FACULTAD DE INFORMÁTICA

UNIVERSIDAD NACIONAL DE LA PLATA

SEMINARIO TÉCNICO IMPLEMENTANDO SEGURIDAD EN LAS REDES Y SERVICIOS SEGURIDAD EN RUTEO Año 2020	**Carrera:** Maestría en Redes de Datos **Docente Responsable:** Lic. Nicolás Macia **Duración:** 40 hs.

OBJETIVOS GENERALES:

- Realizar un repaso sobre el funcionamiento del ruteo en Internet.
- Introducir a los alumnos sobre distintos problemas de seguridad relacionados con la
- gestión de la infraestructura de red y el ruteo en Internet de las organizaciones.
- Analizar problemas de seguridad existentes
- Analizar mecanismos de mitigación posibles
- Brindar mejores prácticas y posibilidades en la detección y mitigación de problemas detectados realizando actividades prácticas sobre los distintos conceptos dados

CONTENIDOS MINIMOS:

- Ruteo interno y externo
- Repaso de atributos y configuraciones BGP
- Robo de rutas BGP y ataques de MITM
- Ataques de DDoS
- Buenas prácticas y mecanismos de mitigación

PROGRAMA:

- Unidad 1 - Introducción de ruteo en internet: Ruteo interno. Repaso OSPF. Ruteo externo. Repaso BGP. Transit AS. Multihome AS. Atributos. Route-maps.
- Unidad 2 - Problemas asociados: Robo de rutas. Cierre de sesiones BGP. BGP dampening. MITM por robo o hijacking de rutas BGP
- Unidad 3 - Ataques de reflexión y amplificación. Servicios vulnerables. Detección y evaluación de presencia de estos servicios en mi red.

- Unidad 4 - Buenas prácticas en ruteo: Filtros Bogons, Full bogons, DROP List y BCP38.
- Unidad 5 - Técnicas de mitigación para la protección de la infraestructura ante ataques de DoS / DDoS: RTBH, UTRS, Clean Pipes y Scrubbing Centers. Protección de Websites: DNS, Anycast. Sinkholes

ACTIVIDADES EXPERIMENTALES y DE INVESTIGACION

El seminario consolida el entendimiento, la configuración y la resolución de problemas relacionados en una modalidad de aprendizaje tipo taller.

Se suministra importante bibliografía para facilitar el camino de la elección de tesis para aquellos que estén interesados en estos temas.

METODOLOGIA DE EVALUACION

Para aprobar el seminario deben aprobar las distintas actividades prácticas entregables. En este sentido, se tienen 3 entregas relacionadas con las siguientes temáticas:

- Entrega 1: Práctica de ruteo en Internet
- Entrega 2: Práctica de mecanismos de mitigación
- Entrega 3: Trabajo final

BIBLIOGRAFÍA

BGP

- Internet Routing Architectures (2nd Edition). Autor: Sam Halabi

Ataques DDOS, robo de rutas, MITM y errores de configuración:

- https://www.us-cert.gov/ncas/alerts/TA14-017A
- https://www.imperva.com/blog/infrastructure-ddos-protection-dns-bgp/
- https://www.nimbusddos.com/cloud-based-ddos-attack-platform.htm
- https://github.com/mininet/mininet/wiki/BGP-Path-Hijacking-Attack-Demo
- https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf
- https://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/
- https://arstechnica.com/information-technology/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/
- https://dyn.com/blog/mitm-internet-hijacking/
- https://bgpmon.net/the-canadian-bitcoin-hijack/
- https://www.wired.com/2014/08/isp-bitcoin-theft/
- https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit
- https://btc-hijack.ethz.ch/
- https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris case-study

- https://bgpmon.net/chinese-isp-hijacked-10-of-the-internet/

Buenas prácticas

- https://tools.ietf.org/html/bcp38
- https://team-cymru.com/community-services/bogon-reference/
- https://team-cymru.com/community-services/utrs/

NETFLOW

- https://tools.ietf.org/html/rfc3954

FLOWSPEC

- https://tools.ietf.org/html/rfc5575
- https://blog.marquis.co/what-is-bgp-flowspec/
- https://netcraftsmen.com/bgp-flowspec-step-forward-ddos-mitigation/

S-BGP

- https://tools.ietf.org/html/draft-clynn-s-bgp-protocol-01

RPKI

- https://www.lacnic.net/1150/1/lacnic/rpki-faq
- https://tools.ietf.org/html/rfc6487
- https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/
- 2016/15551-EC/7A.pdf