Investigación Aplicada: Análisis de Seguridad del Protocolo IPv6

Resumen de la investigación

El presente proyecto presenta un análisis de seguridad del Protocolo IPv6 en redes locales, desarrollado en el marco de una investigación aplicada liderada por la Universidad Católica de Salta (Argentina) y la Universidad Estadual de Campinas (Brasil), en colaboración con LACNIC. Con el objetivo de identificar vulnerabilidades y proponer configuraciones seguras, se utilizó una metodología deductivo-inductiva y experimental, apoyada en la herramienta *Containerlab* para simular diferentes topologías IPv6. Se analizaron ataques basados en ICMPv6, especialmente en los procesos SLAAC y NDP, derivando en recomendaciones técnicas para su mitigación. Los resultados obtenidos sirvieron como base para guías prácticas destinadas a operadores de red.

Este trabajo tiene aplicación directa en redes IPv6-only y en procesos de transición IPv4/IPv6, además de fomentar el aprendizaje práctico en entornos académicos. Se recomienda continuar explorando soluciones automatizadas basadas en telemetría para mejorar la respuesta ante amenazas en redes IPv6.

Mgr. Ernesto Sánchez

PhD Henri Alves de Godoy

Antecedentes, problemática y relevancia del estudio

Las universidades y redes académicas cumplen un rol crucial en el desarrollo de IPv6 y se convierten en aliados naturales de LACNIC en la capacitación de las partes interesadas: personal de ingeniería, operación y mantenimiento de los ISP, proveedores de contenido, instituciones gubernamentales, entre otros. Es así que un grupo de investigadores de la Universidad Católica de Salta (Argentina) y la Universidad Estadual de Campinas (Brasil), evidenciaron la necesidad de generar experiencias en el análisis de aspectos de seguridad del protocolo IPv6, con la finalidad de acompañar las acciones desarrolladas por LACNIC para garantizar un pronto y exitoso despliegue final de ésta nueva versión.

Metodología y diseño del estudio

El proyecto de investigación “Análisis de Seguridad del Protocolo IPv6 en el ámbito de Redes de Área Local” se ejecutó en el ámbito de la Universidad Católica de Salta, aplicando una metodología deductiva inductiva, con el objetivo de estudiar, diseñar y realizar configuraciones seguras en redes de área local, en base a la recopilación documental de estándares y normas de seguridad del protocolo IPv6. Aplicando una metodología experimental se realizaron configuraciones de seguridad mediante el uso de la herramienta de virtualización de redes Containerlab, en la que se desplegarán diferentes topologías de redes LAN IPv6.

Principales resultados

Durante la ejecución del proyecto de investigación, (marzo 2024-abril 2025), se realizó un análisis de los ataques basados en el protocolo ICMPv6 para los procesos de autoconfiguración de direcciones sin estado, (SLAAC) y descubrimiento de vecinos, (NDP). A partir de los resultados obtenidos, se realizaron presentaciones en Foro Técnico LACNIC 41, 42 y 43 donde se destacaron conjuntos de buenas prácticas y recomendaciones para el correcto filtrado de ICMPv6 y propuestas de configuraciones seguras para mitigar los posibles vectores de los ataques antes mencionados.

Potencial uso y aplicación de los resultados

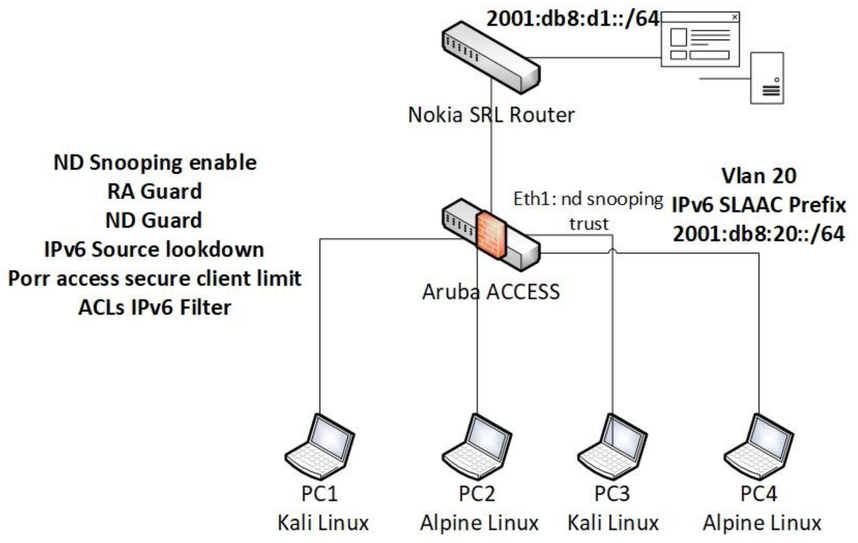
Las propuestas de configuraciones seguras y recomendaciones de buenas prácticas tienen una aplicación directa en el despliegue de redes IPv6 only y en procesos de transición IPv4/IPv6. Los ejemplos de topologías de redes creados a partir de la herramienta de virtualización Containerlab, permitieron poner a disposición de la comunidad técnica en general y de operadores de redes en particular, un entorno controlado para continuar con el análisis de seguridad, sin comprometer los dispositivos y servicios brindados en entornos en producción.

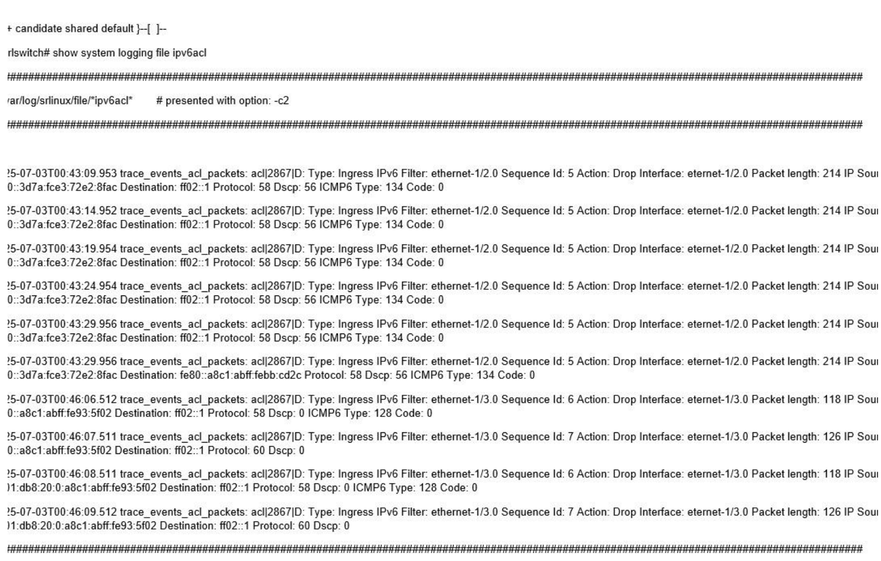
En el ámbito académico, la transferencia de los conocimientos adquiridos es inmediata ya que los alumnos participan en los procesos de enseñanza-aprendizaje, creando diferentes escenarios de redes que permiten llevar lo abstracto del estudio del protocolo al plano de lo concreto. Del mismo modo, para la comunidad técnica se exponen casos de uso impartiendo webinars, como por ejemplo el webinar “Seguridad en IPv6” organizado por LACNIC.

Potenciales líneas de desarrollo futuro y conclusiones

Uno de los desafíos que enfrentamos para lograr la adopción definitiva de esta nueva versión es, “desaprender IPv4, para aprender IPv6”. Consideramos que los trabajos realizados contribuyeron en gran medida a comprender las funcionalidades y cambios introducidos en los protocolos intervinientes desde un aspecto fundamental como lo es la seguridad. Asimismo, entendemos que son esenciales para el despliegue oportuno los aspectos prácticos como los puntos de vista de la calidad de servicio, las ventajas de IPv6 y las restricciones del uso de solo IPv4, entre otros.

Entre las líneas de desarrollo a futuro, encontramos la necesidad de abordar el estudio de técnicas y mecanismos que permitan escalar y reaccionar de manera automática ante amenazas a la seguridad y disponibilidad de los servicios desplegados en las redes de datos, aplicando tecnologías como telemetría para la recolección de información útil para la toma de decisiones.





```
+ candidate shared default }--{  }--
rlswitch# show system logging file ipv6acl
##########################################################################################################################################
/var/log/srlinux/file/"ipv6acl"       # presented with option: -c2
##########################################################################################################################################

2025-07-03T00:43:09.953 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/2.0 Sequence Id: 5 Action: Drop Interface: eternet-1/2.0 Packet length: 214 IP Sou
0::3d7a:fce3:72e2:8fac Destination: ff02::1 Protocol: 58 Dscp: 56 ICMP6 Type: 134 Code: 0

2025-07-03T00:43:14.952 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/2.0 Sequence Id: 5 Action: Drop Interface: eternet-1/2.0 Packet length: 214 IP Sou
0::3d7a:fce3:72e2:8fac Destination: ff02::1 Protocol: 58 Dscp: 56 ICMP6 Type: 134 Code: 0

2025-07-03T00:43:19.954 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/2.0 Sequence Id: 5 Action: Drop Interface: eternet-1/2.0 Packet length: 214 IP Sou
0::3d7a:fce3:72e2:8fac Destination: ff02::1 Protocol: 58 Dscp: 56 ICMP6 Type: 134 Code: 0

2025-07-03T00:43:24.954 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/2.0 Sequence Id: 5 Action: Drop Interface: eternet-1/2.0 Packet length: 214 IP Sou
0::3d7a:fce3:72e2:8fac Destination: ff02::1 Protocol: 58 Dscp: 56 ICMP6 Type: 134 Code: 0

2025-07-03T00:43:29.956 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/2.0 Sequence Id: 5 Action: Drop Interface: eternet-1/2.0 Packet length: 214 IP Sou
0::3d7a:fce3:72e2:8fac Destination: ff02::1 Protocol: 58 Dscp: 56 ICMP6 Type: 134 Code: 0

2025-07-03T00:43:29.956 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/2.0 Sequence Id: 5 Action: Drop Interface: eternet-1/2.0 Packet length: 214 IP Sou
0::3d7a:fce3:72e2:8fac Destination: fe80::a8c1:abff:febb:cd2c Protocol: 58 Dscp: 56 ICMP6 Type: 134 Code: 0

2025-07-03T00:46:06.512 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/3.0 Sequence Id: 6 Action: Drop Interface: eternet-1/3.0 Packet length: 118 IP Sou
0::a8c1:abff:fe93:5f02 Destination: ff02::1 Protocol: 58 Dscp: 0 ICMP6 Type: 128 Code: 0

2025-07-03T00:46:07.511 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/3.0 Sequence Id: 7 Action: Drop Interface: eternet-1/3.0 Packet length: 126 IP Sou
0::a8c1:abff:fe93:5f02 Destination: ff02::1 Protocol: 60 Dscp: 0

2025-07-03T00:46:08.511 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/3.0 Sequence Id: 6 Action: Drop Interface: eternet-1/3.0 Packet length: 118 IP Sou
01:db8:20:0:a8c1:abff:fe93:5f02 Destination: ff02::1 Protocol: 58 Dscp: 0 ICMP6 Type: 128 Code: 0

2025-07-03T00:46:09.512 trace_events_acl_packets: acl|2867|ID: Type: Ingress IPv6 Filter: ethernet-1/3.0 Sequence Id: 7 Action: Drop Interface: eternet-1/3.0 Packet length: 126 IP Sou
01:db8:20:0:a8c1:abff:fe93:5f02 Destination: ff02::1 Protocol: 60 Dscp: 0

##########################################################################################################################################
```

Afiliación

Universidad Católica de Salta

Universidade Estadual de Campinas

Contactos

esanchez@ucasal.edu.ar

henri.godoy@fca.unicamp.br

investigacionaplicada@lacnic.net

Reconocimientos

Agradecemos especialmente a Alessia Zucchetti y Alejandro Acosta por su apoyo constante y la valiosa oportunidad brindada por LACNIC para desarrollar esta investigación. Su compromiso y confianza fueron fundamentales para avanzar en el análisis de seguridad del protocolo IPv6, fortaleciendo el conocimiento técnico en nuestra región.

Esta investigación es parte de la colaboración desarrollada por LACNIC con grupos de investigación e instituciones académicas regionales en el marco del **Proyecto de Colaboración Efectiva para Investigación Aplicada (LACNIC).**

Citación de esta publicación

E. Sánchez, H. Alves de Godoy, “Investigación Aplicada: Análisis de Seguridad del Protocolo IPv6” [Presentación de póster]. Presentado en: LACNIC 44-LACNOG 2025, 6-10 de octubre de 2025, San Salvador, El Salvador.