GT-CSIRT: Grupo de Trabajo de RedCLARA CSIRT

Liliana Solha
Coordinadora del GT

15th RedCLARA Technical Meeting
07-08 de Noviembre, 2011
Montevideo, Uruguay

This project is funded by the European Union
A project implemented by CLARA

Agenda

- Propuesta del GT
- Miembros
- Líneas de acción
- Status
  - Tareas, entregables, cronograma
  - Próximos pasos

Propuesta

- GT-CSIRT
  - Consolida acciones del GT-Seg
  - Alcance reducido
- Propuesta focalizada en tres líneas de acción:
  1. Monitoreo de actividad maliciosa
  2. Tratamiento de incidentes de seguridad
  3. Apoyo a la creación de CSIRTs
- Categoría del GT: *Despliegue de un piloto de nueva tecnología/servicio*

Miembros

- Miembros

Institución	NREN	Nombre
INICTEL	RAAP	José Luis Quiroz
INICTEL	RAAP	Javier Richard Quinto
CEDIA	CEDIA	Claudio Chacón
RAU	RAU	Sergio Ramirez
REUNA	REUNA	Claudia Inostroza
CONARE	CONARE	Danny Silva
RNP	RNP	Frederico Costa
RNP	RNP	Carla Freitas
UFRN	RNP	Mário Sérgio
UTPL	CEDIA	Marco Antonio Cevallos

- Asistente: Rildo Souza (RNP)

LA-1: Monitoreo de actividad maliciosa

- Tareas y entregables:
  - [T1] Estructuración del ambiente de monitoreo (piloto).
    - Documentación de instalación y uso de la solución de monitoreo
    - Informe final de ejecución del piloto
    - Término de adhesión para la NREN
  - [T3] Entrenamiento
    - Material del curso
    - Curso hands-on (Taller CLARA-Tec 2012)
  - [T4] Despliegue
    - Cronograma de implantación
    - Estructura implantada en todas las NRENs
    - Informes periódicos de implantación

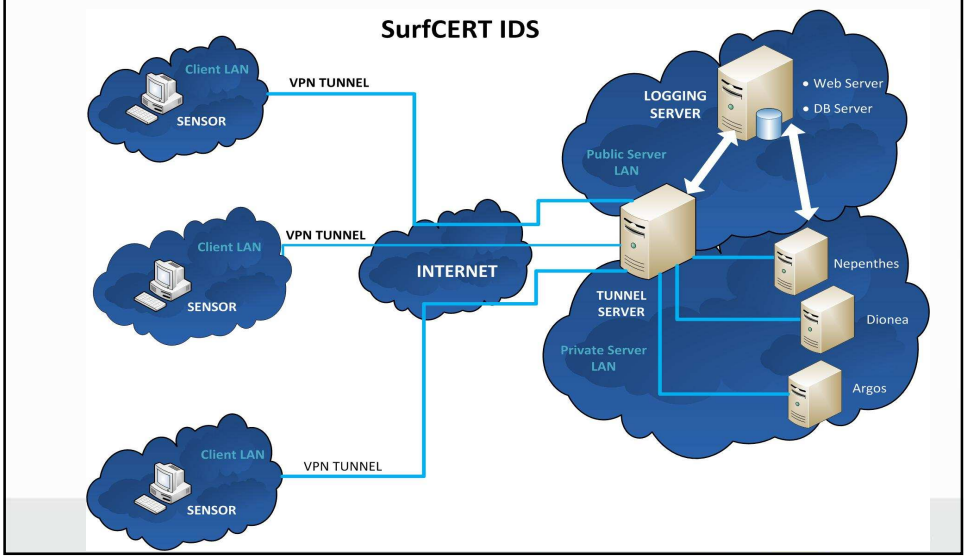
LA-1: Monitoreo de actividad maliciosa

- Solución de Monitoreo: Surf IDS

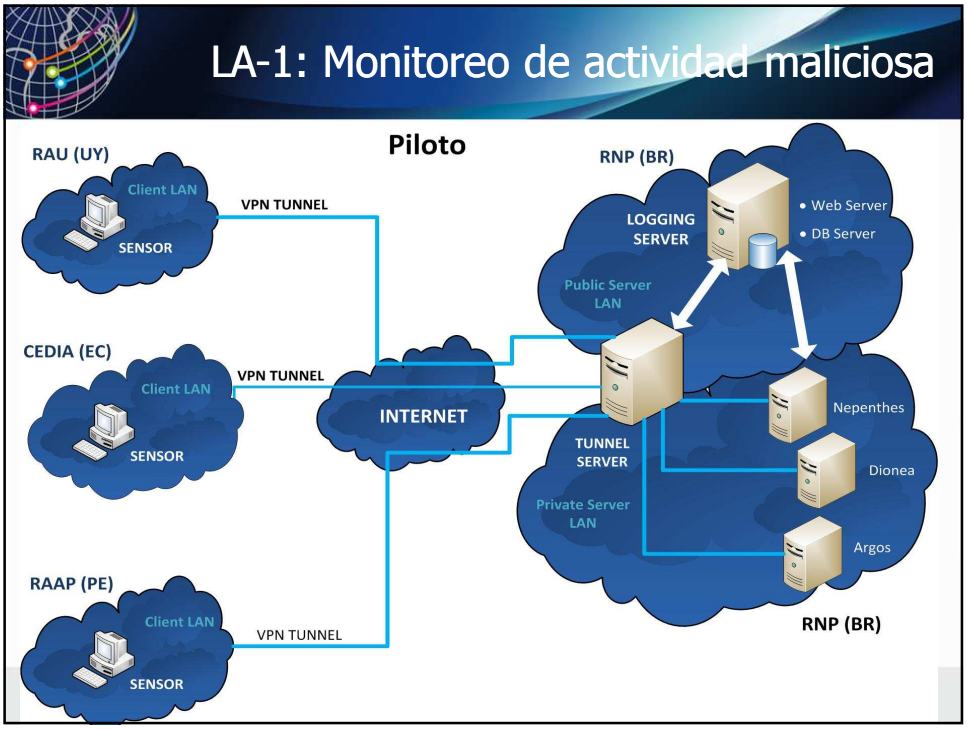
- IDS Distribuido (D-IDS) desarrollado por SurfNET (red académica holandesa)
  - http://www.surfnet.nl/
  - http://ids.surfnet.nl
- Modelo focalizado em ambientes donde el uso de la red no es muy controlado (NREN)
- Focalizado en la detección de worms, tentativas de acceso no autorizadas y outro tipo de tráfico malicioso.
- Ventajas: Instalación simple, bajo número de falsos positivos, fácil actualización.

LA-1: Monitoreo de actividad maliciosa

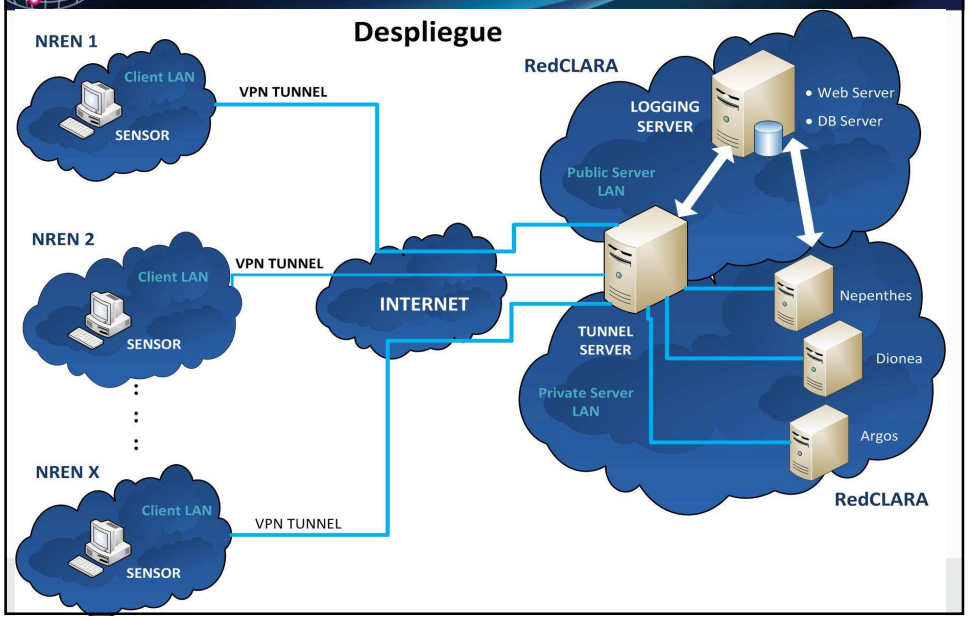
SurfIDS: Modus operandi



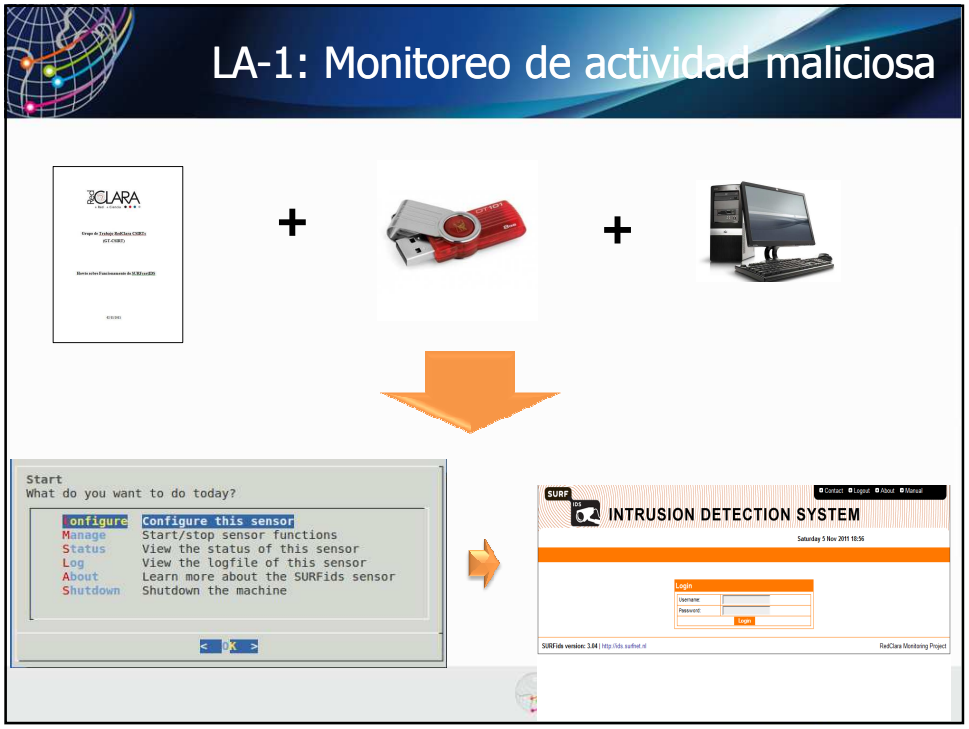
LA-1: Monitoreo de actividad maliciosa



LA-1: Monitoreo de actividad maliciosa

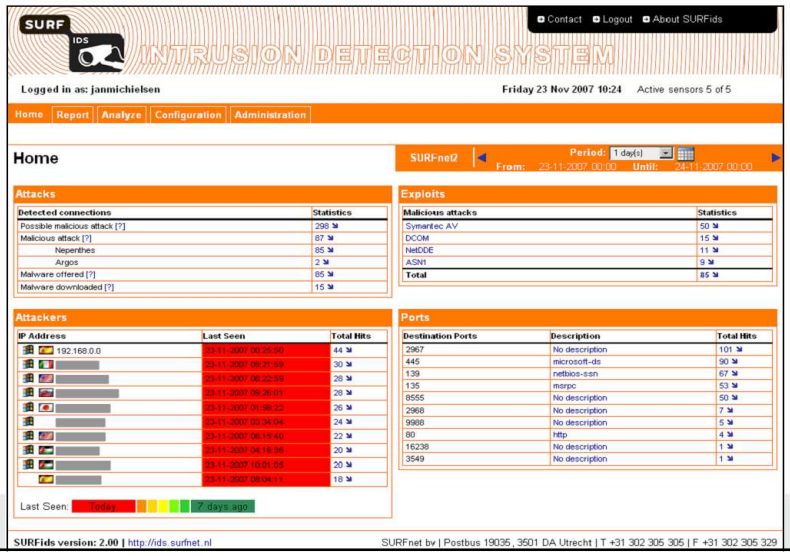


LA-1: Monitoreo de actividad maliciosa



LA-1: Monitoreo de actividad maliciosa

Interface web



LA-1: Cronograma

# tarea	Nombre de la tarea	Periodo de ejecución de la tarea	Relación de dependencia
T-1	Estructuración del ambiente de monitoreo de actividad maliciosa	Jul/11 – Ene/2012 Ago/11 – Feb/2012	Ninguna
T-2	Estructuración del ambiente de tratamiento a incidentes de seguridad	Jul/11 – Ene/2012	Ninguna
T-3	Entrenamiento sobre Monitoreo y Tratamiento de Incidentes de Seguridad	1a Reunión CLARA-TEC 2012	T-1 y T-2 finalizadas
T-4	Implantación de la solución de monitoreo en las NRENs	May 2012 – Jun 2013 Jun 2012 – Jun 2013	T-3 finalizada
T-5	Implantación del ambiente de tratamiento de incidentes en las NRENs.	May 2012 – Jun 2013	T-3 finalizada
T-6	Estableciendo un CSIRT	Jul 2011 – Dic 2011	Ninguna

LA-1: Monitoreo de actividad maliciosa

- Cronograma – ok
- Próximos pasos:
  - Instalación de los sensores en las NRENs (piloto)
  - Iniciar proceso de "monitoreo asistido" (duración: 2 meses)
  - Análisis y validación del modelo
  - Elaboración del Término de Adhesión.
  - Preparación del material del curso (CLARA-Tec).
    - Riezgo: Entrenamiento no ocurrir durante evento jun/2012.

LA-2: Tratamiento de incidentes

- Tareas y entregables:
  - [T2] Estructuración del ambiente de respuesta (piloto).
    - Estructura para recibimiento de incidentes (checklist)
    - Templates de notificación y respuesta desarrollados
    - Toolkit de tratamiento de incidentes de seguridad
    - Informe final de ejecución del piloto
  - [T3] Entrenamiento
    - Material del curso
    - Curso hands-on
  - [T5] Despliegue
    - Cronograma de implantación
    - Estructura implantada en todas las NRENs
    - Informes periódicos de implantación

LA-2: Tratamiento de incidentes

- Proceso de tratamiento de incidentes

  - Recibimiento de la notificación
    - Sensores de Monitoreo (GT-CSIRT – Monitoreo)
    - Fuentes de incidentes de organizaciones/proyectos/iniciativas/csirts
      - Shadowserver, zone-h, spamcop, acuerdos, etc
    - Notificaciones diversas (administradores, usuarios comunes, otros CSIRTs, etc).

LA-2: Tratamiento de incidentes

- Dificultades encontradas (experiencia RNP)
  - Gran cantidad de incidentes (NREN)
  - Muchos de ellos seguían un padrón
    - Aún así eran tratados manualmente!
  - Algunos clientes requerían incidentes agrupados
  - Elaboración de scripts de automatización no seguían un procedimiento padrón, no documentados
  - Difícil actualización de la base de datos de contactos.

LA-2: Tratamiento de incidentes

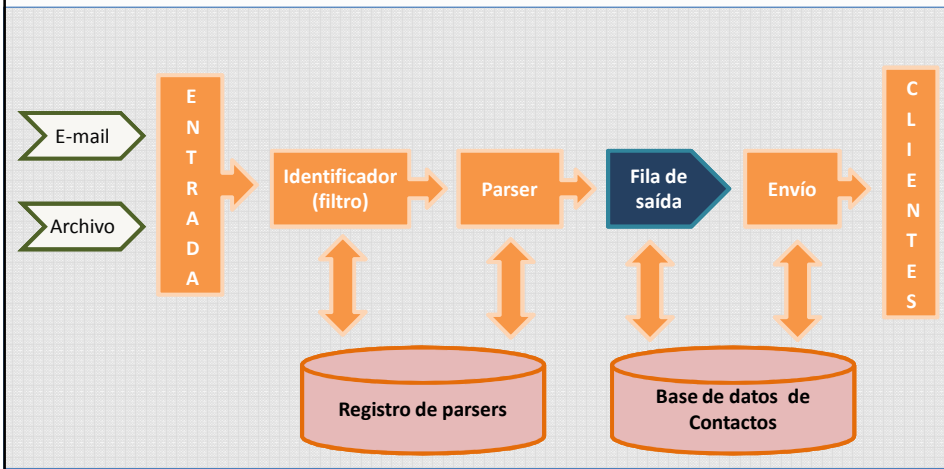
- Dificultades encontradas (experiencia RNP)
  - Gran cantidad de incidentes (NREN)
  - Muchos de ellos seguían un padrón
    - Aún así eran tratados manualmente!
  - Algunos clientes requerían incidentes agrupados
  - Elaboración de scripts de automatización no seguían un procedimiento padrón, no documentados
  - Difícil actualización de la base de datos de contactos.

GENICS

GENICS → RedCLARA!

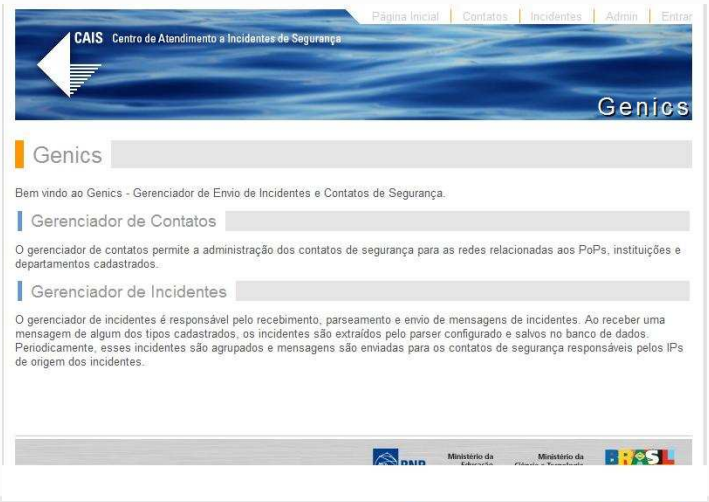
LA-2: Tratamiento de incidentes

GENICS: Modus operandi



LA-2: Tratamiento de incidentes

Página inicial



LA-2: Tratamiento de incidentes

Gerenciador de contactos: Panel de control

LA-2: Tratamiento de incidentes

Gerenciador de contactos: Visión PoPs (NRENs)

LA-2: Tratamiento de incidentes

Gerenciador de contactos: Detalles de la NREN

LA-2: Tratamiento de incidentes

Gerenciador de contactos: Detalles de la Institución

LA-2: Tratamiento de incidentes

Gerenciador de incidentes: Panel de control

LA-2: Tratamiento de incidentes

Gerenciador de incidentes: Parsers

LA-2: Tratamiento de incidentes

Gerenciador de incidentes: Detalles del parser

LA-2: Cronograma

# tarea	Nombre de la tarea	Periodo de ejecución de la tarea	Relación de dependencia
T-1	Estructuración del ambiente de monitoreo de actividad maliciosa	Jul/2011 – Ene/2012	Ninguna
T-2	Estructuración del ambiente de tratamiento a incidentes de seguridad	Jul/2011 – Ene/2012 Ago/2011 – Feb/2012	Ninguna
T-3	Entrenamiento sobre Monitoreo y Tratamiento de Incidentes de Seguridad	1a Reunión CLARA-TEC 2012	T-1 y T-2 finalizadas
T-4	Implantación de la solución de monitoreo en las NRENs	May/2012 – Jun/2013	T-3 finalizada
T-5	Implantación del ambiente de tratamiento de incidentes en las NRENs.	May/2012 – Jun/2013 Jun/2012 – Jun/2013	T-3 finalizada
T-6	Estableciendo un CSIRT	Jul 2011 – Dic 2011	Ninguna

LA-2: Tratamiento de incidentes

- Cronograma – ok
- Próximos pasos:
  - Finalizar la infra-estructura base de respuesta (piloto)
    - RFC 2142: abuse@dominio [11/14], security@dominio [6/14]
    - Responsables de seguridad (NREN SPoCs) [11/14]
    - Detalles adicionales de los responsables de seguridad (RFC 2350)
    - Detalles de las NRENs
      - ASNs, Fajas IPs designados
    - Incluir "abuse-c" en el LACNIC Whois
      - Como? Individualmente? RedCLARA/LACNIC?
    - Incluir csirt@redclara.net en el campo "remarks" en el LACNIC Whois (?)
  - Implantar GENICS en infra-estructura RedCLARA

LA-3: Apoyo a la creación de CSIRTs

- Tareas:
  - [T6] Implementación de un CSIRT
    - Orientaciones de cómo crear un CSIRT
    - Checklist de implementación de un CSIRT
    - Piloto: UTPL (CEDIA), RNP: CSIRT CEDIA.
      - Nuevo entregable
- Cronograma: ok
  - Modificado para abrigar entregable #3 (Piloto).
  - Ago/2011 – Jun/2012.

LA-3: Cronograma

# tarea	Nombre de la tarea	Periodo de ejecución de la tarea	Relación de dependencia
T-1	Estructuración del ambiente de monitoreo de actividad maliciosa	Jul/11 – Ene/2012	Ninguna
T-2	Estructuración del ambiente de tratamiento a incidentes de seguridad	Jul/11 – Ene/2012	Ninguna
T-3	Entrenamiento sobre Monitoreo y Tratamiento de Incidentes de Seguridad	1a Reunión CLARA-TEC 2012	T-1 y T-2 finalizadas
T-4	Implantación de la solución de monitoreo en las NRENs	May 2012 – Jun 2013	T-3 finalizada
T-5	Implantación del ambiente de tratamiento de incidentes en las NRENs.	May 2012 – Jun 2013	T-3 finalizada
T-6	Estableciendo un CSIRT	Jul 2011 – Dic 2011 Ago/2011 – Jun/2012	Ninguna

Preguntas

Liliana Velásquez Solha
nina@cais.rnp.br