CASO DE ESTUDIO: PROTEGIENDO LA RED CON MIKROTIK DE LOS ATAQUES INTERNOS ARP SPOOFING, MAC FLOODING Y DHCP SPOOFING.

Pedro Alcívar Marcillo
Maestría en Tecnologías de la Información Mención Redes y Sistemas Distribuidos ESPAM MFL
palma1124@hotmail.es

Arturo Cox Benites
Maestría en Tecnologías de la Información Mención Redes y Sistemas Distribuidos ESPAM MFL
arturocox@hotmail.com

Resumen

La seguridad de la información y de la infraestructura tecnológica se ha convertido en una de las prioridades de control para las organizaciones, ya que los efectos de que se vea comprometido alguno de los activos antes mencionados pueden ser considerables, por esta razón, en este documento se analiza el comportamiento de los equipos de la marca Mikrotik frente a los ataques: ARP spoofing, MAC flooding y DHCP spoofing, los cuales pueden ser ejecutados desde la red interna sin un mayor conocimiento técnico, además se establecen las configuraciones necesarias para prevenir los ataques antes mencionados. Para el desarrollo de este trabajo se utiliza la herramienta de simulación de redes GNS3, la cual se integra con VMware y Virtualbox para implementar la red simulada en la que se realizaron las pruebas, desde la página oficial de Mikrotik se descargó una imagen del sistema operativo RouterOS, el cual se integra con un *appliance* de GNS3 para crear un entorno más realista. En principio se puede observar que los equipos Mikrotik son vulnerables a los ataques antes mencionados, al igual que cualquier dispositivo de red en el que no se configuren las opciones de seguridad, pero también es importante mencionar que las medidas de prevención para estos ataques en particular son sencillas de implementar en esta marca, por lo tanto no se justifica que un administrador de red no las configure.

Palabras clave: Seguridad, ARP, MAC, DHCP, Mikrotik.

Introducción

La importancia de la infraestructura de red en las organizaciones es indiscutible, más aun teniendo en cuenta que por dicha red transita el activo más valioso que es la información (Rivero, 2014). Con este preámbulo se hace énfasis en la protección del canal de transmisión de los datos, además se identifica la importancia de este estudio al considerar la fuerte incursión de Mikrotik en las infraestructuras de red de los países en vías de desarrollo, como es el caso de gran parte de Suramérica y Centroamérica (Escalante, 2015).

Este documento resalta la importancia de configurar parámetros de seguridad en la infraestructura de red utilizando soluciones de bajo costo, teniendo en cuenta que mediante está práctica se incrementa el nivel de disponibilidad del servicio y además se fortalece la seguridad de la información.

En la investigación de (Hoque, Bhuyan, Baishya, Bhattacharyya, & Kalita, 2014) se menciona la importancia de conocer de manera general las herramientas de auditoria de redes, para prevenir incidencias y defender la infraestructura de posibles ataques, también se realiza una comparativa entre las herramientas para determinar pros y contras de las mismas en determinados escenarios.

En el estudio de (Rahman, 2018) considera que la administración y control de servidores basados en linux debe complementarse con las características de administración de red que ofrece RouterOS, para evitar la saturación de los servicios e incrementar los filtros de seguridad en la infraestructura.

Las opciones a nivel de seguridad que brinda Mikrotik son eficientes y pueden integrarse con otras soluciones del tipo IDS como SNORT, tal como indica en su trabajo (Sagala & Pardosi, 2017), en el cual realizan esta combinación de soluciones para prevenir ataques de denegación de servicios y otros tipos de intrusiones que se pueden presentar en soluciones SCADA.

Según la investigación de (Pauzhi I. W., 2016) menciona que muchas de las empresas dedicadas a la seguridad informática en Ecuador cuentan con un portafolio de soluciones con opciones variadas. Entre los productos que

predominan la lista se encuentran marcas como: Cisco, Mikrotik, Huawei, Fortinet y Checkpoint con sus respectivas soluciones de seguridad.

En el ámbito local el trabajo realizado por (Pauzhi & Coronel, 2015) hace mención a datos estadísticos relacionados con los incidentes informáticos de seguridad en el Ecuador, para el caso particular de las redes de datos indica que ataques del tipo *spoofing, man in the middle*, denegación de servicios, *wardriving,* punto de acceso no autorizado, entre otros, están entre los más habituales en las empresas del tipo WISP (*wireless internet service provider*).

En el mercado de equipos de red se pueden encontrar variedad de soluciones, pero Mikrotik se está afianzando al tener una relación costo/beneficio alta (Toapanta & Tenenuela, 2016), la simplicidad de su sistema RouterOS y la integración de características adicionales como firewall, sistema de monitoreo, entre otros, favorecen la administración y el control de la red (Realpe, 2018).

Materiales y métodos

Para el desarrollo de este trabajo, se creó un entorno de laboratorio, el cual constaba de 2 routers Mikrotik simulados mediante una imagen de disco del sistema operativo RouterOS (Burgess, 2011) en combinación con un *appliance* de la herramienta de simulación de la red. Se integró VMware Workstation y Virtualbox con GNS3 (Welsh, 2013) para instalar los sistemas operativos que iban a desempeñas los roles de víctima (ubuntu 16.04) y atacante (linux mint 18.1) y finalmente se agregaron 4 PC’s virtuales de ubuntu docker guest para complementar la topología.

Para poder comprender mejor el escenario de la simulación, en la figura 1 se muestra la topología de la red, y en la tabla 1 se detalla el direccionamiento IP de los equipos.

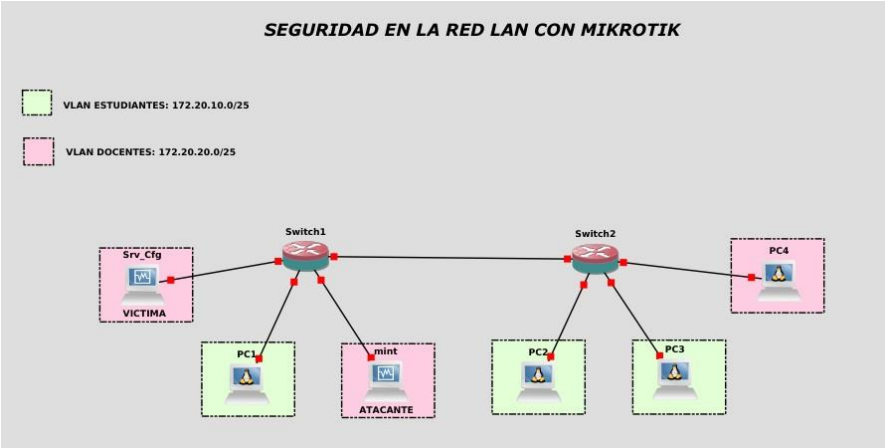

Fig. 1. Topología de la red simulada

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Puerta de Enlace
Switch 1	br-est	172.20.10.1	255.255.255.128	N/A
	br-doc	172.20.20.1	255.255.255.128	N/A
Switch 2	br-est	N/A	N/A	N/A
	br-doc	N/A	N/A	N/A
Linux mint	Ethernet	DHCP	DHCP	DHCP
Srv-cfg	Ethernet	DHCP	DHCP	DHCP
PC 1	Ethernet	DHCP	DHCP	DHCP
PC 2	Ethernet	DHCP	DHCP	DHCP
PC 3	Ethernet	DHCP	DHCP	DHCP
PC 4	Ethernet	DHCP	DHCP	DHCP

Tabla 1. Direccionamiento IP de la red simulada

ARP Spoofing

Este ataque consiste en enviar mensajes ARP falsos a la red con el objetivo de vincular su dirección MAC con la IP de un equipo legítimo en dicha red, en la mayoría de los casos se trata de suplantar al gateway de la red para capturar todo el tráfico.

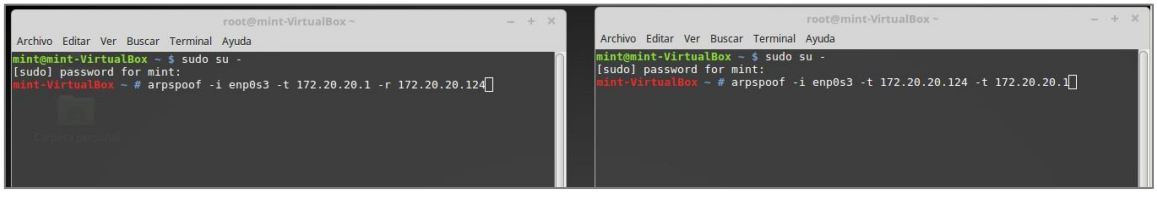

Fig. 2. En el equipo atacante ejecutamos los comandos para generar el envenenamiento ARP.

Luego de ejecutar el envenenamiento ARP se debe iniciar un sniffer de red, en este caso se utilizó wireshark y además es necesario permitir el reenvío de datos con el comando ***echo 1 > /proc/sys/net/ipv4/ip_forward.***

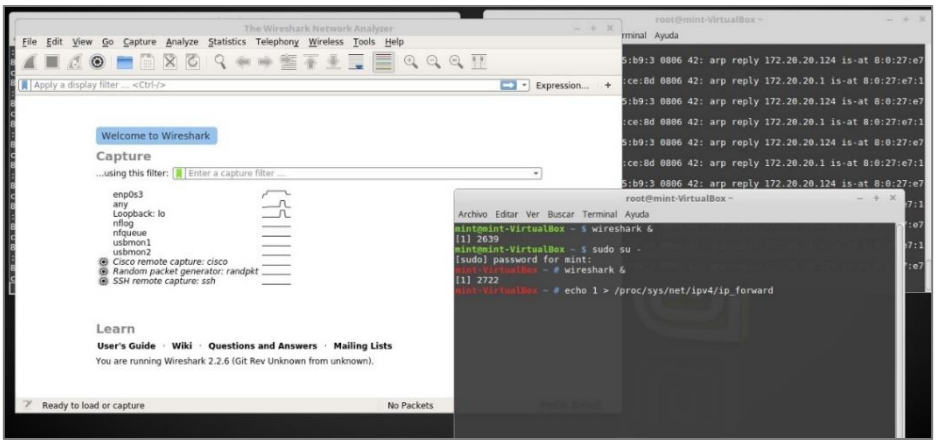

Fig. 3. Iniciando wireshark y habilitando el reenvío de tráfico

Para verificar que el ataque se efectuó de manera correcta la víctima se conectó al Mikrotik por telnet para la administración remota del dispositivo.

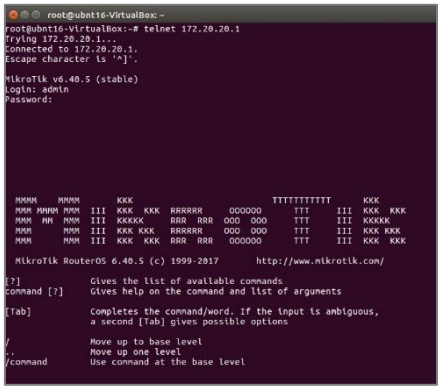

Fig. 4. El Administrador de la red se conecta de manera remota al equipo Mikrotik mediante telnet

Por último se especificó un filtro en el sniffer para obtener los paquetes que tengan la IP de la víctima y que usen telnet como protocolo de conexión remota.

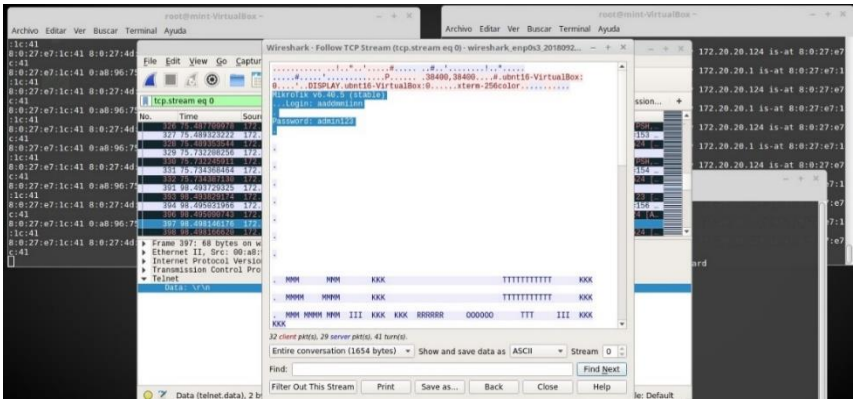

Fig. 5. Al aplicar el filtro de búsqueda en el sniffer se encontraron los paquetes de inicio de sesión

MAC Flooding

El ataque por inundación de direcciones MAC (MAC Flooding) consiste en enviar miles de direcciones MAC falsas hacia el switch para llenar su tabla CAM y que colapse al no poder almacenar más registros.

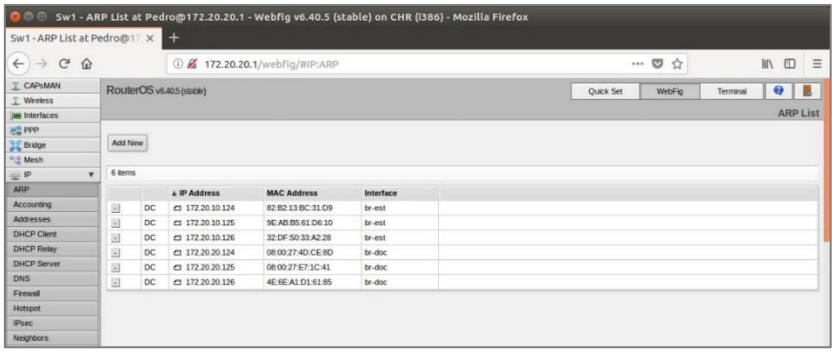

Fig. 6. En el Mikrotik Sw1 se muestra la tabla ARP de los equipos conectados

Desde linux mint se ejecutó el ataque con el comando ***macof -i enp0s3 -n 100000***, -i indica la interfaz de salida y –n la cantidad de direcciones a enviar.

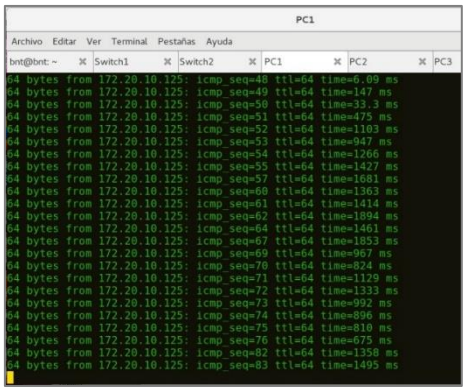

Fig. 7. Al probar conectividad entre dos PC's en la red, se puede observar cómo afecta en el time

Para comprobar todas las direcciones MAC que registro el equipo, se ejecutó el comando ***interface bridge host print,*** ya que se crearon 2 bridges.

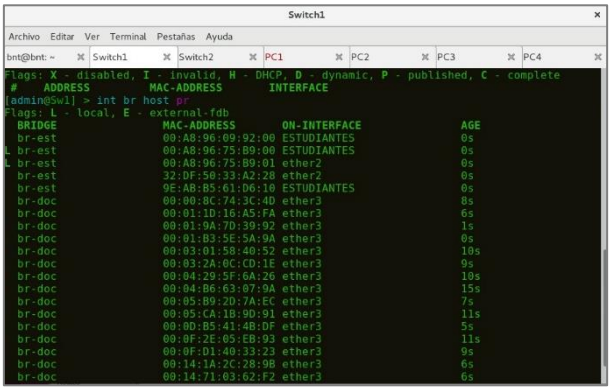

Fig. 8. Se muestran las MAC que ingresan por la interfaz que está conectado el atacante

Se comprobó la cantidad de direcciones MAC que se registraron mediante el comando ***interface bridge host print count-only.***

Fig. 9. Se muestran registradas 91080 direcciones MAC

DHCP Spoofing

El ataque de suplantación de DHCP consiste en implementar un servidor DHCP falso el cual va a ofertar direcciones a los usuarios de la red para espiar el tráfico generado por dichos usuarios, el éxito del ataque depende de que se envíen tantas peticiones al servidor válido, hasta que este sature el rango de asignación de direcciones y pueda entrar en acción el servidor atacante.

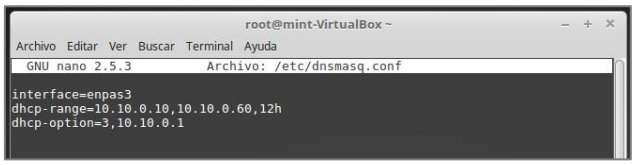

Fig. 10. Se instala y configura un servidor DHCP en linux

Para saturar el servidor de DHCP podemos usar una herramienta como yersinia (Rodríguez, 2016).

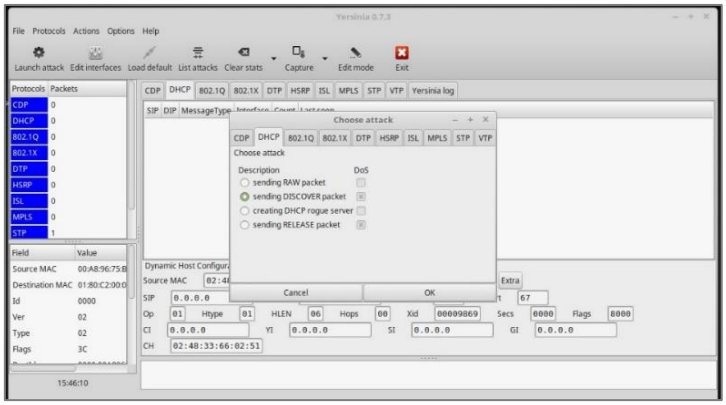

Fig. 11. Ejecutando el envío de paquetes DISCOVER al servidor de DHCP

Para comprobar que yersinia (Rodríguez, 2016) saturo las direcciones disponibles en el servidor, se observan las direcciones asignadas en el Mikrotik.

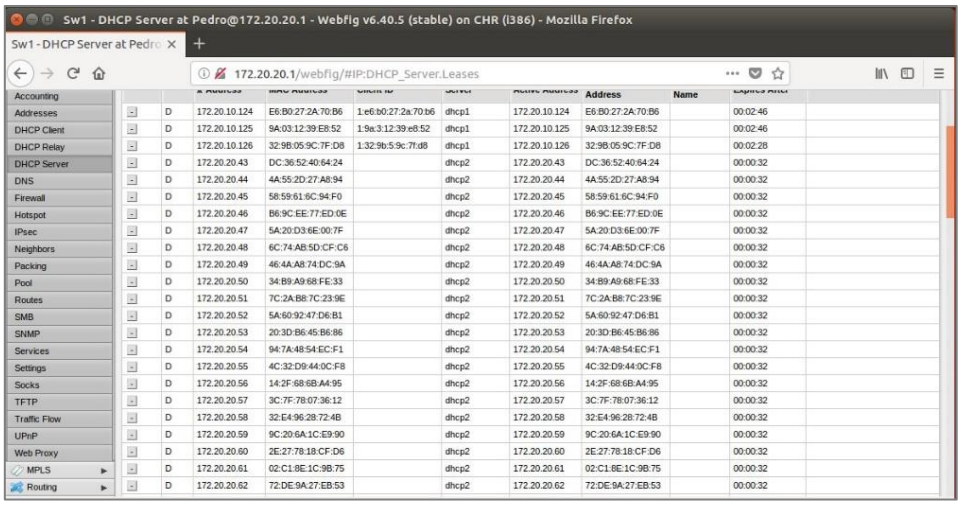

Fig. 12. Direcciones IP asignadas por el servidor DHCP atendiendo las peticiones de yersinia

Finalmente se comprueba que los equipos en la red que tengan configurado DHCP, se les asignaron una IP del segmento del servidor falso.

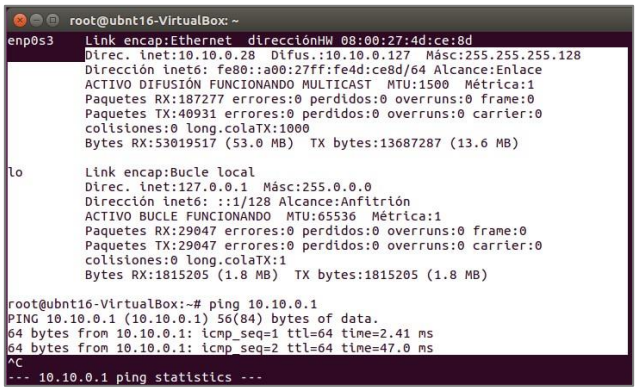

Fig. 13. Los equipos con DHCP recibieron direcciones IP del servidor falso

Resultados y discusión

Para prevenir los ataques desarrollados dentro de la red LAN simulada se aplicaron procesos muy sencillos de configurar en los dispositivos Mikrotik, a continuación se detalla cada procedimiento y el sentido de su aplicación.

En primer lugar se debe establecer los pool de direcciones como estáticos para todos los servicios DHCP levantados en el equipo, además se marca la casilla de ***add ARP for Leases.*** Estos procesos se realizan para mitigar los ataques de ARP Y DHCP spoofing, dejando de manera estáticas las conexiones.

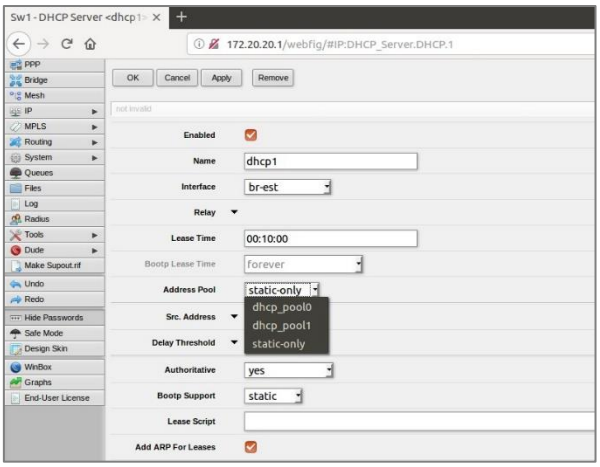

Fig. 14. Configurando los servicios de DHCP levantados en el equipo

El siguiente paso es cambiar en las interfaces bridge el modo de ARP de ***`enable`*** a ***`reply-only`***, este paso se realiza para que la interfaz bridge donde se levante el servicio de DHCP no asocie más direcciones que las que ya estén definidas, adicionalmente se puede realizar este proceso en las interfaces Ethernet que estén conectadas a equipos para mitigar el ataque MAC flooding o se podría asociar una dirección directamente en la interfaz.

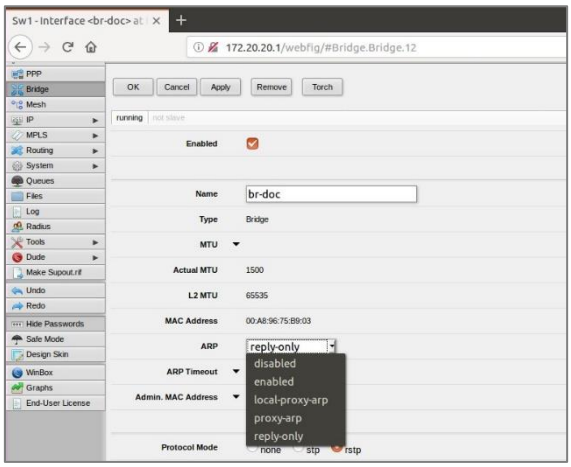

Fig. 15. Especificando el modo arp reply-only en las interfaces

Por último se deben definir como ***`make-static`*** todas las conexiones existentes en los *leases* de DHCP, o también se pueden gregar nuevos hosts relacionando la IP con la MAC *address.*

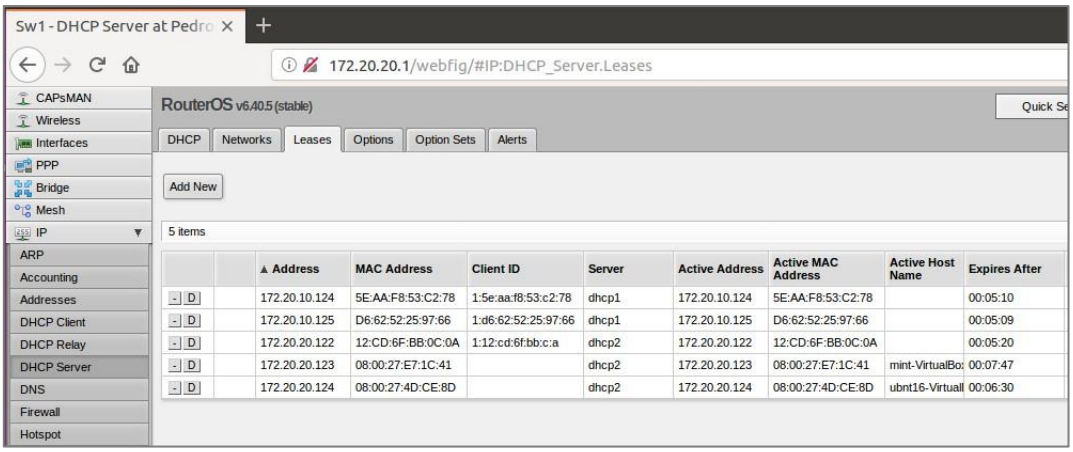

Fig. 16. Marcando como estáticas las entradas en los *leases* de DHCP y creando nuevas entradas

La Organización Internacional de estandarización declara medidas que se deben contemplar para fortalecer la seguridad de las redes, en la obra de (Fan, Huang, Zhang, Wang, & Su, 2015) se especifican varias opciones a tener en cuenta, con el enfoque de este trabajo se asemeja la idea expuesta en varios párrafos de la obra citada.

El trabajo de (Bull & Matthews, 2016)explora los ataques a la red que se producen en la capa 2 en un entorno totalmente virtualizado al igual que se desarrolla en este artículo, los investigadores concluyen luego de realizar varias pruebas, que las vulnerabilidades identificadas en los equipos físicos son muy similares a las que se logra determinan en sus prácticas virtualizadas.

Conclusiones

Los ataques mostrados en este documento no tienen un alto nivel de complejidad en cuanto al proceso de ejecución se refiere, por tal razón cualquier usuario de la intranet podría llevarlos a cabo haciendo uso de las herramientas adecuadas.

Es importante mencionar que ninguna tecnología viene pre-configurada con los parámetros de seguridad necesarios para salvaguardar la infraestructura de red, ya que cada escenario es diferente y los activos a proteger van a variar conforme a los objetivos del negocio.

Los equipos de la marca Mikrotik proveen muchas opciones de seguridad intrínsecas en el servicio de firewall que se encuentra implementado en el

sistema RouterOS, además de varias funcionalidades adicionales incluidas en otras características del sistema.

Bibliografía

Bull, R. L., & Matthews, J. N. (2016). Critical analysis of layer 2 network security in virtualised environments. *International Journal of Communication Networks and Distributed Systems (IJCNDS)*.

Burgess, D. (2011). *Learn RouterOS.* lulu.com.

Escalante, M. (2015). *Ruteo Avanzado y Alta Disponibilidad con Mikrotik RouterOS.* Guayaquil.

Fan, W., Huang, W., Zhang, Z., Wang, Y., & Su, D. (2015). A Near Field Communication (NFC) security model based on OSI reference model. *IEEE*.

Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 307-324.

Pauzhi, I. W. (2016). *Análisis e implementación de políticas de seguridad para WISP mediante equipos mikrotik y elementos de red.* Cuenca.

Pauzhi, W., & Coronel, J. (2015). Security for WISP through Mikrotik equipment. *Information and Communication Technologies (CHILECON)*, 299-233.

Rahman, M. D. (2018). *Linux server configuration and mikrotik administration.* Bangladesh: Daffodil International University.

Realpe, R. J. (2018). *Sistema de monitoreo de redes y equipos networking utilizando la herramienta MRTG y la tecnología MIKROTIK para la Empresa J&STECHNOLOGY .* Ibarra: Universidad Técnica del Norte.

Rivero, P. J. (2014). Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras. *Revista Cubana de Ciencias Informáticas*, 52-73.

Rodríguez, P. E. (2016). Proceso de auditoría interna y Ethical .

Sagala, A., & Pardosi, R. (2017). Improving SCADA Security using IDS and MikroTIK. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 133.137.

Toapanta, M. A., & Tenenuela, T. J. (2016). *Análisis de Implementación en Tecnología WIFI a Través de Equipos Mikrotik y Ubiquiti (Doctoral dissertation.* Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas.

Welsh, C. (2013). *GNS3 network simulation guide.*