CSIRT académico de la Universidad Nacional de La Plata

Lic. Einar Lanfranco

Sobre CERTUNLP

La UNLP brinda servicios de red y servicios de Internet a Facultades, Colegios y Laboratorios

Misión de CERTUNLP:

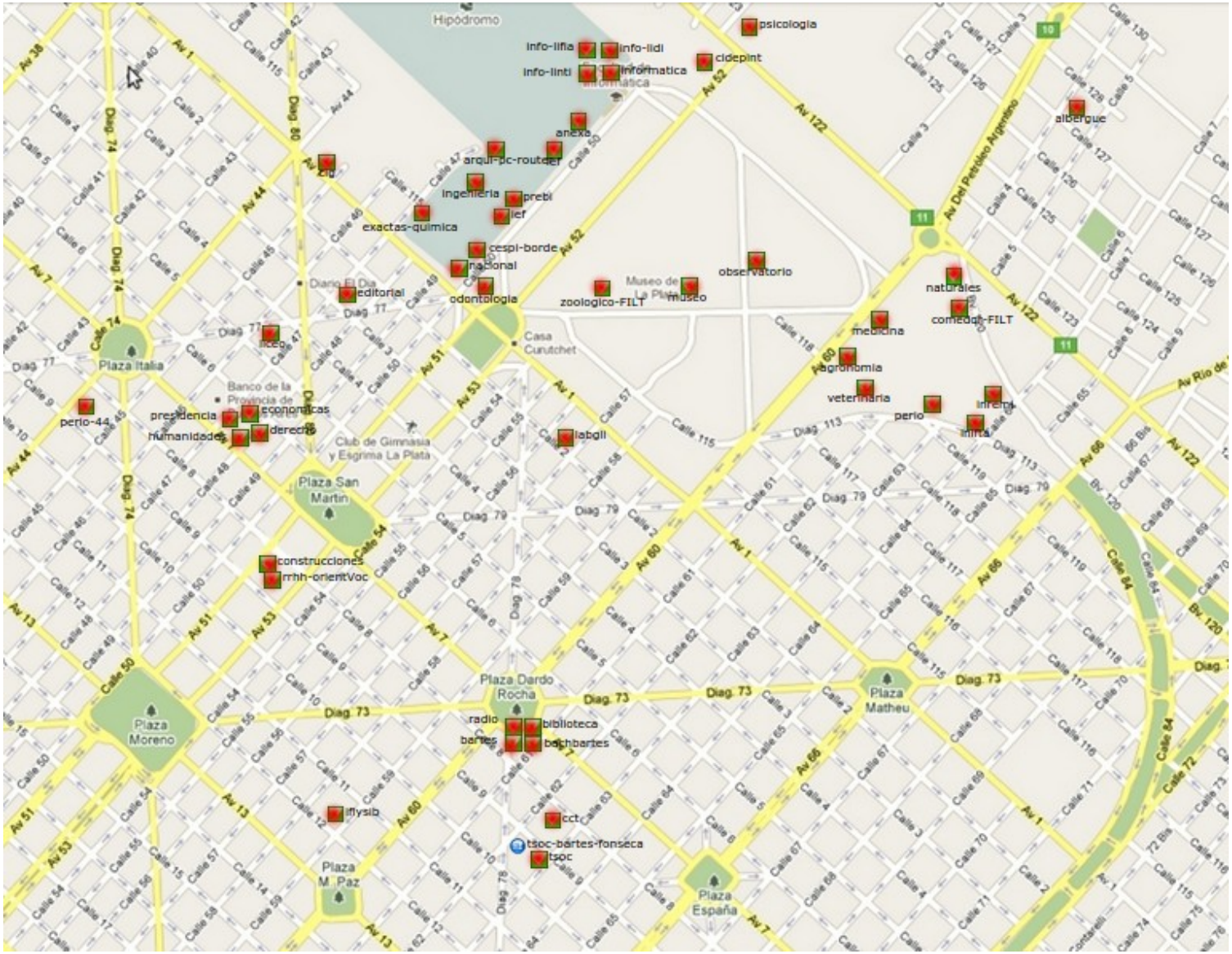
- Gestionar incidentes de seguridad y prevenir, detectar e investigar problemas de seguridad, coordinando acciones para la protección de los usuarios y los servicios académicos de la UNLP.
- Año de Creación: 2008

Comunidad objetivo:

- Red de la UNLP:
  - Sistema Autónomo: 5692
  - Bloque IPv4: 163.10.0.0/16
  - Bloque IPv6: 2800:340::/32
- Dominio: *.unlp.edu.ar

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

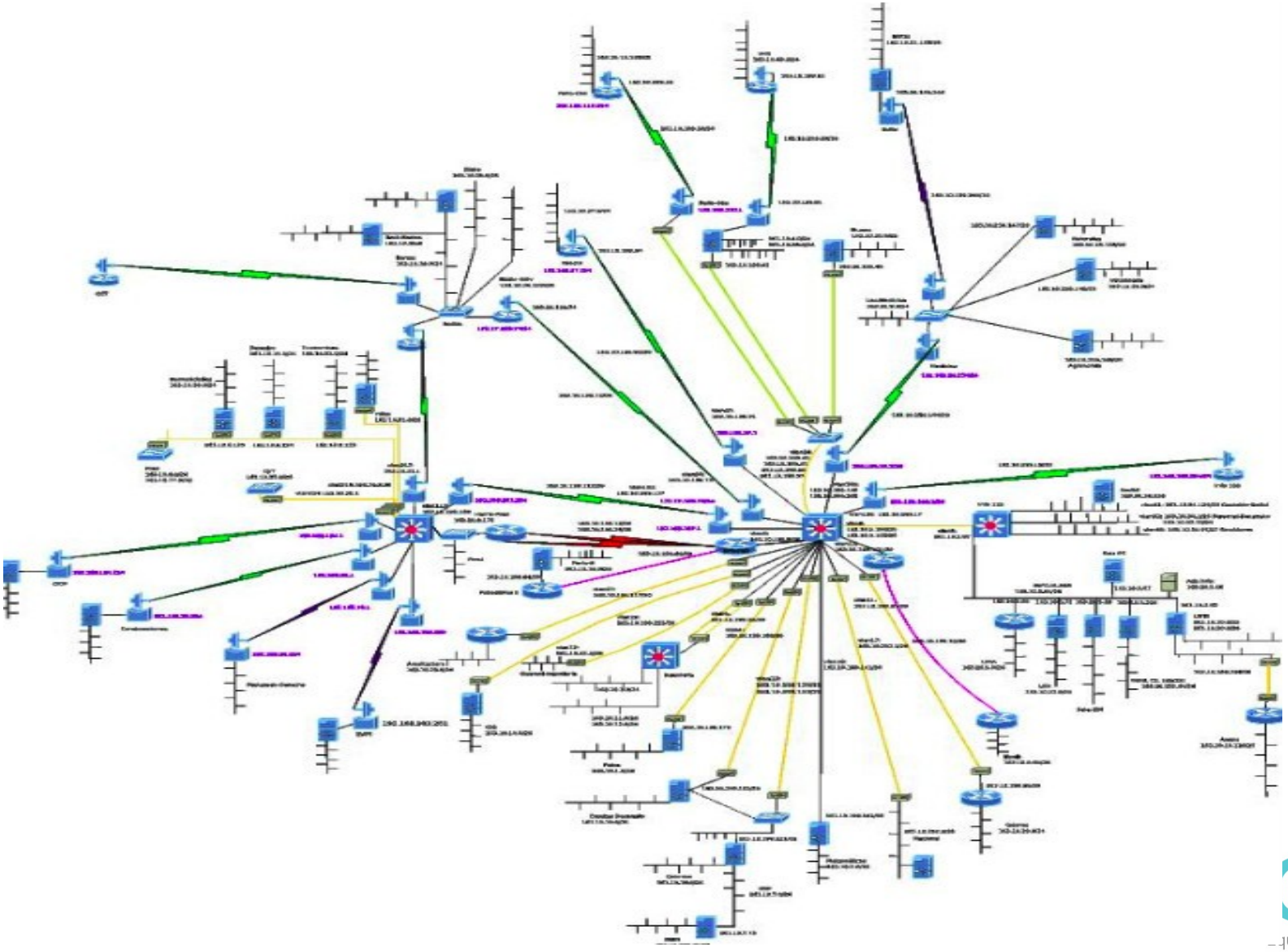
Red de la UNLP



CERT UNLP

Equipo de Respuesta a Incidentes de Seguridad

Red de la UNLP



CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

RRHH de CERTUNLP

Director:

- Francisco Javier Díaz

Coordinadores:

- Nicolás Macia, Einar Lanfranco y Paula Venosa

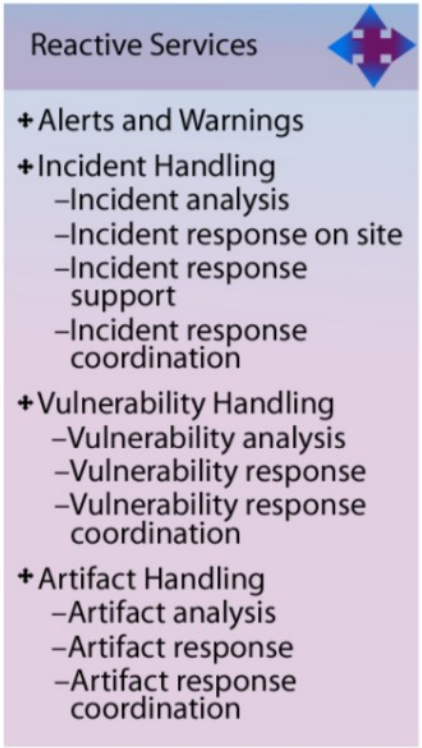
Miembros de CERTUNLP:

- Damián Rubio, Mateo Durante, Cristian Barbaro y Gastón Bezzi

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

Servicios Reactivos de CERTUNLP

- Avisos y Alertas de seguridad
- Gestión de Incidentes:
  - Análisis de incidentes
    - Análisis Forense
  - Soporte en la solución
  - Coordinación



Referencia: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

Servicios Proactivos de CERTUNLP

- Anuncios
- Auditorías de seguridad (Pentests)
- Monitoreo, detección y prevención de intrusiones
- Desarrollo de herramientas de Seguridad

Referencia: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

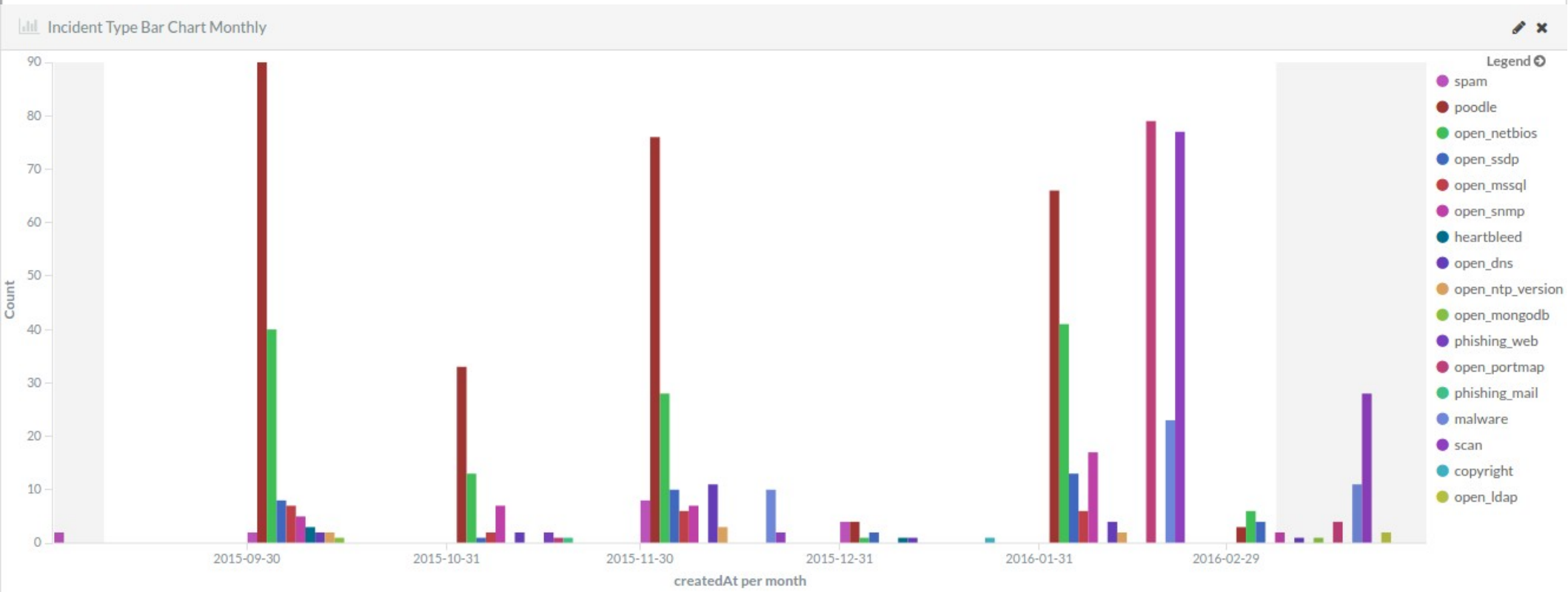
CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Servicios de Gestión de Calidad la Seguridad de CERTUNLP

- Consultoría
- Concientización
- Educación / Entrenamiento

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

Incidentes recepcionados y detectados - últimos 6 meses



CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Actividades en la comunidad

Participación en **LACCSIRTs** – Espacio interno de LACNIC para CSIRTs

- Coordinación de las reuniones virtuales (host).
- Presentaciones en eventos.

Coordinación con CABASE (Cámara argentina de bases de datos y servicios en línea):

- Presentaciones en encuentros de técnicos de CABASE.
- Relevamiento de seguridad en servicios en miembros del NAP CABASE LPL

Otras actividades:

- Análisis de seguridad en aplicaciones y servicios internos y externos: UNLP, SIU, CONICET y AUGM.
- Participación en competencias de seguridad: CTF (Capture The Flag)
  - 1ros en INTERNACIONAL CYBEREX 2015 - Organizado por: OEA e INCIBE.
  - 4tos en iCTF 2012 - Organizado por: University of California (UCSB).
  - 2dos en Da.Op3n 2005. Organizado por Darmstadt University of Technology – Alemania
- Participación en eventos internacioneles como Cyberdrill organizado por la UIT.

Herramientas utilizadas

En la operatoria de un CSIRT se utilizan distintas herramientas para la realización de los diferentes servicios brindados.

En el caso de CERTUNLP se desarrollaron herramientas propias que se usan y se dan a la comunidad como software libre:

- **Ngen:** CSIRT Incident Report System
- Otras herramientas que aún están en fase de desarrollo:
  - **Scripts de procesamiento de archivos netflow y sflow**
    - Detectan ataques de fuerza bruta y scannings TCP
    - Detectan uso de protocolos UDP que se prestan a ataques de DDOS
  - **Servicio de scanner de vulnerabilidades** via API REST para la detección de:
    - Servicios vulnerables que se prestan a posibles ataques de amplificación en DDOS (NTP info, NTP monlist, Open DNS, Open Netbios)
    - Servicios con distintas vulnerabilidades (heartbleed, poodle, open smtp relays)
    - Servicios proxies HTTP y SOCKs abiertos

Herramientas en servicios reactivos

- Ngen: CSIRT Incident Report System.
  - ElasticSearch y Kibana para el reporte de incidentes tratados / Tablero de control
- Nicinfo: cliente RDAP para consultar responsable asociado a un bloque IP (reemplazo de whois)
- ShadowServer: Se estableció un punto de contacto para la recepción de problemas detectados en nuestra red.
- Google, Shodan, etc.

Herramientas en servicios reactivos (Análisis Forense)

- The Sleuth Kit: librería de herramientas (fls, mactime, mmls)
- Autopsy: interfaz gráfica para Sleuth Kit
- Distribuciones Linux: SIFT, DEFT.
- log2timeline/plaso - herramientas para generar supertimelines.
- Herramientas Linux: grep, dd, awk, cut, hexdump, md5sum, shasum, etc.
- FTK Imager
- Digital Forensics Framework
- Volatility
- EnCase

Herramientas en servicios proactivos

- Pentest:
  - Hping3, ncat, Nmap, etc
  - Nessus, Metasploit
  - ZAP Zed Attack Proxy, Acunetix, mole, sqlmap
  - John The Ripper, Swarming
- Monitoreo de seguridad de red:
  - IDS (BRO, Snort, Suricata)
  - Netflows: Nfdump y Nfsen. Scripts CERTUNLP
- Otras:

  PGP, OpenVPN, SSH, SSL, Tripwire, Iptables, Fail2ban, etc..