Reporte de incidentes

Denegaciones de Servicio

Tipo de Documento:	Guía
Fecha de Publicación:	04 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
04/diciembre/2015	Adaptación a formato	Alan Rodríguez	1.1
26/enero/2016	Ediciones	Alan Rodríguez	1.2

Contenido

1. Objetivos 4
1.1. Objetivo general 4
1.2. Objetivo específico 4
2. Guía de recolección de evidencia 4
3. Información de contacto: 5

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 denegaciones de servicio.

2. Guía de recolección de evidencia

Reportando denegaciones de servicio

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 y/o *WAF* (*Web Application Firewall*) enviar registros de actividad al menos dos días antes del descubrimiento del incidente y dos días después (si aplica el caso).
- ✓ Presentar actividad de tráfico como: direcciones IP de origen y de destino, tipo de servicio/puerto y marcas de tiempo.

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	

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 – Denegación de Servicio**.

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