TÉCNICAS DE ATAQUE Y DETECCIÓN DE INTRUSOS

ING. SILER AMADOR DONADO

samador@unicauca.edu.co

AGENDA

- Algunas definiciones
- Escenario de ejemplo
- Análisis del escenario
- Fases del análisis forense digital
- Cadena de custodia
- Ciclo de auditoría forense
- Política de ejemplo
- Sistema detección de intrusos
- Demostración

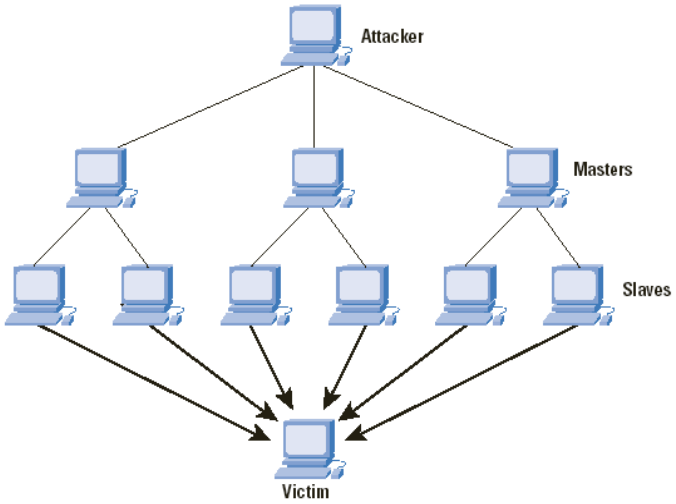
ALGUNAS DEFINICIONES

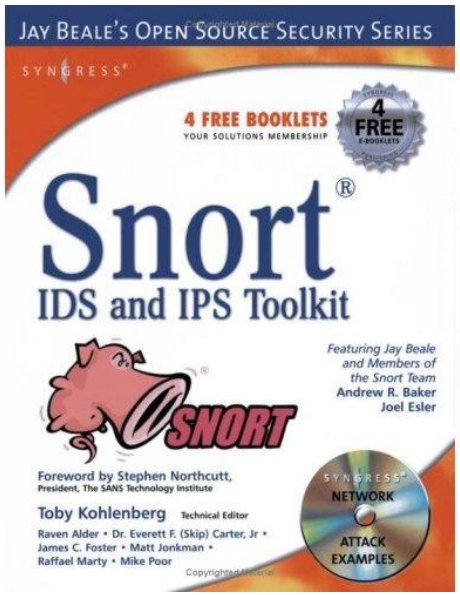
CERT

DDOS

GUSANO

SNORT





CERT Computer Emergency Response Team

UNAM CERT

CERT
www.cert.org

US-CERT

PakCERT
Pakistan Computer Emergency Response Team

ESCENARIO DE EJEMPLO (1/3)

Un viernes por la tarde comienza a circular por Internet un nuevo “gusano”. Éste aprovecha una vulnerabilidad de Microsoft Windows XP que había sido publicada oficialmente un par de semanas atrás y que se acompañó del correspondiente “parche”. Se conoce que el “gusano” se extiende automáticamente enviándose por e-mail usando todas las direcciones que encuentra en el sistema infectado,

ESCENARIO DE EJEMPLO (2/3)

...además está programado para generar diferentes nombres de archivos adjuntos y sus extensiones pueden variar, al tiempo que elige entre un centenar de asuntos y cuerpos de mensaje diferentes. Cuando el "gusano" infecta un sistema realiza una escalada de privilegios hasta obtener derechos de Administrador,

ESCENARIO DE EJEMPLO (3/3)

…realizando entonces la descarga, desde diferentes direcciones IP y vía FTP, de un agente para la ejecución de ataques de denegación de servicio distribuido (DDoS). Aunque los fabricantes de software antivirus alertan inmediatamente del "gusano" su expansión ha sido muy rápida y aún no se dispone de su firma. Su organización ya ha sufrido una infección importante por la ejecución del "gusano" unas tres horas antes de que dispusiese de la firma para su antivirus y este se encuentra activo en algunos sistemas de su red.

ANÁLISIS DEL ESCENARIO (1/2)

Ante un escenario de este tipo, podríamos hacernos las siguientes preguntas:

¿Tiene su organización un equipo de respuesta a incidentes como parte de su política de seguridad?

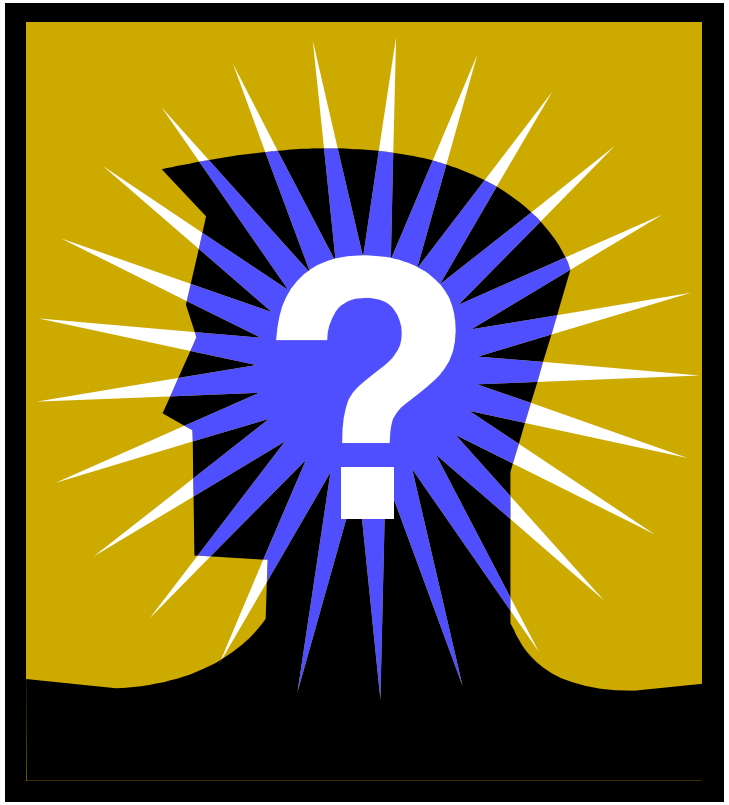
¿Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación?

ANÁLISIS DEL ESCENARIO (2/2)

¿Podría informar y justificar a sus empleados una anulación temporal de sus cuentas de correo electrónico para su investigación?

Si el ataque DDoS está programado para atacar al servidor Web de otra organización, por ejemplo a la mañana siguiente, ¿sería capaz de manejar una situación en la que dicha organización le pidiese responsabilidades tras detectar que el ataque se ha producido desde direcciones IP suyas?

Y QUÉ PODEMOS HACER?



FASES DEL ANÁLISIS FORENSE DIGITAL

1ª. Identificación del incidente.

2ª. Recopilación de evidencias.

3ª. Preservación de la evidencia.

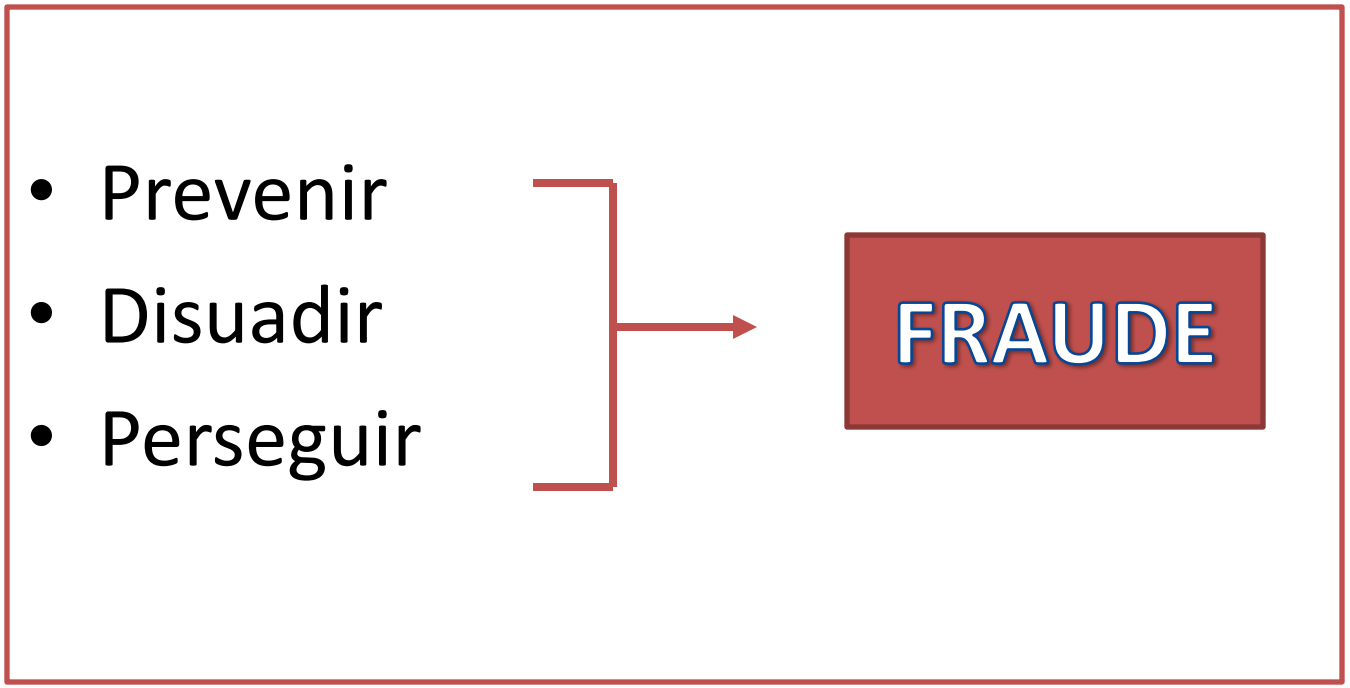
4ª. Análisis de la evidencia.

5ª. Documentación y presentación de los resultados.

CADENA DE CUSTODIA

- ✓ Dónde, cuándo y quién manejó o examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc?
- ✓ Quién estuvo custodiando la evidencia, durante cuanto tiempo y dónde se almacenó?
- ✓ Cuando se cambie la custodia de la evidencia también deberá documentarse cuándo y como se produjo la transferencia y quién la transportó?

CICLO DE AUDITORÍA FORENSE



PREVENIR

- Establecer políticas/códigos de Conducta
- Capacitación y socialización de las políticas
- Establecer adecuados controles preventivos

DISUADIR

- Establecer comité de ética y comunicar su existencia
- Establecer canales de denuncia
- Establecer sistemas de detección de intrusos

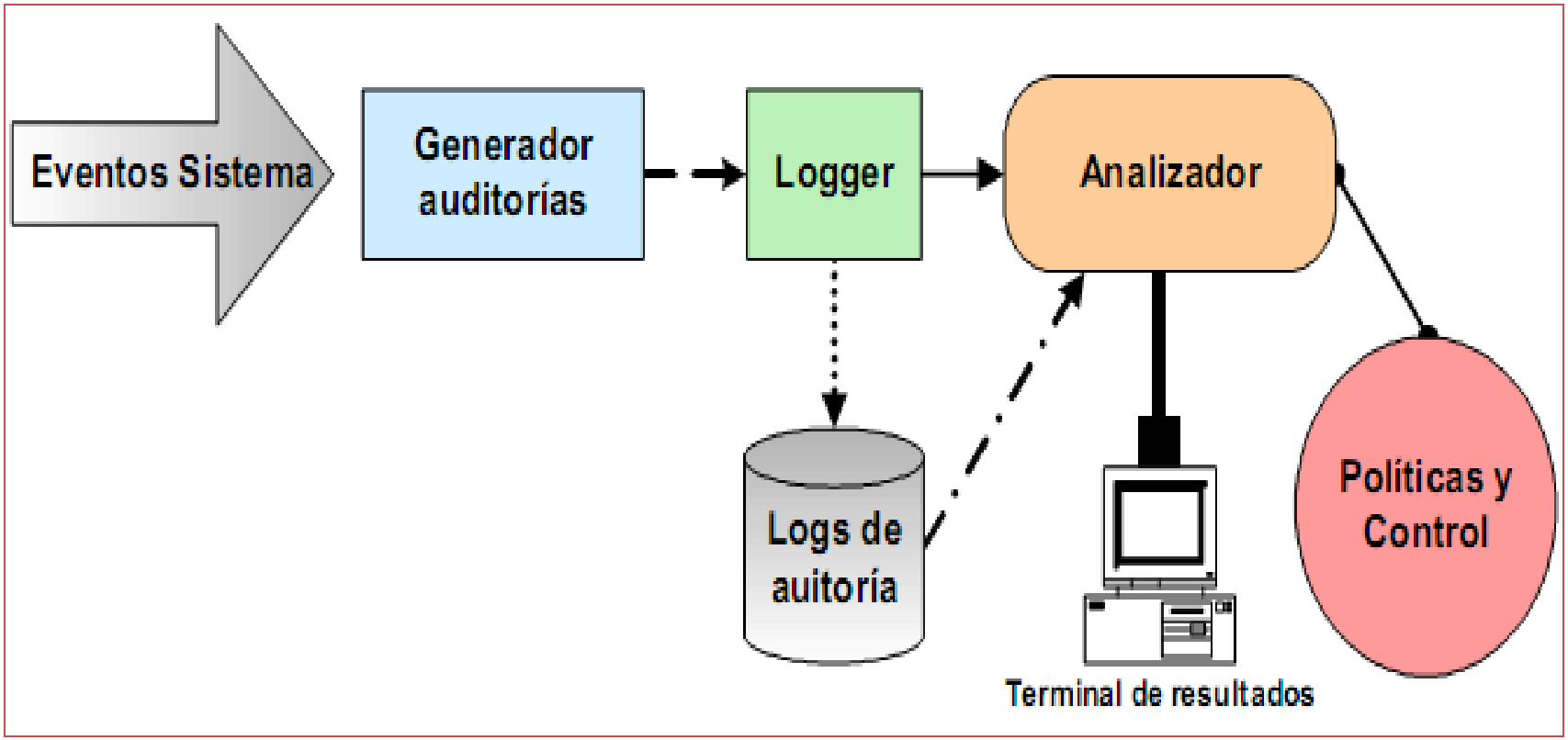
PERSEGUIR

- Investigar irregularidades
- Denunciarlas ante la Justicia Penal
- Re – evaluar los controles en los casos de fraude

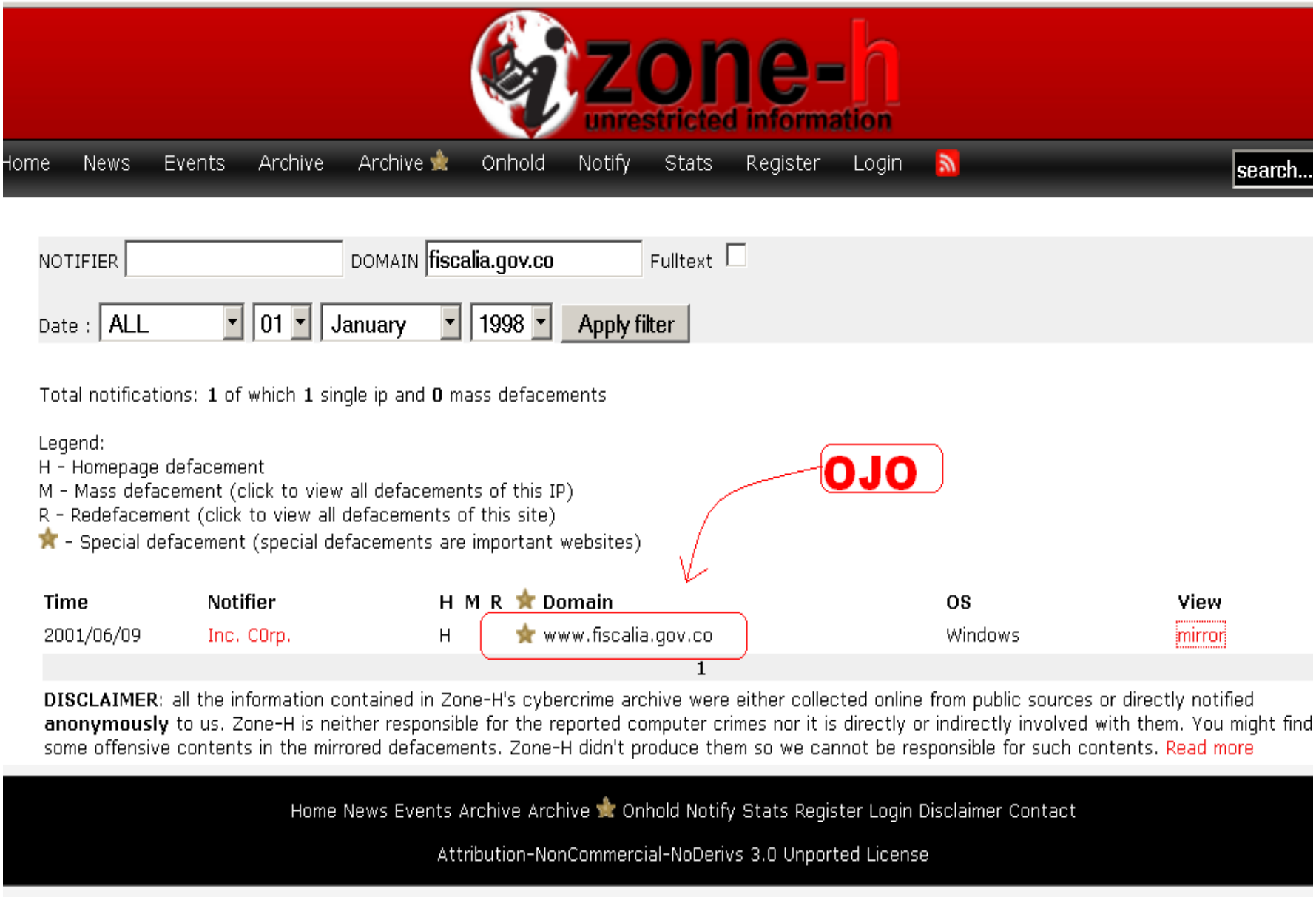
POLITICA DE EJEMPLO

Política	Procedimiento	Práctica
Necesitamos proteger nuestro servidor Web contra accesos no autorizados.	Se mantendrá actualizado el servidor Web en cuanto a seguridad.	Se comprobará diariamente si existen parches de seguridad del servidor Web, en cuyo caso se aplicarán.
	Se instalará un IDS configurado para comprobar que la actividad en el servidor Web es normal.	Se instalará la última versión del "`Snort`", y se aplicarán los cambios de configuración pertinentes para concentrar la vigilancia especialmente en el servidor Web.

SISTEMA DETECCIÓN DE INTRUSOS




zone-h
unrestricted information
Home News Events Archive Archive Onhold Notify Stats Register Login
search...
Mirror saved on: 2008-11-02 13:43:37
Notified by: Dark_Mare
System: Linux
Domain: http://www.unicauca.edu.co/teleminga
Web server: Apache
IP address: 190.5.195.137
Notifier stats
Joomla! Logo
OJO
Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here
Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here Dark_Mare Was Here


zone-h
unrestricted information
Home News Events Archive Archive Onhold Notify Stats Register Login
search...
NOTIFIER
DOMAIN fiscalia.gov.co
Fulltext
Date : ALL 01 January 1998 Apply filter
Total notifications: 1 of which 1 single ip and 0 mass defacements
Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
- Special defacement (special defacements are important websites)
OJO
Time Notifier H M R Domain OS View
2001/06/09 Inc. C0rp. H www.fiscalia.gov.co Windows mirror
1
DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. Read more
Home News Events Archive Archive Onhold Notify Stats Register Login Disclaimer Contact
Attribution-NonCommercial-NoDerivs 3.0 Unported License

DEMOSTRACIÓN

AVISO IMPORTANTE

Esta demostración se realiza en un ambiente 100% virtual y tiene fines exclusivamente académicos, el autor no se hace responsable del uso indebido o con fines ilegales del mismo.