América Latina Inter Conectada con Europa
Introducción al EWS SurfIDS
CLARATEC
Frederico Costa, Analista de seguridad
Centro de Atención a los Incidentes de Seguridad – CAIS
Red Nacional de Enseñanza e Investigación de Brasil – RNP
This project is funded by the European Union
A project implemented by CLARA

Introducción al EWS SurfIDS
Derechos de autor© 2012 CAIS/RNP - Centro de Atención a los Incidentes de Seguridad de la Red Nacional de Enseñanza e Investigación de Brasil – RNP. Todos los derechos reservados.
La reproducción total o parcial de este material está totalmente prohibida, así como su uso para cualquier propósito, comercial u otro.

Sobre el curso

- **Objetivo**
  - Presentar los conceptos del Early Warning System (EWS) - o "Sistema de Alerta Temprana" - que le permitirán al alumno detectar las amenazas contra sus redes para iniciar contramedidas ágiles y, especialmente, para correlacionar los datos y analizarlos con el objetivo de generar un sistema inteligente que eviten los ataques o cualquier otro tipo de actividad maliciosa.
- **Instructor**
  - Frederico Costa

Agenda

- Introducción
  - ✓ Introducción sobre EWS
  - ✓ Introducción sobre el SurfIDS
- Operación del SurfIDS
  - ✓ Sensores
  - ✓ Honeypots
  - ✓ Módulos de detección
  - ✓ Interface de la web
- Utilizando la interface

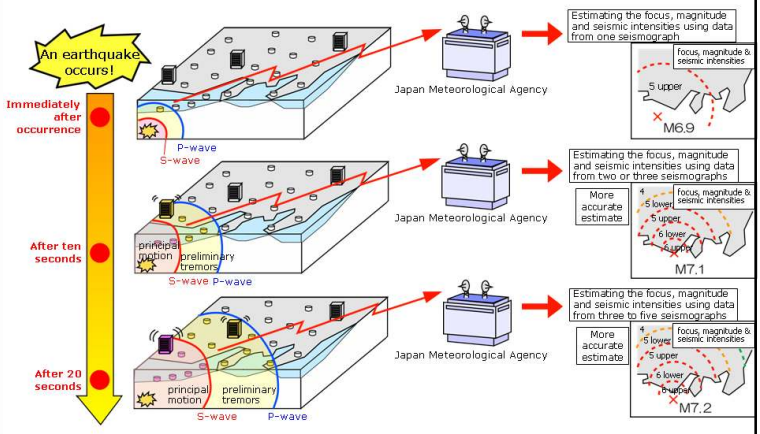
Introducción

¿Qué es un EWS?

- ***Early Warning System* (EWS)**
- **Sistema capaz de proporcionar informaciones completas a todas las víctimas posibles de un ataque o falla inminente con el objetivo de prevenir un "desastre"**
- **Aplicaciones:**
  - Previsión de terremotos
  - Previsión de tsunamis
  - Previsión de actividades volcánicas
  - Previsión de ataques contra la infraestructura de TI

EWS (1)

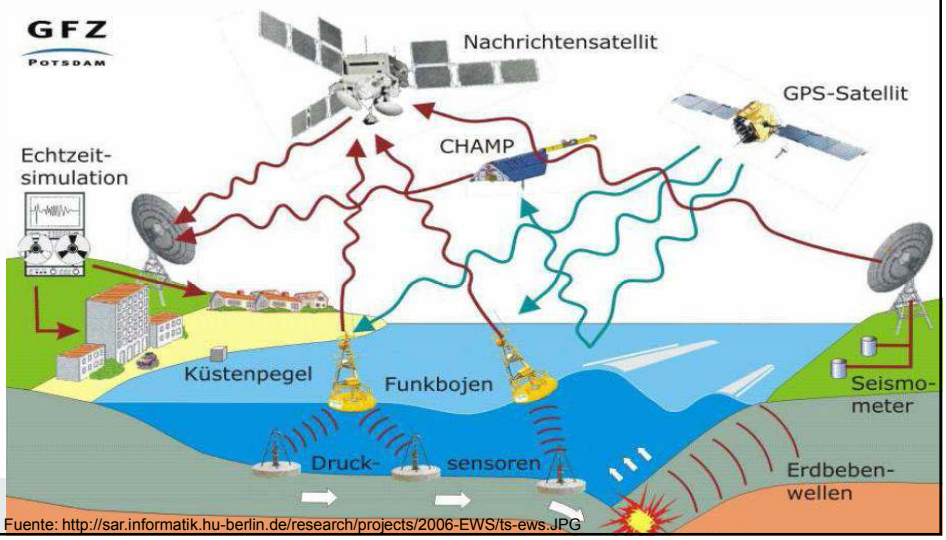
- **Previsión de terremotos**



Fuente: http://www.jma.go.jp/jma/en/Activities/image/eew1.png

EWS (2)

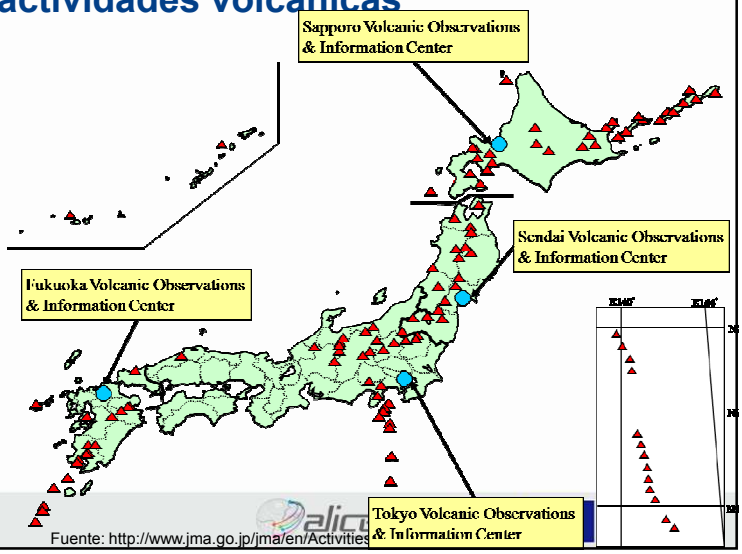
- **Previsión de tsunamis**



Fuente: http://sar.informatik.hu-berlin.de/research/projects/2006-EWS/ts-ews.JPG

EWS (3)

- **Previsión de actividades volcánicas**



Fuente: http://www.jma.go.jp/jma/en/Activities

EWS (4)

- **Previsión de ataques contra la infraestructura de TI**

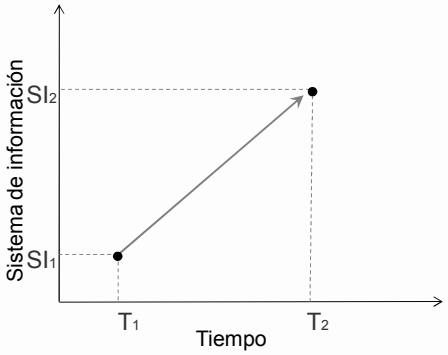
Fuente: http://news.techworld.com/security/3229816/nsa-may-be-building-early-warning-system-for-cyber-attacks/

Requisitos de un EWS en SegInfo (1)

- **Por lo menos dos sistemas de información distintos en el ciberespacio**
  - SI_1 y SI_2
- **Por lo menos dos instancias de tiempo**
  - T_1 y T_2
  - ($T_1 < T_2$) => "*temprano*"
- **Disponibilidad de información útil para la prevención de daños**
  - "*alerta*"

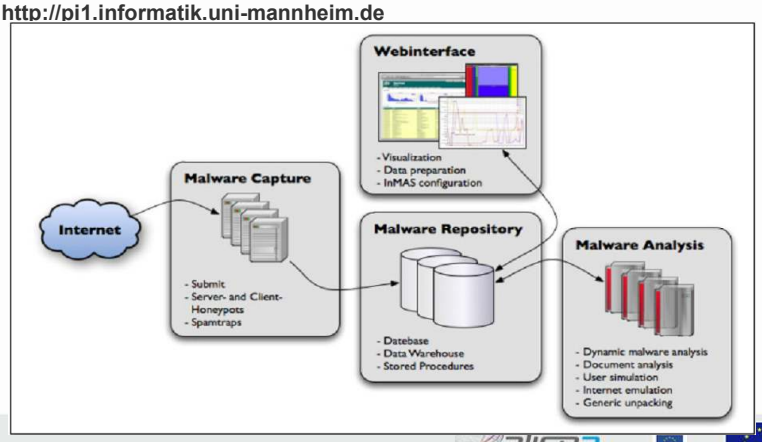
Requisitos de un EWS en SegInfo(2)

- **Información útil**
  - Información para prevenir futuros daños en SI_2
- **Anticipación**
  - La información debe estar disponible de forma anticipada
    - T_2 debe ocurrir antes que la actividad iniciada en SI_1 alcance SI_2



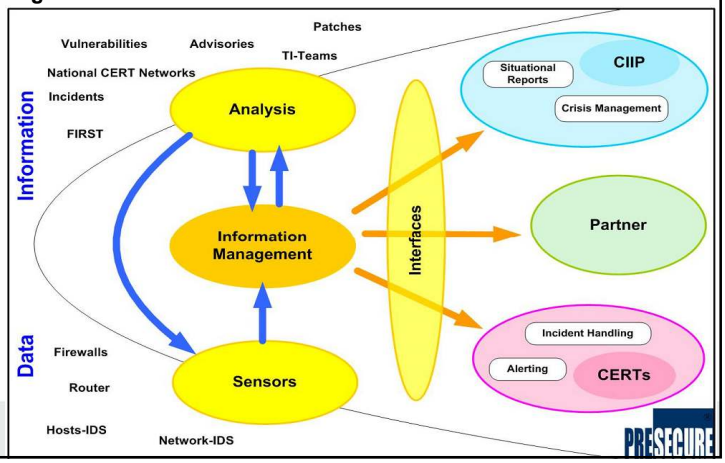
Ejemplos de EWS (1)

- **InMAS**
  - Universidad de Mannheim y BSI (Alemania)
  - Enfocado en los análisis de malwares
  - **http://pi1.informatik.uni-mannheim.de**



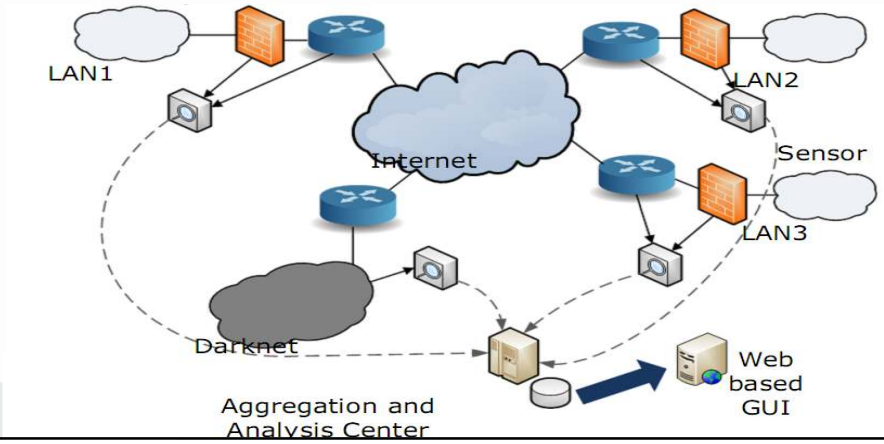
Ejemplos de EWS (2)

- **CarmentiS**
  - BSI junto con los CERTs alemanes (Alemania)
  - Plataforma colaborativa de intercambio de informaciones entre los CERT
  - **http://www.carmentis.org**



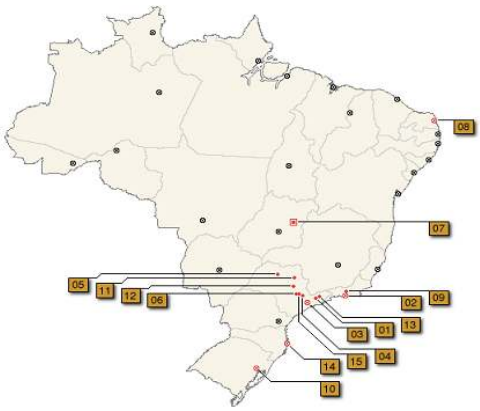
Ejemplos de EWS (3)

- **Arakis**
  - CERT Polska NASK (Polonia)
  - Plataforma de detección y caracterización de nuevas amenazas
  - **http://arakis.cert.pl/en**



Ejemplos de EWS (3)

- **Projecto de honeypots distribuidos**
  - CERT.BR (Brasil)
  - Red de honeypots distribuidos
  - **http://www.honeypots-alliance.org.br/**



Misión de un EWS

- automatizar la detección de nuevas amenazas;
- automatizar el proceso de análisis de ataques;
- desarrollar una metodología para la creación de firma de ataques que serán utilizadas en firewalls, IDS e IPS;
- desarrollar un proceso automático de análisis de tendencias de las actividades maliciosas;
- mapear el estado de seguridad de las redes;
- apoyar el proceso de respuesta ante incidentes de seguridad;
- proporcionar estadísticas de ataques contra las redes.

Preguntas sobre la implementación de un EWS (1)

- Definición de la línea de acción del EWS – ¿Qué será monitoreado?
- Definición de los sensores que serán utilizados – ¿Cómo monitorear?
  - Cantidad de sensores
    - ¿Cuánto mayor número es mejor?
- Definición de técnicas de correlacionamiento de datos– ¿Cómo generar información?
- Almacenamiento de datos– ¿Qué datos serán almacenados?
  - Privacidad
  - Capacidad de almacenamiento

Preguntas sobre la implementación de un EWS(2)

- **Procesamiento de datos– ¿Cómo procesar una gran cantidad de información?**
  - ($T_1 < T_2$) => "*temprano*"
  - Tiempo real
- **Visualización de informaciones – ¿Cómo presentar las informaciones obtenidas?**
  - Log (bitácoras)
  - Gráficos (tipos?)

Preguntas sobre la implementación de un EWS (3)

- **Herramientas – ¿Qué herramientas utilizar para obtener y procesar los datos?**
  - Desarrollar
  - FOSS
  - Appliances
- **Inteligencia – ¿Cómo "retroalimentar" el sistema?**
  - Análisis de malwares
- **Colaboración – ¿Cómo interactuar con socios?**
  - IETF – IODEF (*Incident Object Description and Exchange Format*)
  - IETF – IDMEF (*Intrusion Detection Message Exchange Format*)

Valores agregados de um EWS

- **Capacidad de monitoreo**
- **Capacidad de respuesta**
- **Capacidad de interacción**
- **Capacidad de previsión**
- **Mejora continua**

Introducción al SurfIDS

http://www.collectors-badges.com/images/Badges%20Military/nato_headquarters-early_warning_force.jpg

Introducción

- **IDS Distribuido (D-IDS) desarrollado por la SurfNET (red académica holandesa)**
  - http://www.surfnet.nl/
  - http://ids.surfnet.nl
- **Modelo enfocado en ambientes donde el uso de la red no está muy controlada (academia)**
- **Enfocado en la detección de worms, intentos de accesos indebidos y otros tráficos maliciosos en la red**

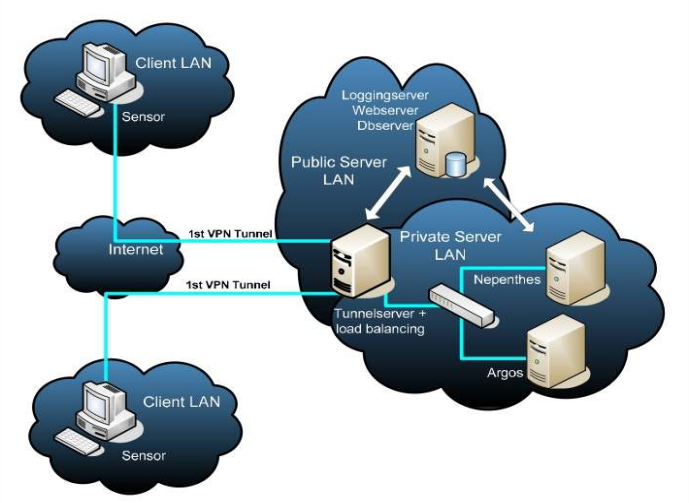
IDS Distribuido (D-IDS)

- **Características de un D-IDS tradicional**
  - Cliente-servidor
    - Cliente (sensor) – honeypot /análisis pasivo
    - Servidor – correlacionamiento de los logs obtenidos a través de los sensores
  - Problemas
    - Sensor necesita upgrades (nuevas suscripciones, honeypots, etc.)
    - Exposición del sensor (vulnerabilidades en el honeypot)
    - Instalación compleja del sensor
    - Dependiendo de los datos recolectados por el sensor se puede obtener una alta tasa de falsos positivos
      - Logs de firewall
      - Netflow

D-IDS con SurfIDS (1)

- **Sensores**
  - Totalmente pasivo y libre de mantenimientos
  - Basado en honeypots para evitar falsos positivos
  - Sensor puede ser pode un workstation normal que ejecuta el SO a partir de un pendrive
  - Instalación simples
- **Servidores**
  - Honeypots instalados en un servidor central (*tunnel server*)
  - Datos analizados e interface de acceso instalada en un servidor a parte

D-IDS con SurfIDS (2)



http://ids.surfnet.nl

D-IDS con SurfIDS (3)

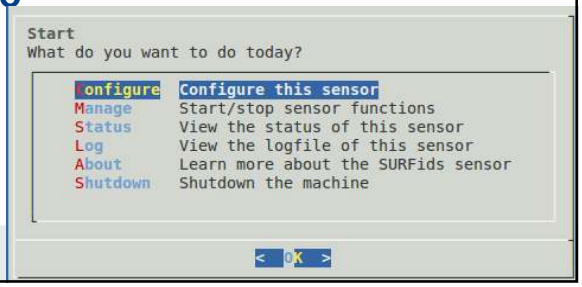
- **Modus operandi**
  - Sensor inicia un túnel VPN L2 (bridge) para el *tunnel server*
  - *Tunnel server* obtiene una dirección IP de la red del sensor y crea una interface virtual con ese IP para ejecutar el honeypot
  - El honeypot Nepenthes simula algunas vulnerabilidades conocidas de Windows
  - Todos los ataques al honeypot son registrados en un banco de datos (Postgresql)
  - Una interface web permite el acceso a las informaciones de los ataques

Operación del SurfIDS

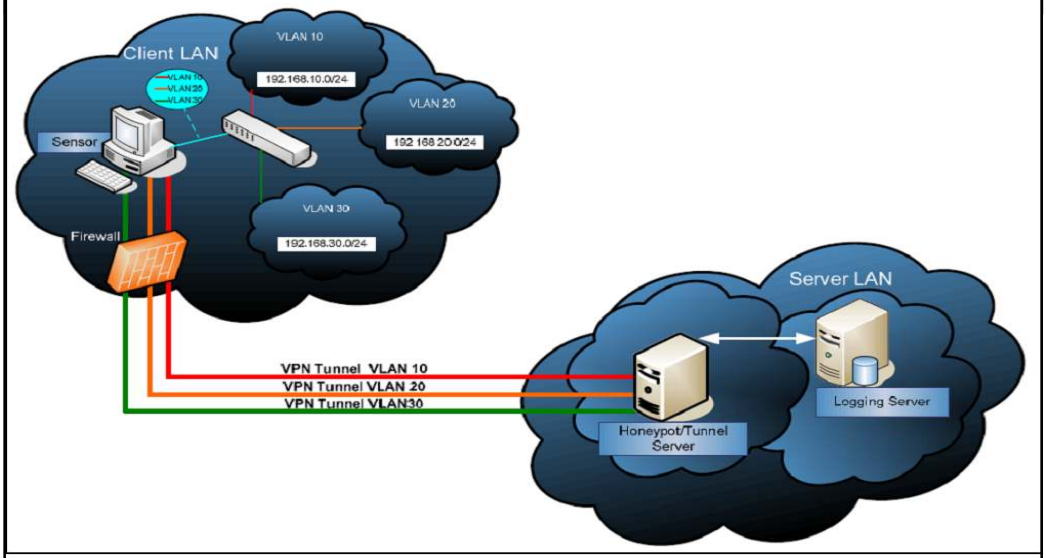
http://4.bp.blogspot.com

Sensores (1)

- **Instalación**
  - apt-get instala surfids-sensor
  - Knoppix live usb
  - Vmware
- **Crea un ambiente 100% pasivo en la red cliente**
- **Bridge con *tunnel server***
- **Libre de mantenimiento**
- **Fácil operación**



Sensores (2)



SurfIDS Manual v1.0

Honeypots

- **Ejecutan en un servidor central**
  - Nepenthes
    - Honeypot default del SurfIDS
    - Puede efectuar el download de malwares
    - Alto rendimiento
    - Solamente detecta ataques conocidos (pre-analizados)
    - Análisis detallado del ataque
  - Argos
    - Honeypot de alta interacción
    - Bajo rendimiento
    - Detecta ataques conocidos y nuevos ataques

Otros módulos de detección

- **ARP *poisoning***
  - Detecta ataques de adulteración en la resolución ARP
- ***Rogue* DHCP**
  - Detecta servidores DHCP intrusos en la rede
- **Snort *plugin***
  - Registra los mensajes de Snort en la base de datos del SurfIDS
  - Módulo no oficial
- **SMTP honeypot**
  - Recolecta SPAM y reporta/baja links de malware
  - Módulo no oficial y en fase de desarrollo

Utilizando la interface

"You can't just punch in 'let there be light' without writing the code underlying the user interface functions."

© 1997 J. P. Rini from The Cartoon Bank. All rights reserved.

Configurando el SurfIDS

Administración de usuarios (1)

- **Permite firmar los e-mails enviados (alertas)**
- **Administración de los sensores**
  - Solamente lectura (0)
  - Administración remota (1)
  - Configuración de módulos extra (2) – Argos, arp poisoning
- **Administración de cuentas de usuarios**
  - No permite alterar los datos de ningún usuario, ni el propio (0)
  - Puede alterar los datos de la misma cuenta (1)
  - Puede alterar los datos de usuarios del mismo dominio (2)

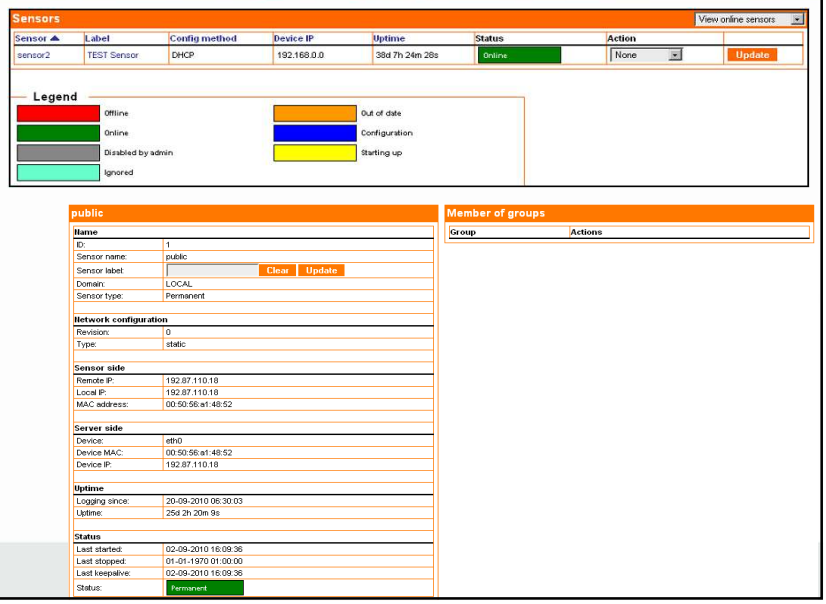
Administración de usuarios (2)

Username	jan
Password	
Confirm Password	
Domain	SURFnet
Email address	jan@website.com
Email signing	○ Enable GPG signing ◉ Disable GPG signing
Access: Sensor	◉ 0 - Read only access ○ 1 - Remote control access ○ 2 - ARP & ARGOS access
Access: Search	◉ 1 - Domain records
Access: User Admin	○ 0 - No access ○ 1 - Own account ◉ 2 - Domain accounts
	update

Configuración de los Sensores (1)

- **Ejecutar comandos predefinidos en los sensores**
  - Reboot
  - SSH on/off
  - Stop/Start:
  - Enable/Disable:
  - Ignore/Unignore
  - Enable/Disable ARP
- **Verificar status**
- **Ver detalles de configuración**

Configuración de los Sensores (2)



Configuración del Argos

- **Pasar el tráfico sospechoso hacia Argos**
  - Especifica IP/faja que será analizada
  - Especifica template a ser usado:
    - All traffic to the sensor
    - Top 100 your sensors
    - Top 100 all sensors
    - Top 100 specific sensor
- **Configurar detalles del Argos (administradores)**
  - Imagen de SO que será utilizada

Informes

Estadísticas (1)

- **Ranking**
  - Compara las informaciones de actividades maliciosas entre los sensores de un dominio específico (derecha) con relación a todos los dominios presentes en SurfIDS
- **Cross Domain**
  - Levanta las informaciones sobre cuáles IP de un determinado dominio son responsables por las actividades maliciosas
- **Maps**
  - Hace un ploteo de la aproximación de los orígenes del ataque geo-localizadas (google maps)
- **Traffic**
  - Hace un ploteo del tráfico de la red que cruza por el túnel VPN de cada sensor

Estadísticas(2)

- **Server info**
  - Hace un ploteo de la utilización de recursos de los servidores (administradores)
- **Detected Protocols**
  - Nombre y tipo de todos los protocolos detectados por los sensores
- **Graphs**
  - Hace un ploteo de los gráficos personalizados a partir de las informaciones obtenidas por el IDS
- **My Reports**
  - Genera informes sobre determinadas acciones y los envía por e-mail

Análisis

Análisis (1)

- **Attacks**
  - Informa sobre (posibles) ataques detectados por el SurfIDS
- **Exploits**
  - Informa sobre los tipos de exploits detectados por el Nephentes
- **Malware Offered**
  - Informa sobre el protocolo utilizado para transferir el malware, IP que pone a disposición el malware u el nombre del archivo
- **Malware Downloaded**
  - Análisis de los malwares bajados por el Nepenthes (resultado de antivirus, informaciones sobre el binário)

Análisis (2)

- **Malware Hosts**
  - Informa el IP de los mayores huéspedes de malwares
- **Search**
  - Posibilita la búsqueda personalizada por análisis

Referencias

Referencias (1)

I. **Página oficial del SurfIDS**
   - http://ids.surfnet.nl

II. **Manual SurfIDS**
   - http://www.surfnet.nl/Documents/Manual_IDS_v1.0.pdf

III. **Imagen VMWare de exámenes**
   - http://ids.surfnet.nl/downloads/SURFids_2.0-v4.zip

GRACIAS

Centro de Atención a los Incidentes de Seguridad – CAIS/RNP

http://www.rnp.br/cais/

@cais_rnp

Notificación de Incidentes

Para notificar incidentes de seguridad que involucre las redes conectadas a la RNP:

1. E-mail: cais@cais.rnp.br

Para el envío de informaciones en criptografías use la clave PGP pública del CAIS:http://www.rnp.br/cais/cais-pgp.key

2. Formulario para la Notificación de Incidentes de Seguridad: http://www.rnp.br/cais/atendimento_form.php

Hotline INOC-DBA (Inter-NOC Dial-By-ASN): 1916*800

Atención de emergencia: Para comunicarse fuera de horas laborables (09:00 - 18:00 - Horario de Brasilia) por favor llame al (61) 3226–4699 .

Alertas del CAIS: El CAIS mantiene la lista rnp-alerta@cais.rnp.br. Suscripción abierta a la comunidad de seguridad. Inscripción a través del formulario en: http://www.rnp.br/cais/alertas/