# Metodologías para Garantizar la Seguridad en Routers

*Hernández, Mauricio. Jaramillo, Juan Fernando. Tobar, Juan Camilo.* Docente*: Urcuqui, Christian.*

## I. INTRODUCCIÓN

A lo largo de la historia de la computación tanto el software como el hardware han mutado para ir evolucionando a pasos cada vez más adelantados, para redefinir procesos u optimizar situaciones en las que un humano necesita ayuda. No obstante, es inevitable que existan personas con conocimientos de alto impacto en la industria de la computación con propósitos malignos para las personas y organizaciones. Por tal motivo es supremamente importante la seguridad en esta era, seguridad que debe ser transversal en todos los elementos y sistemas computacionales, por lo tanto, es indispensable que un nodo tan orientado al usuario como el router tenga una prioridad al momento de pensar en seguridad en la red.

## II. CONTEXTO

A mediados de este año, se disparó una noticia sobre un aprovechamiento de la vulnerabilidad de routers, donde más de 100.000 usuarios de routers domésticos de Brasil, Bolivia y Argentina eran redirigidos a falsas páginas de bancos donde se interceptaba toda la información privada de las cuentas [1].

En otra parte del mundo, investigadores chinos encontraron que más de 200.000 routers del fabricante Mikrotik, fueron hackeados para hacer minería de cryptocurrencies a partir de los recursos del usuario [2].

Gracias a lo planteado en los diferentes titulares de prensa y demás medios, es importante reconocer que necesitamos un cambio de enfoque hacia la seguridad a nivel de la capa de red. Los especialistas deberían priorizar no sólo a los controles de gestión, sino también a elementos como el router, ya que es completamente orientado al cliente final y están a disposición de ser fácilmente alterados.

## III. OBJETIVOS

Proponer un entorno de pruebas basado en el establecimiento de máquinas virtuales para llevar a cabo el test.

Describir mecanismos de prueba basados en el uso de SSH, Telnet y SNMP para hallar fallas en la configuración de RouterOS versión 6.42.

## IV. MARCO TEÓRICO

Las vulnerabilidades en los routers son causadas por tres diferentes situaciones:

### *A. Fallas en software*

Los errores en el software son los alocados en los Sistemas Operativos de los routers, que es aquella capa que se encarga de enrutar de manera óptima los paquetes. Estos fallos son de complejidad alta, ya que existe un alto riesgo en función de los permisos concedidos a los atacantes de datos. Una de las fallas más frecuentes es el desbordamiento del buffer.

### *B. Fallas en configuración*

Las fallas en configuración se deben a los valores ingresados o la forma en la que las personas parametrizan y configuran un router. Aunque también es muy probable que existan fallos en las configuraciones de fábrica.

Estas fallas son las que están a mayor disposición de ciberatacantes, debido a que gracias a errores típicos como puertos abiertos permanentemente, contraseñas con permisos dejadas por defecto o

activación de protocolos que planteen vacíos en comunicación.

### *C. Errores en diseño*

Estos errores son los referidos al diseño físico de los elementos, o diseño industrial, en cuestión de infraestructura. Esto se puede deber al uso de tecnologías obsoletas o aplicación de arquitecturas incorrectas. Para corregir este tipo de errores se requiere de altos recursos en términos de tiempo, fuerza humana de mantenimiento y capital, debido a lo que implica cambiar componentes físicos que están geográficamente dispersos.

## V. PROCEDIMIENTO

Dentro del estudio citado, se realizó una prueba de penetración(*Penetration testing*) a algunos routers MikroTik por medio de la creación de máquinas virtuales y configuración de NATs, en las que posteriormente se estudiaron tres protocolos(SSH, TELNET Y SNMP) que en cierta medida pueden ser inseguros y adecuados para este tipo de test. Las pruebas de los tres protocolos se llevaron a cabo de manera similar, como primera medida se hacía un escaneo de puertos disponibles por medio de Nmap, luego se realizaban ataques de fuerza bruta para obtener combinaciones de cadenas, nombres y contraseñas para finalmente detenerse cuando el acceso sea concedido.

## VI. PROPUESTA A FUTURO

Gracias a lo anteriormente dicho, es de suma importancia que se diseñen, implementen y sepan analizar pruebas para elementos como el router en entornos apropiados. Debido a aquello, nuestra propuesta como estudiantes de Ingeniería de Sistemas, mediante enfoque práctico, es poder generar espacios de diseño, desarrollo y análisis de pruebas de penetración (*Penetration testing*) sobre los elementos de la red de alta relevancia en la industria.

Los espacios mencionados pueden ser basados en entornos controlados como los laboratorios virtuales, donde se pueden hacer muestras de mayor volúmen, con mejores datos y sin problemas para la exhaustividad de carga; además, serían de mejor apropiación si son fundamentados y hechos desde el currículo base de la carrera en materias como Redes o Seguridad, lo que nos enfocaría a pensar que la seguridad no es un add-on sino un elemento transversal en cualquier sistema de software para cualquier tipo de mercado y de industria.

Referencias:

[1] J. Harán. (2018, Oct 1). Brasil: aprovechan vulnerabilidad en routers para redirigir a usuarios a falsas páginas de Bancos [Online]. Available: https://www.welivesecurity.com/la-es/2018/10/01/brasil-aprovechan-vulnerabilidad-en-routers-para-redirigir-usuarios-falsas-paginas-de-bancos/

[2] S. Khandelwal. (2018, Seot 3). Thousands of MikroTik Routers Hacked to Eavesdrop On Network Traffic [Online]. Available: https://thehackernews.com/2018/09/mikrotik-router-hacking.html

[3] E. Ugur, M. Ali, S. Ganal, "Developing a Penetration Test Methodology in Ensuring Router Security and Testing it in a Virtual Laboratory", pp. 1-7, Sept 2015.