).
- *Webshells* (capturas de pantalla y rutas *URL* en caso de conocerlas).
- Registros de acceso y errores del servicio *web*
  - En *Apache/Ngnix: access.log* y *error.log*
  - En *IIS: C:\inetpub\logs\LogFiles* y *C:\Windows\System32\LogFiles*

Centro Nacional de Respuesta a Incidentes Informáticos - CSIRT Panamá | Autoridad Nacional para la Innovación Gubernamental
| Edificio Balboa 757, Corregimiento Ancón, Ciudad de Panamá
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

- Puertos abiertos al momento de descubrir la fuga de información

Puertos abiertos

Comando *Linux*	Comandos equivalentes *Windows*
$ netstat -a | cat > netstat-a_fecha	C:\Windows\system32>netstat -nao > netstat_fecha
$ netstat -s | cat > netstat-s_fecha	

Presentar en formato comprimido (*zip, rar, tar, bz2*) y **cifrar con llave pública del *CSIRT Panamá*** que se encuentra a continuación en la sección "Información de contacto". Ver guías "CERT-306 – Compresión de archivos (Linux)", "CERT-307 – Compresión de archivos (Windows)" y "CERT-252 - Guía de firma y cifrado de archivos utilizando PGP".
Enviar evidencia a la dirección info@cert.pa colocando en el asunto del correo: **Institución – Fuga de información**.

3. Información de contacto:

CSIRT PANAMA

Computer Security Incident Response Team
Autoridad Nacional para la Innovación Gubernamental
E-Mail: info@cert.pa
Phone: +507 520-CERT (2378)
Web: http://www.cert.pa
Twitter: @CSIRTPanama
Facebook: http://www.facebook.com/CSIRTPanama
Key ID: 16F2B124