FAST TRACK
¿QUÉ VEMOS EN ARGENTINA?

U.N.L.P.
Universidad **N**acional de **L**a **P**lata

Contacto: info@cert.unlp.edu.ar

Nuestro rol en la UNLP

UNIVERSIDAD NACIONAL DE LA PLATA

- Somos parte de un grupo que trabaja en el ámbito de la Universidad Nacional de La Plata:
  - Operando el CSIRT académico CERTUNLP.

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

CeSPI
UNIVERSIDAD NACIONAL DE LA PLATA

UNIVERSIDAD NACIONAL DE LA PLATA

  - Realizando docencia, investigación y extensión en la Facultad de Informática.

PKIUNLP
Grid

SYPER
Cátedra de Grado y Postgrado

CÁTEDRAS DE GRADO
REDES Y SERVICIOS
Avanzadoso en Internet

DSA
Desarrollo Seguro de Aplicaciones

Sobre CERTUNLP

UNIVERSIDAD NACIONAL DE LA PLATA

Misión de CERTUNLP:

- Gestionar incidentes de seguridad. Prevenir, detectar e investigar problemas de seguridad. Coordinar acciones para la protección de los usuarios y los servicios académicos de la UNLP.

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

Servicios:

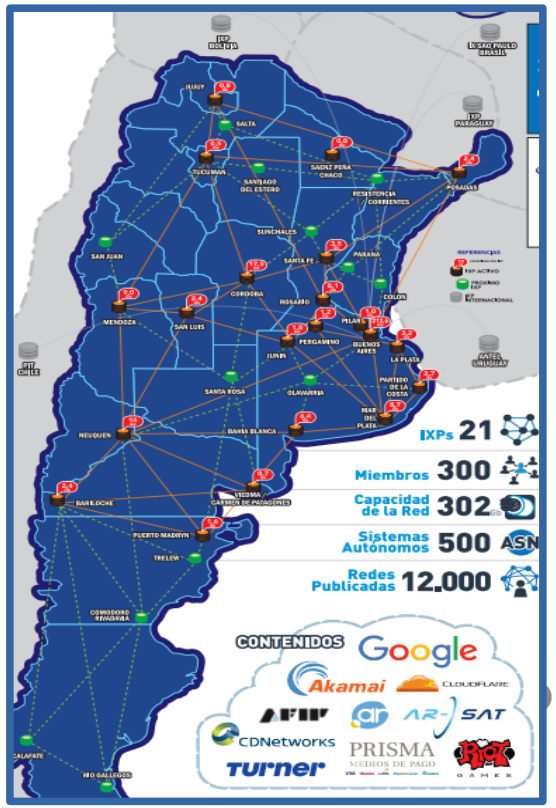
- Gestión de Incidentes: análisis, Análisis Forense, Soporte en la solución, Coordinación.
- Auditorías de seguridad de redes y servicios
- Monitoreo de seguridad de red
- Desarrollo de herramientas
- Concientización
- Entrenamiento

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

Acciones en la comunidad de CABASE

UNIVERSIDAD NACIONAL DE LA PLATA

- 2014 - 1er análisis de vulnerabilidades en las redes de los miembros del NAP regional CABASE LPL
- 2016 - 2do análisis de seguridad en NAP regional La Plata



1er análisis de seguridad en NAP regional La Plata

UNIVERSIDAD NACIONAL DE LA PLATA

Realizado en diciembre de 2014.

- Por entonces había 9 miembros conectados
- Se analizaron **13.056** direcciones IPs
- Se buscaron vulnerabilidades de distintos tipos:
  - Heartbleed: en distintos puertos seguros
  - DNS: Open resolvers
  - SMTP: Open relays
  - NTP: monlist

```
Resultados
--------------------
 3 Heartbleed
19 DNS: Open Resolver
 0 SMTP: Open relays
 7 NTP: Monlist
```

- Se reportaron individualmente a cada miembro del NAP los problemas encontrados en sus bloques de red.

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

2do análisis de seguridad en NAP regional La Plata

UNIVERSIDAD NACIONAL DE LA PLATA

- En Mayo de 2016 se presentó un nuevo informe de vulnerabilidades en redes de miembros del NAP LPL
  - Se analizaron las redes de los 10 miembros conectados por ese entonces
    - Se analizó solamente el espacio IPv4
    - Se analizaron **78.848** direcciones IPv4
    - Se hizo foco en la búsqueda de problemas relacionados con ataques de amplificación y DDoS:
      - Open DNS y transferencia de zonas, OpenSNMP, OpenNetbios, NTP Monitor y version, Open SMTP Relays, Heartbleed y Poodle

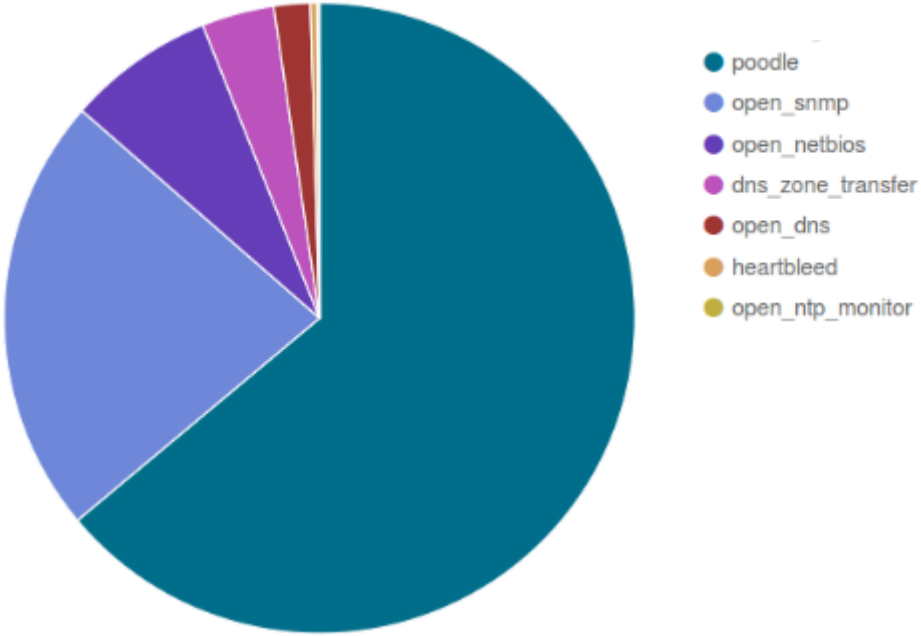
CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

2do análisis de seguridad Resultados

UNIVERSIDAD NACIONAL DE LA PLATA

Distribución de vulnerabilidades:

- De un total de 78.848 IPv4



Vulnerabilidad	Encontrados	Porcentaje
Poodle	551	63,92%
Heartbleed	3	0,35%
Open NTP Monitor	1	0,12%
Open NTP Version	0	0%
Open Netbios	65	7,54%
DNS Zone Tansfer	32	3,71%
Open DNS	16	1,86%
Open SNMP	194	22,51%
Open SMTP Relay	0	0%
Total	862	100%

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

¿De qué hablamos antes?

UNIVERSIDAD NACIONAL DE LA PLATA

- ARNOG en Río Tercero noviembre de 2015
  - Título: **Ataques de amplificación y protección de servicios esenciales**
  - DEMO amplificación NTP
- ARNOG en Buenos Aires abril de 2016:
  - Título: **Alternativas en la detección y mitigación**
  - DEMO de amplificación DNS y RLL

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

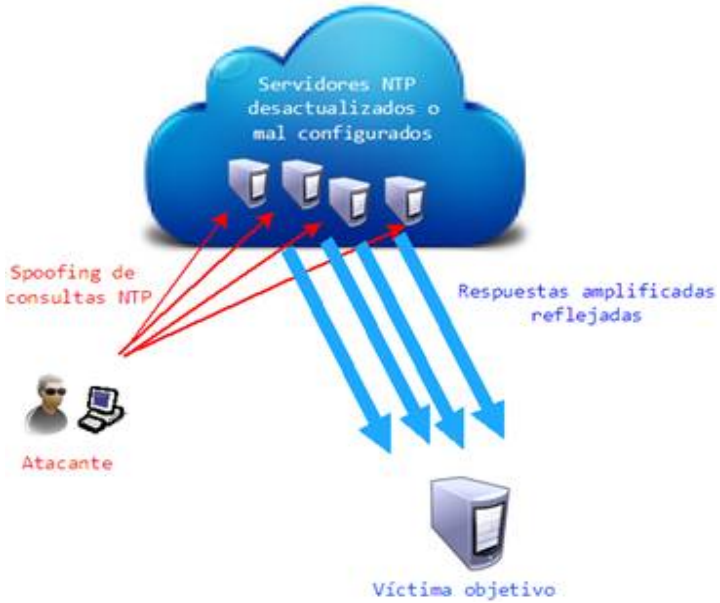
Ataques de DDoS

UNIVERSIDAD NACIONAL DE LA PLATA

Es un ataque cuyo objetivo es dejar sin disponibilidad un servicio a través de la generación de grandes volúmenes de tráfico.

Para ello, algunas técnicas utilizadas por los atacantes son la amplificación y la reflexión de los paquetes de un servicio determinado.

- **Amplificación**: Un atacante envía un requerimiento que genera una respuesta con un volumen de datos mucho mas grande.
- **Reflexión**: Un atacante envía muchos requerimientos amplificables utilizando una IP origen spoofeada, la cual recibirá un gran volumen de datos producto de las respuestas.



CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Servicios afectados
Factores de Amplificación

UNIVERSIDAD NACIONAL DE LA PLATA

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request

Fuente: https://www.us-cert.gov/ncas/alerts/TA14-017A

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Estado de situación en Argentina

UNIVERSIDAD NACIONAL DE LA PLATA

- Siempre nos dicen que no hay estadísticas generalmente se comenta que es porque los usuarios no reportan sus problemas.
- Pero hay muchas fuentes con datos.
- Entonces ….. se nos ocurrió que sería una buena medida realizar un análisis para obtener una foto de nuestro país. Siempre mediante el uso de fuentes abiertas de información.
- ¿Y adivinen qué pasó?

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Estado de situación en Argentina

UNIVERSIDAD NACIONAL DE LA PLATA

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Estado de situación en Argentina

UNIVERSIDAD NACIONAL DE LA PLATA

Resultados:

	En el mundo	En Argentina	En CABASE
DNS (UDP/53)	4773000	35622	22928
Portmap (UDP/111)	1194837	2534	3017
NTP version (UDP/123)	426482	8790	8115
NTP monlist (UDP/123)			
Chargen (UDP/19)	27585	204	203
SSDP (UDP/1900)	2683653	202013	19500
SNMP (UDP/161)	1816085	20800	11273
Netbios (UDP/137)	1007482	58412	5268
Total	**11929124**	**337165**	**78419**

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Estado de situación en Argentina

UNIVERSIDAD NACIONAL DE LA PLATA

Resultados:

	En CABASE	Analizados en CABASE	Vulnerables en CABASE
DNS (UDP/53)	22928	11380	2657
Portmap (UDP/111)	3017	1765	1530
NTP version (UDP/123)	8115	3445	3183
NTP monlist (UDP/123)			23
Chargen (UDP/19)	203	203	0
SSDP (UDP/1900)	19500	7454	3419
SNMP (UDP/161)	11273	6386	3826
Netbios (UDP/137)	5268	3463	1665
Total	**78419**	**37541**	**16303**

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Estado de situación en Argentina

UNIVERSIDAD NACIONAL DE LA PLATA

Resultados:

	Vulnerables en CABASE	
DNS (UDP/53)	2657	!!!!!!!!!!!!!!
Portmap (UDP/111)	1530	!!!!!!!
NTP version (UDP/123)	3183	!!!!!
NTP monlist (UDP/123)	23	!!!!!!!!!!!!!!
Chargen (UDP/19)	0	!!!!!!!!!!!!!!
SSDP (UDP/1900)	3419	!!!!!
SNMP (UDP/161)	3826	!!!!!!!!
Netbios (UDP/137)	1665	!!!!!
Total	**16303**	

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Estado de situación en Argentina

UNIVERSIDAD NACIONAL DE LA PLATA

Resultados:

	En el mundo	En Argentina	En CABASE	Analizados en CABASE	Vulnerables en CABASE	
DNS (UDP/53)	4773000	35622	22928	11380	2657	!!!!!!!!!!!!!
Portmap (UDP/111)	1194837	2534	3017	1765	1530	!!!!!!!
NTP version (UDP/123)	426482	8790	8115	3445	3183	!!!!!
NTP monlist (UDP/123)					23	!!!!!!!!!!!!!
Chargen (UDP/19)	27585	204	203	203	0	!!!!!!!!!!!!!
SSDP (UDP/1900)	2683653	202013	19500	7454	3419	!!!!!
SNMP (UDP/161)	1816085	20800	11273	6386	3826	!!!!!!!!
Netbios (UDP/137)	1007482	58412	5268	3463	1665	!!!!!
Total	**11929124**	**337165**	**78419**	**37541**	**16303**	

Contacto: info@cert.unlp.edu.ar

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Gracias!!!

info@cert.unlp.edu.ar