DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED DE DATOS PARA EL CASO DE ESTUDIO DE LA EMPRESA XYZ A PARTIR DE UN ENTORNO VIRTUALIZADO

HAROLD YESID MARTINEZ RIPE

MABEL ROCIO BRAVO LEON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTA

2019

DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED DE DATOS PARA EL CASO DE ESTUDIO DE LA EMPRESA XYZ A PARTIR DE UN ENTORNO VIRTUALIZADO

HAROLD YESID MARTINEZ RIPE

MABEL ROCIO BRAVO LEON

PROYECTO APLICADO

Ing. JOEL CARROL VARGAS M.Sc

DIRECTOR DE PROYECTO DE GRADO

YENNY STELLA NUÑEZ

TUTORA PROYECTO DE SEGURIDAD INFORMATICA II

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTA

2019

DEDICATORIA

El presente documento se lo dedicamos a nuestro señor Dios por habernos brindado la sabiduría para alcanzar estas metas de nuestras vidas académicas. A nuestros padres por ser nuestro apoyo incondicional durante todo este proceso. A nuestros hermanos y hermanas por ser el ejemplo e inspiración. A nuestras parejas por su amor y comprensión. A nuestros amigos y todas aquellas personas que nos han acompañado en el transcurso de nuestra vida.

AGRADECIMIENTOS

Agradecemos a la Universidad Nacional Abierta y a Distancia y los docentes que nos han impartido su catedra, ya que nos han brindado espacios para compartir conocimientos y experiencias útiles en el proceso de formación de esta especialización en seguridad informática, especialmente a los directores de proyecto grado Luis Fernando Zambrano (semestre 16-04 2018) y Joel Carrol Vargas (semestre 16-04 2019), y al tutor de proyecto de seguridad informática II Yenny Stella Núñez, por guiarnos en la elaboración de este proyecto aplicado y ser partícipe de otro objetivo alcanzado.

RESUMEN

La empresa XYZ, es una compañía dedicada a la realización de cobranzas con sedes en la ciudad de Bogotá, Medellín, Cali y Bucaramanga, que cuenta con una infraestructura de red de datos centralizada que ofrece servicios de telefonía, almacenamiento de archivos y plataformas web. Este modelo de infraestructura tecnológica está ocasionando problemas de transmisión y seguridad en los datos que están conllevando a la afectación de los procesos y además, sus aplicativos tecnológicos no han sido evaluados en materia de seguridad, generando riesgos que puedan afectar la compañía.

La implementación de una nueva tecnología para el mejoramiento de la seguridad de la infraestructura de red de datos de la empresa XYZ, permitirá la optimización de los procesos de la compañía de manera que se pueda compartir la información entre las diferentes sedes y se facilite la administración de recursos tecnológicos, garantizando la disponibilidad, integridad y confidencialidad de la información, esto debido que la empresa presenta inconvenientes de conectividad entre las nuevas sedes a nivel nacional en el suministro y recepción de información. Adicionalmente, debido a que el software para la gestión de procesos con los clientes llamado Badstore nunca ha sido sometido a test de seguridad, existe una alta probabilidad de que contenga diversos tipos de vulnerabilidades en su desarrollo que puedan ser explotadas por atacantes o amenazas informáticas o que no cuente con las medidas de aseguramiento necesarias para su protección, lo cual puede generar riesgos para los activos tecnológicos de la empresa y todos sus interesados, afectando de manera considerable la credibilidad y operatividad la compañía.

Por lo anterior se tiene como objetivo el mejoramiento de una infraestructura de red de datos para la empresa XYZ haciendo uso de una metodología que incluye investigación aplicada donde, a partir del conocimiento del problema se realizará una investigación acerca de los procedimientos y técnicas de pentesting, y el uso de tecnología Mikrotik para posteriormente realizar las actividades necesarias que contribuyan a la seguridad y mejoramiento de los procesos

Los resultados esperados de este proyecto es el mejoramiento de la red de datos que permita el envío y recepción de información entre las 4 sedes de la empresa de una manera rápida y eficaz garantizando la seguridad en la transmisión y el almacenamiento de dicha información, así como la identificación de 8 vulnerabilidades en el software Badstore, a las cuales se les propondrá sus respectivas medidas para su aseguramiento.

PALABRAS CLAVES

Red, LAN, Mikrotik, servidor, entorno virtualizado, WAN, VPN, pentesting, Badstore, ataque, vulnerabilidad

ABSTRACT

The business XYZ, is a company dedicated to realization of collections with headquarters in Bogota, Medellin, Cali and Bucaramanga, whish has a data network infraestructure centralize that offers services of telephony, file storage and web platforms. That model of technological infrastructure is causing transmission and security data problems that are entails to the affectation of the processes and besides, their technological applications have not been evaluated with respect to security, generating risks that can affect the company

The implementation of a new technology to improvement the data network infrastructure security of business XYZ, will allow the optimization of the company's processes so that it can share the information between differents headquarters and be facilitated the administration of technological resources, guaranting availability, integrity and condifencialityof the information, this becouse the company presents connectivity issues between the new headquarters nationwide in the supply and reception of information. Additionally, because the software for customer process management called badstore has never been undergone a safety test, exist a high probability that contains diverses kind of vulnerabilitys in its develop that can be exploit by informatic attackers or does not have the assurance measures neccesarys to its protection, which can generate risks to the company's technological assets and all its stakeholder, significantly affecting the enterprise credibility and effectiveness

Therefore, the objective is to improve of a data network infrastructure to company XYZ making use of a methodology that includes applied investigation where, from problem's knowledge will be performed an investigation about the procedures and techniques of pentesting, and the use of Mikrotik technology to later perform the necessary activities that contribute to security and improvement of processes

The expected results of this project is the improvement of the data network that allow to send and reception information between four headquarters quickly and effective, guaranteeing the security in the information transmition and storage, as well the identification the eight vulnerabilitys in the Badstore software, to which their respective measures will be proposed for their assurance.

KEYWORDS

File storage, security, information, Virtual Private Network, Wide Area Network, services, Local Area Network, pentesting, Badstore, attack, vulnerability

TABLA DE CONTENIDO

LISTAS DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

En la actualidad las redes informáticas han cobrado una gran importancia para las personas y las compañías dado que estas permiten la conexión a nivel mundial en los diferentes ámbitos, ya sean personales o comerciales[1]. Las plataformas de interconexión han contribuido con el desarrollo y crecimiento en área sociales y científicas permitiendo la optimización de los procesos cotidianos conllevando a una mejora en el bienestar de las personas y un aumento de productividad y disminución de costos para la empresa.

La empresa XYZ se encuentra ubicada en las ciudades Medellín, Cali y Bucaramanga con sede principal en Bogotá y cuenta con un sin número de agentes que día a día hacen uso de los recursos tecnológicos de la organización para la ejecución de sus funciones. El desarrollo y crecimiento de esta empresa ha fomentado la obligación de optimizar la infraestructura TI para la transmisión de información y el uso de recursos compartidos produciendo efectos que conlleva al mejoramiento de procesos y estar a la vanguardia de la seguridad informática.

Teniendo en cuenta que las redes evolucionan constantemente en cuanto a su diseño e implementación, en este proyecto se llevó a cabo la implementación de una red informática haciendo uso de tecnología de última generación, donde los componentes fueron integrados permitiendo una mejor administración de la infraestructura y la reducción costos relacionados con la inversión de equipos para cubrir las mismas necesidades. Adicionalmente se planeó la ejecución de un análisis de seguridad que contribuyo a la disminución de los riesgos y afectaciones por la presencia de brechas de seguridad no identificadas que pudieron comprometer la integridad, disponibilidad y confidencialidad de los activos informáticos y la ejecución de las operaciones de la compañía.

El presente documento busca dar a conocer la implementación de un sistema tecnológico que permite la continuidad del negocio con una conectividad entre sedes manteniendo niveles óptimos de seguridad informática con el que se garantiza el mejoramiento de los procesos, la minimización de costos y el decrecimiento de riesgos relacionadas con la presencia de amenazas y vulnerabilidades. De igual forma, contiene la ejecución los resultados de un pentesting realizado al aplicativo Badstore utilizado en la compañía, y a partir de esto, se proponen soluciones de mejorar que permitan reducir el accionar criminal que se pueda presentar mediante la explotación de dichos fallos.

[1]MOLARES, Estela. [En Linea]. Internet y Sociedad: Relación y compromiso de beneficios colectivos e individuales, 2004. [Citado 11, diciembre, 2019]. Disponible en: http://www.revista.unam.mx/vol.5/num8/art49/sep_art49.pdf

PLANTEAMIENTO DEL PROBLEMA

La empresa XYZ, es una organización dedica a la realización de cobranzas para la recuperación de cartera a través de agentes call center ubicados en la ciudad de Bogotá, Medellín, Bucaramanga y Cali. Actualmente, cuenta con una infraestructura tecnológica centralizada en la ciudad de Bogotá en donde se alojan los servicios de telefonía, almacenamiento y distribución de archivos, los servicios web de la empresa y los aplicativos utilizados para la consulta de clientes.

Aunque inicialmente, el objetivo de este tipo de infraestructura era el de optimizar los recursos de los servidores y de agilizar los procesos de los agentes, debido a los grandes volúmenes de trabajo y de información, y a la necesidad de tener comunicación con otras sedes en el país, esta distribución tecnológica empezó a ser poco eficaz debido a que carecía de sistemas de conectividad que le permitiera suministrar y recibir información proveniente de otros agentes en las demás ciudades. Asimismo, debido a la falta de interconexión entre las sucursales y el nodo central, se ha evidenciado una dificultad para administrar y monitorear los procesos ejecutados por las demás sedes, lo que ha traído consigo problemas operacionales que han puesto en tela de juicio la eficiencia y la calidad de los servicios prestados por la compañía.

Adicional a esto, debido a la falta de unificación y estandarización de los elementos informáticos de la compañía, se han producido fallos de seguridad que han comprometido la disponibilidad, integridad y confidencialidad de los activos de tecnológicos y de información de la organización. Al carecer de una infraestructura tecnológica unificada, los servicios tecnológicos de cada ciudad quedan expuestos ante el aprovechamiento de vulnerabilidades por amenazas debido a que los sistemas de seguridad no cuentan con la suficiente capacidad de respuesta ante la presencia de riesgos.

De igual forma, debido a la necesidad de mejorar la seguridad y el funcionamiento de su aplicativo para la consulta de clientes, la empresa XYZ desconoce el nivel de seguridad con el que cuenta el software Badstore y dada la importancia que este tipo de herramienta ha tenido para el crecimiento del negocio, puede llegar a ser el objetivo principal para los delincuentes informáticos, ya que a través de este elemento, se puede generar grandes afectaciones económicas, operativas o de imagen en la organización; todo esto, a raíz de la presencia de vulnerabilidades que son causadas por brechas de seguridad que se establecen debido a los malos procesos de desarrollo del software o la carencia de medidas de protección para el aseguramiento de estos recursos.

¿De qué manera se puede mejorar la seguridad en una infraestructura red de datos para el caso de estudio de la empresa XYZ?

JUSTIFICACIÓN

La realización de este proyecto se justifica en la medida en la que es importante realizar el mejoramiento de la infraestructura de red de datos para el caso de estudio de la empresa XYZ que permita interconectar las distintas sedes de la compañía entre sí, para garantizar una correcta administración de los servicios ofrecidos por la organización.

La implementación de este proyecto ayudará a disminuir los riesgos por afectaciones de amenazas informáticas en el software Badstore y la infraestructura de la red de datos, ya que la centralización de los recursos tecnológicos permitirá realizar una mejor configuración de las políticas y medidas de respuesta ante la presencia de elementos que afectan los procesos y la información de la compañía.

El desarrollo de este proyecto contribuirá a la adquisición de conocimiento acerca de nuevas tecnologías que automatizan la infraestructura de las redes de datos, así como las técnicas utilizadas para ejecutar procedimientos de pentesting. Asimismo, mediante la investigación y la práctica se afianzarán los conocimientos y se adquirirá experiencia en la ejecución de proyectos de este tipo.

Mediante el desarrollo de este proyecto para el caso de estudio de la empresa XYZ, se contribuirá a mejorar la confidencialidad de la información, de la cual, la empresa es responsable de su custodia, y de esta manera, las personas se encuentran menos expuestas a ser víctimas de amenazas informáticas.

OBJETIVOS

OBJETIVO GENERAL

Diseñar e implementar, a partir de un entorno virtualizado, el mejoramiento de una infraestructura de red de datos para el caso de estudio de la empresa XYZ que permita el aseguramiento de los procesos y la información.

OBJETIVOS ESPECIFICOS

- Realizar la creación de entornos virtualizados que permitan la realización de actividades para el mejoramiento de la seguridad de la infraestructura de la red de datos de la compañía.
- Implementar una solución de seguridad perimetral que permita el aseguramiento de los procesos y la información.
- Realizar la identificación de vulnerabilidades en el software Badstore mediante técnicas de pentesting
- Proponer acciones de mejora para evitar la explotación de las vulnerabilidades que presente el software Badstore

MARCO REFERENCIAL

Los sistemas Mikrotik es una tecnología que combina diversas funcionalidades para la implementación de infraestructuras tecnológicas seguras. Según los autores del presente proyecto muchas compañías relacionadas con las telecomunicaciones y las redes deciden ofrecer este tipo de sistemas con el fin aumentar su credibilidad como proveedor de recursos informáticos. La empresa FIS Soluciones, es un claro ejemplo de esto, que al ofrecer productos Mikrotik a través de catálogo se ha consolidado como una empresa líder en el sector de las telecomunicaciones en Ecuador[2]. En Colombia, se tiene la evidencia que la empresa Solutek Informática se ha consolidado en el mercado de los servicios tecnológicos debido a la venta, distribución y asesoría de diferentes tipos de productos Mikrotik[3], al igual que la compañía Nat Colombia, la cual se especializo en la oferta de productos, cursos y servicios a nivel empresarial relacionados con este tipo de sistemas[4]. Otro ejemplo a nivel local se puede referir a la empresa DistriVoIP, que mediante el ofrecimiento y venta de producto Mikrotik a través de su página web, se ha consolidado en Medellín como una de las organizaciones líderes en soluciones de tecnología[5].

Gracias a las utilidades que poseen los sistemas Mikrotik, se han presentado diversos casos de éxito en la implementación de estas tecnologías. El consejo profesional de Cs Económicas de Santa Fe en el país de Argentina, realizo la configuración de su red IPSEC otorgando autenticación de acceso a los usuarios[6]; en la ciudad de Sevilla, la compañía Digital Herrera realizo la instalación de una infraestructura tecnológica con una red wifi y un servidor de telefonía IP para más de 4000 usuarios[7]; en la organización SpeedyCom de Ecuador, mediante Mikrotik se realizó la implementación de servidor de telefonía IP con troncales SIP para más de 4000 usuarios[8]; en la Universidad Católica de Santiago del Este o en Argentina se configuro el ancho de banda de la red para proveer de internet a usuarios y profesores de manera eficiente[9]; Integra de México realizo la configuración de balance de red con varias WAN optimizando así la calidad de los servicios[10];

[2] FIS SOLUCIONES [En línea]. FIS Soluciones. [Citado 17, octubre, 2018]. Disponible en: http://www.fisoluciones.com/
[3] SOLUTEK INFORMATICA. [En Linea]. MIKROTIK COLOMBIA. [Citado 17, octubre, 2018]. Disponible en: http://mikrotik.solutekcolombia.com/
[4] NAT COLOMBIA. [En Linea]. Construye y administra redes MikroTik & Ubiquiti. [Citado 17, octubre, 2018]. Disponible en: http://natcolombia.com/
[5] DISTIVOIP. [En Linea]. DistiVoIP. [Citado 17, octubre, 2018] Disponible en: http://www.distrivoip.com/cart/34_mikrotik
[6] MKE SOLUTIONS. [En Linea]. Consejo Profesional de Cs Económicas de Santa Fe. [Citado 17, octubre, 2018] Disponible en: https://www.mkesolutions.net/mke-solutions/casos-de-exitos/
[7] MKE SOLUTIONS. [En Linea]. Digital Herrera. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/mke-solutions/casos-de-exitos/
[8] MKE SOLUTIONS. [En Linea]. SpeedyCom. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/mke-solutions/casos-de-exitos/
[9] MKE SOLUTONS. [En Linea]. Universidad Católica de Santiago del Estero. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/mke-solutions/casos-de-exitos/
[10] MKE SOLUTIONS. [En línea]. Integra. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/mke-solutions/casos-de-exitos/

Nuskope de Australia realizo la implementación de router que permite la validación de usuarios externos[11]. Otros casos de éxito evidenciados en la implementación de Mikrotik es el presentado en el municipio de Colonia Alpina en donde se realizó la instalación de 10 cámaras de seguridad administradas en Mikrotik[12]; en San Salvador se realizó la implementación de 510 equipos wifi en los cuales se configuraron accesos VPN bajo esta tecnología[13]; en RT TELECOM se tiene una integración con Mikrotik con EdgePoint 6 y EdgeRouter ER-X-SFP, además de equipos de la serie CCR[14]. El caso de éxito más relevante en la implementación de Mikrotik, es la implementación de estos dispositivos dentro de los datacenter de Amazon[15]; PTP 21 KM Mikrotik el cual tiene un enlace de 40mhz dando capacidad de 100mb[16].

Se han evidenciado casos de ataques a Mikrotik debido a las malas configuraciones de seguridad realizadas en los dispositivos. En agosto del 2018, 170.000 Mikrotik se vieron comprometidos ya que eran convertidos en virus y eran utilizados para sobrecargar monedas digitales debido a un fallo producido por 0-day[17]. Otra afectación de seguridad debido a malos procedimientos en el uso de Mikrotik, es el sucedido en los casos generados por el grupo de ciberdelincuentes Slingshot, que aprovechando las vulnerabilidades que estos dispositivos ofrecían, realizaron implantación de malware en equipos Windows[18]. Para solución a esto, Mikrotik ha desplegado una serie de actualizaciones para reducir 4 vulnerabilidades que eran aprovechadas por las amenazas[19]

La infraestructura tecnológica en Colombia presenta deficiencias en cuanto a seguridad informática debido a que no se encuentran en la evolución de la tecnología generando vulnerabilidades que pueden ser eventualmente aprovechadas por los ciberdelincuentes. Según UpSistemas, se ha evidenciado que las organizaciones que lideran el mercado de infraestructura tecnológica en Colombia corresponden a los sectores de servicios, banca y telecomunicaciones, las cuales han logrado aumentar su productividad al renovar el hardware y software disminuyendo así, los riesgos generados por las amenazas informáticas presentes en la red. Sin embargo, las medianas empresas se han visto afectados por el

[11] NUSKOPE. [En línea]. *Australia Lawful interception, 2008*. [Citado 17, octubre, 2018]. Disponible en: https://forum.mikrotik.com/viewtopic.php?t=87763

[12] INTEGRAL COMUNICACIONES SRL. [En línea]. *Solución de Cámaras Urbanas.* [Citado 17, octubre, 2018]. Disponible en: http://www.integralcomunicaciones.com/site/casos-de-exito/

[13] FLYNET. [En línea]. *Casos de exito*. [Citado 17, octubre, 2018]. Disponible en: http://flynetwifi.com/casosexito.html

[14] INTERNETWORK SOLUTION. [En línea]. *Caso de exito: RT TELECOM.* [Citado 17, octubre, 2018]. Disponible en: https://www.iws.ec/blog/caso-de-exito-rt-telecom

[15] INTERNETWORK SOLUTION. [En línea]. *Noticia #2: mikrotik en amazon datacenter, 2017*. [Citado 17, octubre, 2018]. Disponible en: https://www.iws.ec/blog/noticia-2-mikrotik-en-amazon-datacenter

[16] INTERNETWORK SOLUTION. [En línea]. *Caso de exito: ptp 21km mikrotik, 2017*. [Citado 17, octubre, 2018]. Disponible en: https://www.iws.ec/blog/caso-de-exito-ptp-21km-mikrotik

[17] VELASCO, Ruben. [En línea]. *170.000 routers MikroTik convertidos en una botnet y utilizados para minar criptomonedas por un fallo 0-day, 2018*. [Citado 17, octubre, 2018]. Disponible en: https://www.redeszone.net/2018/08/02/routers-mikrotik-botnet-minar-monedas/

[18] CRESPO, Adrian . [En línea]. *Utilizan routers MikroTik para infectar equipos Windows, 2018*. [Citado 17, octubre, 2018]. Disponible en: https://www.redeszone.net/2018/03/10/mikrotik-infectar-windows-malware/

[19] MKE SOLUTIONS. [En línea]. *Actualización de seguridad en RouterOS, 2018*. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/noticias/actualizacion-de-seguridad-en-routeros/

panorama general del país en cuanto a la infraestructura tecnológica, ya que se estima que un 50% de organizaciones que pertenecen al sector de salud, agropecuario y transporte cuenta con soluciones informáticas básicas que no brindan garantías de seguridad, haciendo que su tecnología entre en obsolescencia. Un factor en la actualización de sistemas de seguridad en las compañías de debe a que existen entes reguladores que obligan a las empresas a implementar altos estándares de calidad para operar los negocios de estos sectores, pero desafortunadamente, no todas las organizaciones son reguladas y por tal razón no ven la necesidad de renovar su tecnología, y además desconocen la importancia de la implementación de seguridad en la infraestructura, arriesgándose a la perdida de información[20].

Las redes empresariales y su tecnología están sufriendo una serie de transformaciones debido al desarrollo de distintos desarrollos tecnológicos que se han creado en los últimos años y al cambio de orientación de las tecnologías de la información. Más allá de la transigencia y la manera dinámica de que hoy requieren las redes, su implementación y administración, el incremento del uso de dispositivos personales como los teléfonos inteligentes en las empresas ha exigido una extensión de las redes hacia este fenómeno diferente, así como un incremento en el alcance de las redes inalámbricas, y la estimación de estructuras en las políticas de acceso y seguridad. En cuanto a las temáticas de desarrollo tanto desde la de política como de regulación para el sector TIC a nivel mundial, dejan ver que existen tres grandes frentes de trabajo referentes a:
los planes de masificación de banda ancha y despliegue de backbone,
la migración a las redes de nueva generación
el análisis de mercados

En base a lo anterior, estos retos, han conllevado a que la política en materia de TIC haya gestionado sistemas orientados a estructurar las bases necesarias para realizar las tareas en la cuales el país está comprometido. Esto hace parte de las iniciativas establecidas en el Plan de TIC 2008-2019 “Colombia en línea con el futuro” (PNTIC), el Pacto Social Digital.

[20] CORPORACION COLOMBIA DIGITAL. [En línea]. *¿Cuáles son los sectores que más han avanzado en infraestructura tecnológica?, 2017.* [Citado 21, octubre, 2018] Disponible en: https://colombiadigital.net/actualidad/noticias/item/9608-cuales-son-los-sectores-que-mas-han-avanzado-en-infraestructura-tecnologica.html

MARCO CONCEPTUAL

Para implementación de una infraestructura de red con tecnología Mikrotik, se deben tener en cuenta los modelos de referencia para los protocolos red OSI o TCP/IP. El modelo OSI es un estándar que está conformado por 7 capaz las cuales determinan cada una de las fases por la que debe pasar un paquete o la información. Este modelo fue desarrollado por la Organización Internacional para la Estandarización (ISO) como una guía para establecer un conjunto de protocolos, donde su finalidad era la de establecer normas para la interconexión de sistemas y dispositivos. Este modelo define los protocolos que deben ser implementados en cada capa, por tal razón es considerado un modelo de referencia para el aprendizaje acerca de la comunicación[21]

Uno de los estándares más utilizados a nivel mundial en las infraestructuras de comunicaciones es el modelo TCP/IP, que corresponde a protocolo de control de transmisión/protocolo de internet. Este establece las capas para la comunicación de sistemas que pertenecen a diferentes redes mediante el empleo de protocolos. TCP permite el intercambio de información entre dos anfitriones asegurándose de que la entrega de paquetes se haga de manera completa y ordenada. IP utiliza las direcciones para establecer la comunicación entre dos dispositivos[22]

El inicio de las redes de comunicaciones se estableció mediante conexiones alámbricas haciendo uso de cables de datos también llamados cables de red o de Ethernet, los cuales están compuestos de hilos conductores que transmiten información y que permiten interconectar diferentes elementos de la red entre si[23]. Las redes alámbricas se clasifican según la topología en la que se implementen. Estas redes se catalogan en:

1. Red en topología estrella: Consiste en la conexión de equipos de cómputo en la cual se establece un servidor central para establecer en control de la red.
2. Red en topología en bus: Consiste en la conexión de equipos de cómputo de forma lineal que comparten el mismo canal de datos
3. Red en topología anillo: Consiste en la conexión de equipos en un círculo cerrado permitiendo la transmisión de información en una sola dirección
4. Red en topología de malla: Este tipo de conexión permite la comunicación entre todos los nodos de la red, eliminando así, las

[21] UNICEN. [En Linea]. *El modelo OSI*. [Citado 27, noviembre, 2019]. Disponible en: http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf
[22] IBM. [En línea]. Protocolos TCP/IP. [Citado 02, diciembre, 2019]. Disponible en: https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/network/tcpip_protocols.html
[23] IDEONEOS.ORG. [En línea]. *Redes Alambricas*. [Citado 17, octubre, 2018]. Disponible en: http://idoneos.org/ovas/60/redes_alambricas.html

interrupciones en la comunicación.

Teniendo en cuenta que las redes en los últimos años han evolucionado de manera considerable hasta la evolución de redes inalámbricas y que estas a su vez se pueden clasificar en 3:

1. Red WLAN: La red inalámbrica de área local hace uso del aire para emitir la transmisión, este tipo de redes están basadas en estándares de capa física, tales como el IEEE802.11b y el IEEE802.11g, los cuales funcionan en banda de frecuencia 2.4 GHz y el otro estándar IEE802. a tiene funcionalidad en la banda de frecuencia de 5 GHz[24]

2. Red WWAN: Las redes inalámbricas de área amplia se caracterizan por utilizar tecnología enfocada a la telefonía móvil, estas redes comprenden una variedad de ellas desde la más sencilla hasta la más avanzada como lo son GSM o 2G hasta LTE o 4G respectivamente y se encuentra en estudio una red G5 que promete ser 250 veces más rápida que la red 4G[25]

3. WPAN: La red inalámbrica de área personal son redes de cobertura limitada que se encuentran dentro de categorías como HOMERF, Bluetooth, ZIGDEE o RFID. La cobertura de esta red es a pocos metros del emisor con una velocidad de transmisión inferior al megabit por segundo[26]

Actualmente, la telefonía IP está siendo integrada dentro de la infraestructura de red ya que permite la integración de voz y datos reduciendo los costos, optimizando el rendimiento de red, simplificando la infraestructura y la unificando las comunicaciones en una organización. La telefonía IP se caracteriza por hacer uso de elementos como servidores, puertas de enlace y terminales a través de protocolos que permiten dividir los paquetes de audio que se trasmiten mediante la red. Los más utilizados por las organizaciones son: SIP, H.323, RTP, RTCP, SRTP, y SDP[27]

- Mikrotik

En la actualidad, la infraestructura tecnológica esta un constante crecimiento debido a la expansión operacional de las compañías dando origen a la

[24] ANDREU, Fernando;PELLEJERO,Izaskun;LESTA, Amaia. [En línea]. Fundamentos y aplicaciones de seguridad en redes WLAN. [Citado 20, octubre, 2018]. Disponible en: https://books.google.es/books?hl=es&lr=&id=k3JuVG2D9lMC&oi=fnd&pg=PA1&dq=RED+WLAN&ots=8Ftd_ziXdJ&sig=rCt6XJqQlaI1nPoZS5MDsFejia0#v=onepage&q&f=false

[25] GALLEGO, Jose. [En línea]. *Instalacion y mantenimiento de redes para transmision de datos*. [Citado 17, octubre, 2018]. Disponible en : https://books.google.com.co/books?id=qt_SCQAAQBAJ&pg=PA37&dq=Red+WWAN&hl=es&sa=X&ved=0ahUKEwj3t4ijha_mAhWoxVkKHVS7AwMQ6AEIQjAD#v=onepage&q=Red%20WWAN&f=false

[26] ANDREU,Joaquin. [En línea]. *Servivios en red*. [Citado 17, octubre, 2018]. Disponible en: https://books.google.com.co/books?id=vhit3ZmGQPsC&pg=PA213&dq=RED+WPAN&hl=es&sa=X&ved=0ahUKEwii5IeJiq_mAhUqqlkKHYmFBREQ6AEIKTAA#v=onepage&q=RED%20WPAN&f=false

[27] 3CX. [En línea]. ¿Qué es la telefonia IP?. [Citado 05, diciembre, 2019]. Disponible en: https://www.3cx.es/voip-sip/telefonia-ip/

implementación de nuevos modelos tecnológicos para el soporte de las actividades que conllevan al cumplimiento del core del negocio.

Mikrotik: Es una compañía letona, fundada en el año de 1995 dedicada a la distribución de productos de comunicación inalámbrica como Routersboards y el sistema operativo que los controla RouterOS[28]

RouterOS: Según Duarte, RouterOS es el sistema operativo por defecto de los dispositivos Mikrotik, el cual está basado por un núcleo Linux, integrado por utilidades de firewall, routing, MPLS, VPN, WLAN, hostpot y está basado por un núcleo Linux, integrado por utilidades de firewall, routing, MPLS, VPN, WLAN, hostpot y proxy[29]. Este sistema operativo puede ejecutarse desde un disco SATA IDE o desde una memoria flash.

El sistema operativo RouterOS cuenta con diversas utilidades que permiten el control de seguridad a través de la configuración de Firewall; ayudan al control de VPN´s mediante la utilización de canales encriptados que protegen la información. Asimismo, ofrece calidad de servicio al administrar de manera controlada los anchos de banda para el uso de los recursos; otorga medidas de controles de acceso y controles hostpot para la seguridad los dispositivos y la navegación[30]

Los dispositivos Mikrotik, para el establecimiento de sus comunicaciones, emplea protocolos de comunicación que permiten la administración y transmisión de información entre dispositivos y redes. Los protocolos más utilizados para en esta tecnología son: el 802.11 que se encarga del uso de las redes inalámbricas, el NV2 un protocolo propio de Mikrotik para las conexiones wifi y el protocolo Nstreme, que al igual que NV2 es exclusivo de la marca y que se enfoca en mejorar el desempeño de las redes inalámbrica[31].

El sistema RouterOS de Mikrotik este compuesto por las siguientes características:

- Configuración
  - Ingreso mediante teclado
  - Mediante consola serial
  - A través de Telnet y SSH

[28]MIKROTIK. [En línea]. *About us*. [Citado 17, octubre, 2018]. Disponible en: https://mikrotik.com/aboutus

[29] DUARTE, Ernesto. [En línea]. ¿Qué Es Mikrotik RouterOS?, 2014. [Citado 17, octubre, 2018]. Disponible en: http://blog.capacityacademy.com/2014/04/09/que-es-mikrotik-routeros/

[30] ANRRANGO, Rodrigo. [En línea]. Características Importantes de los Equipos Mikrotik, 2015. [Citado 17, octubre, 2018]. Disponible en: https://configurarmikrotikwireless.com/blog/caracteristicas-importantes-equipos-mikrotik.html

31 ANCHONDO, Daniel. [En línea]. Mikrotik - Protocolos de comunicación para enlaces inalámbricos. Citado 21, octubre, 2018]. Disponible en: https://soporte.syscom.mx/redes-inalambricas-enlaces/mikrotik/mikrotik-protocolos-de-comunicacion-para-enlaces-inalambricos

    - Por medio de la interfaz gráfica WinBox
- Firewall
    - Filtrado de paquetes integrado
    - Funciones de seguridad para la transmision de datos que provienen y salen del dispositivo
    - Uso de NAT para evitar accesos no autorizados
    - Filtrado de IP a traves de puertos TCP/UDP, rango de direcciones, entre otros
- Routing
    - Compatible con IPv4. Admite protocolos RIP v1 y v2, OSPF v2, BGP v4
    - Compatible con IPv6. Admite protocolos RIPng, OSPFV v3 y BGP
- MPLS
    - Vinculación de etiquetas estáticas para IPv4
    - Protocolo de distribución de etiquetas para IPv4
- VPN
    - IPSec
    - Túneles de punto a punto
    - Túneles simples
    - VLAN
    - VPN basado en MPLS
- Conexiones inalámbricas
    - Punto de acceso y cliente inalámbrico IEEE802.11a/b/g/n
    - Protocolos Nstreme y Nstreme2
    - Punto de acceso virtual
    - Encriptación WEP, WPA, WPA2
    - Protocolo de ruteo inalámbrico MME
- Hospot
    - Creación de redes de acceso publico
    - soporta autenticación de servidores RADIUS
- Web proxy
    - Proxy HTTP regular
    - Proxy transparente
    - Almacenamiento del cache en Discos externos
    - Soporte a proxy SOCKS
    - Lista de acceso cache para especificar los recursos deben ser accedidos directamente y cuales vía otro servidor
- Administración de red
    - Prueba de ancho de banda
    - SSH
    - Herramientas para el envio de Email y SMS
    - Servidor TFTP
    - Servidor NTP
    - SNMP

- RADIUS

Estas son algunas de las características más importantes de los dispositivos Mikrotik[32]

- Entornos virtuales

El proceso de virtualización consiste en la creación de entornos informáticos controlados que simulan el uso de un entorno físico en los cuales se pueden incluir el uso de hardware, software, dispositivo de almacenamiento, etc. En la virtualización, cada entorno o máquina virtual, puede trabajar de manera conjunta o individual con otros aplicativos y/o recursos informáticos. Este concepto de computación es muy utilizado a nivel empresarial debido a que mejora la escalabilidad y las cargas de trabajo de los procesos informáticos, permitiendo así, una reducción en los costos de infraestructura, mantenimiento y consumos de energía [33]

Existen diversos tipos de virtualización enfocados en la solución u optimización de un tipo de recurso tecnológico en específico. La virtualización de datos consiste en la agrupación, organización y transformación de datos provenientes de diferentes fuentes con el fin de mejorar las capacidades de procesamiento de información de las organizaciones. La virtualización de escritorios permite a un administrador de infraestructura tecnología, implementar entornos simulados de escritorio facilitando la realización de configuraciones, actualizaciones y controles de seguridad de forma masiva en todos los escritorios virtuales de una empresa. La virtualización de servidores consiste en la simulación física de un servidor con el objetivo de optimizar la ejecución de servicios facilitando la ejecución de más funciones específicas y tareas simultaneas. La virtualización de sistemas operativos se basa en la implementación de máquinas virtuales con sistemas operativos propios e independientes, los cuales permiten la reducción de costos en hardware, el aumento de la seguridad tecnológica y un mejoramiento en la administración de infraestructura. La virtualización de funciones de red consiste en la simulación de entornos de red enfocadas en el mejoramiento de los procesos de comunicación de una compañía con el fin de reducir los de costos de implementación de componentes de red.

- Análisis de riesgos

Actualmente, para el mejoramiento de una infraestructura tecnológica se deben

[32] DUARTE, Ernesto. [En línea]. *¿Qué Es Mikrotik RouterOS?, 2014 [Citado 17, octubre, 2018]. Disponible en:* http://blog.capacityacademy.com/2014/04/09/que-es-mikrotik-routeros/

[33] MICROSOFT. [En línea]. ¿Qué es virtualización? [Citado 04, noviembre, 2018]. Disponible en: https://azure.microsoft.com/es-es/overview/what-is-virtualization/

tener en cuenta metodologías de análisis de riesgos para la detección de peligros que puedan comprometer la integridad, disponibilidad y confidencialidad de los componentes tecnológicos. Para ello, la metodología MAGERIT permite la identificación de activos informáticos los cuales pueden estar conformados por la información, los procesos, servicios, los componentes hardware y software, y las instalaciones físicas de una compañía. Una vez identificados dichos activos, MAGERIT sugiere la identificación de amenazas, la determinación de los niveles de impacto y la probabilidad de ocurrencia del riesgo que presentan cada uno de los activos para posteriormente proceder a la creación de controles para cada uno de ellos y de esta manera definir la gestión de los riesgos.

En una infraestructura tecnológica basada en sistemas Mikrotik, se puede adoptar la metodología MAGERIT para la identificación de riesgos en los servidores que permita evaluar las vulnerabilidades surgidas a partir de la implementación de esta tecnología y de esta manera contemplar mecanismos alternos para el aseguramiento de la infraestructura y de la información, además implementar planes de gestión de riesgos que permitan dar cumplimiento a la política de seguridad informática de la compañía y de esta manera garantizar el mejoramiento de los procesos y la continuidad del negocio de una manera más competida.

- ¿Qué es el Pentesting?

El pentesting es la abreviatura de las palabras penetración y testing y consiste en la ejecución de ataques dirigidos a sistemas con el fin de descubrir fallas tecnológicas o vulnerabilidades y así determinar el alcance, las posibilidades de éxito y la repercusión que dichos errores tendrían sobre el recurso informático. De igual forma, este tipo de prácticas contribuyen a la identificación de debilidades no detectadas por softwares especificados para tal fin y a medir la capacidad de respuesta que tendría el equipo de seguridad informática ante la presencia de un ataques real.[34]

- Tipos de Pentesting

    - Pentesting de caja blanca: Al realizar este tipo de test se conoce muy bien la infraestructura, se posee una gran cantidad de información de los activos tecnológicos y normalmente es realizado por profesionales de la misma área de TI.
    - Pentesting de caja negra: Este test se puede comparar con un ataque por parte del cibercrimen ya que no se pose información acerca de la infraestructura y se podría decir que se realiza a ciegas por sus

[34] PANDA. [En línea]. Pentesting: Una herramienta muy valiosa para tu empresa, 2018. [Citado 11, diciembre, 2019]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

características
    - Pentesting de caja gris: Este test es el más recomendado ya que es una combinación del test de caja blanca y el test de caja negra, donde se posee cierta información y a partir de ello se sumarán esfuerzos para encontrar vulnerabilidades.[35]

- Fases o métodos de pentesting

Teniendo en cuenta los requerimientos del cliente y las características de los sistemas es importante definir el método que se utilizara para llevar a cabo el pentesting

    - ISSAF (Information Systems Security Assessment Framework): se basa en los criterios de evaluación que previamente han sido documentados por expertos, para organizar la información.
    - PCI DSS (Payment Card Industry Data Security Standard): Este método es utilizado por entidades que almacenan, procesan y realizan envíos de información de los titulares de tarjetas débito y crédito.
    - PTES (Penetration Testing Execution Standard): Es utilizado por profesionales reconocidos en el ámbito de la tecnología y las vulnerabilidades y es un modelo a seguir que se encuentra en libros relacionados con el pentesting
    - OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad): Es un modelo muy reconocido y aporta de cierta manera un método a seguir para la ejecución de pruebas para garantizar la seguridad

- Tipos de ataques:
    - Cross Site Scripting (XSS): Es la inyección de código javascript en un aplicativo web o navegador que permite a un atacante informático, robar los datos contenidos en el sitio afectado o re direccionar a las víctimas a sitios web falsos
    - Inyección SQL: Es un tipo de ataque informático en el cual se añade una instrucción SQL a un campo de entrada para así obtener, modificar o eliminar la información contenida en una base de datos
    - Modificacion de cookies: La modificación o envenenamiento de coockies consiste en modificar el contenido de estos elementos para evitar mecanismos de seguridad.[36]
    - Tampering de parámetros: Consiste en la modificación de los parámetros

[35] PRENAFETA, Javier. [En línea]. *Tipos de Pentesting, 2018*. [Citado 11, septiembre, 2018]. Disponible en: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/

[36] DRAGONJAR. [En línea]. *Video: Ataque de envenenamiento de cookies (Cookie-Poisoning)*. [Citado 04, septiembre, 2019]. Disponible en: https://www.dragonjar.org/video-ataque-de-envenamiento-de-cookies-cookie-poisoning.xhtml

que se envían al servidor web como puntos de entrada de la aplicación[37].

- Directory transversal: Es un ataque que consiste en acceder a directorios restringidos para ejecutar comandos fueran del directorio raíz del servidor web[38]
- Navegación forzada: es un ataque cuyo objetivo es acceder a los recursos a los que la aplicación no hace referencia, pero que aún son accesibles.
- Denegacion de servicios: Un ataque de denegación de servicio (DDoS) consiste en provocar la inaccesibilidad de un determinado recurso mediante en el envío de una gran cantidad de peticiones provocando la saturación de los recursos del servidor, generando la inoperatividad del mismo y conllevando a la denegación de los servicios a los usuarios que intenten acceder a estos recursos.[39]
- Cookie snooping: Este ataque consiste en el uso no autorizado de datos para el acceso a información de terceros con fines ilícitos

MARCO LEGAL

- Legislación en el campo de la informática

Anteriormente en los inicios del internet no existían normas para el intercambio de información mediante las redes, sin embargo en la medida que la tecnología ha avanzado se generado la necesidad de crear mecanismos para la regulación de este proceso, con el objetivo de certificar la confidencialidad de la información y de proteger a las personas o empresas dueñas de esta, debido a que han surgido modalidades delictivas en las redes informáticas que buscan ocasionar daños a terceros generalmente con fines lucrativos a partir del robo de información o diferentes tipos de daños que se pueden ocasionar una vez se vulnera la seguridad de las redes.

- Que es la seguridad informática

La seguridad informática nace a partir de la necesidad de asegurar los recursos de los sistemas de información de una compañía, y se puede definir como la disciplina que se enfoca en mantener la integridad, confidencialidad y disponibilidad de la información. En ese sentido cada país debe crear sus mecanismos cuanto a la ciberseguridad.

[37] HENRYRAUL. [En línea]. *¿Que es un ataque de tipo "Parameter Tampering" y como puede evitarse?, 2017.* [Citado 04, septiembre, 2019]. Disponible en: https://henryraul.wordpress.com/2017/02/26/en-que-consisten-los-ataques-parameter-tampering-y-como-pueden-evitarse/

[38] ACUNETIX. [En línea]. *What is a Directory Traversal attack?* [Citado 04, septiembre, 2019]. Disponible en: https://www.acunetix.com/websitesecurity/directory-traversal/#targetText=Directory%20traversal%20or%20Path%20Traversal,Root%20directory

[39] CATORIA, Fernando. [En línea]. Consejos para evitar un ataque de denegación de servicio, 2012 . [Citado 04, septiembre, 2019]. Disponible en: https://www.welivesecurity.com/la-es/2012/03/28/consejos-ataque-denegacion-servicio/

Colombia es uno de los países líderes en Latinoamérica a través de su política nacional en ciberseguridad y ciberdefensa, además cuenta con la ley 1273 de 2009 que establece " la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[40].

- Normas que exponen lineamientos a nivel de informática

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) que detalla cómo se debe gestionar la seguridad de la información en las organizaciones. La actualización más reciente se publicó en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. Existió una primera versión desde 2005 que fue establecida en base a la norma británica BS 7799-2 [41]. ISO27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.

Sistema de Gestión de Seguridad de la Información
Para la Gestión global de la Seguridad de un Sistema de Seguridad de la Información que esté basado en ISO 27001, MAGERIT, es una metodología que permite el análisis y gestión de Riesgos de los sistemas de información[42]

MARCO ESPACIAL

Teniendo en cuenta el planteamiento del problema y los objetivos establecidos para la ejecución de este proyecto aplicado, se implementa una infraestructura de red de datos basada en sistemas Mikrotik para el caso de estudio de la empresa XYZ, la cual cuenta con sedes distribuidas en las ciudades de Bogotá, Medellín, Cali y Bucaramanga.

[40] CONGRESO DE LA REPUBLICA DE COLOMBIA. [En línea]. LEY 1273 DE 2009, 2009. [Citado 04, noviembre, 2019]. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
[41] CONEXIÓN ESAN. [En línea]. ¿Qué es y para que sirve la Norma ISO 27001?, 2016. [Citado 05, diciembre, 2019]. Disponible en: https://www.esan.edu.pe/apuntes-empresariales/2016/05/que-es-y-para-que-sirve-la-norma-iso-27001/
[42] SGSI. [En línea]. ISO 27001: El método MAGERIT, 2015. [Citado 16, noviembre, 2019]. Disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

MARCO METODÓLOGICO

El tipo de investigación para el desarrollo de este proyecto será la investigación aplicada, ya que nos permite la búsqueda de una temática específica a partir de un problema ya establecido y conocido por parte de los ejecutores del proyecto. Esta metodología permite la solución de problemas mediante la práctica, empleando tecnología Mikrotik

Las técnicas de levantamiento de información que se van a emplear para el desarrollo de este proyecto son las siguientes:

1. La observación: Se utiliza la técnica de observación con el fin de determinar la estructura de la red, los administradores y que información o servicios se están compartiendo a través de esta[43]
2. La entrevista: Se utiliza esta técnica para entrar en comunicación con los responsables de la administración de la red con el fin de conocer detalles específicos que permitan el funcionamiento de la red.

- Investigación acerca de técnicas para la implementación de sistemas Mikrotik

Para la ejecución de una infraestructura haciendo uso de tecnología Mikrotik, se elige como referencia lo establecido en la documentación técnica aportada por el proveedor la cual indica los procedimientos y las configuraciones a realizar. Esta información será tomada del siguiente sitio web https://wiki.mikrotik.com/wiki/Manual:TOC

- Análisis del entorno organizacional de la empresa XYZ

Para la implementación de una infraestructura mediante el uso de tecnología Mikrotik se considerarán las siguientes variables:

- Numero de sedes
- El número de usuarios por sedes
- El número total de usuarios
- Redes virtuales privadas
- Servidores
- Ancho en de banda
- Controles de acceso
- Configuraciones de red

[43] CHAVEZ, Dennis. [En línea]. *Conceptos y técnicas de recolección de datos en la investigación*. [Citado 17, octubre, 2018]. Disponible en: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080521_56.pdf

- Procedimiento

Los pasos ejecutados para la implementación de una infraestructura mediante el uso de tecnologías Mikrotik son los siguientes:

1. Descargar los archivos ISO de los sistemas operativos que contaran los servidores.
2. Descargar el archivo ISO del sistema operativo RouterOS.
3. Preparar el ambiente virtualizados.
4. Realizar las configuraciones necesarias para la ejecución del proyecto tecnológico

- Ejecución de pentesting

Para realiza la identificación de vulnerabilidades, ejecutaran prueba de caja gris, el cual permite el descubrimiento de brechas de seguridad a partir de la información otorgada por la compañía y otras que se puedan hallar desde el desconocimiento de los elementos del software.

- Análisis del entorno organizacional de la empresa XYZ

Para el mejoramiento de una infraestructura de red de datos mediante el uso de tecnología Mikrotik y ejecución de técnicas de pentesting se considerarán las siguientes variables:

- Numero de sedes
- El número de usuarios por sedes
- El número total de usuarios
- Redes virtuales privadas
- Servidores
- Ancho en de banda
- Controles de acceso
- Configuraciones de red
- Software Badstore

- Procedimiento para la implementación de un sistema de seguridad perimetral

Los pasos seguir para el mejoramiento de una infraestructura de red de datos mediante el uso de tecnologías Mikrotik son los siguientes:

1. Descargar los archivos ISO de los sistemas operativos que contaran los servidores.
2. Descargar el archivo ISO del sistema operativo RouterOS.
3. Preparar el ambiente virtualizados.
4. Realizar las configuraciones necesarias para la puesta en marcha del proyecto tecnológico

RESULTADOS

Para dar solución a la problemática presentada por el caso de estudio de la empresa XYZ, se llevó a cabo la implementación de un infraestructura de red de datos haciendo uso de dispositivos Mikrotik, en la cual, a través de entornos virtualizados, se implementaron 4 Mikrotik correspondientes a cada sucursal de la compañía, en los cuales se configurando medidas de seguridad para la acceso a la red y el tráfico en general, y mecanismos de conexión segura para facilitar el acceso a los recursos ubicados en la ciudad de Bogotá, donde se encuentran centralizados los servidores del aplicativo de gestión, la página web, servidor de telefonía y el servidor FTP.

Asimismo, se realizó un análisis de pentesting mediante el cual se identificación vulnerabilidades en cuanto ataques de: XSS, SQL Injection, Dos, navegación forzada, modificación de cookies, tampering de parámetros, directory transversal y cookie snopping.

A continuación, se ilustra el proceso realizado y el funcionamiento de dicha solución.

Implementación sistema Mikrotik

1. Configuración de entornos virtualizados, instalación de sistema operativos y asignación de segmentos de red

Como primera medida para el proceso de implementación, se llevó a cabo la fase de alistamiento de los entornos virtualizados a través de una plataforma de virtualización.

Se recolectaron las imágenes de los sistemas operativos Centos, Windows 7, RouterOS y Asterisk y se procedio a la creacion y configuracion de cada uno de estos en el entorno de virtualización de la siguiente manera:

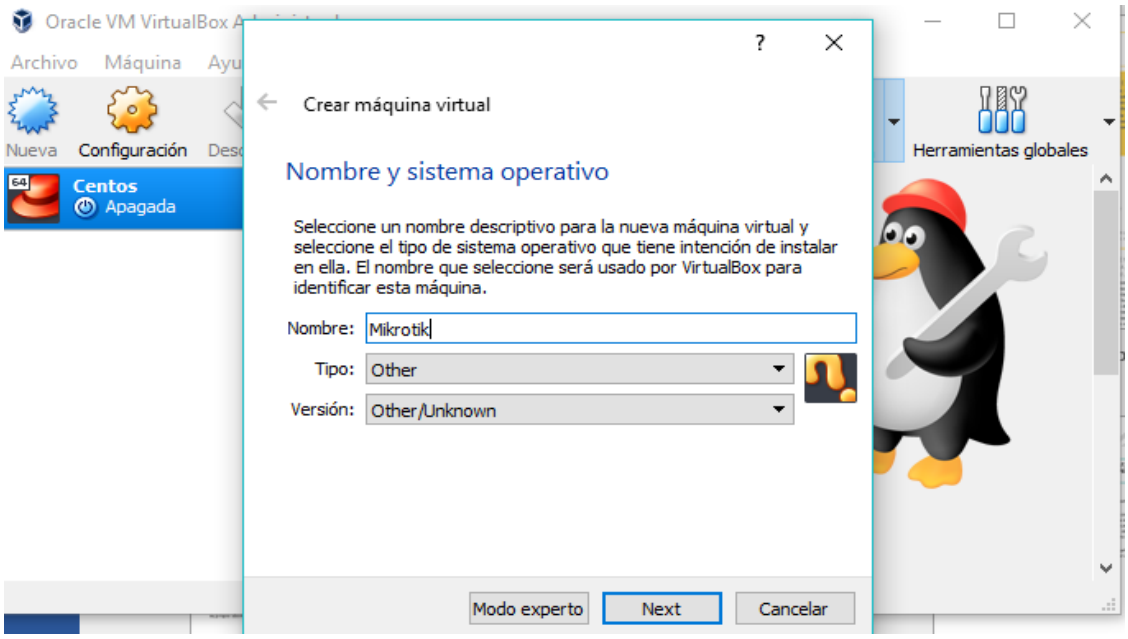


Ilustración 1 Asignación de nombre a máquina virtual

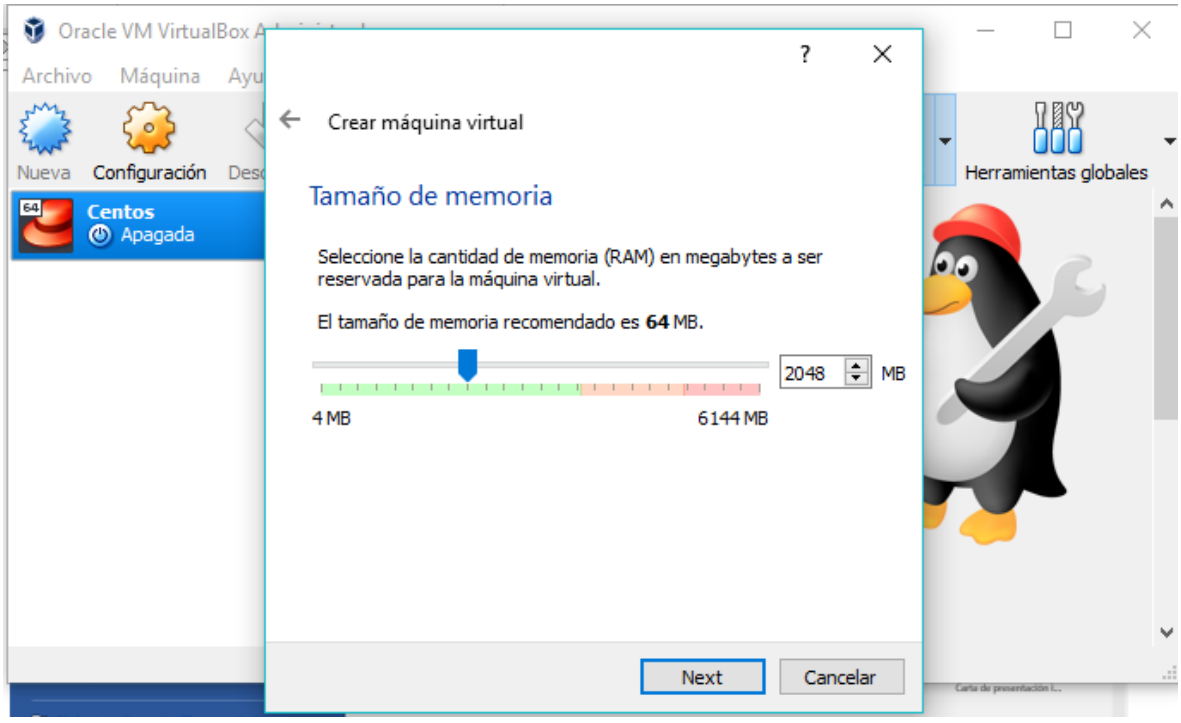


Ilustración 2 Asignación de memoria RAM a máquina virtual

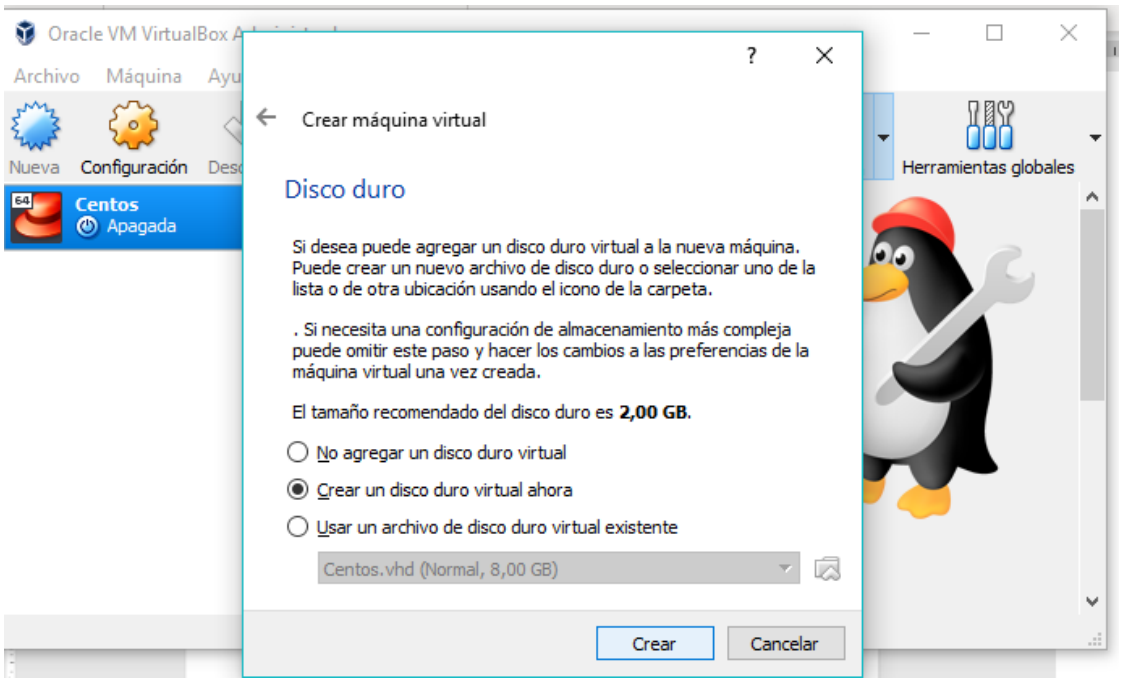


Ilustración 3 Creación de disco virtual

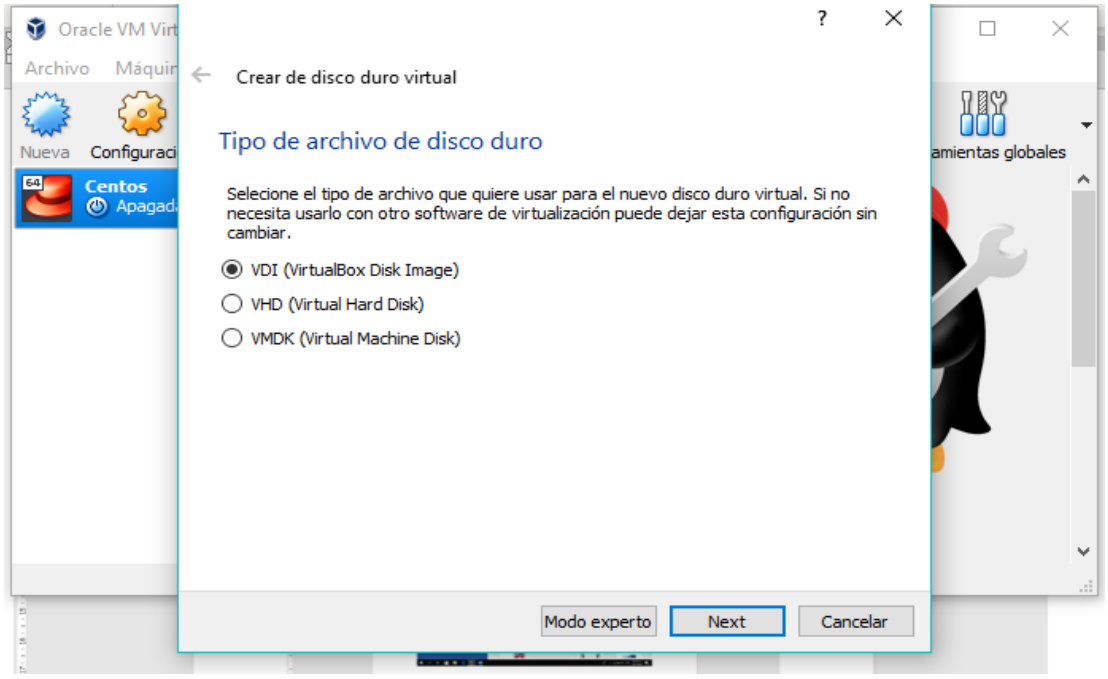


Ilustración 4 Selección tipo de disco duro

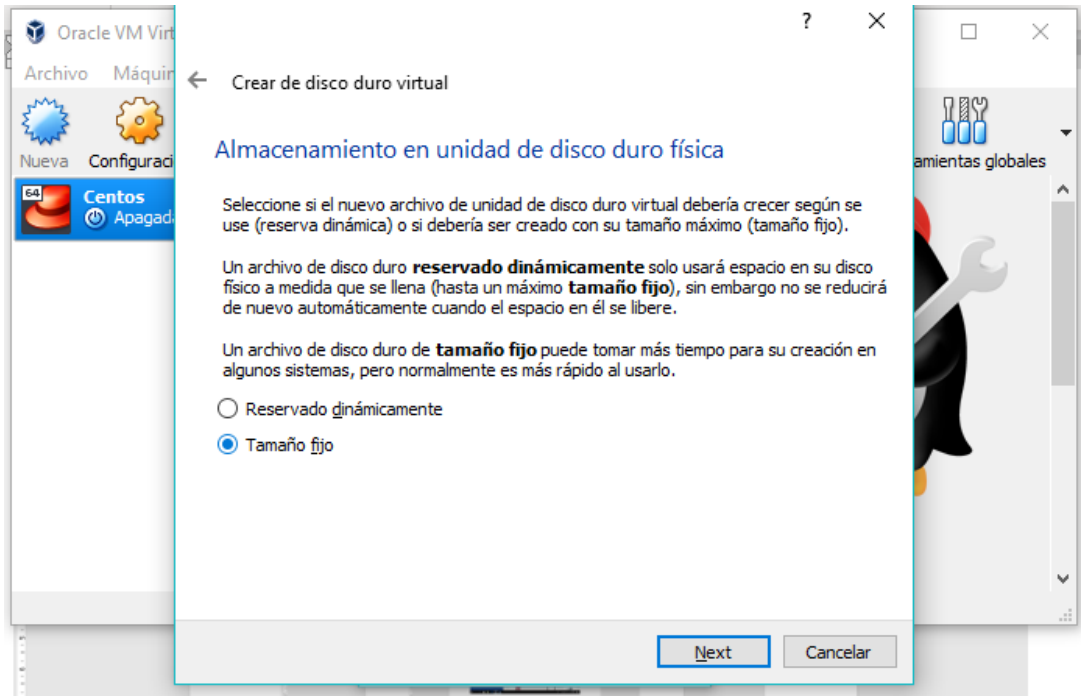


Ilustración 5 Selección tipo de almacenamiento

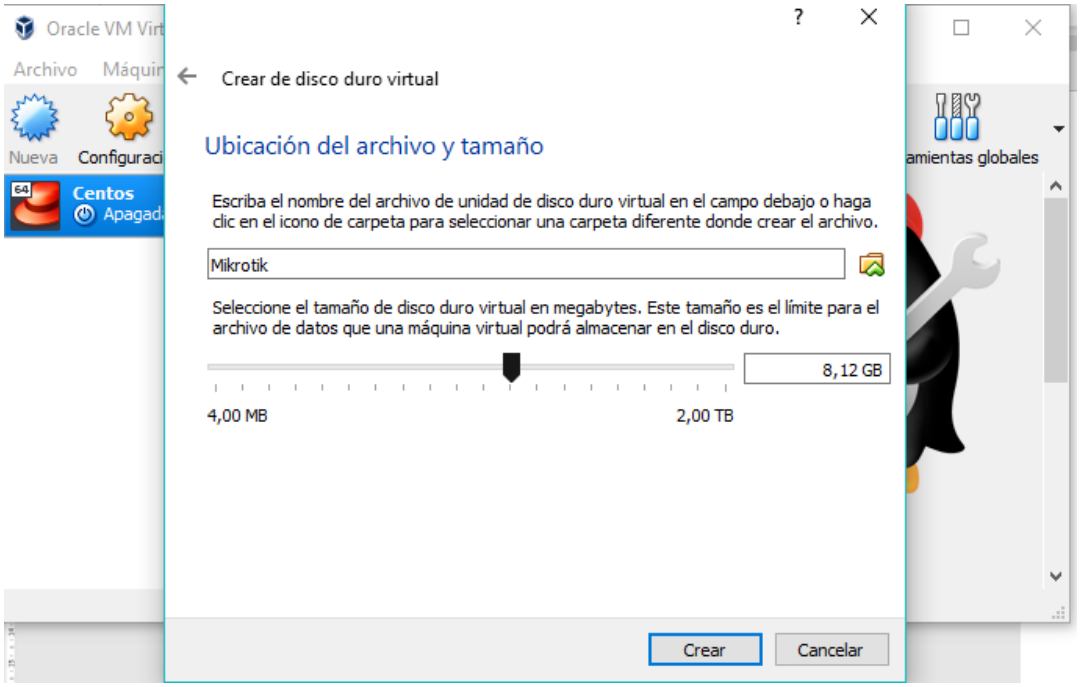


Ilustración 6 Asignación tamaño disco duro

Ilustración 7 Creación de máquina virtual finalizada

Previamente, antes de la instalación de los sistemas operativos, se realizó la distribución de los segmentos de red para cada ciudad quedando de la siguiente manera:

Ciudad	Red	Rango	Mascara	Broadcast
Bogotá	10.11.0.0	10.11.0.1-10.11.0.62	255.255.255.192	10.11.0.63
Cali	10.11.0.64	10.11.0.65-10.11.0.126	255.255.255.192	10.11.0.127
Bucaramanga	10.11.0.128	10.11.0.129-10.11.0.190	255.255.255.192	10.11.0.191
Medellín	10.11.0.192	10.11.0.193-10.11.0.254	255.255.255.192	10.11.0.255

Tabla 1 Lista de segmentos de red

Para efectos del desarrollo de la práctica, se asignaron las siguientes IP's para los dispositivos Mikrotik de cada ciudad, en donde las IP's públicas mencionadas, son direcciones IP privadas la cuales fueron tomadas como publicas debido a la implementación de maquinas virtuales.

Ciudad	IP Privada	IP Publica
Bogotá	10.11.0.2	192.168.0.33
Cali	10.11.0.66	192.168.0.32
Bucaramanga	10.11.0.130	192.168.0.34
Medellín	10.11.0.194	192.168.0.35

Tabla 2 Lista de IP's por ciudad

Se asignaron las siguientes dirección IP privadas a los servidores ubicados en la ciudad de Bogotá:

Servidor	IP Privada
Web	10.11.0.6
FTP	10.11.0.50
Telefonía	10.11.0.62
Aplicativo de gestión	10.11.0.20

Tabla 3 Lista de IP's por servidor

Una vez creadas las maquinas virtuales con las características requeridas para cada sistema operativo, se procede a la instalación de un Mikrotiks para cada una de las ciudades mediante el siguiente procedimiento:

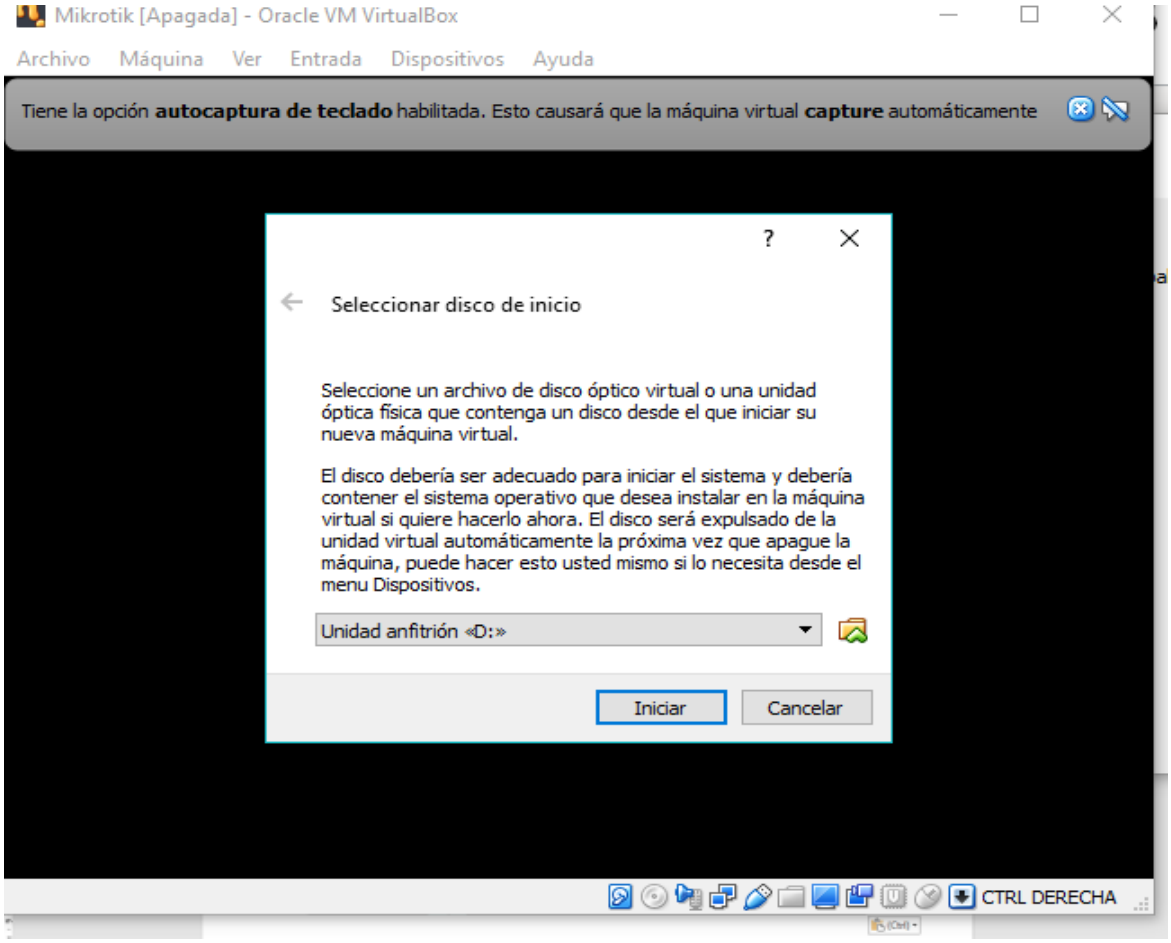


Ilustración 8 Inicio de máquina virtual

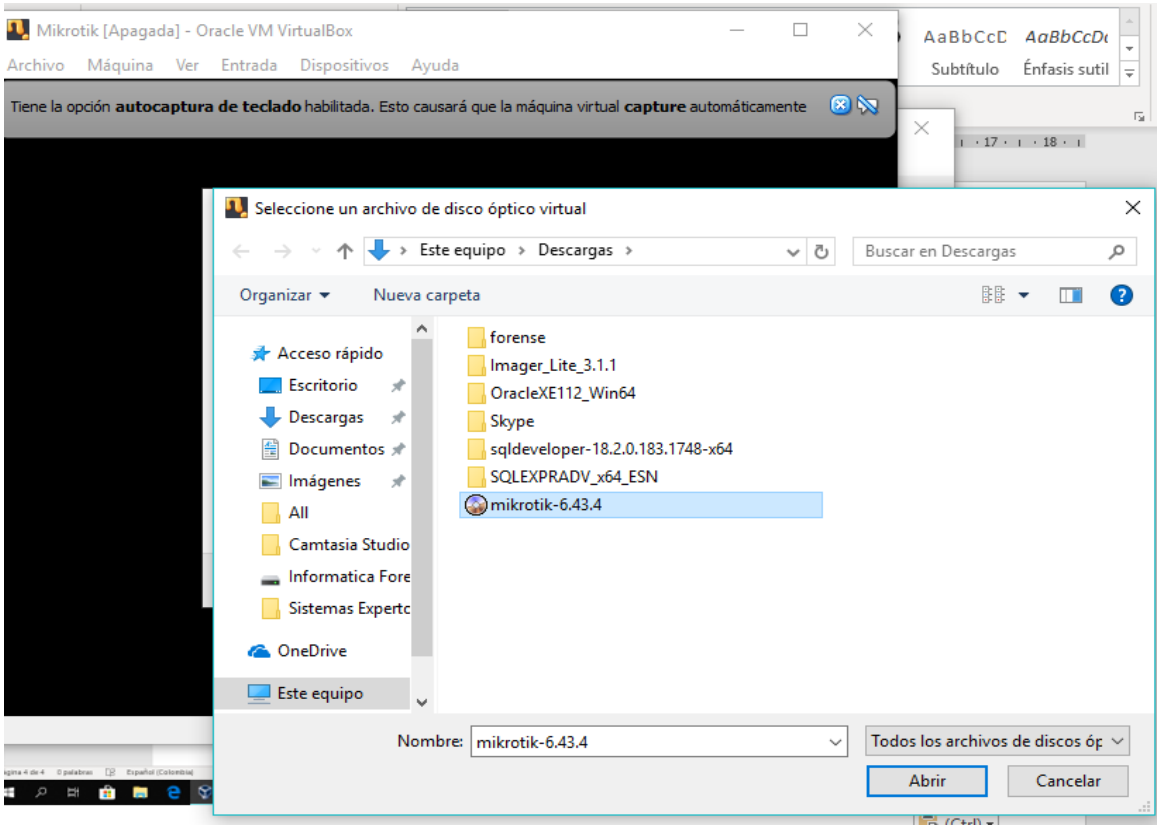


Ilustración 9 Vinculación de máquina virtual con archivo ISO

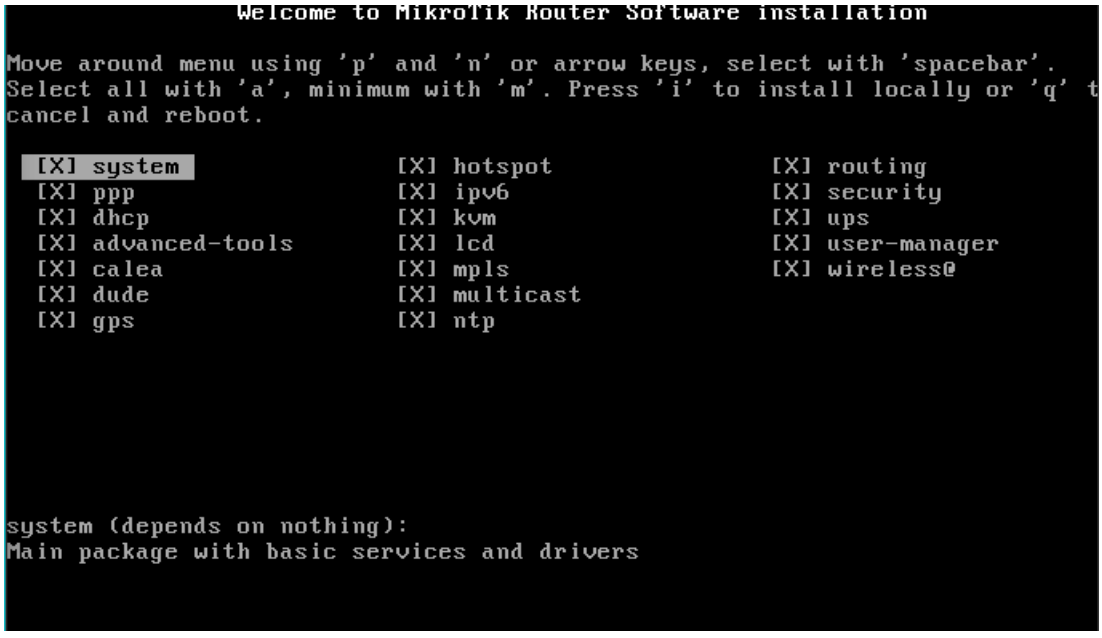


Ilustración 10 Inicio de sistema operativo RouterOS

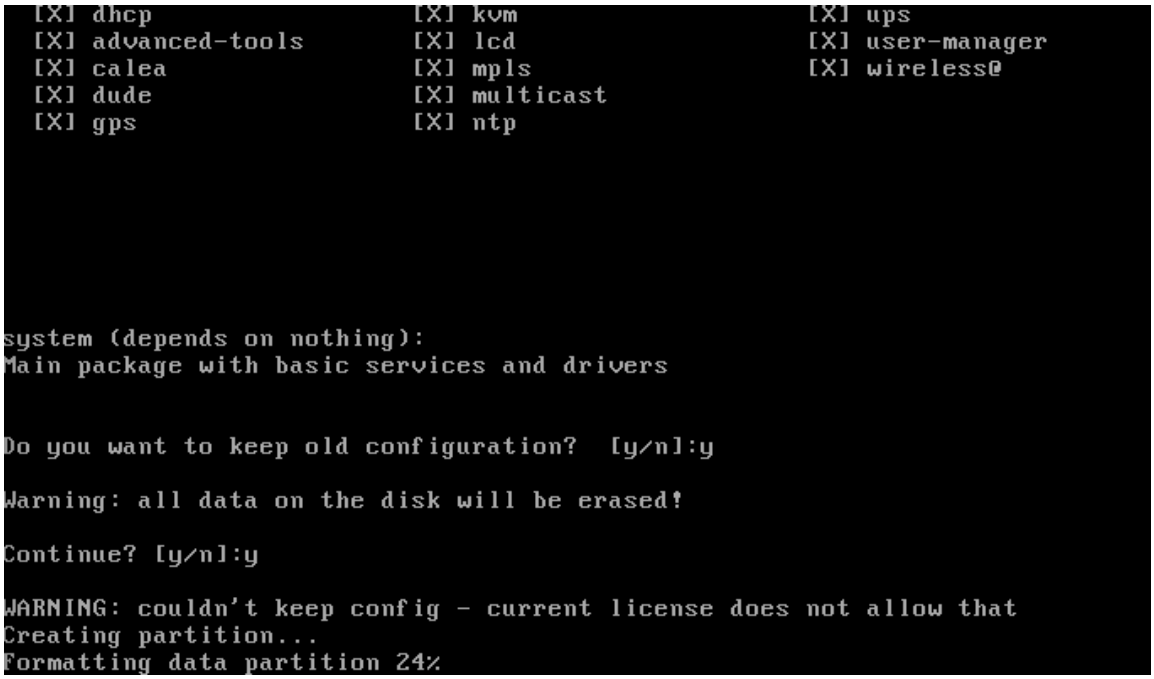


Ilustración 11 Proceso de instalación de sistema operativo RouterOS

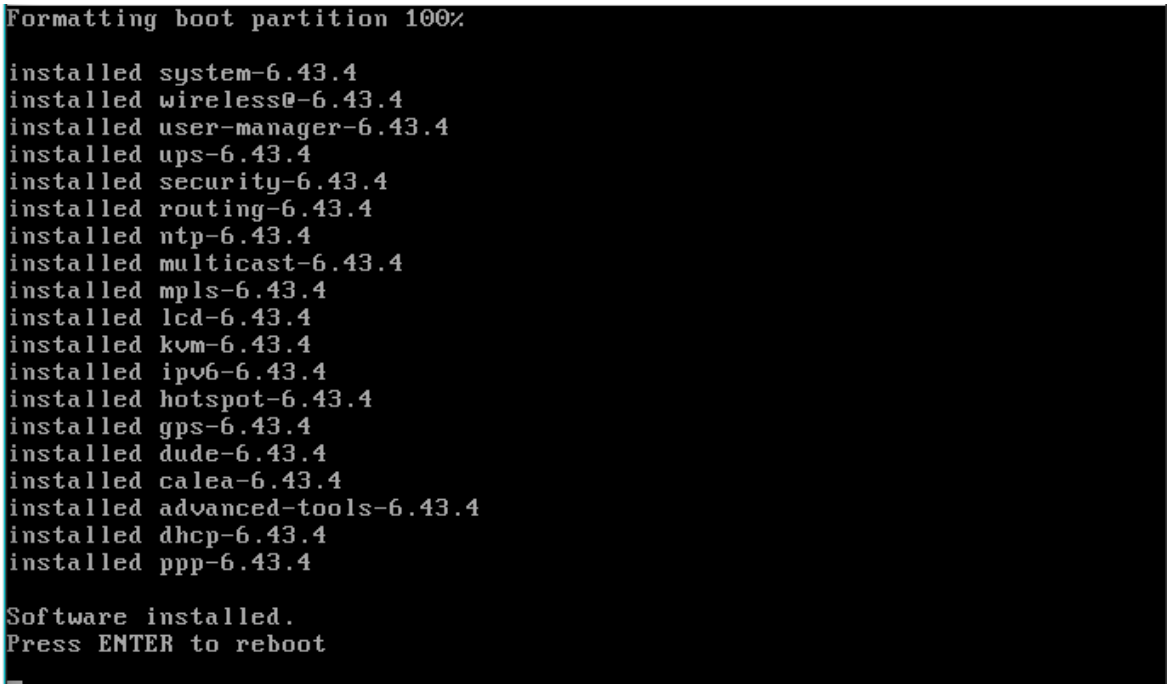


Ilustración 12 Finalización proceso de instalación RouterOS

Ilustración 13 Proceso inicio sistema operativo RouterOS

Ilustración 14 Inicio sistema operativo RouterOS

2. Configuracion Mikrotik Bogotá

La configuracion del Mikrotik correspondiente a la ciudad de bogota, comprende configuraciones como: el acceso a la interfaz grafica desde el aplicativo Winbox, la configuracion de las interfaces de red para la LAN y WAN, la creacion de las VPNs para la conexión desde otras ciudades, la configuracion NAT para dar acceso a internet a la red interna y la creacion de reglas en el firewall para evitar ataques de tipo SSH, Telnet, FTP, denegacion de servicio, web proxy, conexiones no autorizadas, entre otros.

- Configuracion de acceso

Para el acceso al sistema operativo RouerOS de la ciudad de Bogota se debe realizar mediante el componenten grafico de Mikrotik, WinBox, el cual permite tener realizar la administracion del sistema operativo a traves de una interfaz grafica. Esta conexión la realiza mediante la identificacion de la direccion MAC del dispositivo o la direccion IP.

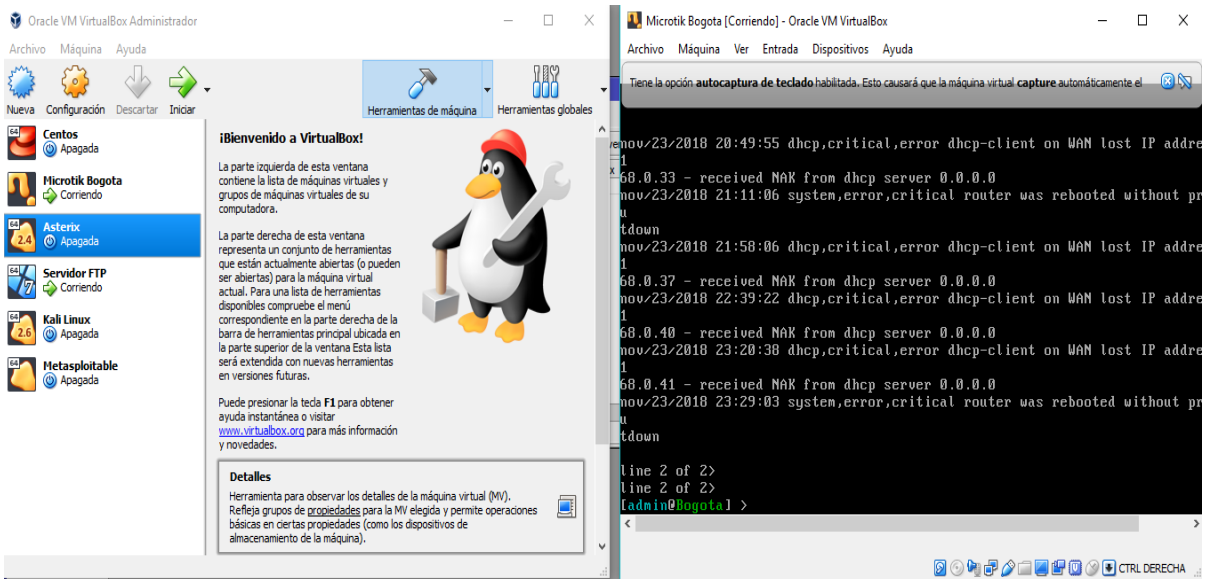


Ilustración 15 Inicio máquina virtual Mikrotik Bogotá

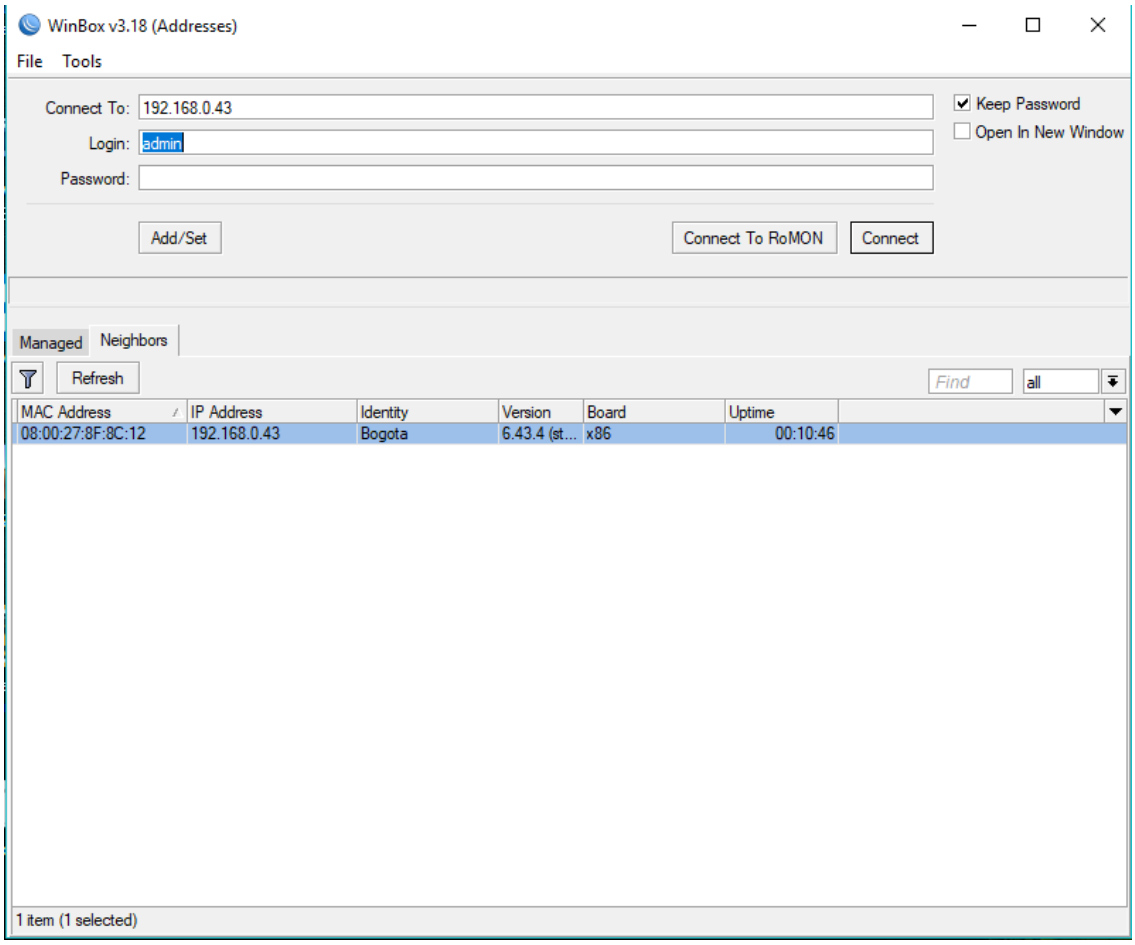


Ilustración 16 Acceso a RouterOS mediante WinBox

- Configuracion de interfaces

A traves de la opcion “Interface” proporcionado por el WinBox, se establece la configuracion de red para la tarjeta LAN la cual permite la comunicación de la red interna con el Mikrotik, y asigna los parametros de conexión para la tarjeta WAN, la cual va a permitir la salida hacia internet.

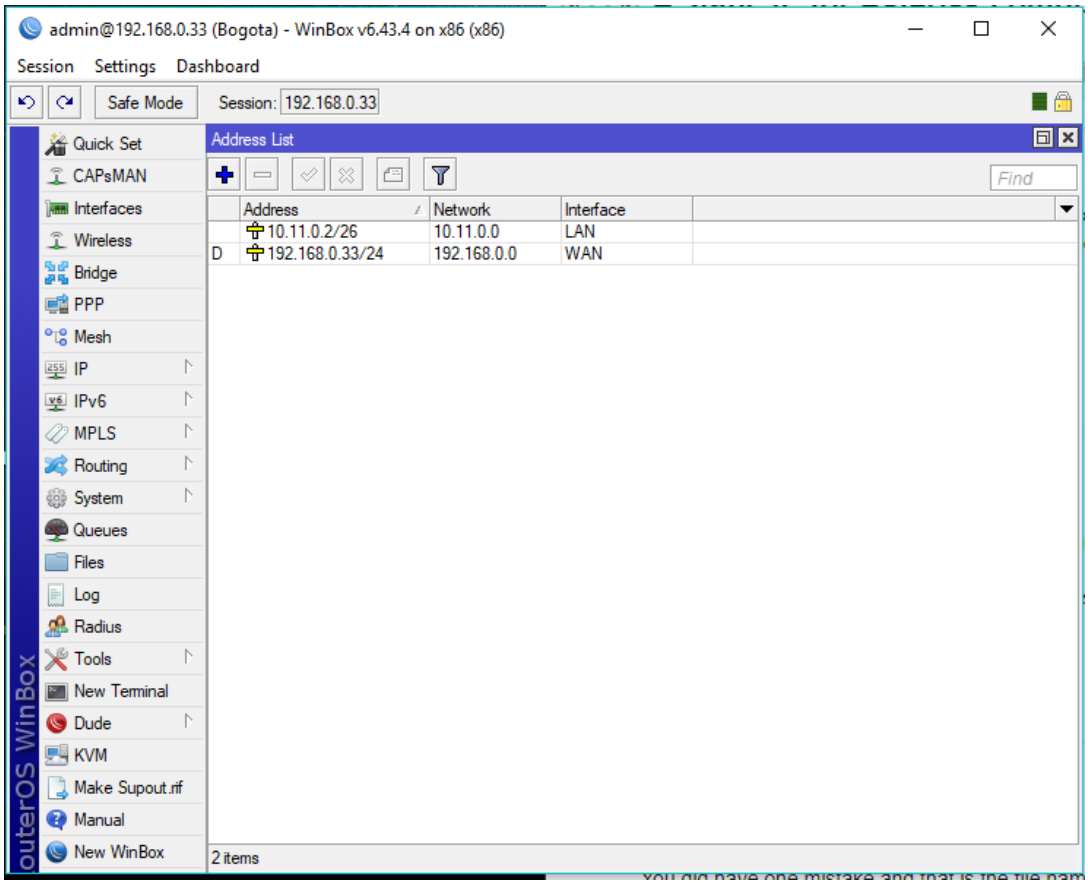


Ilustración 17 Configuración de interfaces de LAN y WAN

- Configuración de VPN

Mediante la opción “PPP”, WinBox permite la creación de las credenciales con las cuales los usuarios de las ciudades de Cali, Medellín y Bucaramanga, se conectarán a los recursos que se encuentra centralizados en la ciudad de Bogotá.

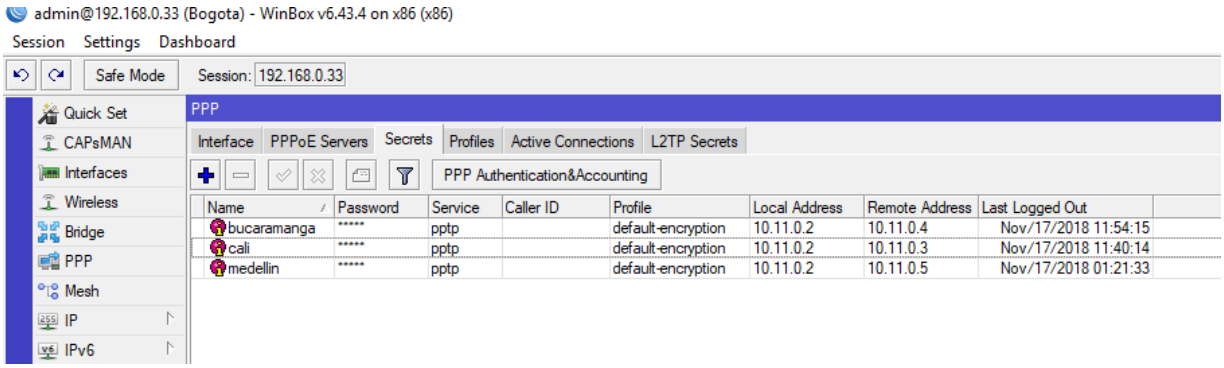


Ilustración 18 Configuración VPN por ciudad

- Configuración NAT

La utilidad “Firewall”, internamente, trae consigo la configuración de NAT la cual permite que los usuarios de la red interna tengan acceso a internet.

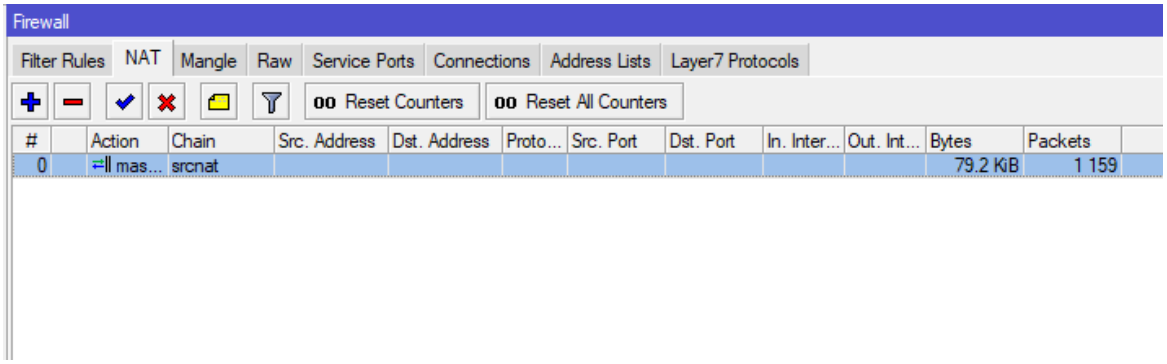


Ilustración 19 Configuración NAT

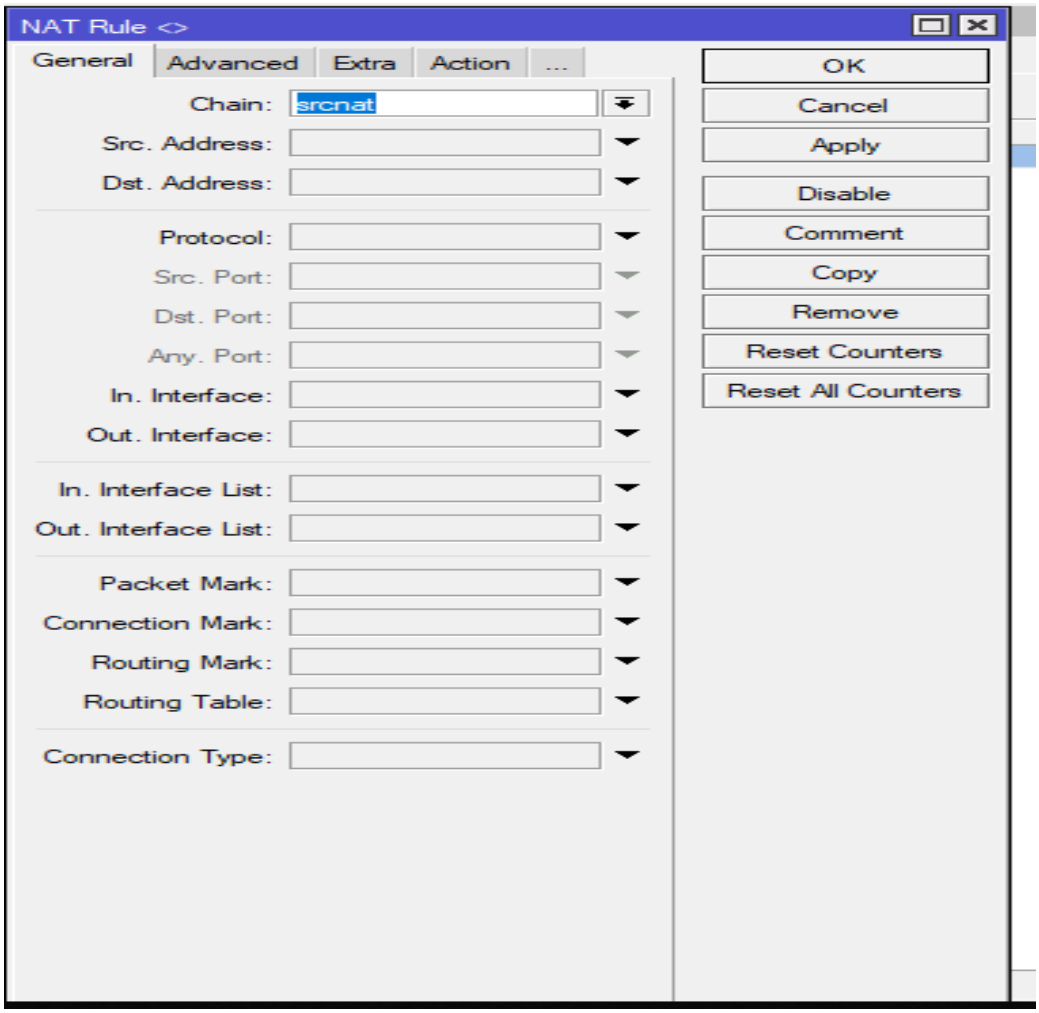


Ilustración 20 Configuración general NAT

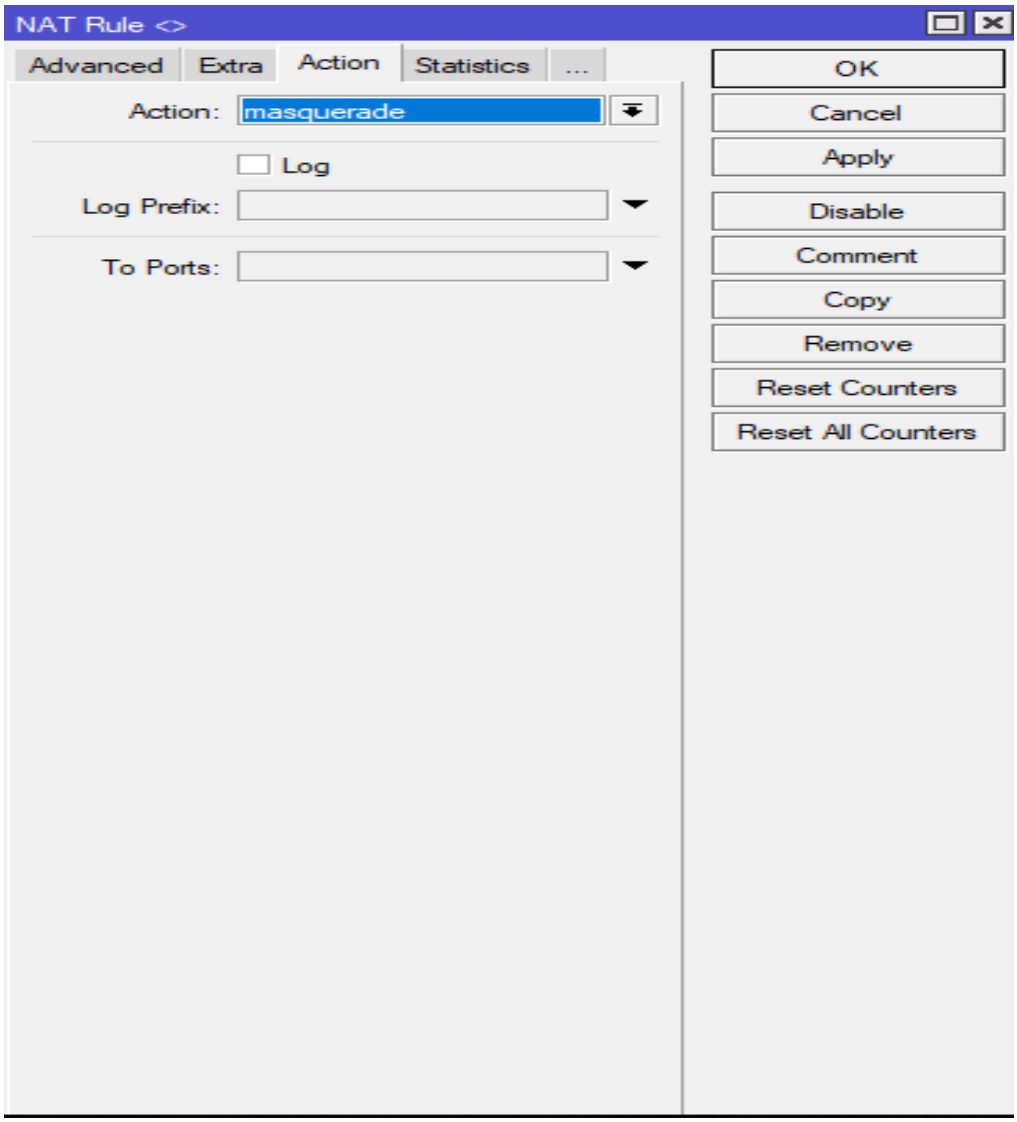
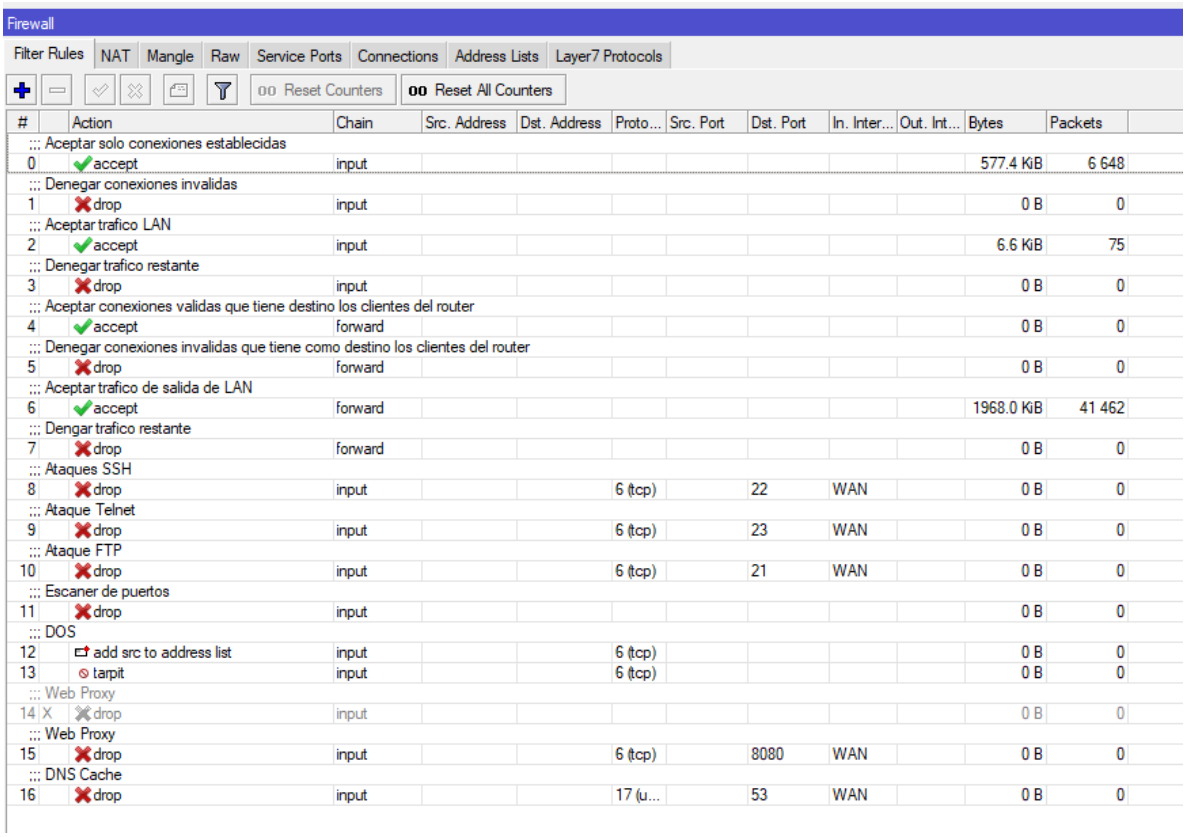


Ilustración 21 Configuración de acción del NAT

- Configuración de políticas del firewall

El sistema operativo RouterOS, permite la creación de políticas y regla de firewall con la cual se pueden prevenir diversos ataques cibernéticos como SSH, Telnet, FTP, escaneo de puertos, ataques DoS, web proxy y DNS cache, asi como la denegación de conexión invalidas y la aceptación o rechazo del trafico de red proveniente o saliente de la red LAN o WAN.



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Aceptar solo conexiones establecidas											
0	accept	input								577.4 KiB	6 648
;;; Denegar conexiones invalidas											
1	drop	input								0 B	0
;;; Aceptar trafico LAN											
2	accept	input								6.6 KiB	75
;;; Denegar trafico restante											
3	drop	input								0 B	0
;;; Aceptar conexiones validas que tiene destino los clientes del router											
4	accept	forward								0 B	0
;;; Denegar conexiones invalidas que tiene como destino los clientes del router											
5	drop	forward								0 B	0
;;; Aceptar trafico de salida de LAN											
6	accept	forward								1968.0 KiB	41 462
;;; Dengar trafico restante											
7	drop	forward								0 B	0
;;; Ataques SSH											
8	drop	input			6 (tcp)		22	WAN		0 B	0
;;; Ataque Telnet											
9	drop	input			6 (tcp)		23	WAN		0 B	0
;;; Ataque FTP											
10	drop	input			6 (tcp)		21	WAN		0 B	0
;;; Escaner de puertos											
11	drop	input								0 B	0
;;; DOS											
12	add src to address list	input			6 (tcp)					0 B	0
13	tarpit	input			6 (tcp)					0 B	0
;;; Web Proxy											
14 X	drop	input								0 B	0
;;; Web Proxy											
15	drop	input			6 (tcp)		8080	WAN		0 B	0
;;; DNS Cache											
16	drop	input			17 (u...		53	WAN		0 B	0

Ilustración 22 Configuración de políticas del firewall

- Ejemplo de la configuración de un equipo cliente ubicado en la ciudad de Bogotá.

  A través de la siguiente imagen, se muestra un ejemplo de la configuración de red de un equipo cliente ubicado en la ciudad de Bogotá.

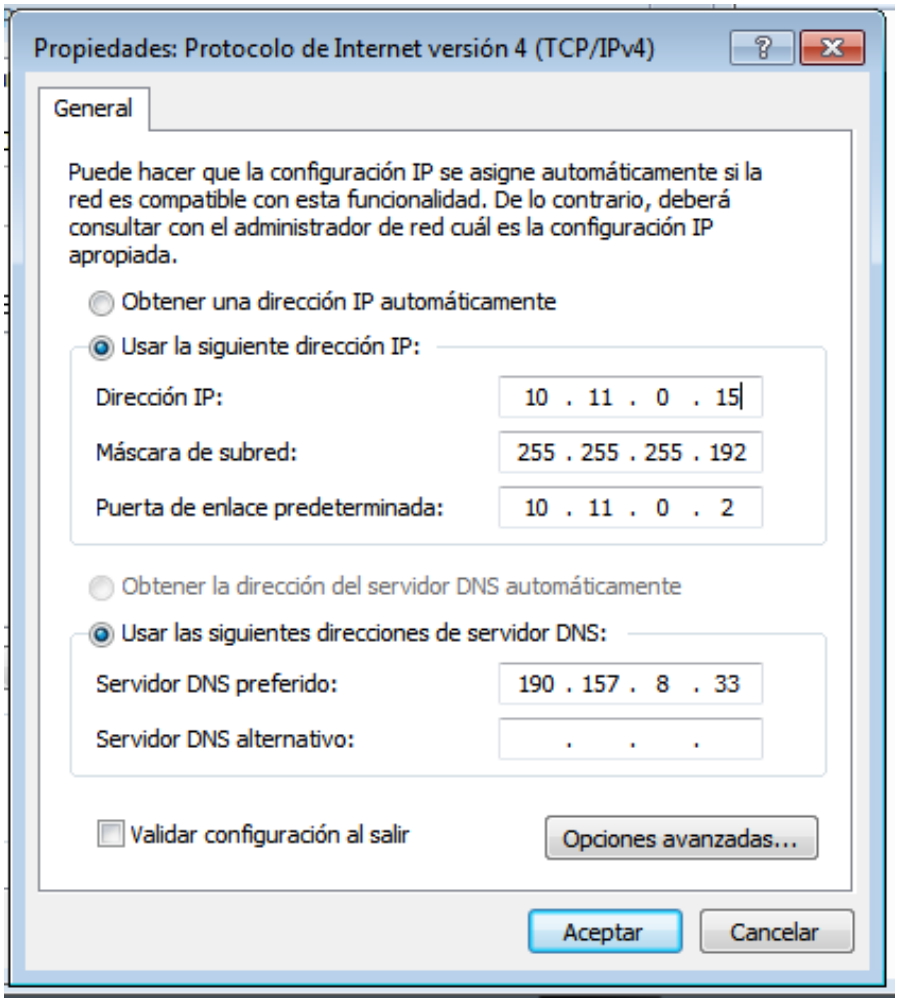


Ilustración 23 Configuración equipo cliente sede Bogotá

- Interfaz de conexión de VPN por ciudad

Una vez establecidas las debidas configuraciones de VPN, los usuarios de las ciudades de Medellín, Cali y Bucaramanga pueden realizar el acceso a los recursos ubicados en la ciudad de Bogotá. En el momento en el que se genera la conexión, el WinBox muestra la conexión establecida realizada a través de la VPN.

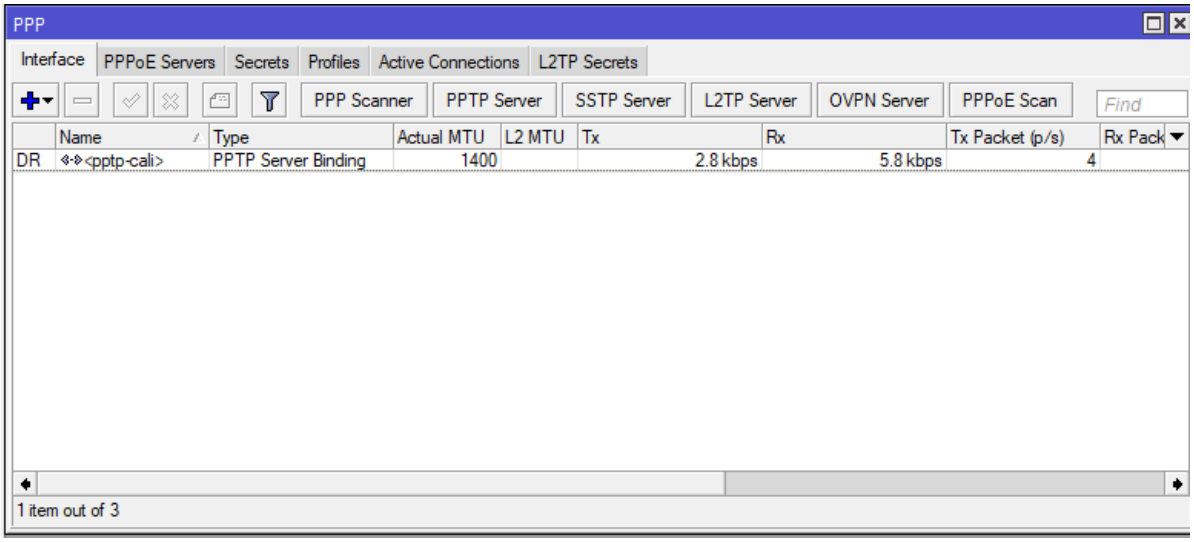


Ilustración 24 Conexión VPN sede Cali

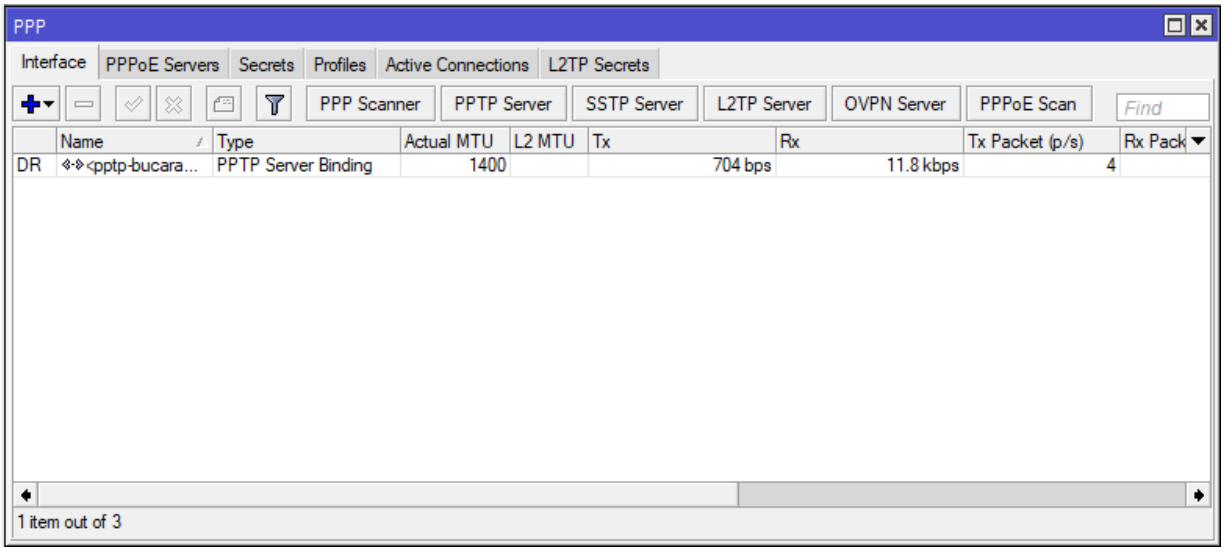


Ilustración 25 Conexión VPN sede Bucaramanga

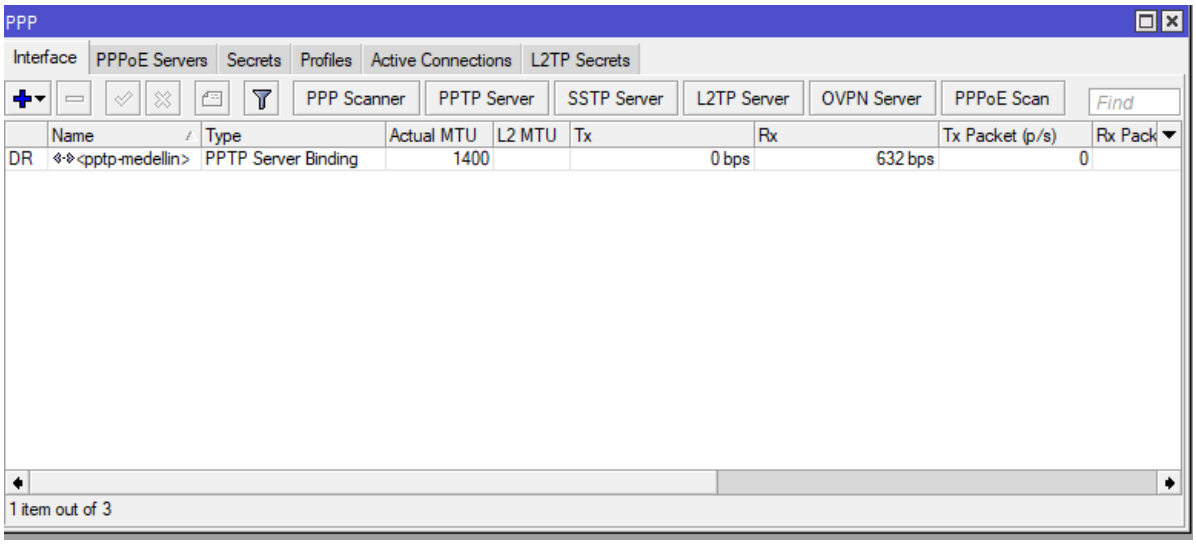


Ilustración 26 Conexión VPN sede Medellín

3. Configuracion Mikrotik Cali

La configuracion del Mikrotik correspondiente a la ciudad de Cali, comprende configuraciones como: el acceso a la interfaz grafica desde el aplicativo Winbox, la configuracion de las interfaces de red para la LAN y WAN, la creacion de las VPNs para la conexión desde otras ciudades, la configuracion NAT para dar acceso a internet a la red interna y la creacion de reglas en el firewall para evitar ataques de tipo SSH, Telnet, FTP, denegacion de servicio, web proxy, conexiones no autorizadas, entre otros.

- Configuracion de acceso

Para el acceso al sistema operativo RouerOS de la ciudad de Cali se debe realizar mediante el componenten grafico de Mikrotik, WinBox, el cual permite tener realizar la administracion del sistema operativo a traves de una interfaz grafica. Esta conexión la realiza mediante la identificacion de la direccion MAC del dispositivo o la direccion IP.

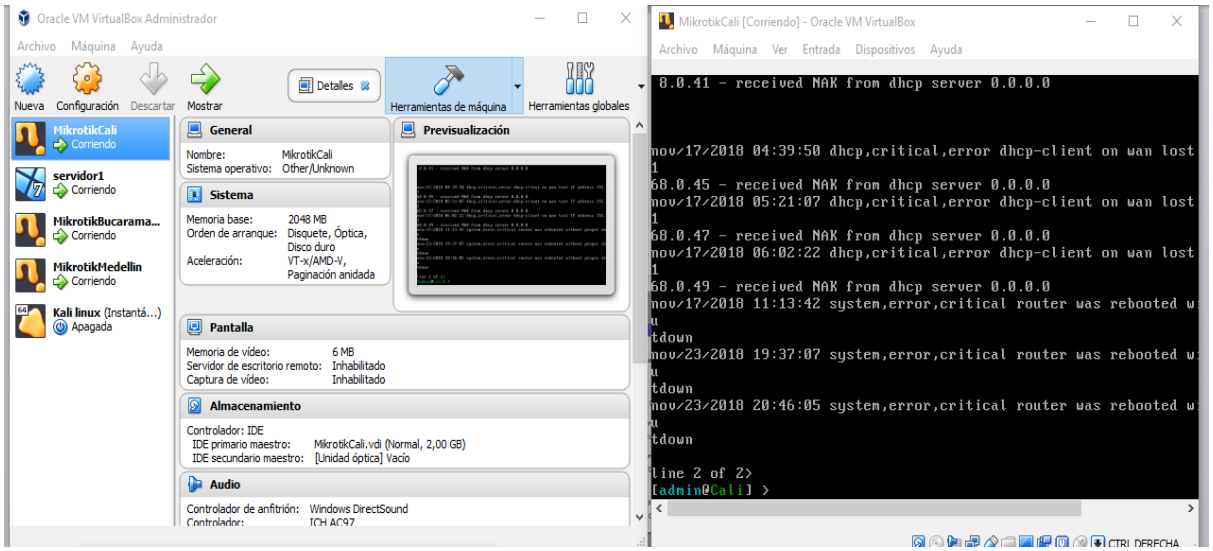


Ilustración 27 Inicio máquina virtual Mikrotik Cali

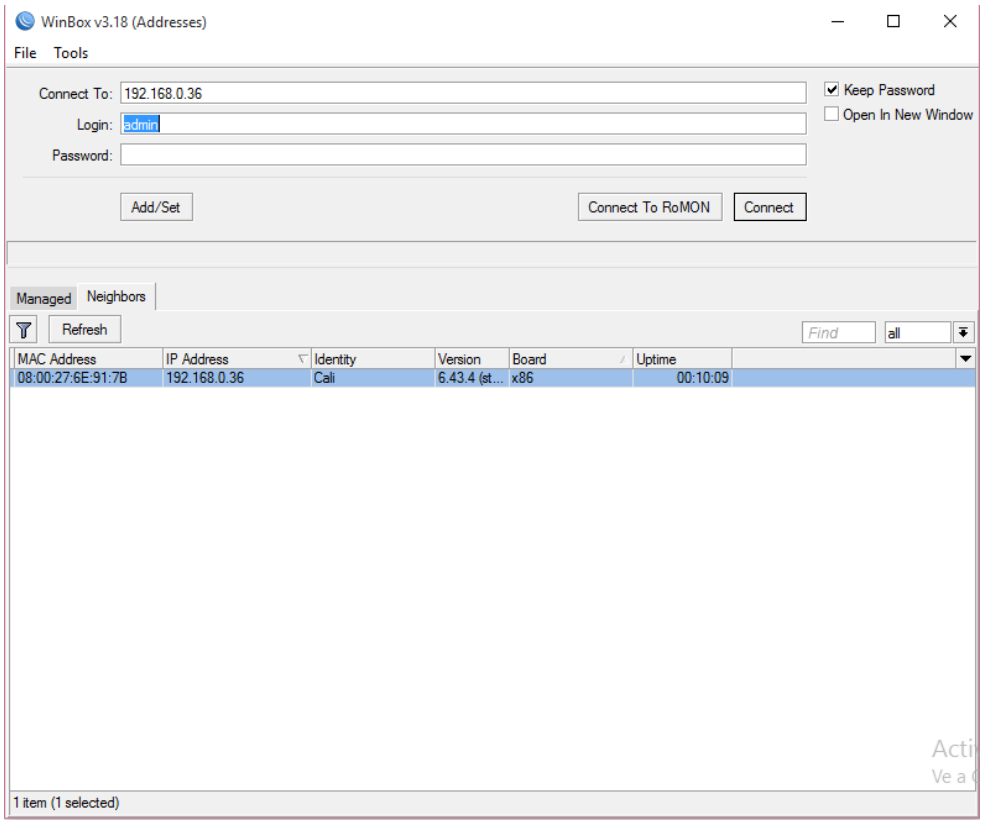


Ilustración 28 Inicio WinBox Mikrotik Cali

- Configuración de interfaces

A traves de la opcion “Interface” proporcionado por el WinBox, se establece la configuracion de red para la tarjeta LAN la cual permite la comunicación de la red interna con el Mikrotik, y asigna los parametros de conexión para la tarjeta WAN, la cual va a permitir la salida hacia internet.

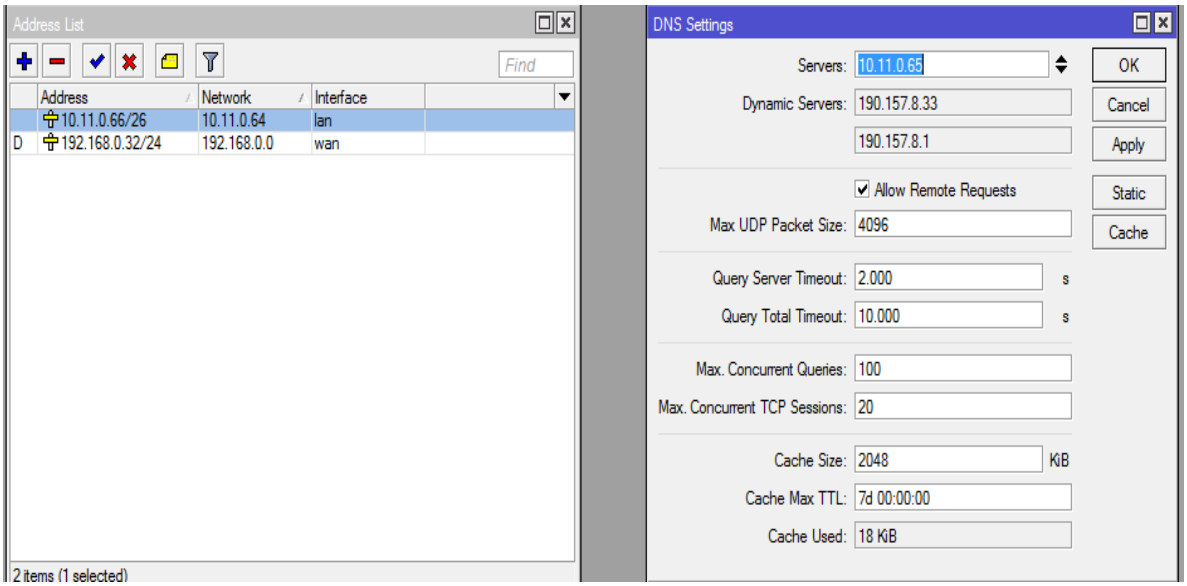


Ilustración 29 Configuración interface Mikrotik Cali

- Configuración NAT

La utilidad “Firewall”, internamente, trae consigo la configuración de NAT la cual permite que los usuarios de la red interna tengan acceso a internet.

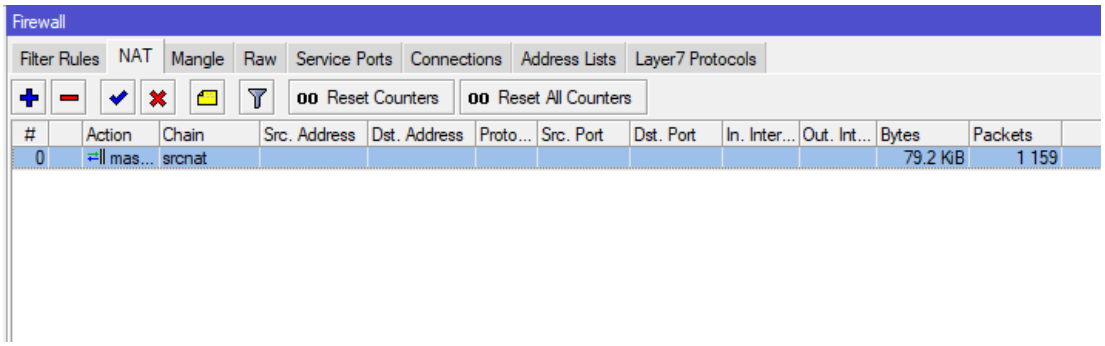


Ilustración 30 Configuración NAT

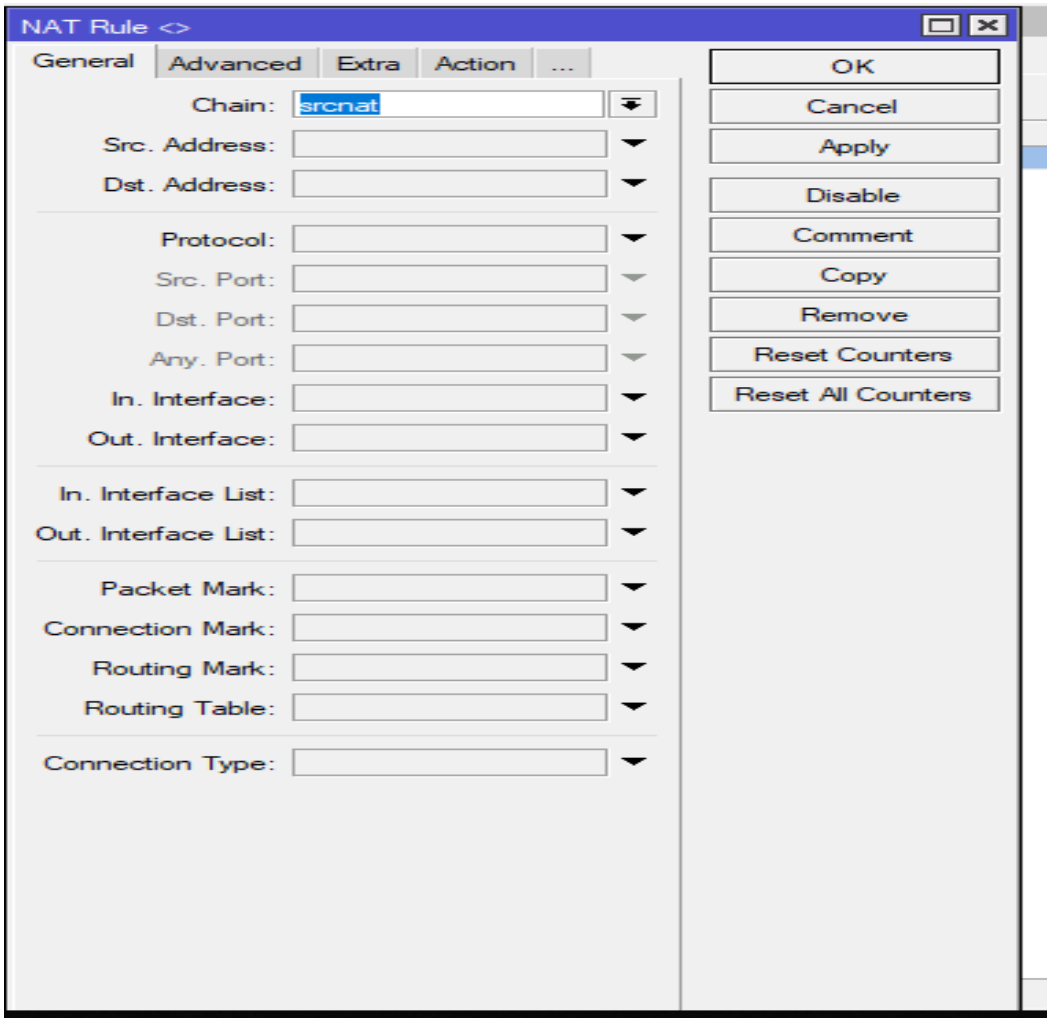


Ilustración 31 Configuración general NAT

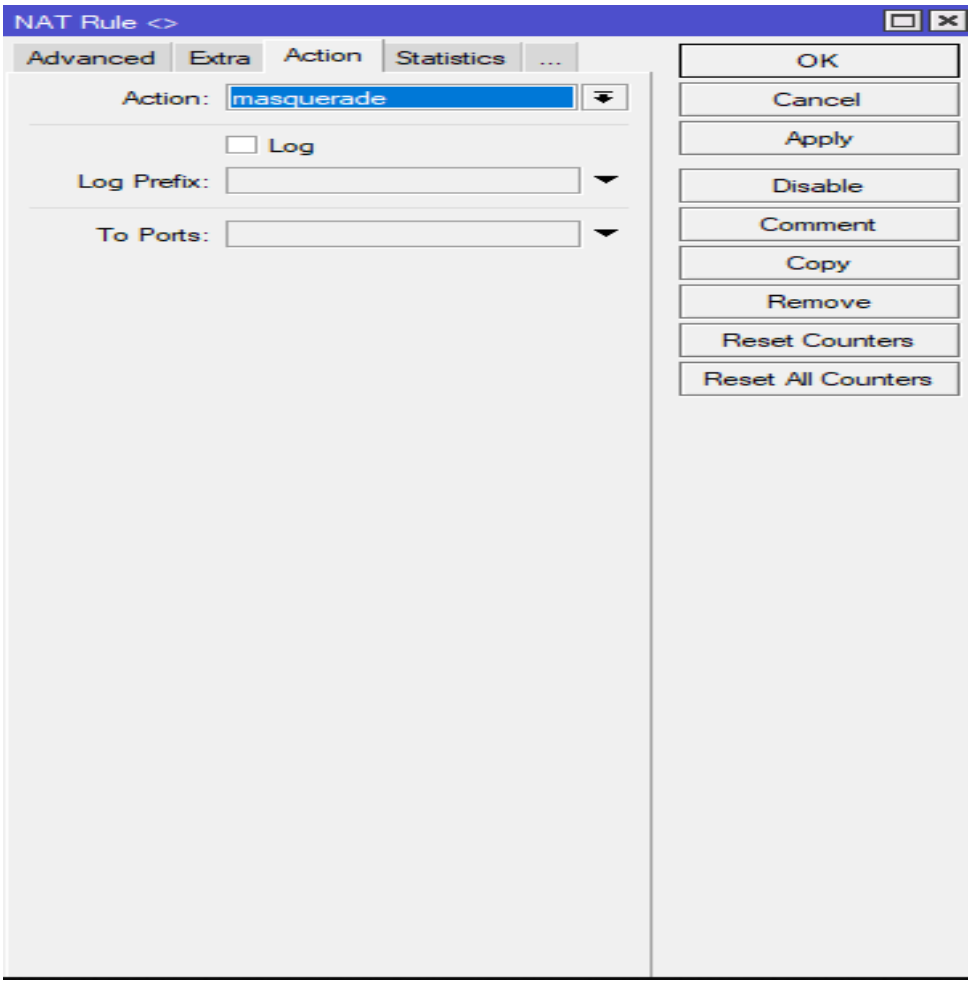
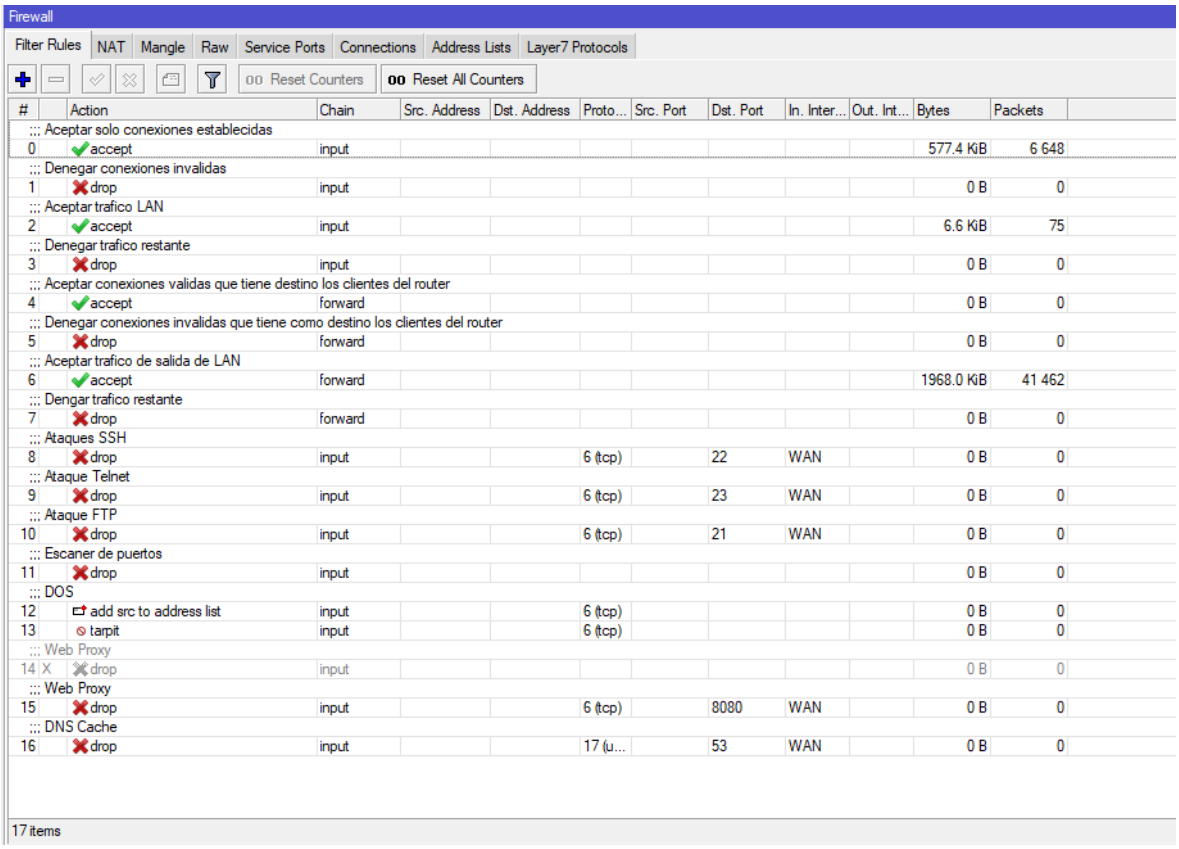


Ilustración 32 Configuración acción NAT

- Configuración Firewall

El sistema operativo RouterOS, permite la creación de políticas y regla de firewall con la cual se pueden prevenir diversos ataques cibernéticos como SSH, Telnet, FTP, escaneo de puertos, ataques DoS, web proxy y DNS cache, así como la denegación de conexión invalidas y la aceptación o rechazo del tráfico de red proveniente o saliente de la red LAN o WAN



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Aceptar solo conexiones establecidas											
0	accept	input								577.4 KiB	6 648
;;; Denegar conexiones invalidas											
1	drop	input								0 B	0
;;; Aceptar trafico LAN											
2	accept	input								6.6 KiB	75
;;; Denegar trafico restante											
3	drop	input								0 B	0
;;; Aceptar conexiones validas que tiene destino los clientes del router											
4	accept	forward								0 B	0
;;; Denegar conexiones invalidas que tiene como destino los clientes del router											
5	drop	forward								0 B	0
;;; Aceptar trafico de salida de LAN											
6	accept	forward								1968.0 KiB	41 462
;;; Dengar trafico restante											
7	drop	forward								0 B	0
;;; Ataques SSH											
8	drop	input			6 (tcp)		22	WAN		0 B	0
;;; Ataque Telnet											
9	drop	input			6 (tcp)		23	WAN		0 B	0
;;; Ataque FTP											
10	drop	input			6 (tcp)		21	WAN		0 B	0
;;; Escaner de puertos											
11	drop	input								0 B	0
;;; DOS											
12	add src to address list	input			6 (tcp)					0 B	0
13	tarpit	input			6 (tcp)					0 B	0
;;; Web Proxy											
14 X	drop	input								0 B	0
;;; Web Proxy											
15	drop	input			6 (tcp)		8080	WAN		0 B	0
;;; DNS Cache											
16	drop	input			17 (u...		53	WAN		0 B	0

Ilustración 33 Configuración firewall Mikrotik Cali

- Ejemplo de la configuración de un equipo cliente ubicado en la ciudad de Cali.

A través de la siguiente imagen, se muestra un ejemplo de la configuración de red de un equipo cliente ubicado en la ciudad de Cali.

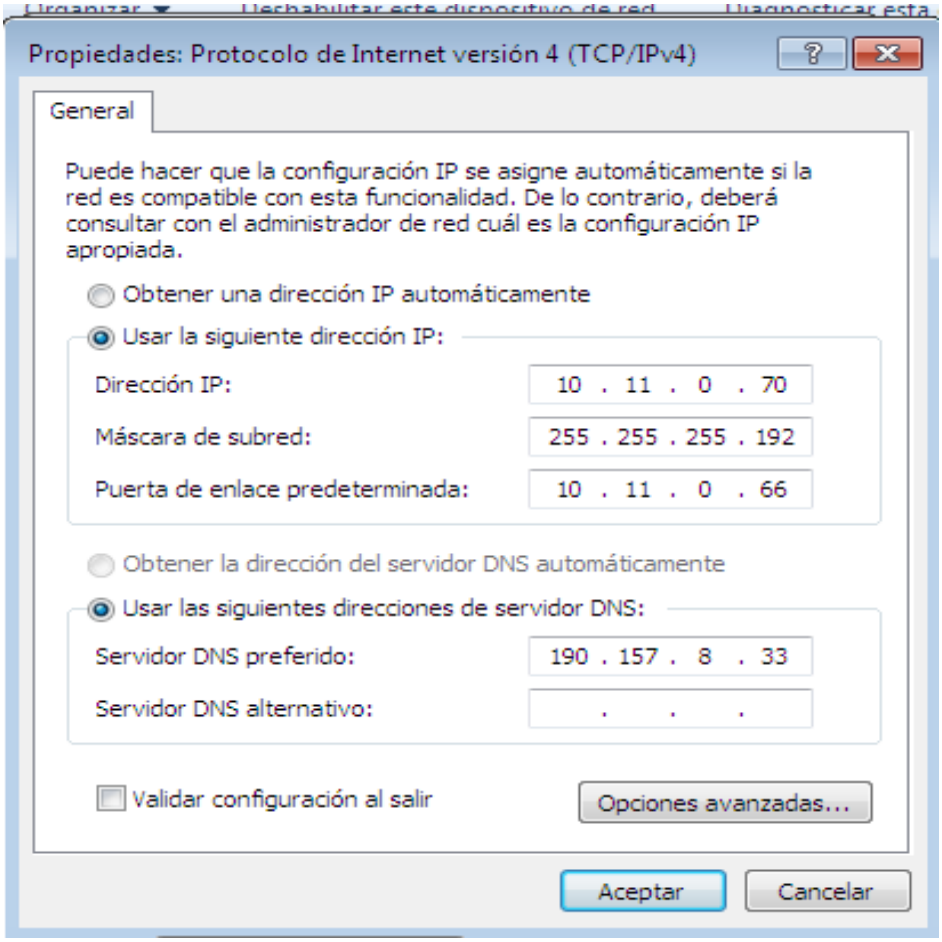


Ilustración 34 Configuración tarjeta red equipo clientes ubicado en la ciudad de Cali

- Conexión a la VPN desde equipo cliente en la sede de Cali

Windows, incorpora una utilidad de configuración de VPN, en el cual, mediante la utilización de la IP pública del Mikrotik y las credenciales creadas en el dispositivo de Bogotá, los usuarios pueden acceder a los recursos alojados allí.

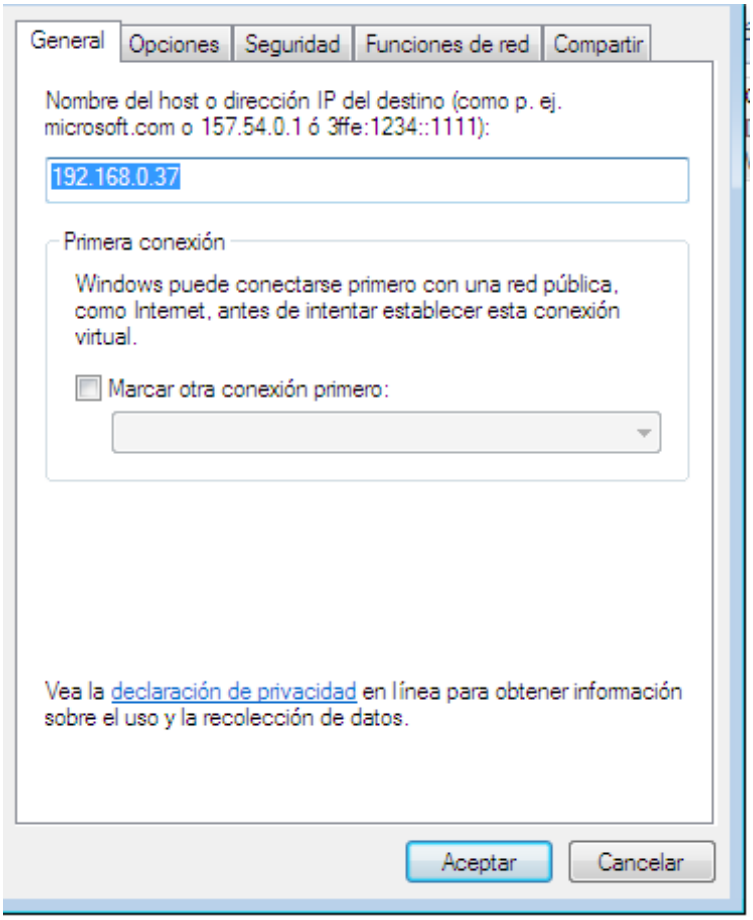


Ilustración 35 Solicitud de IP publica Mikrotik Bogotá

Ilustración 36 Ingreso de credenciales para la conexión de usuario de Cali

- Comprobación de conexión por VPN a través de la ejecución del comando ping

Una vez realizada el acceso a los recursos de la ciudad de Bogotá mediante VPN, se comprueba la conexión al servidor web, de telefonía, FTP y aplicativa de gestión a través del comando ping ejecutado desde la maquina cliente ubicada en la ciudad de Cali.

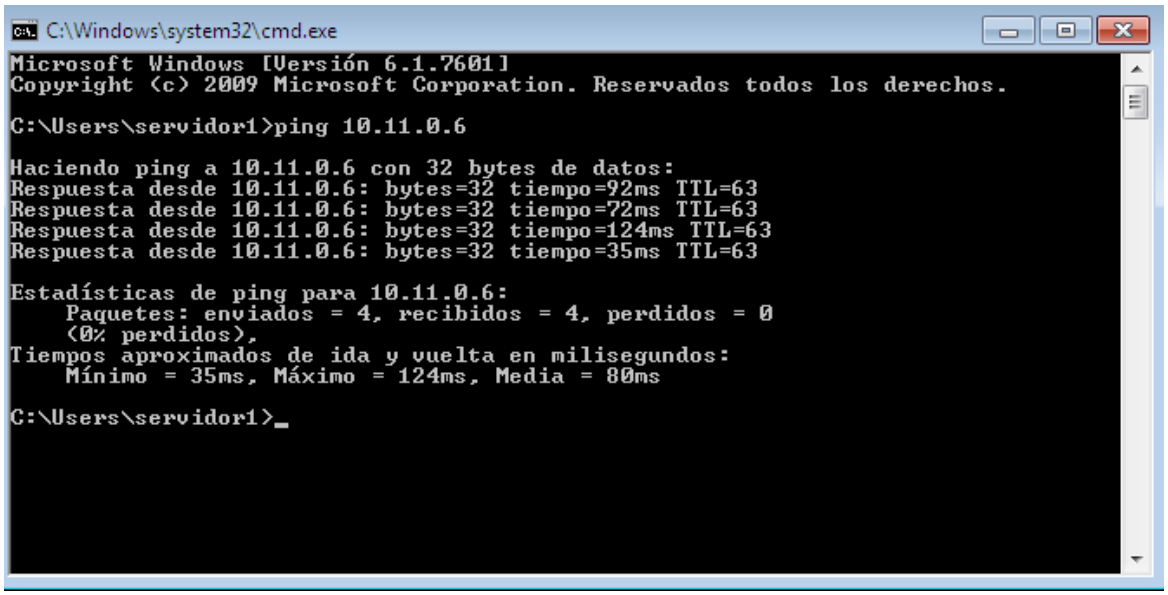


Ilustración 37 Ping servidor web

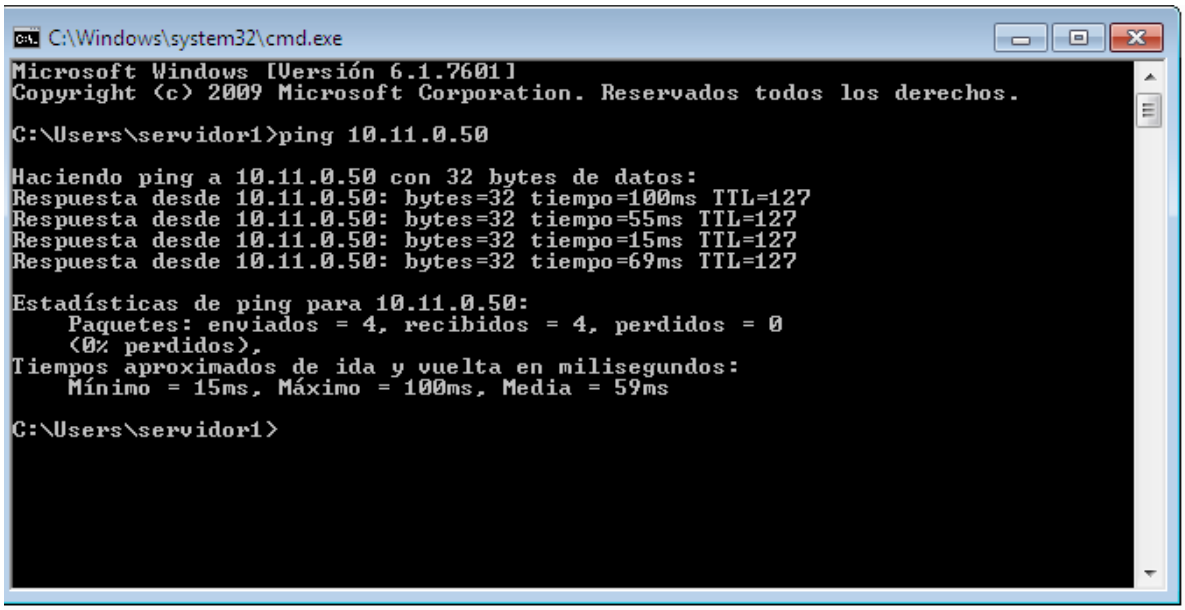


Ilustración 38 Ping servidor FTP

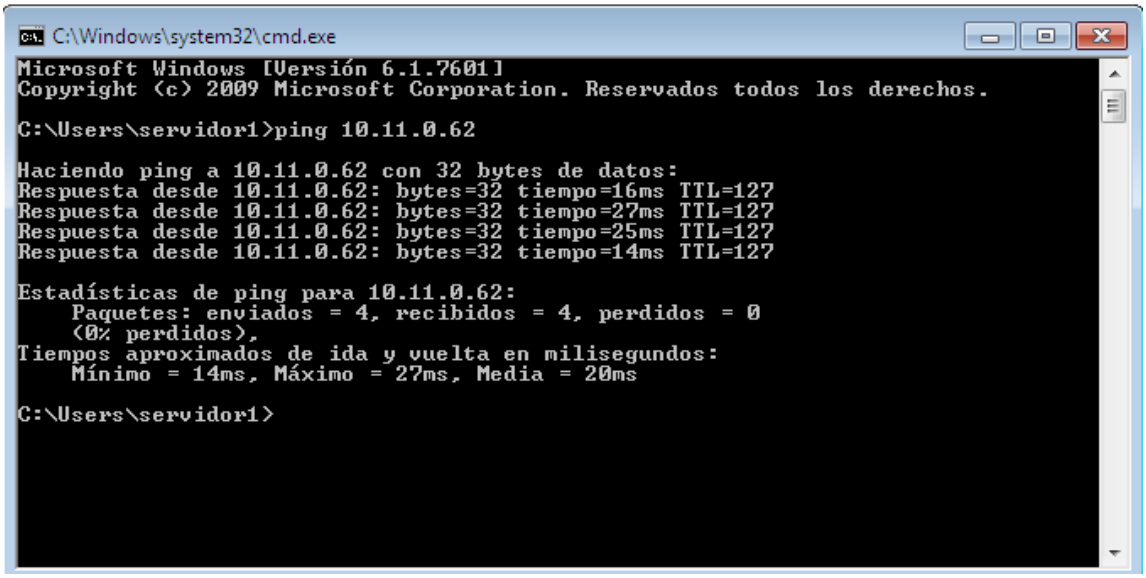


Ilustración 39 Ping servidor de telefonía

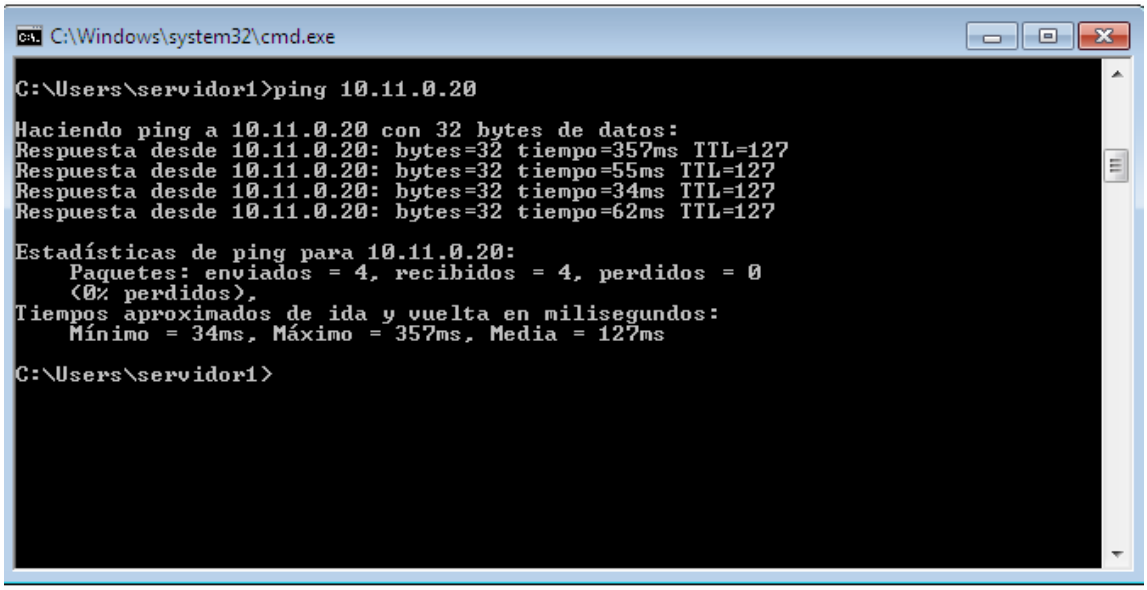


Ilustración 40 Ping servidor aplicativo de gestión

4. Configuracion Mikrotik Bucaramanga

La configuracion del Mikrotik correspondiente a la ciudad de Bucaramanga, comprende configuraciones como: el acceso a la interfaz grafica desde el aplicativo Winbox, la configuracion de las interfaces de red para la LAN y WAN, la creacion de las VPNs para la conexión desde otras ciudades, la configuracion NAT para dar acceso a internet a la red interna y la creacion de reglas en el firewall para evitar ataques de tipo SSH, Telnet, FTP, denegacion de servicio, web proxy, conexiones no autorizadas, entre otros.

- Configuracion de acceso

Para el acceso al sistema operativo RouerOS de la ciudad de Bucaramanga se debe realizar mediante el componenten grafico de Mikrotik, WinBox, el cual permite tener realizar la administracion del sistema operativo a traves de una interfaz grafica. Esta conexión la realiza mediante la identificacion de la direccion MAC del dispositivo o la direccion IP.

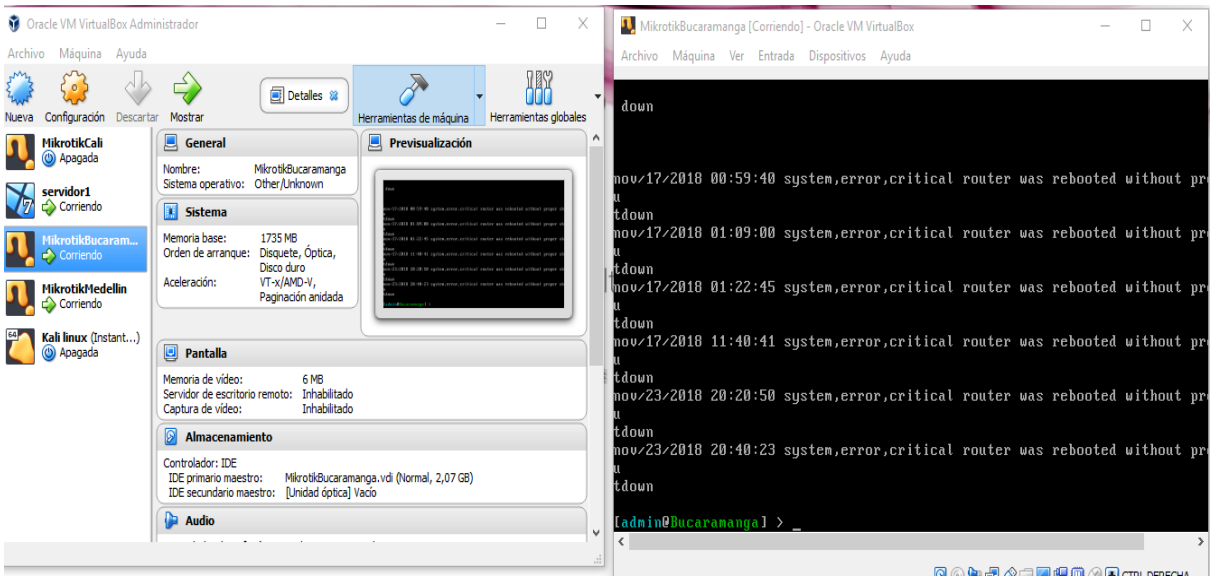


Ilustración 41 Inicio máquina virtual Mikrotik Bucaramanga

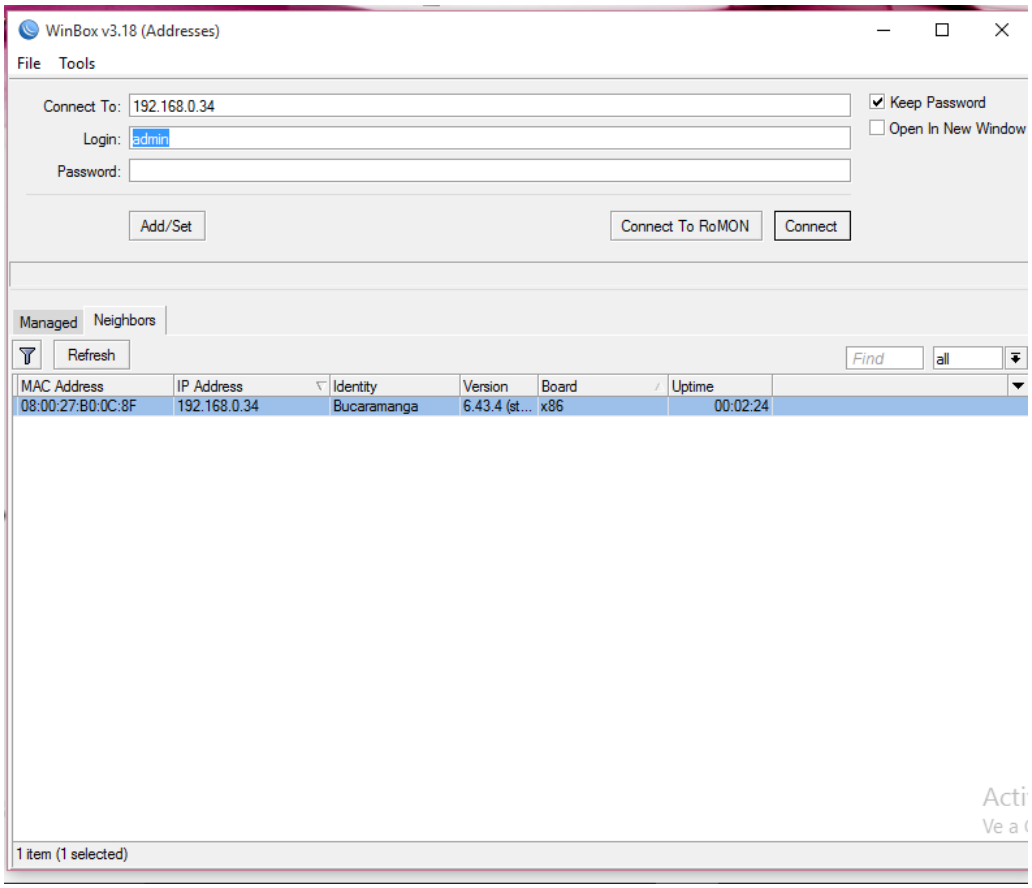


Ilustración 42 Inicio WinBox Mikrotik Bucaramanga

- Configuración de interfaces

A traves de la opcion “Interface” proporcionado por el WinBox, se establece la configuracion de red para la tarjeta LAN la cual permite la comunicación de la red interna con el Mikrotik, y asigna los parametros de conexión para la tarjeta WAN, la cual va a permitir la salida hacia internet.

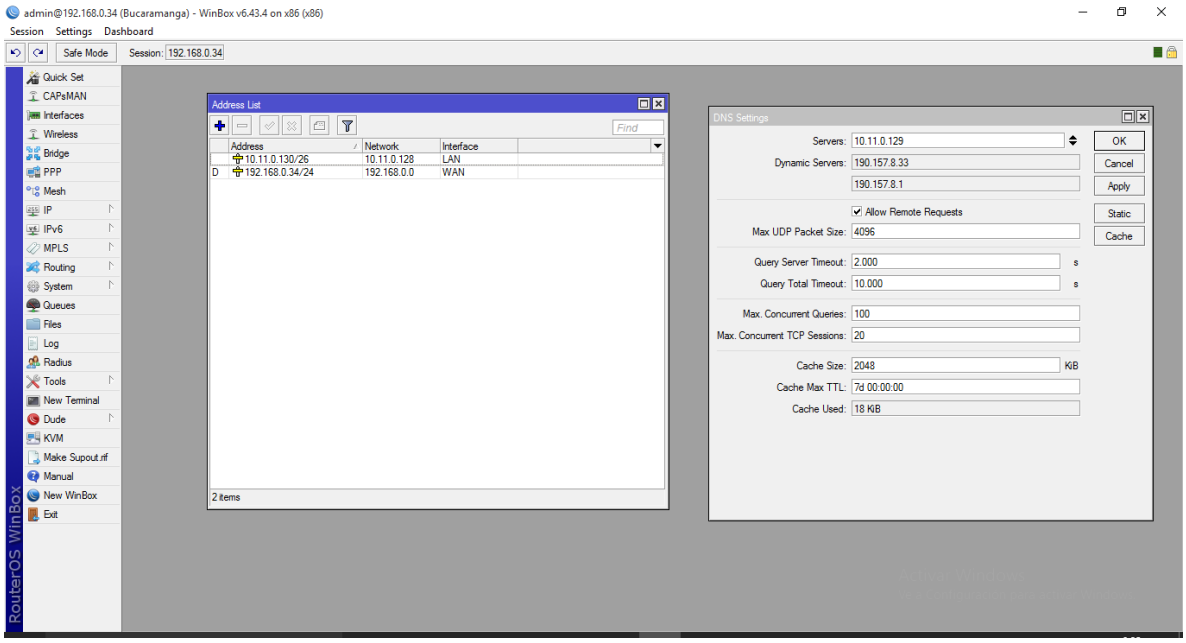


Ilustración 43 Configuración interfaces Mikrotik Bucaramanga

- Configuración NAT

La utilidad “Firewall”, internamente, trae consigo la configuración de NAT la cual permite que los usuarios de la red interna tengan acceso a internet.

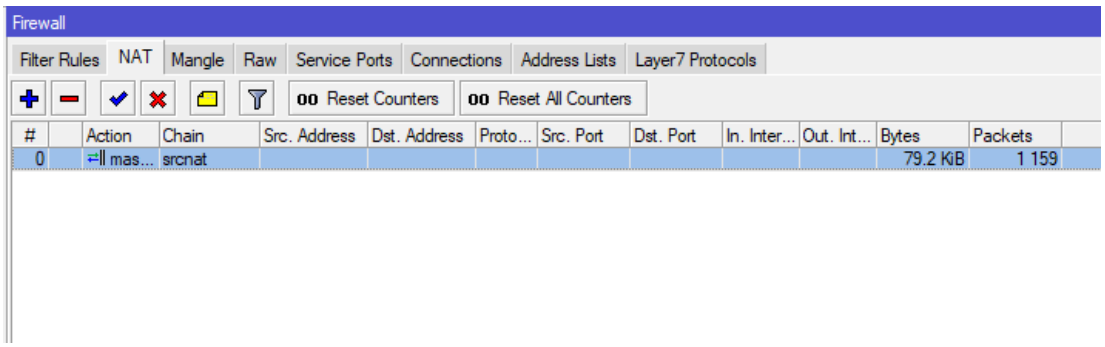


Ilustración 44 Configuración NAT

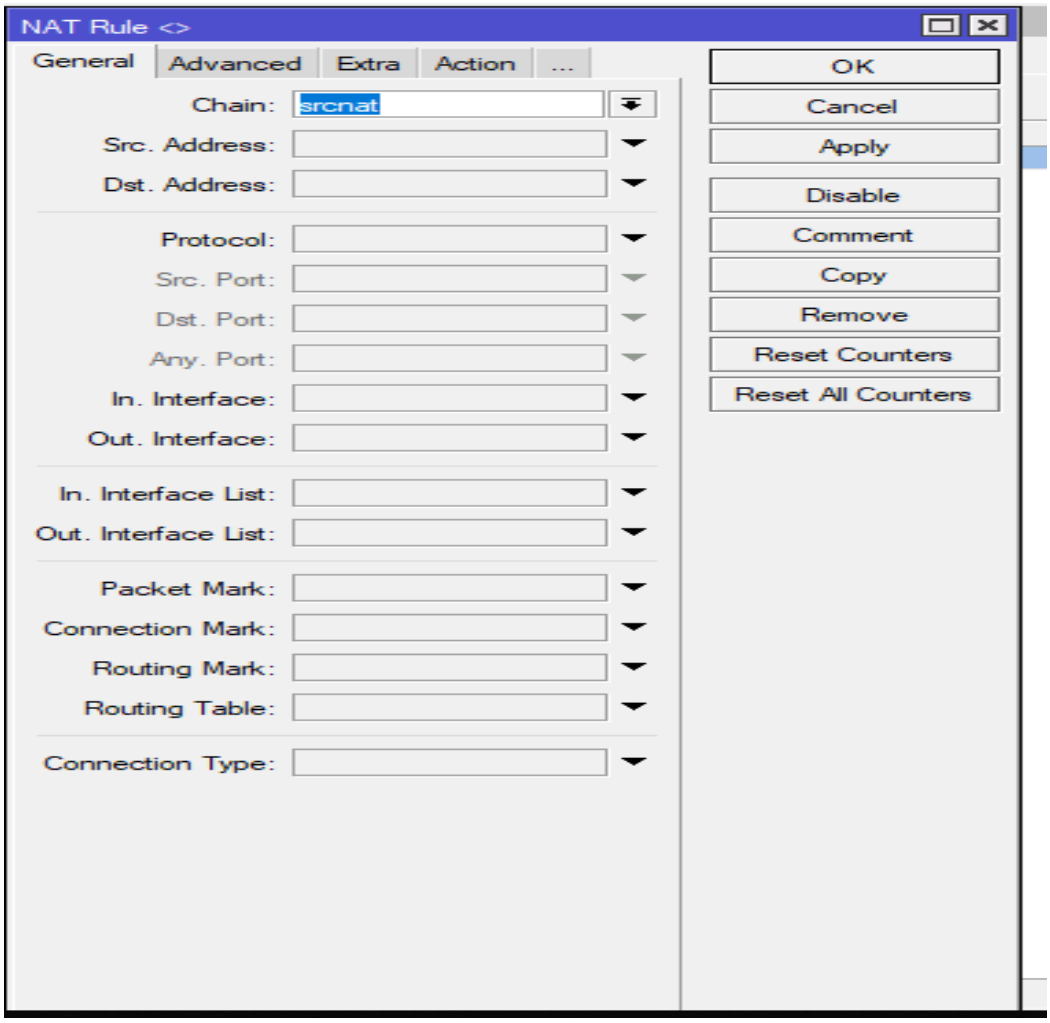


Ilustración 45 Configuración general NAT

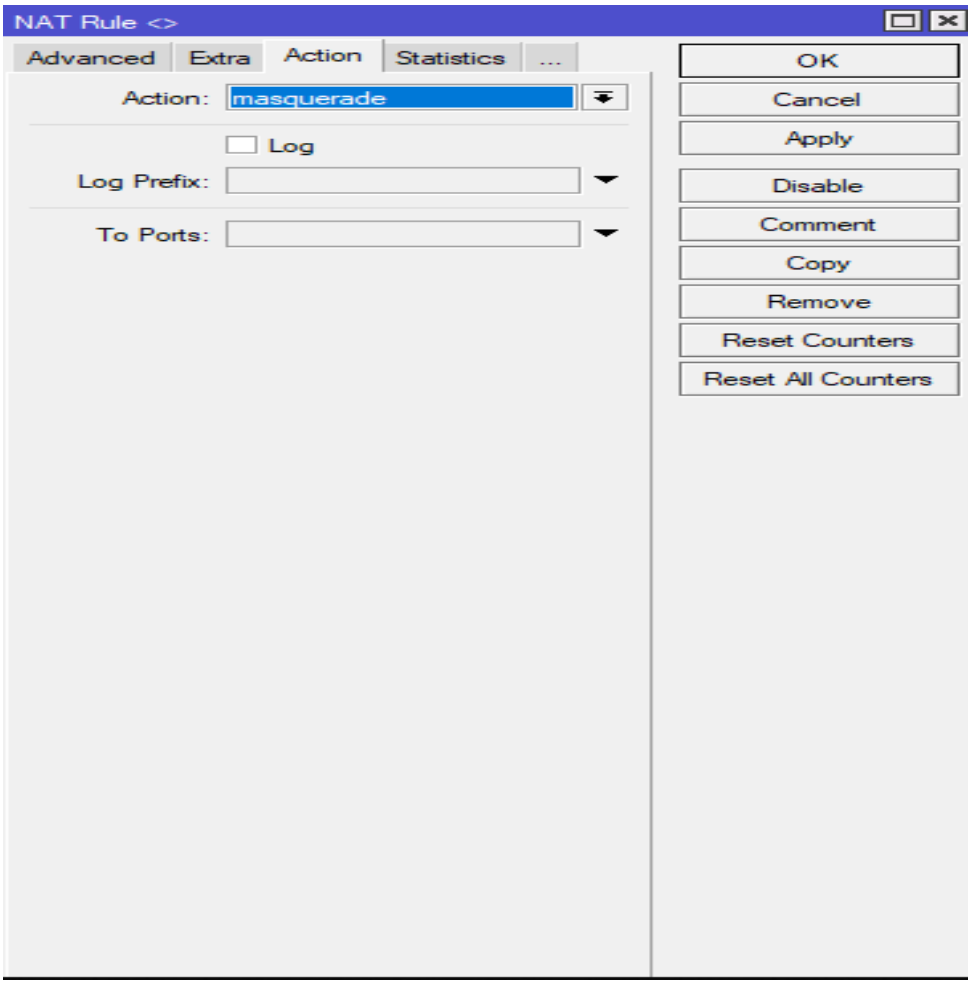
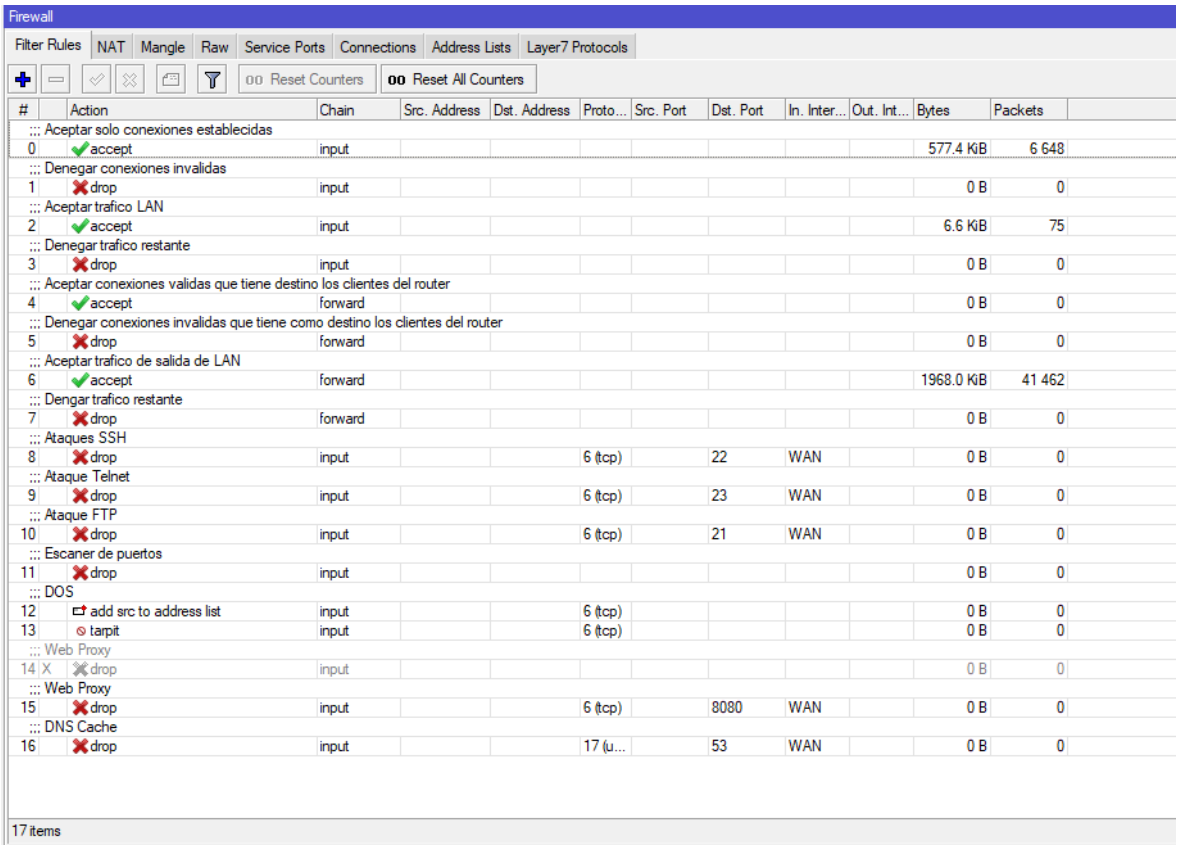


Ilustración 46 Configuración acción NAT

- Configuración Firewall

El sistema operativo RouterOS, permite la creación de políticas y regla de firewall con la cual se pueden prevenir diversos ataques cibernéticos como SSH, Telnet, FTP, escaneo de puertos, ataques DoS, web proxy y DNS cache, así como la denegación de conexión invalidas y la aceptación o rechazo del tráfico de red proveniente o saliente de la red LAN o WAN



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Aceptar solo conexiones establecidas											
0	accept	input								577.4 KiB	6 648
;;; Denegar conexiones invalidas											
1	drop	input								0 B	0
;;; Aceptar trafico LAN											
2	accept	input								6.6 KiB	75
;;; Denegar trafico restante											
3	drop	input								0 B	0
;;; Aceptar conexiones validas que tiene destino los clientes del router											
4	accept	forward								0 B	0
;;; Denegar conexiones invalidas que tiene como destino los clientes del router											
5	drop	forward								0 B	0
;;; Aceptar trafico de salida de LAN											
6	accept	forward								1968.0 KiB	41 462
;;; Dengar trafico restante											
7	drop	forward								0 B	0
;;; Ataques SSH											
8	drop	input			6 (tcp)		22	WAN		0 B	0
;;; Ataque Telnet											
9	drop	input			6 (tcp)		23	WAN		0 B	0
;;; Ataque FTP											
10	drop	input			6 (tcp)		21	WAN		0 B	0
;;; Escaner de puertos											
11	drop	input								0 B	0
;;; DOS											
12	add src to address list	input			6 (tcp)					0 B	0
13	tarpit	input			6 (tcp)					0 B	0
;;; Web Proxy											
14 X	drop	input								0 B	0
;;; Web Proxy											
15	drop	input			6 (tcp)		8080	WAN		0 B	0
;;; DNS Cache											
16	drop	input			17 (u...		53	WAN		0 B	0

Ilustración 47 Configuración firewall Mikrotik Bucaramanga

- Ejemplo de la configuración de un equipo cliente ubicado en la ciudad de Bucaramanga.

A través de la siguiente imagen, se muestra un ejemplo de la configuración de red de un equipo cliente ubicado en la ciudad de Bucaramanga.

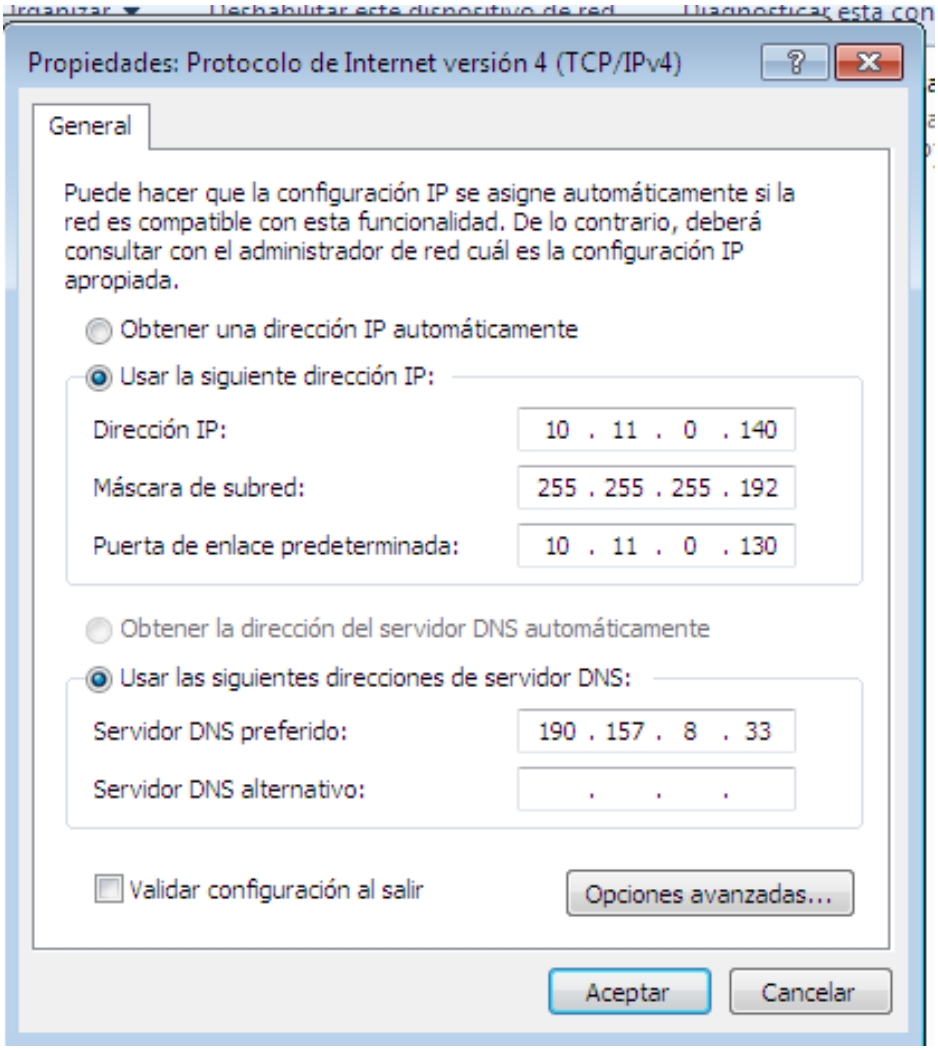


Ilustración 48 Configuración tarjeta de red equipo cliente de la ciudad de Bucaramanga

- Conexión a la VPN desde equipo cliente en la sede de Bucaramanga

Windows, incorpora una utilidad de configuración de VPN, en el cual, mediante la utilización de la IP pública del Mikrotik y las credenciales creadas en el dispositivo de Bogotá, los usuarios pueden acceder a los recursos alojados allí.

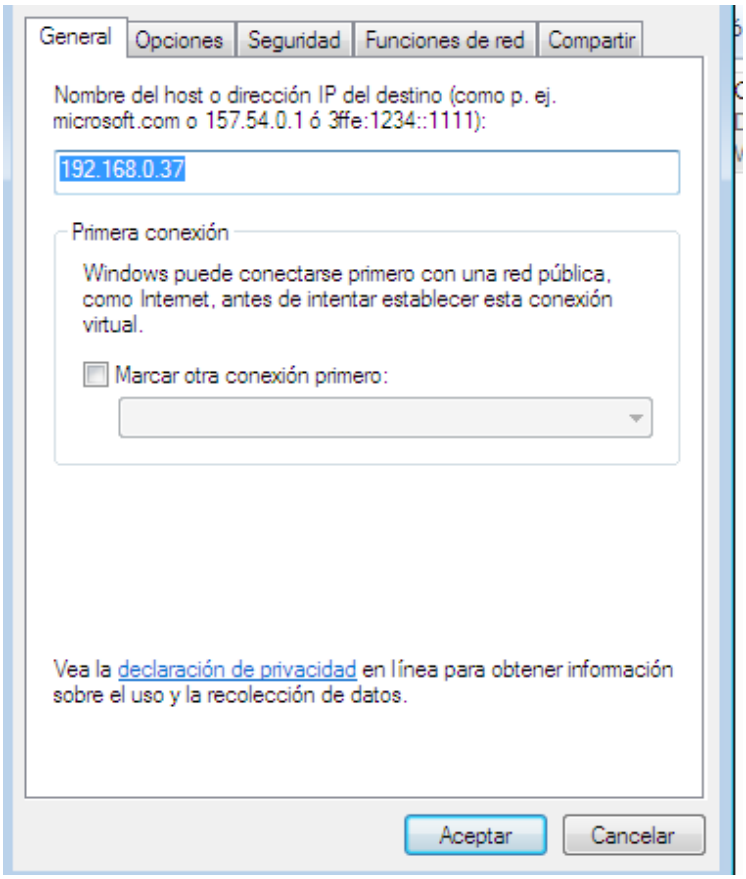


Ilustración 49 Solicitud de IP publica Mikrotik Bogotá

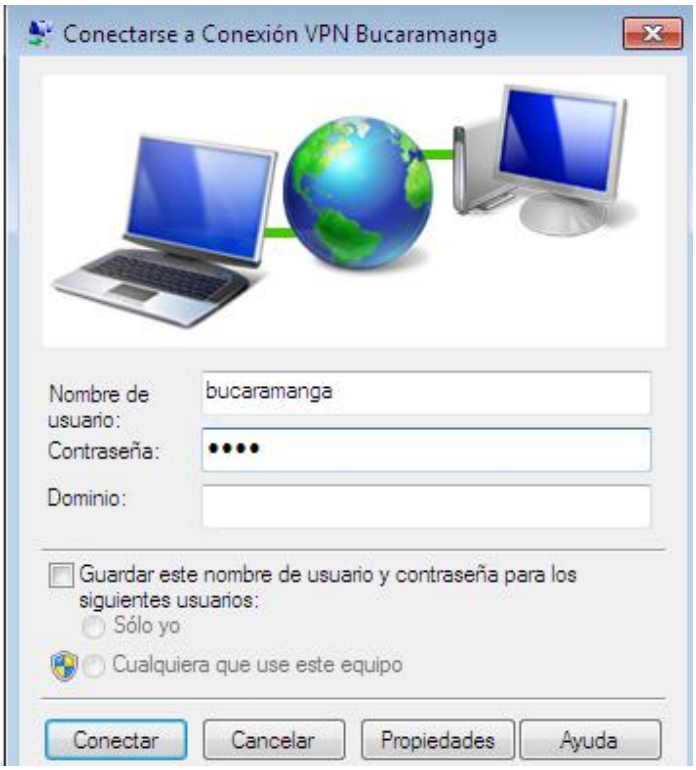


Ilustración 50 Ingreso de credenciales usuarios de la sede de Bucaramanga

- Comprobación de conexión por VPN a través de la ejecución del comando ping

Una vez realizada el acceso a los recursos de la ciudad de Bogotá mediante VPN, se comprueba la conexión al servidor web, de telefonía, FTP y aplicativa de gestión a través del comando ping ejecutado desde la maquina cliente ubicada en la ciudad de Bucaramanga.

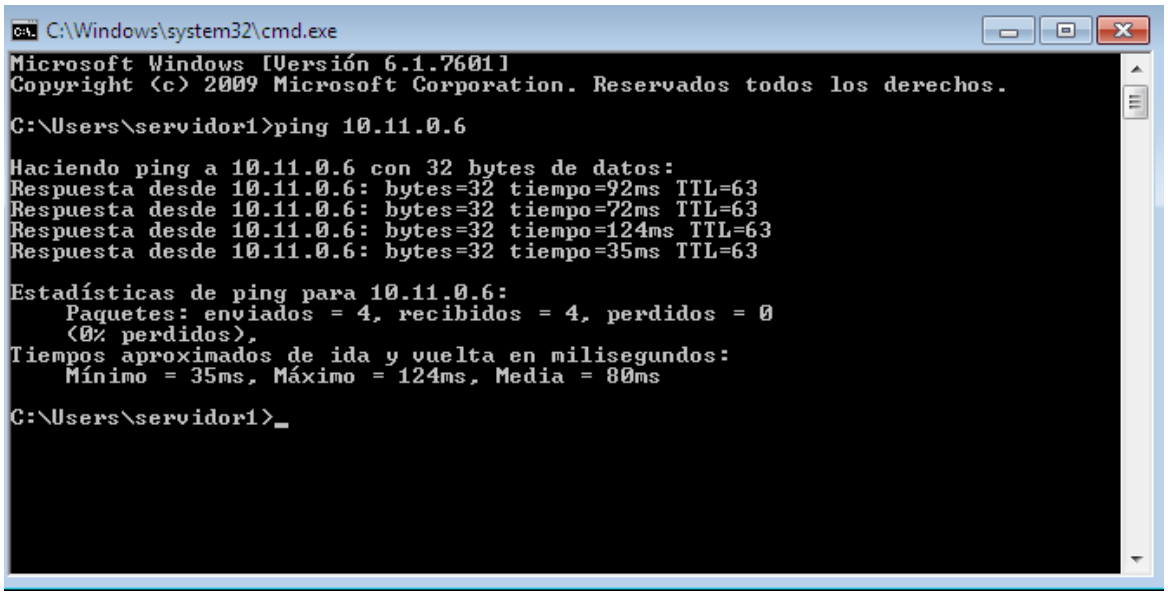


Ilustración 51 Ping servidor web

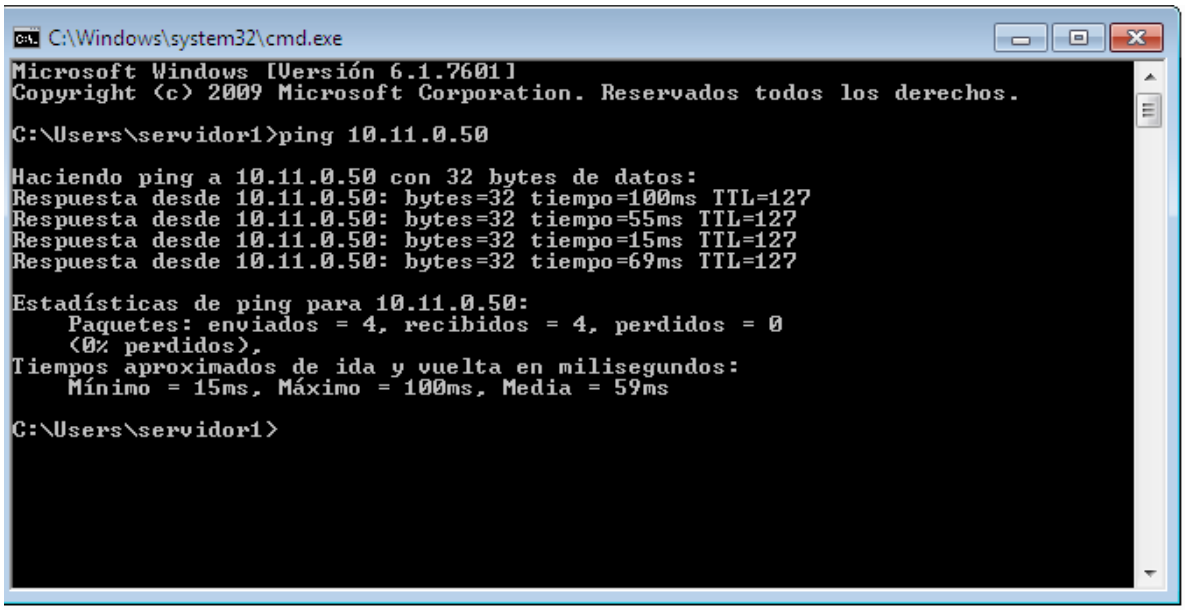


Ilustración 52 Ping servidor FTP

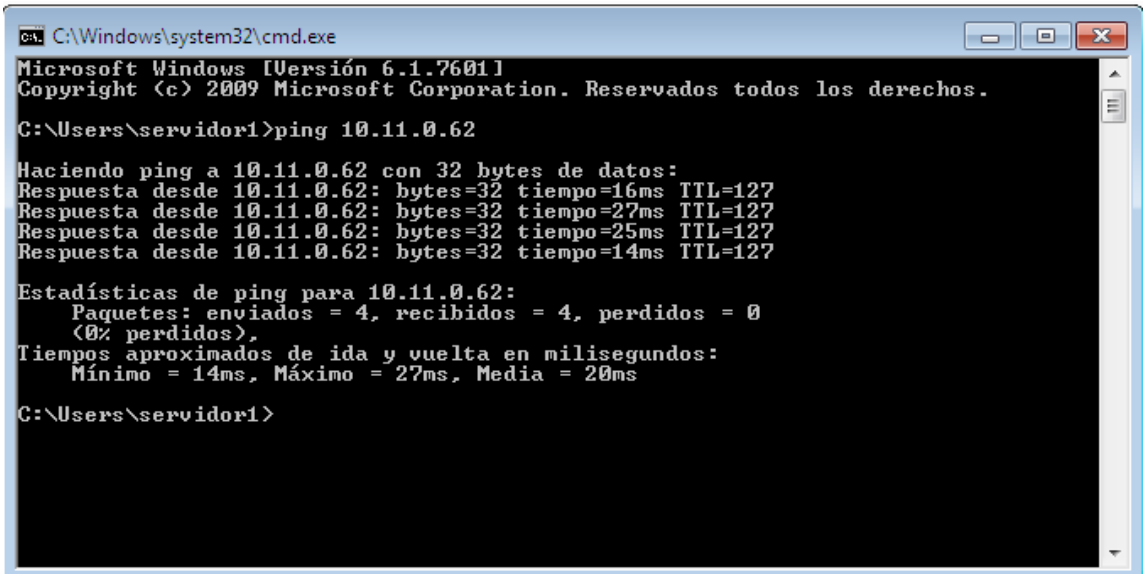


Ilustración 53 Ping servidor de telefonía

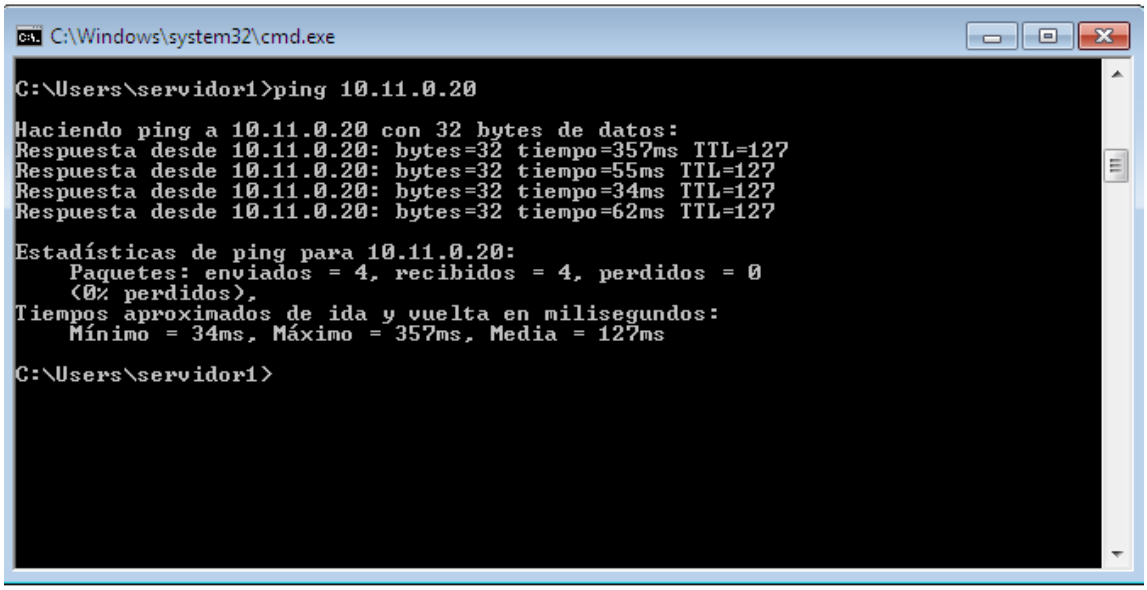


Ilustración 54 Ping servidor aplicativo de gestión

5. Configuracion Mikrotik Medellin

La configuracion del Mikrotik correspondiente a la ciudad de Medellin, comprende configuraciones como: el acceso a la interfaz grafica desde el aplicativo Winbox, la

configuracion de las interfaces de red para la LAN y WAN, la creacion de las VPNs para la conexión desde otras ciudades, la configuracion NAT para dar acceso a internet a la red interna y la creacion de reglas en el firewall para evitar ataques de tipo SSH, Telnet, FTP, denegacion de servicio, web proxy, conexiones no autorizadas, entre otros.

- Configuracion de acceso

Para el acceso al sistema operativo RouerOS de la ciudad de Medellin se debe realizar mediante el componenten grafico de Mikrotik, WinBox, el cual permite tener realizar la administracion del sistema operativo a traves de una interfaz grafica. Esta conexión la realiza mediante la identificacion de la direccion MAC del dispositivo o la direccion IP.

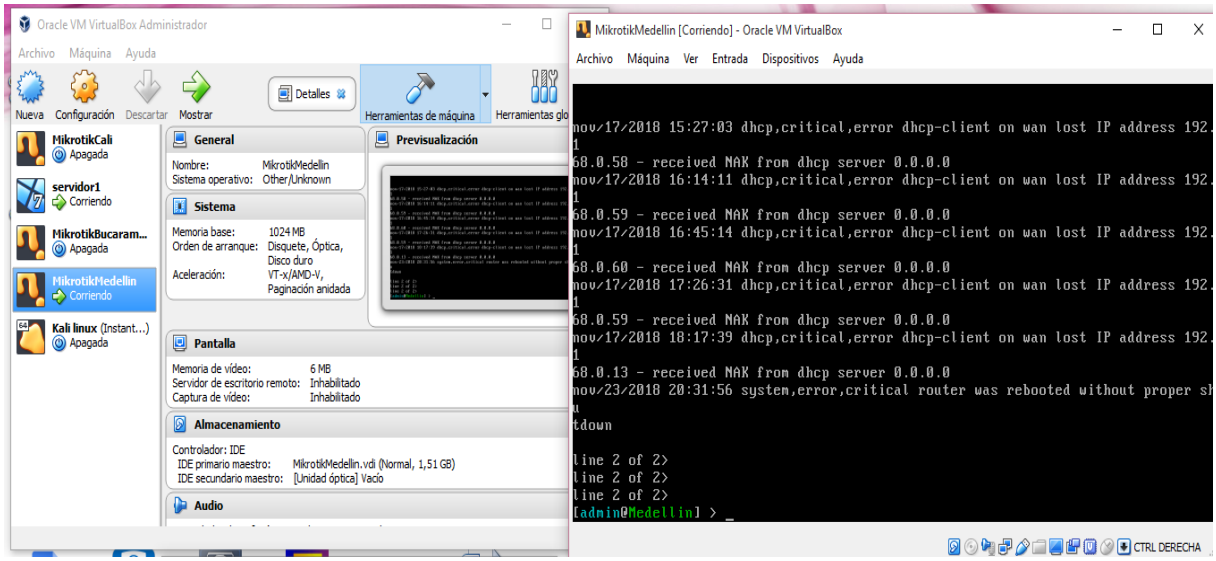


Ilustración 55 Inicio máquina virtual Mikrotik Medellín

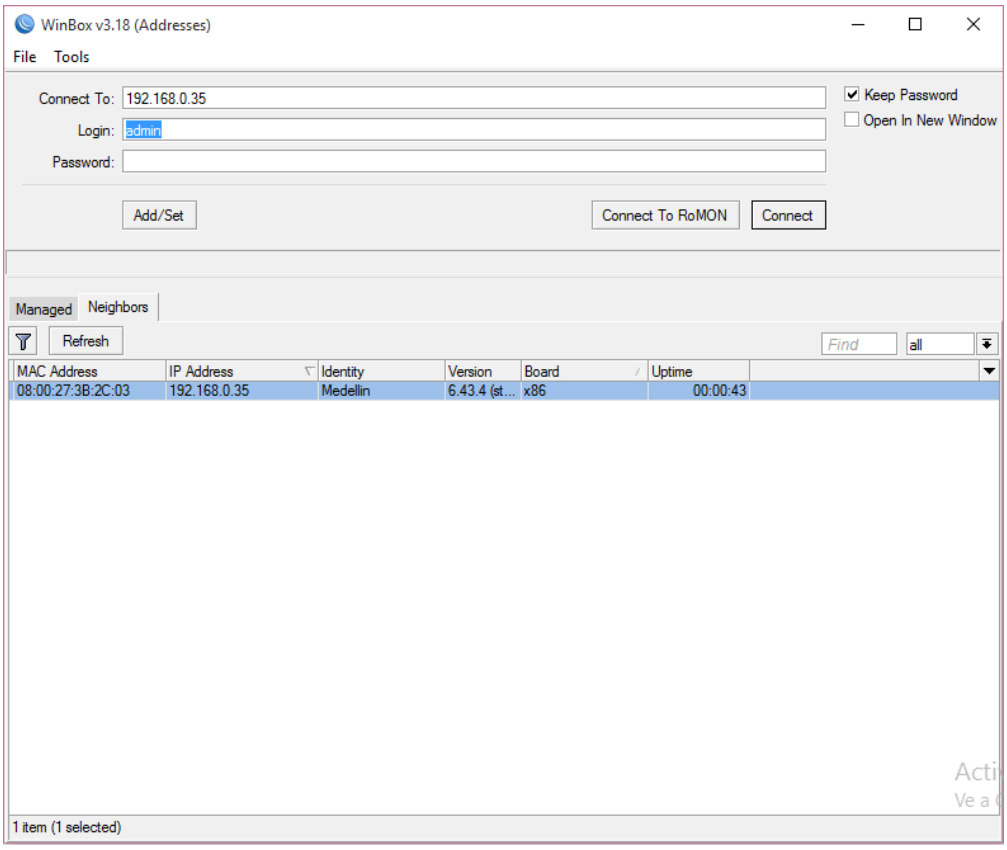


Ilustración 56 Inicio WinBox Mikrotik Medellín

- Configuración de interfaces

A traves de la opcion “Interface” proporcionado por el WinBox, se establece la configuracion de red para la tarjeta LAN la cual permite la comunicación de la red interna con el Mikrotik, y asigna los parametros de conexión para la tarjeta WAN, la cual va a permitir la salida hacia internet.

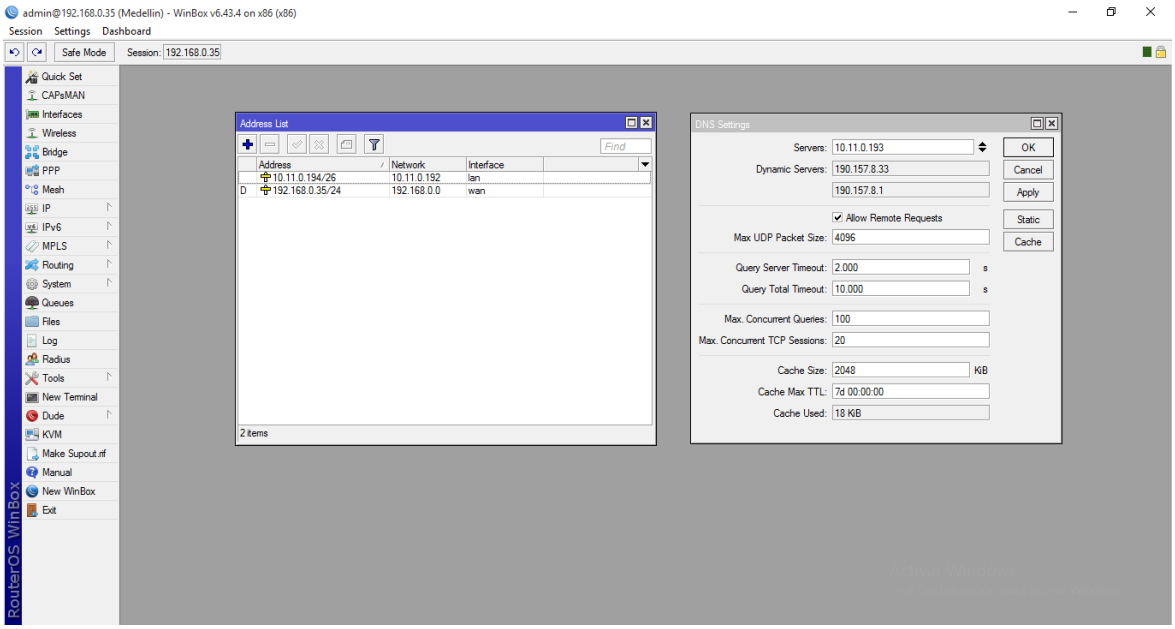


Ilustración 57 Configuración interfaces Mikrotik Medellín

- Configuración NAT

La utilidad “Firewall”, internamente, trae consigo la configuración de NAT la cual permite que los usuarios de la red interna tengan acceso a internet.

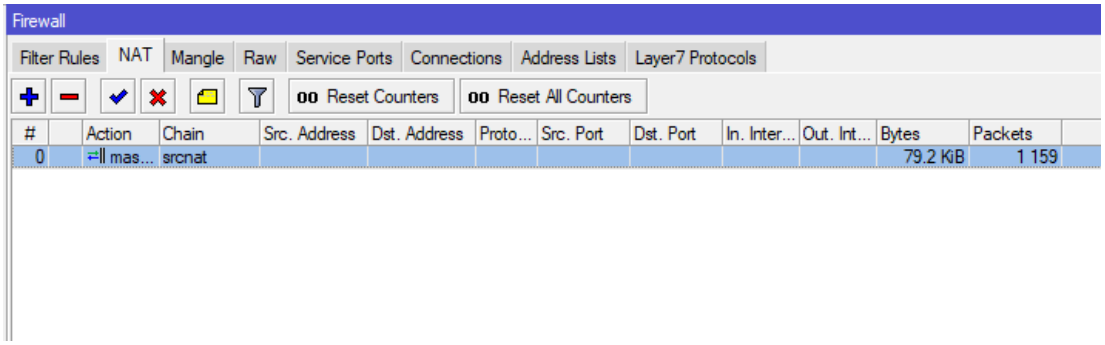


Ilustración 58 Configuración NAT

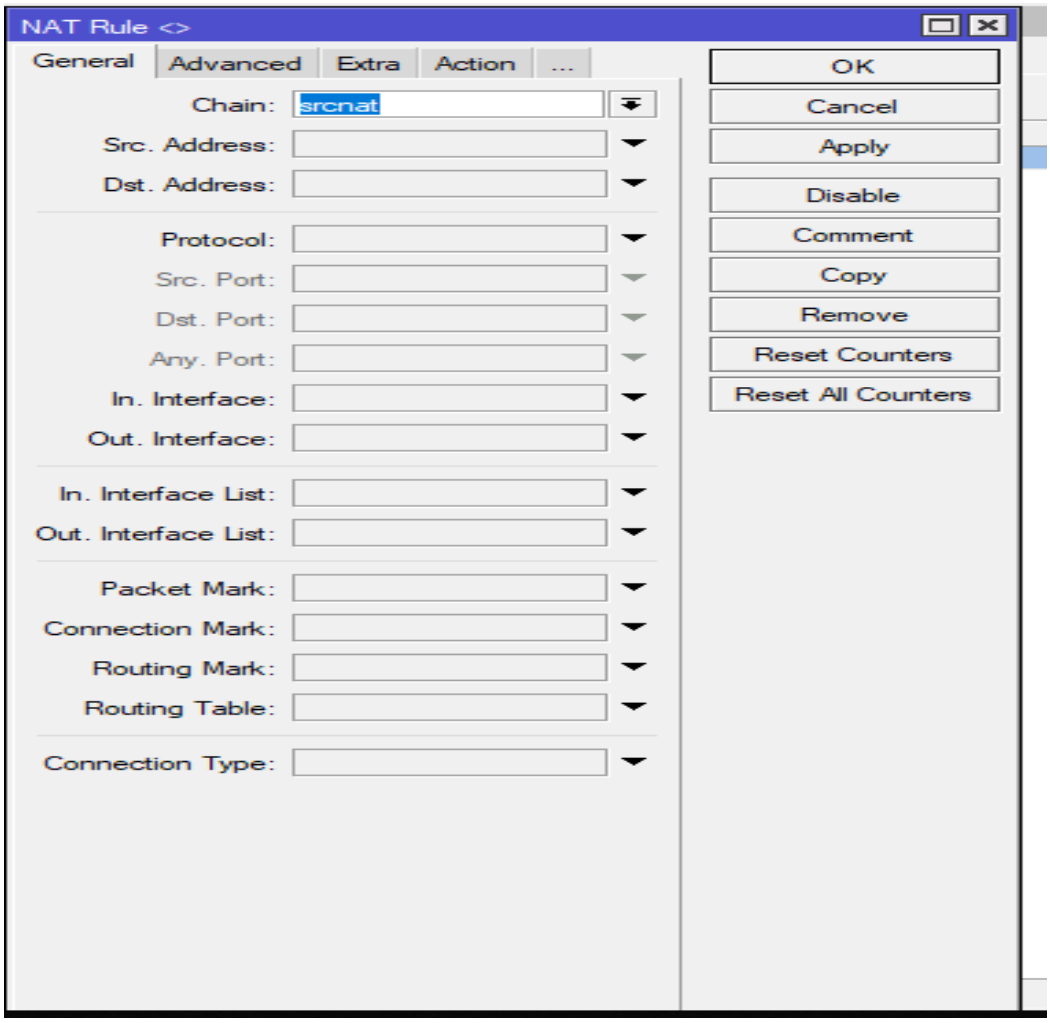


Ilustración 59 Configuración general NAT

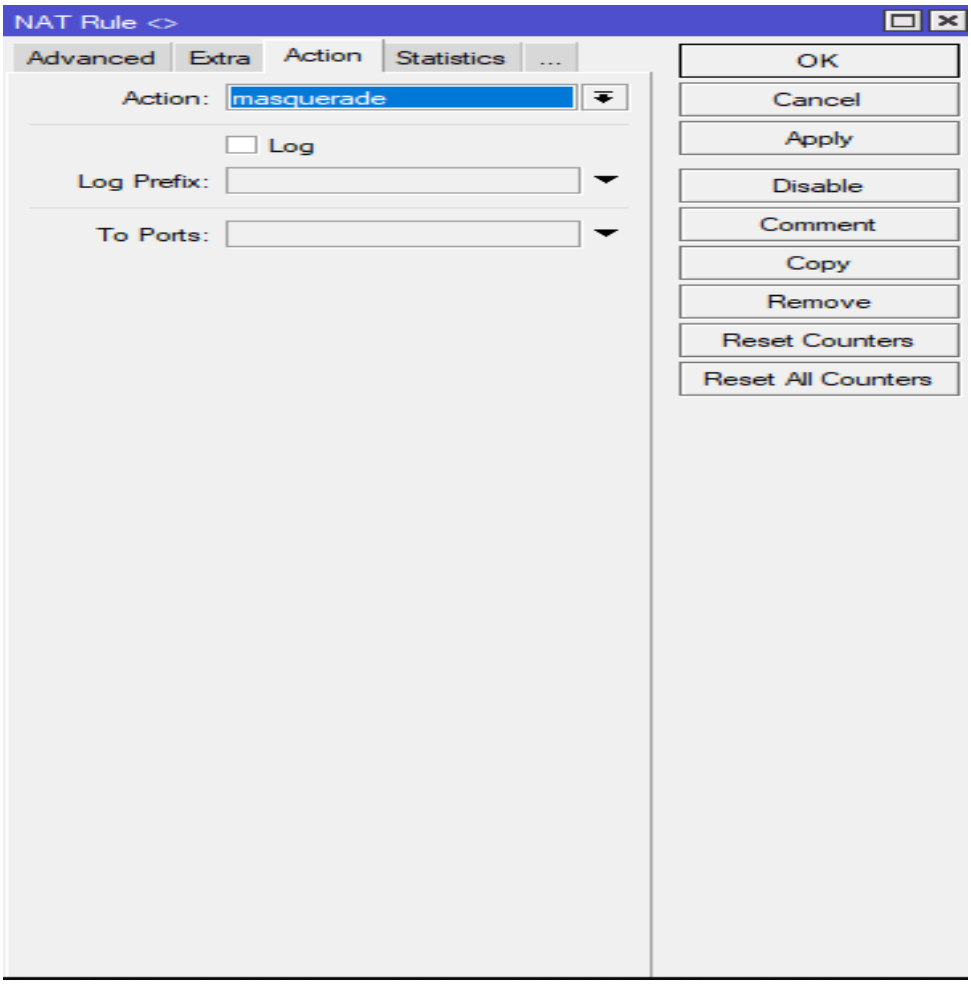
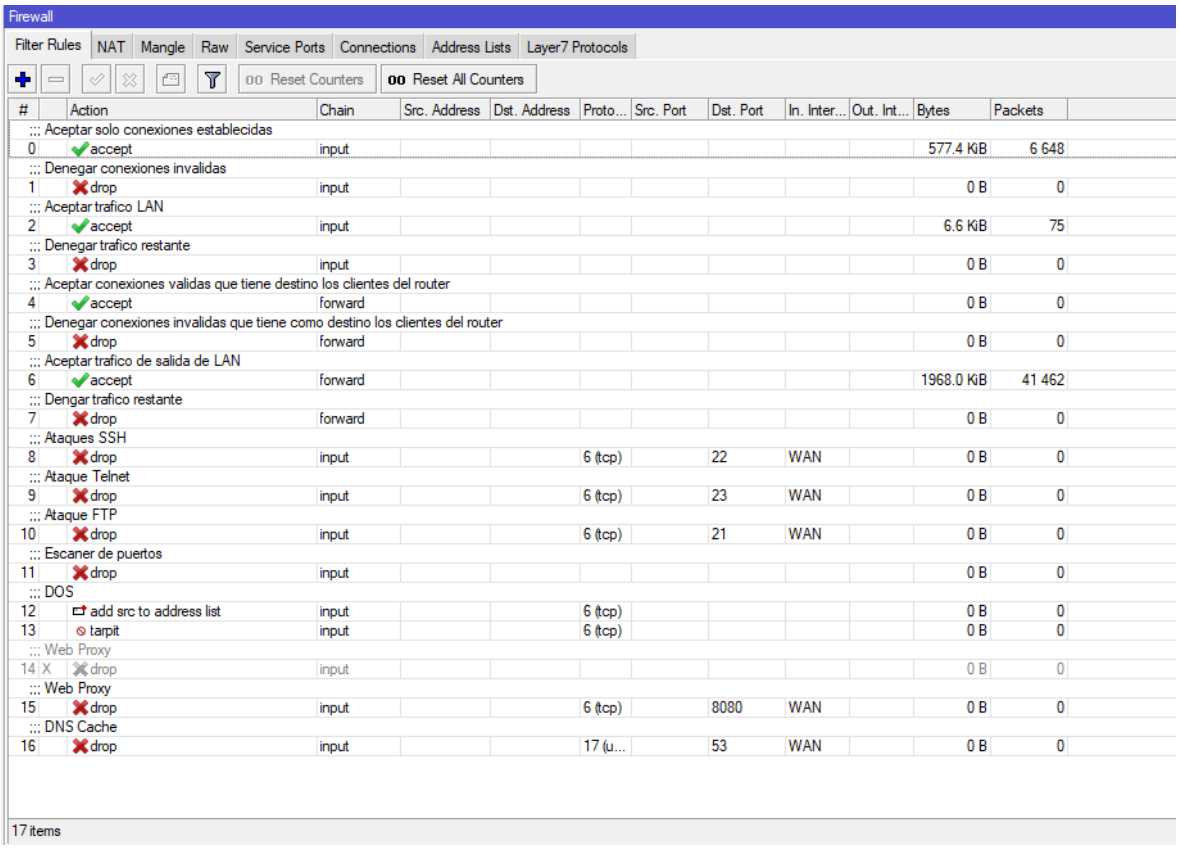


Ilustración 60 Configuración acción NAT

- Configuración Firewall

El sistema operativo RouterOS, permite la creación de políticas y regla de firewall con la cual se pueden prevenir diversos ataques cibernéticos como SSH, Telnet, FTP, escaneo de puertos, ataques DoS, web proxy y DNS cache, así como la denegación de conexión invalidas y la aceptación o rechazo del tráfico de red proveniente o saliente de la red LAN o WAN



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Aceptar solo conexiones establecidas											
0	accept	input								577.4 KiB	6 648
;;; Denegar conexiones invalidas											
1	drop	input								0 B	0
;;; Aceptar trafico LAN											
2	accept	input								6.6 KiB	75
;;; Denegar trafico restante											
3	drop	input								0 B	0
;;; Aceptar conexiones validas que tiene destino los clientes del router											
4	accept	forward								0 B	0
;;; Denegar conexiones invalidas que tiene como destino los clientes del router											
5	drop	forward								0 B	0
;;; Aceptar trafico de salida de LAN											
6	accept	forward								1968.0 KiB	41 462
;;; Dengar trafico restante											
7	drop	forward								0 B	0
;;; Ataques SSH											
8	drop	input			6 (tcp)		22	WAN		0 B	0
;;; Ataque Telnet											
9	drop	input			6 (tcp)		23	WAN		0 B	0
;;; Ataque FTP											
10	drop	input			6 (tcp)		21	WAN		0 B	0
;;; Escaner de puertos											
11	drop	input								0 B	0
;;; DOS											
12	add src to address list	input			6 (tcp)					0 B	0
13	tarpit	input			6 (tcp)					0 B	0
;;; Web Proxy											
14 X	drop	input								0 B	0
;;; Web Proxy											
15	drop	input			6 (tcp)		8080	WAN		0 B	0
;;; DNS Cache											
16	drop	input			17 (u...		53	WAN		0 B	0

Ilustración 61 Configuración firewall Mikrotik Medellín

- Ejemplo de la configuración de un equipo cliente ubicado en la ciudad de Medellín.

A través de la siguiente imagen, se muestra un ejemplo de la configuración de red de un equipo cliente ubicado en la ciudad de Medellín.

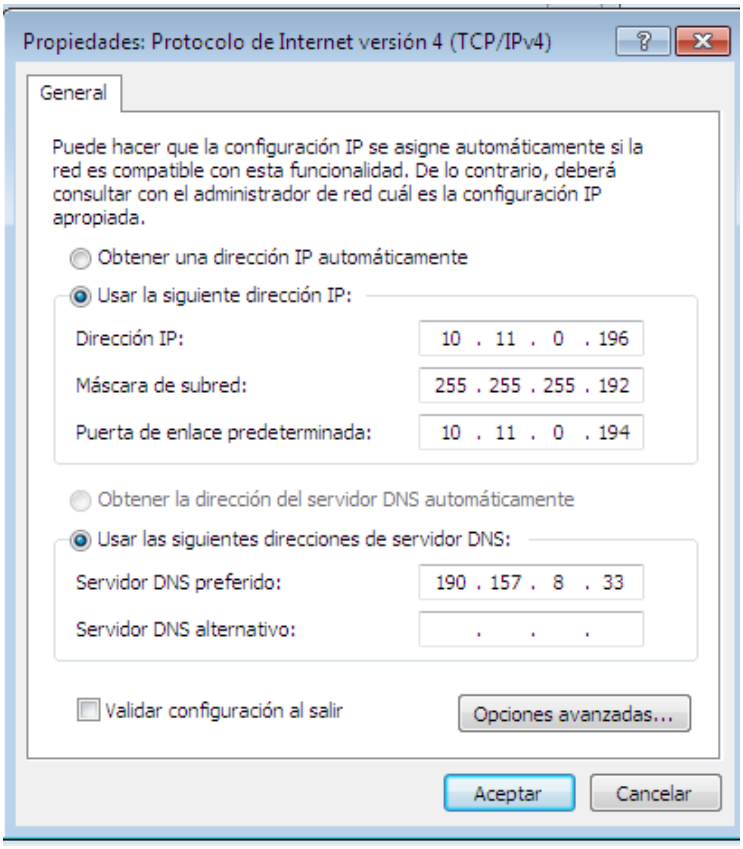


Ilustración 62 Configuración tarjeta de red equipo cliente sede Medellín

- Conexión a la VPN desde equipo cliente en la sede de Medellín

Windows, incorpora una utilidad de configuración de VPN, en el cual, mediante la utilización de la IP pública del Mikrotik y las credenciales creadas en el dispositivo de Bogotá, los usuarios pueden acceder a los recursos alojados allí.

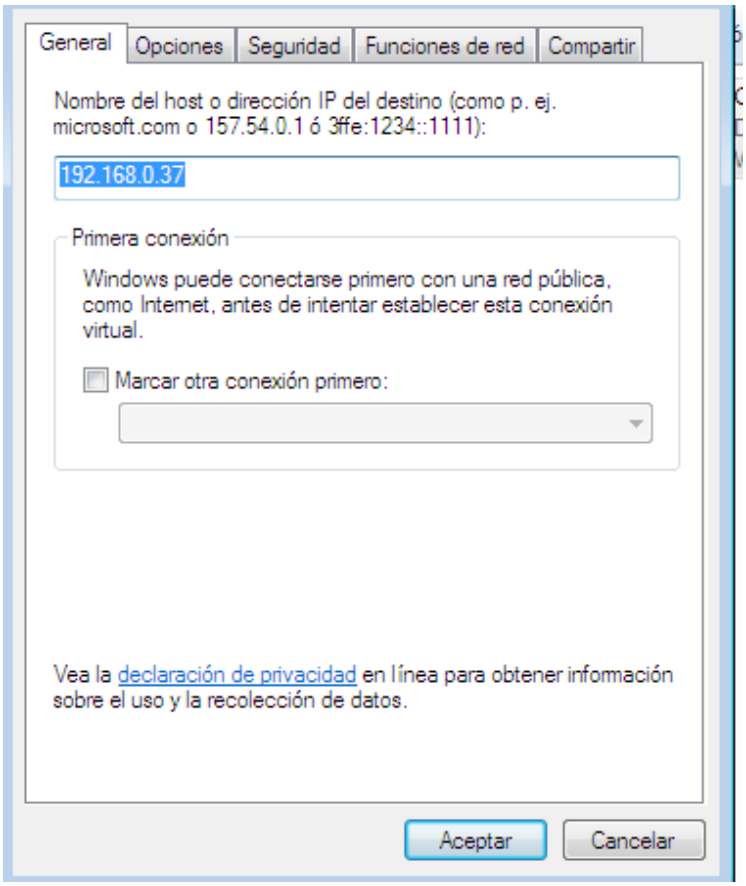


Ilustración 63 Solicitud de IP publica Mikrotik Bogotá

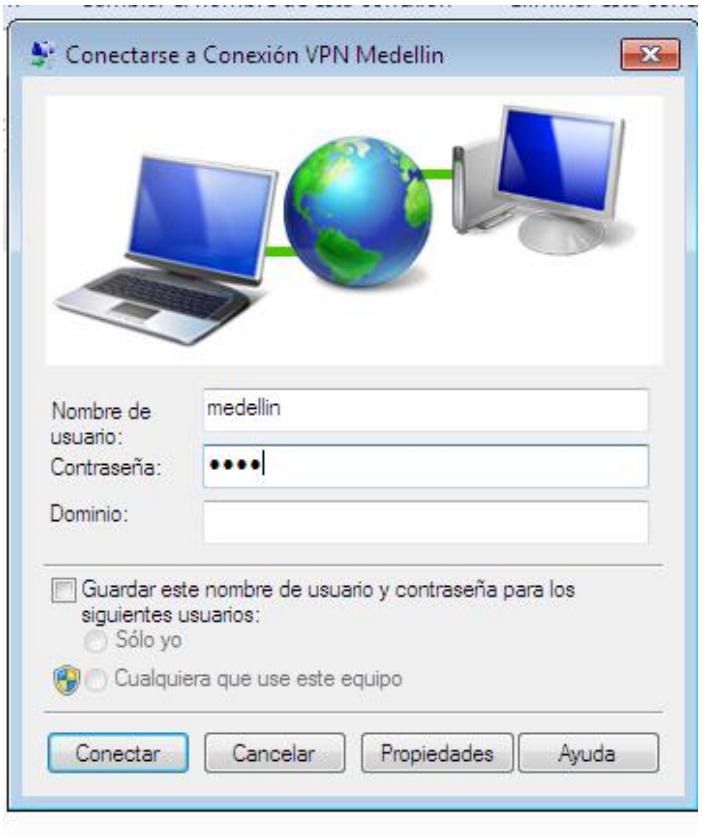


Ilustración 64 Ingreso de credenciales usuarios ubicados en la sede de Medellín.

- Comprobación de conexión por VPN a través de la ejecución del comando ping

Una vez realizada el acceso a los recursos de la ciudad de Bogotá mediante VPN, se comprueba la conexión al servidor web, de telefonía, FTP y aplicativa de gestión a través del comando ping ejecutado desde la maquina cliente ubicada en la ciudad de Medellin.

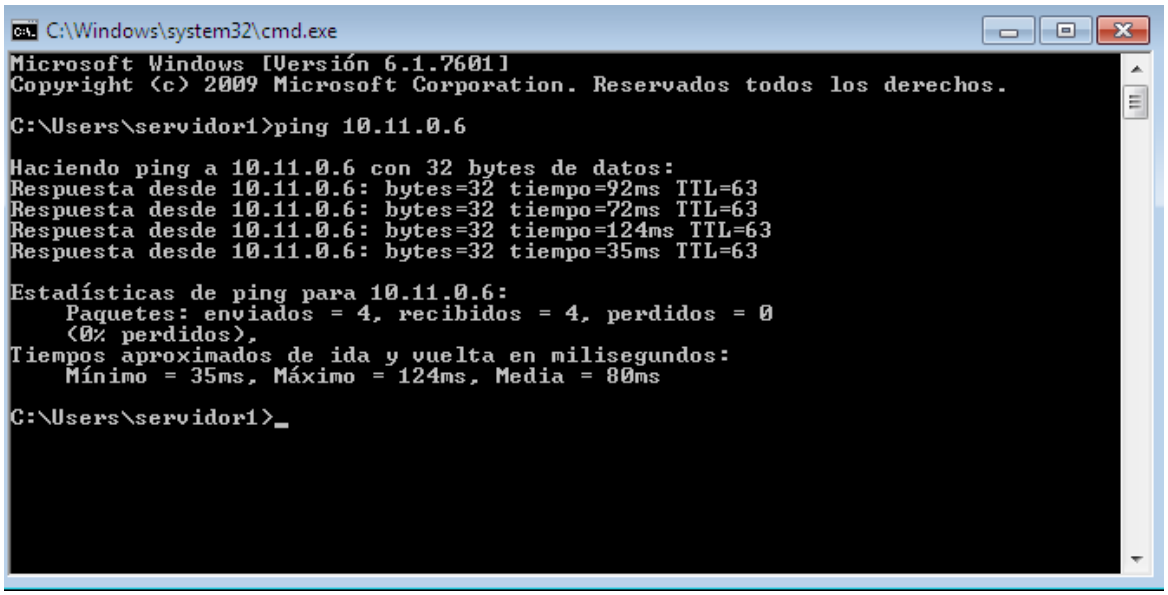


Ilustración 65 Ping servidor web

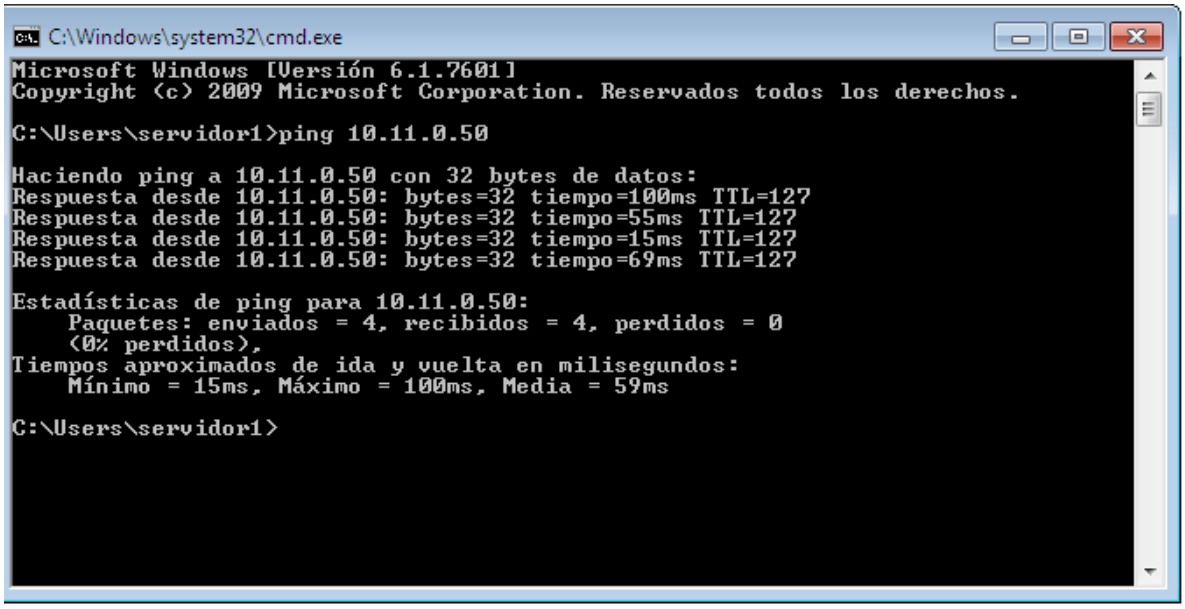


Ilustración 66 Ping servidor FTP

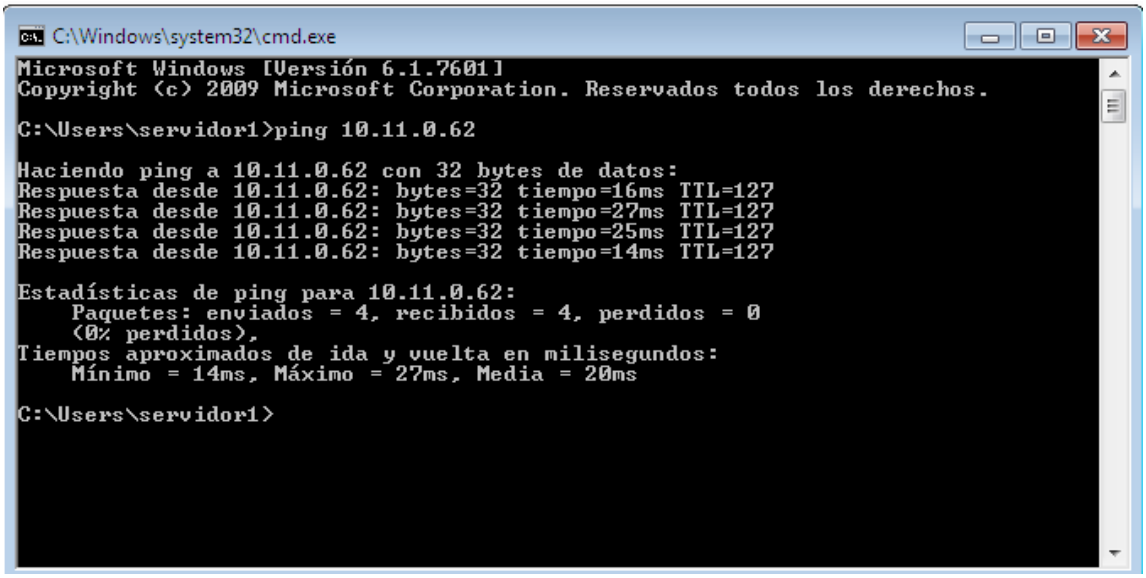


Ilustración 67 Ping servidor de telefonía

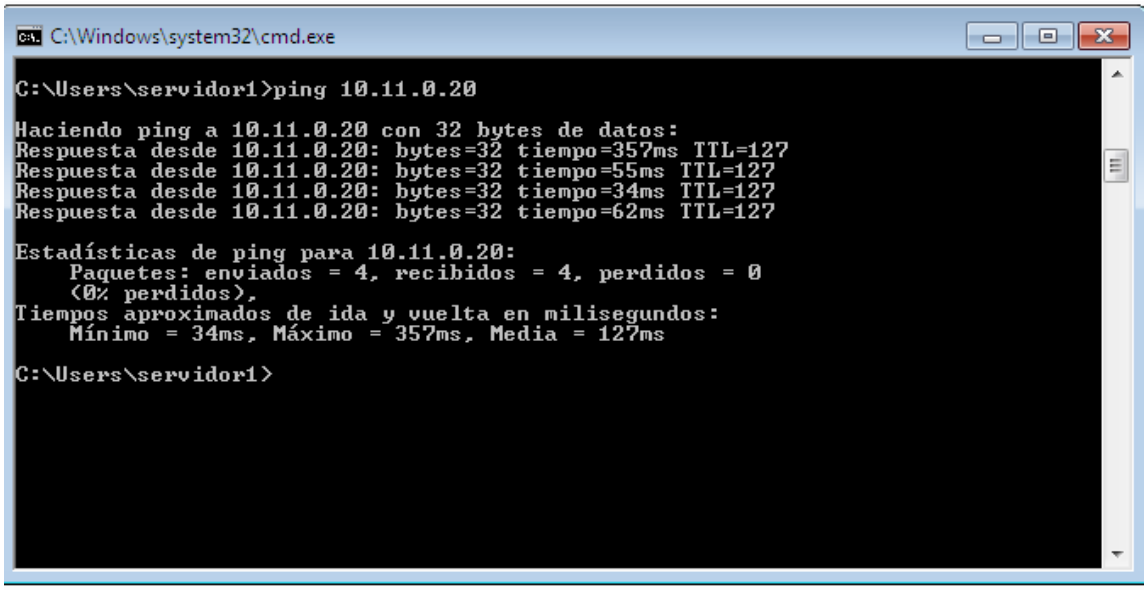


Ilustración 68 Ping servidor aplicativo de gestión

Ejecución de pentesting dirigida al software Badstore

1. Ataques XSS

Mediante un primer ataque realizado, se pudo evidenciar que en el campo de "Email Address" del menú "My Account" se puede introducir una sentencia en lenguaje Javascript que, al ser enviada mediante la opción "Reset User Password" genera una ventana de alerta en la página.

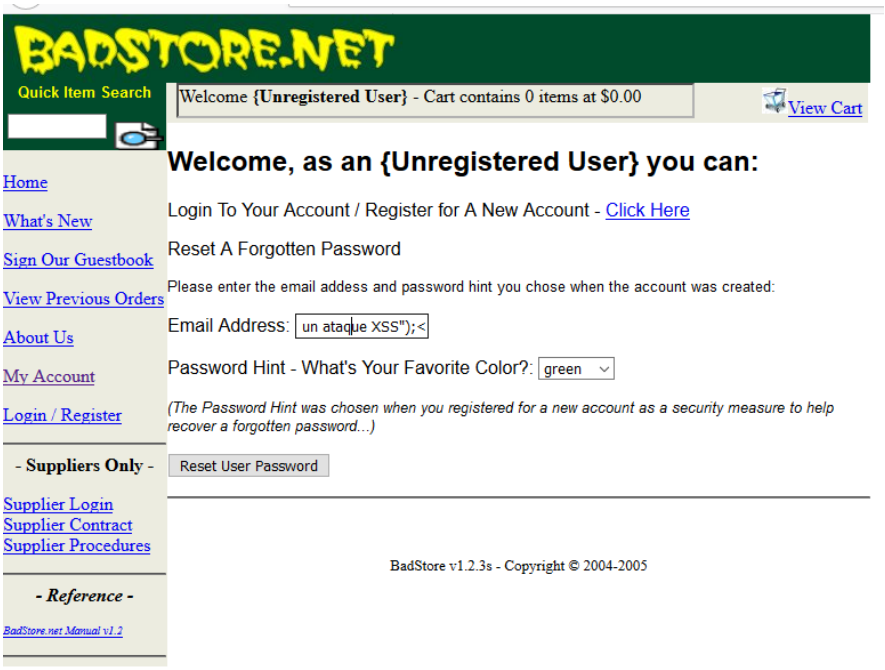


Ilustración 69 Inserción de código Javascript en campo de ingreso

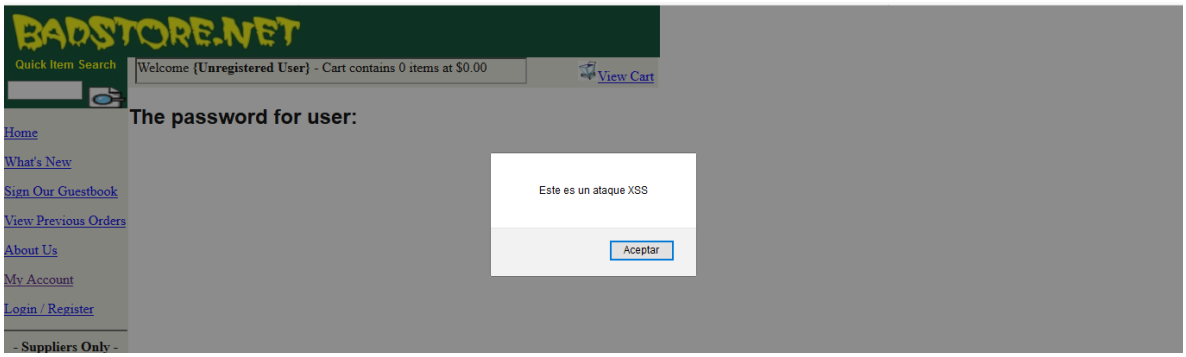


Ilustración 70 Resultado del ataque de Javascript

En un segundo ataque, se puede apreciar que en el campo de “Your Name” del menú de “Sign Our Guestbook” se puede introducir una instrucción en lenguaje Javascript que, al pulsar la opción de “Add Entry” redirige a una pagina externa al software.

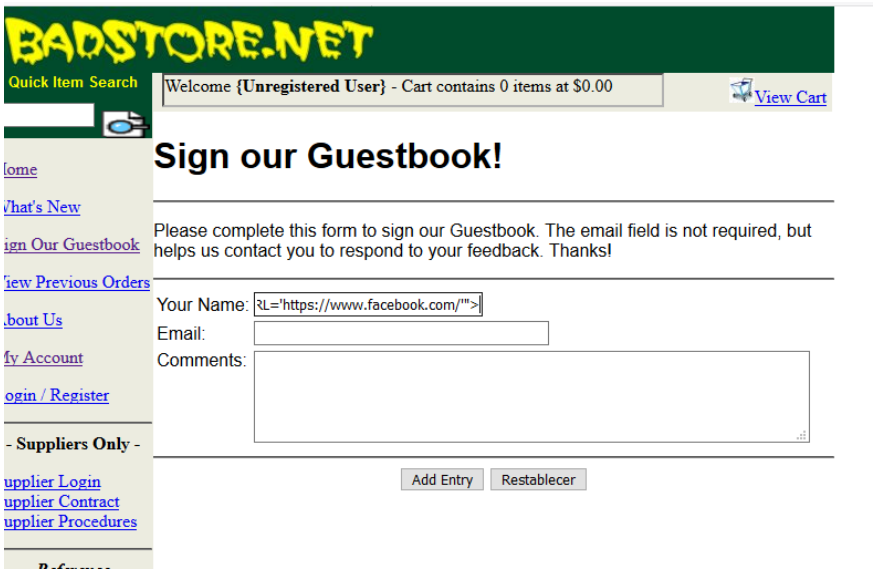


Ilustración 71 Inserción de código Javascript en el menú “Sign Our Guestbook”

Ilustración 72 Resultado de ataque de redirección de página web

2. Ataque SQL Injection

En un primer ataque realizado se pudo evidenciar que, en el campo de búsqueda del aplicativo web, se puede ingresar una instrucción SQL que al ser ejecutada devuelve todos los elementos almacenados en la base de datos, los cuales son 16.

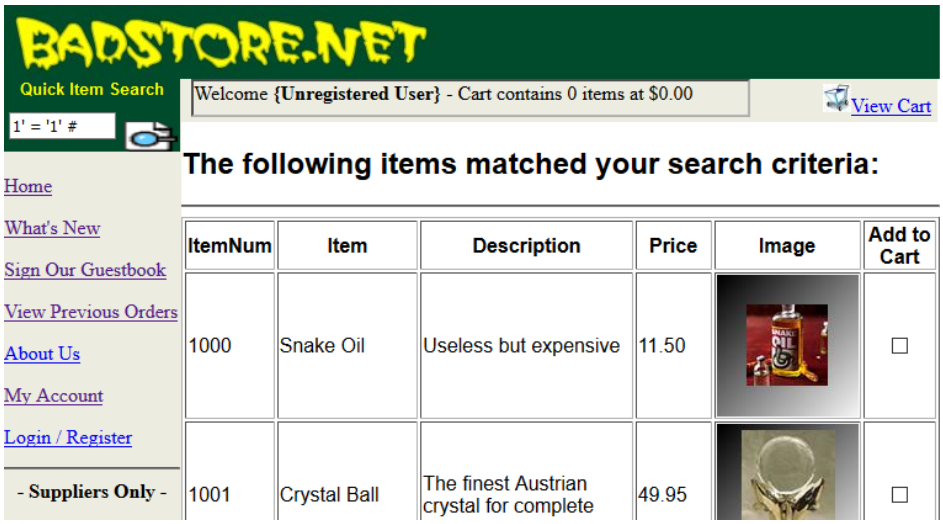


Ilustración 73 Inserción de código SQL en el campo de búsqueda

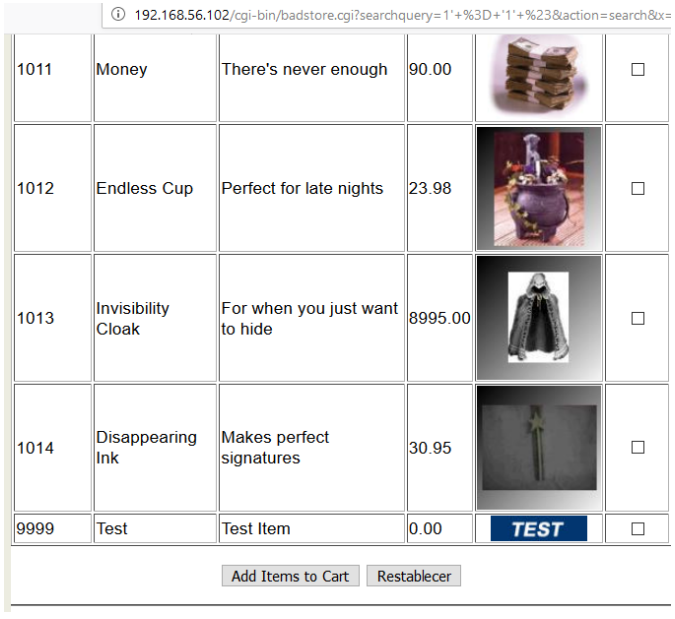


Ilustración 74 Resultado de ejecución de código SQL en el campo de búsqueda

Mediante un segundo ataque, se apreció que, mediante la inserción de una consulta de búsqueda seguido de la URL del aplicativo, el sistema devuelve los datos de acceso del usuario administrador como el nombre de usuario y la contraseña, la cual, esta codificada pero que fácilmente puede ser descifrada mediante un sistema de conversión de MD5.

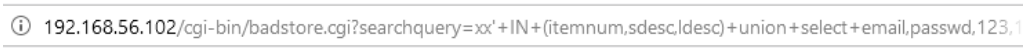


Ilustración 75 Inserción de consulta SQL en la URL de navegación

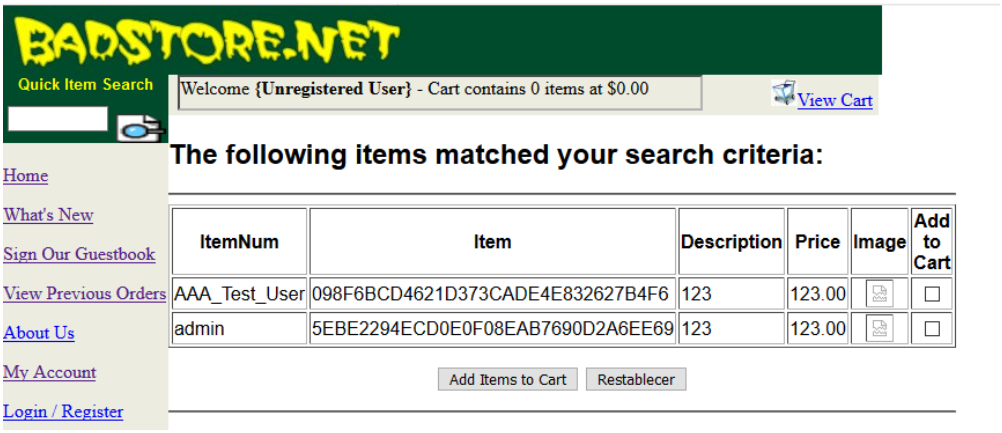


Ilustración 76 Resultado de la consulta SQL en la URL de navegación

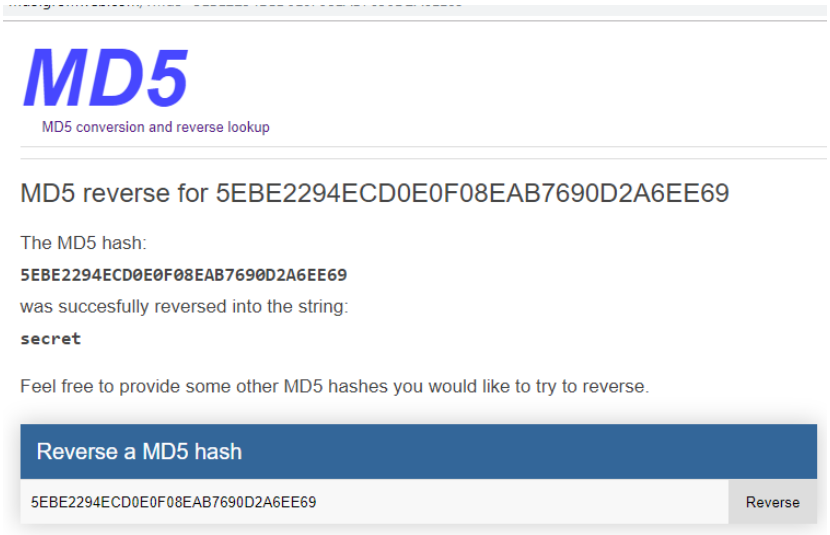


Ilustración 77 Conversión de clave codificada

3. Modificación de cookies

En las siguientes imágenes se puede evidenciar que, mediante la utilización de una herramienta que permite modificar las peticiones del aplicativo web se puede modificar los precio el precio final de carrito de compras. En el ataque se agregaron 4 productos por un valor total de $5046.95 pero, al modificar la cookie de petición de esta actividad, se puede indicar al sistema que la compra tenga un valor de $0.00.

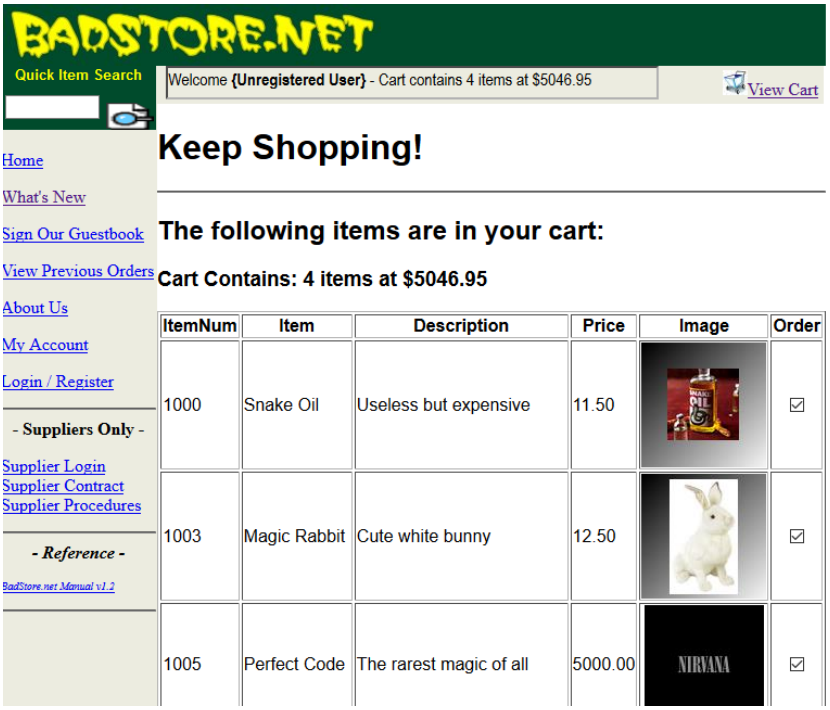


Ilustración 78 Productos agregados al carrito de compras

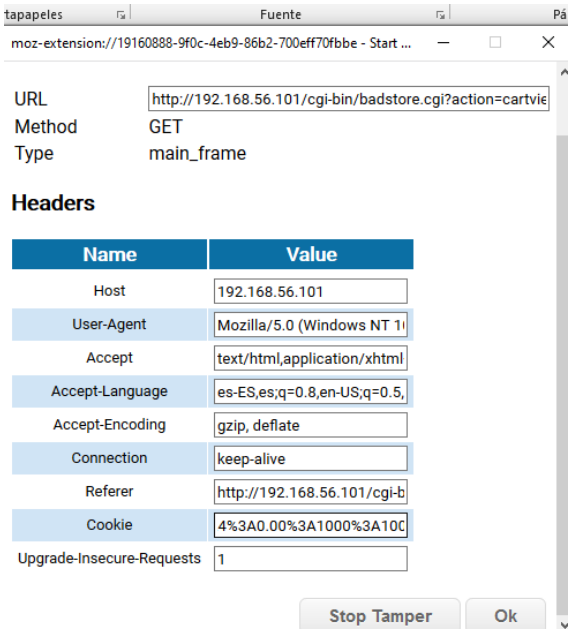


Ilustración 79 Modificación de cookie del carrito de compras

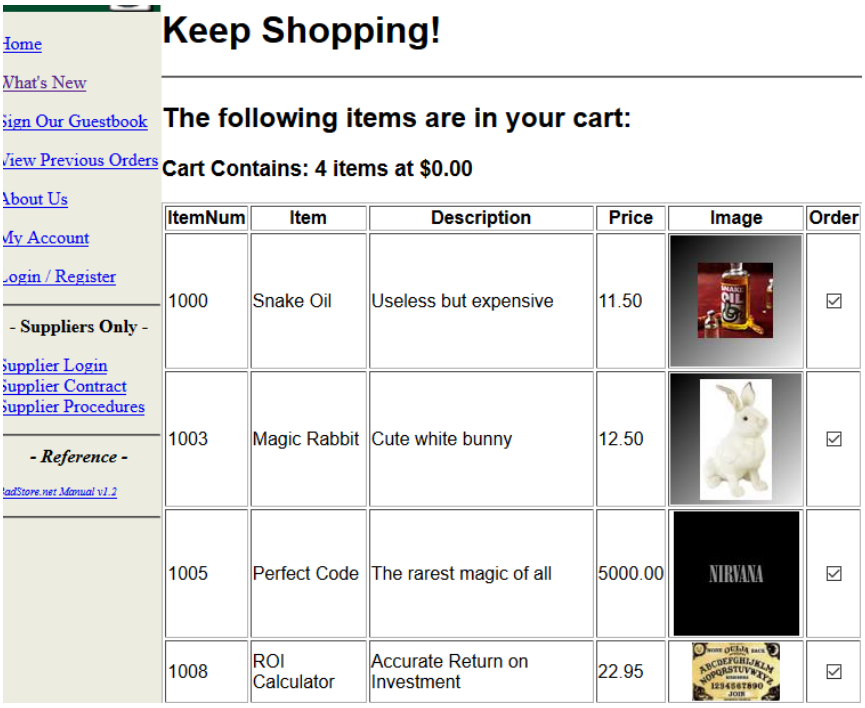


Ilustración 80 Resultado de la modificación de cookies

4. Ataque de navegación forzada

A través del siguiente ataque, se pudo comprobar que el aplicativo web, permite ingresar a diversos directorios únicamente ingresando los nombres de las carpetas que posiblemente el sistema web contenga. En este caso, se evidencio que mediante esa técnica, Badstore permite ingresar a una carpeta de backup y a una ruta llamada “Doing Business” en donde aloja un documento relacionado con las actividades de negocio de la compañía.

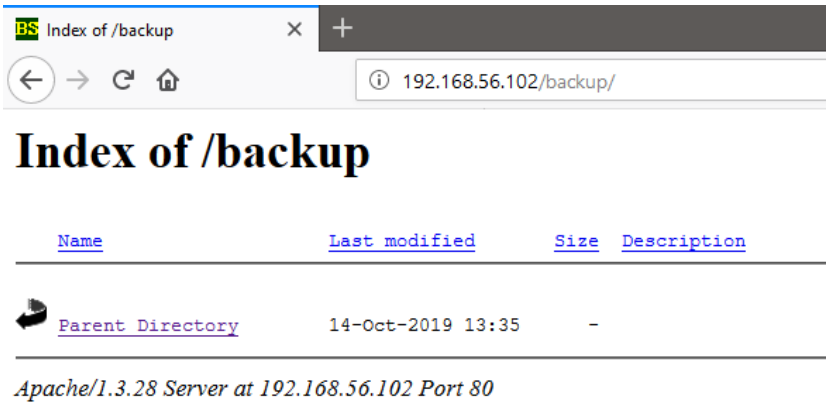


Ilustración 81 Ingreso de la carpeta “Backup” a través de navegación forzada

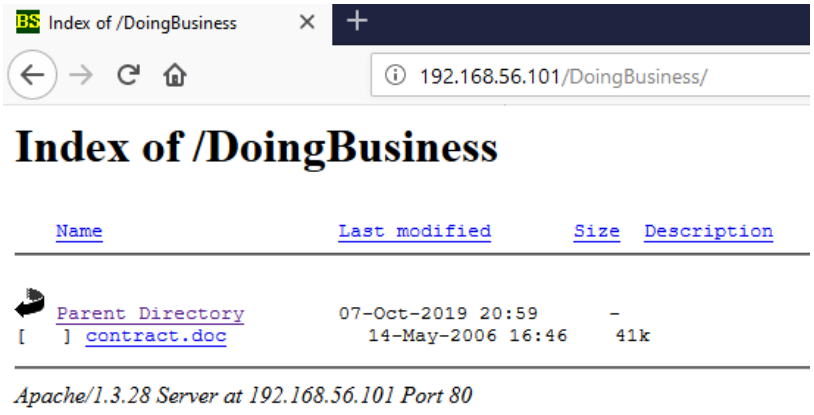


Ilustración 82 Ingreso de la carpeta “DoingBusiness” a través de navegación forzada

Borem and Snorem With BadStore

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Cras eu diam nec ante pellentesque venenatis. Donec sapien. Maecenas neque erat, lacinia consectetuer, tincidunt ut, laoreet sit amet, nisi. Donec egestas nibh eu nulla. Sed vitae neque egestas nunc venenatis condimentum. Morbi dui magna, pellentesque eu, malesuada quis, rutrum quis, nulla. In hac habitasse platea dictumst. Morbi vestibulum, ipsum id suscipit auctor, augue tellus lacinia libero, et sagittis leo diam eget urna. Nunc tincidunt suscipit magna. Aliquam velit pede, consectetuer ut, convallis a, auctor quis, tellus. Vivamus varius aliquam nunc. Suspendisse rhoncus sem ut magna. Quisque ultricies tempus neque. Fusce hendrerit elit vitae leo tristique nonummy.

Maecenas nec est. Pellentesque venenatis, est at gravida bibendum, urna nibh eleifend urna, vel vulputate arcu libero eget nisi. Suspendisse et ante. Etiam auctor nonummy felis. Cras elit mi, ullamcorper sed, venenatis at, vehicula eu, enim. Duis nec quam in nisl suscipit suscipit. Integer nec metus sit amet erat feugiat scelerisque. Praesent suscipit tempor nisl. Maecenas tellus arcu, adipiscing a, convallis id, porta vel, sem. Vestibulum sed tortor quis mi blandit varius. Praesent vitae erat non orci ultricies viverra. Nunc mattis, pede ac mollis fringilla, turpis odio semper tellus, a mattis augue nisi sit amet neque. Nulla a libero. Sed ante. Duis tortor tortor, dictum a, eleifend vel, dignissim quis, libero. Curabitur nec dui ac quam consectetuer consequat. Ut egestas ante at dolor. Etiam sit amet elit eu leo sollicitudin pretium. Phasellus non sapien venenatis nunc dapibus

Ilustración 83 Acceso al documento contenido en la carpeta "DoingBusiness" a través de navegación forzada

5. Ataque de tampering de parámetros

Mediante el siguiente ataque, se pudo identificar una vulnerabilidad en el aplicativo web, el cual permite modificar los parámetros del código fuente para iniciar de manera fraudulenta al sistema con privilegios de administrador. Esto se realizó copiando la estructura del menú de "Login/Registrer" en un archivo plano, cambiando el comportamiento del botón de "Registrer" para que, al ser pulsado, redirija al sistema original y allí se cambie el parámetro de "Registrer" por el de "admin".

Ilustración 84 Código fuente del menú de "Login/Registrer" copiado en un archivo plano con la modificación en la acción del botón de "Registrer"

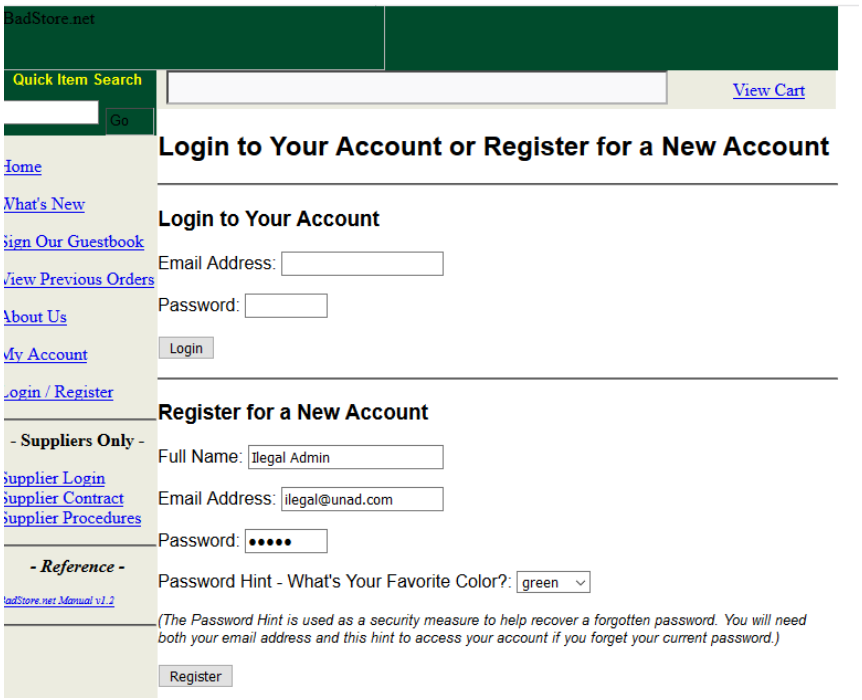


Ilustración 85 Registro fraudulento de un usuario

Ilustración 86 Usuario registrado en el sistema

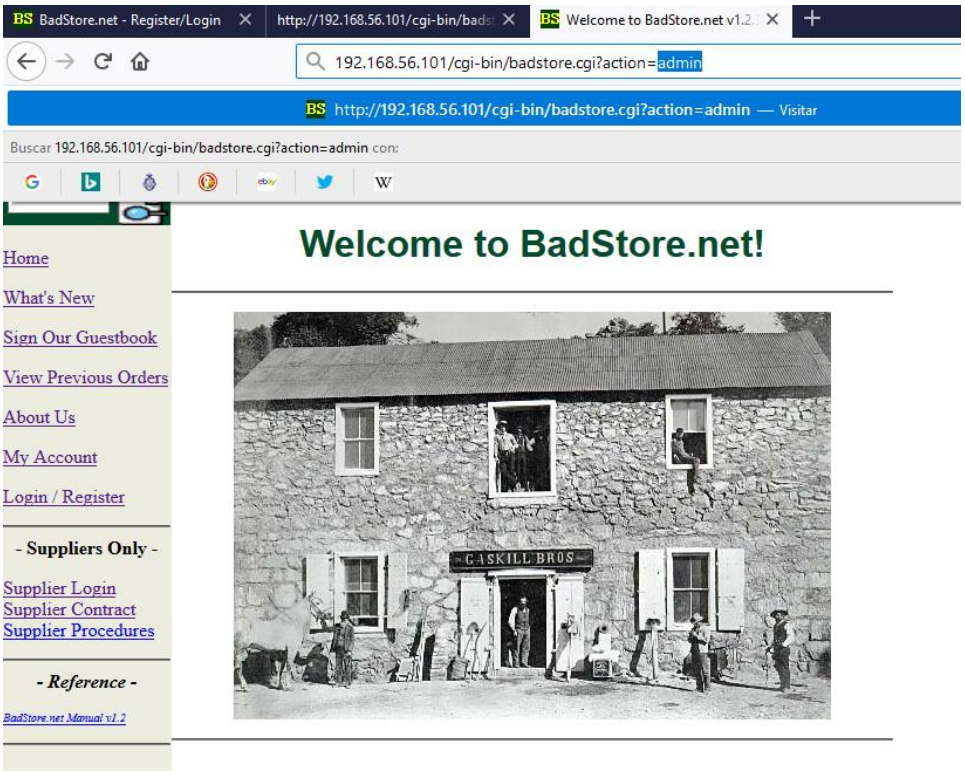


Ilustración 87 Modificación del parámetro "Registrer" por "Admin"

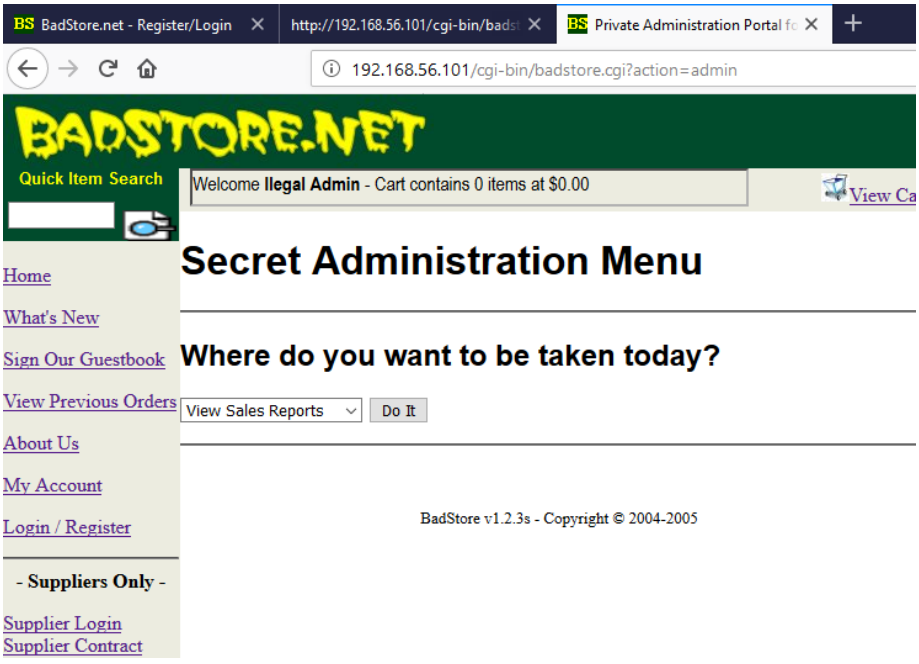


Ilustración 88 Usuario logeado como administrador

6. Ataque de cookie snooping

En este ataque, a través de una herramienta que permite visualizar y modificar cada uno de los comportamientos del sistema web, como las peticiones, la entrada de los datos, entre otros, se realizó la captura de una cookie en donde se realizó el cambio de la variable U = user a la de A = admin de un usuario previamente registrado.

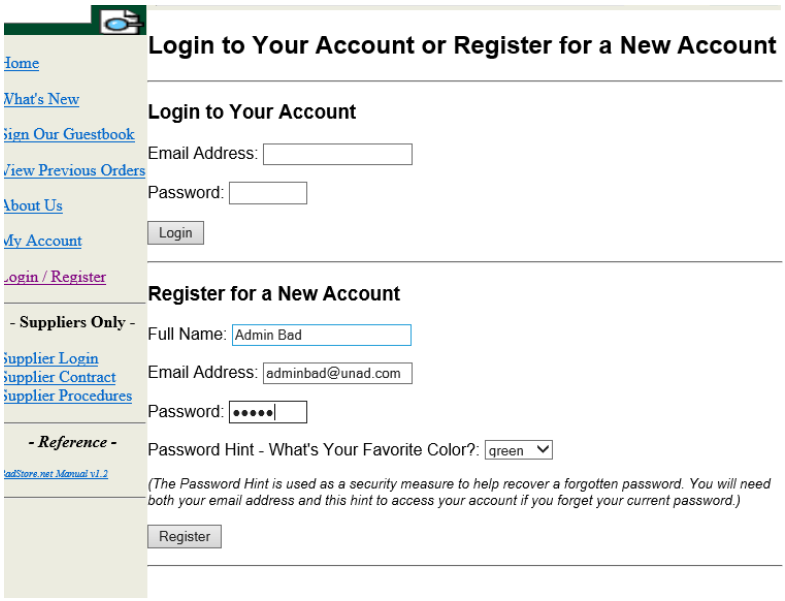


Ilustración 89 Registro de usuario

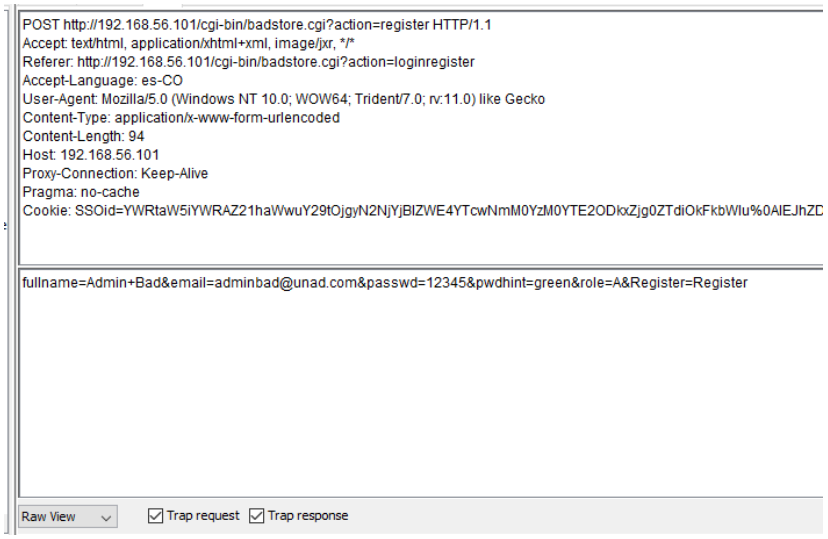


Ilustración 90 Modificación de la variable "U" por "A"

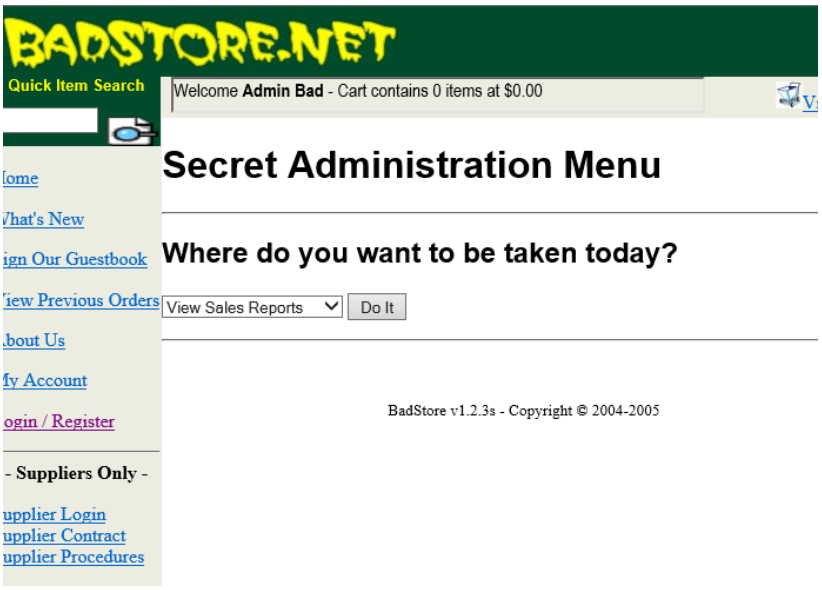


Ilustración 91 Usuario logeado como administrador

7. Ataque de denegación de servicio

A través de la utilización de las utilidades integradas en el sistema operativo Kali Linux, se pudo comprobar que el aplicativo web Badstore es susceptible a ataques como los de denegación de servicio ya que, a través de unas cuantas peticiones hechas mediante un conjunto de instrucciones, el sistema dejo de funcionar y se volvió inaccesible.

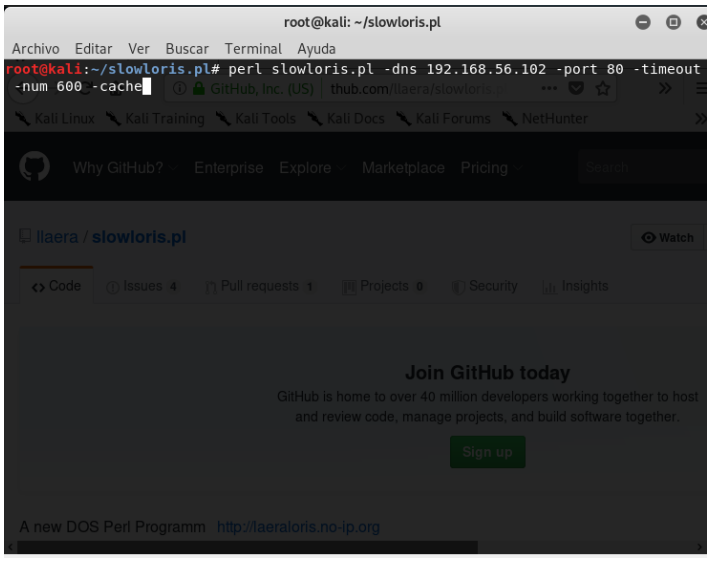


Ilustración 92 Ataque de denegación de servicio desde Kali Linux

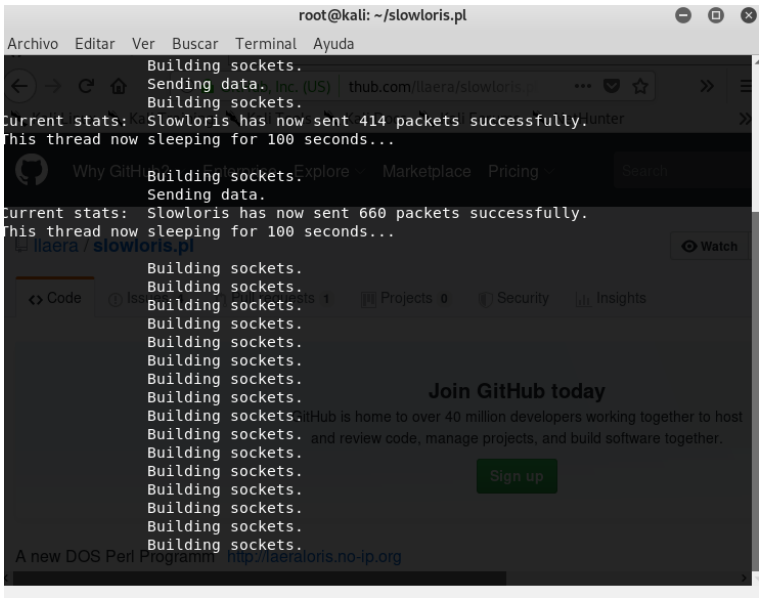


Ilustración 93 Envió de peticiones al aplicativo web Badstore

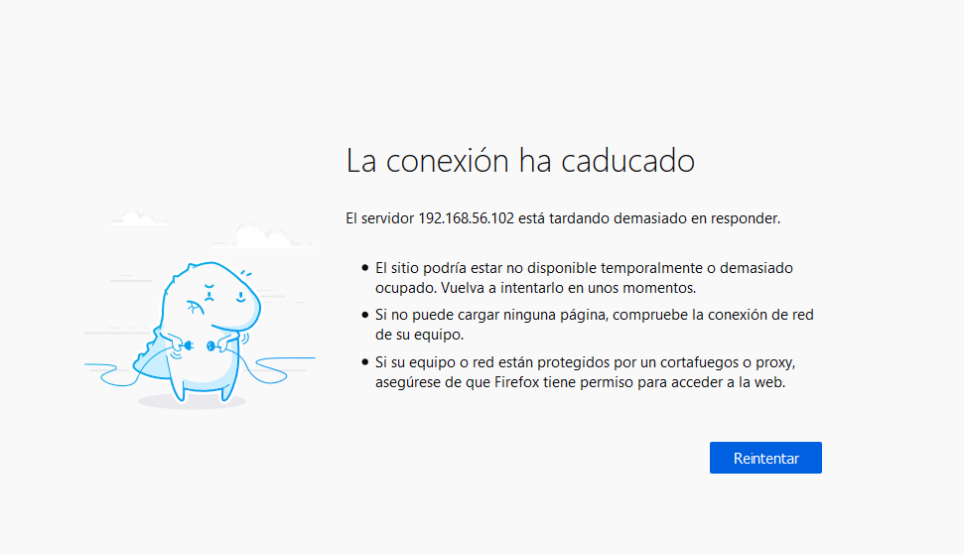


Ilustración 94 Sistema web inaccesible

8. Ataque de directory transversal

Las pruebas de pentesting permitieron comprobar que Badstore permite realizar ataques de tipo directory transversal, permitiendo realizar una navegación entre los directorios y facilitando el acceso a diversos archivos como las imágenes de los productos, el directorio de los menus, entre otros.

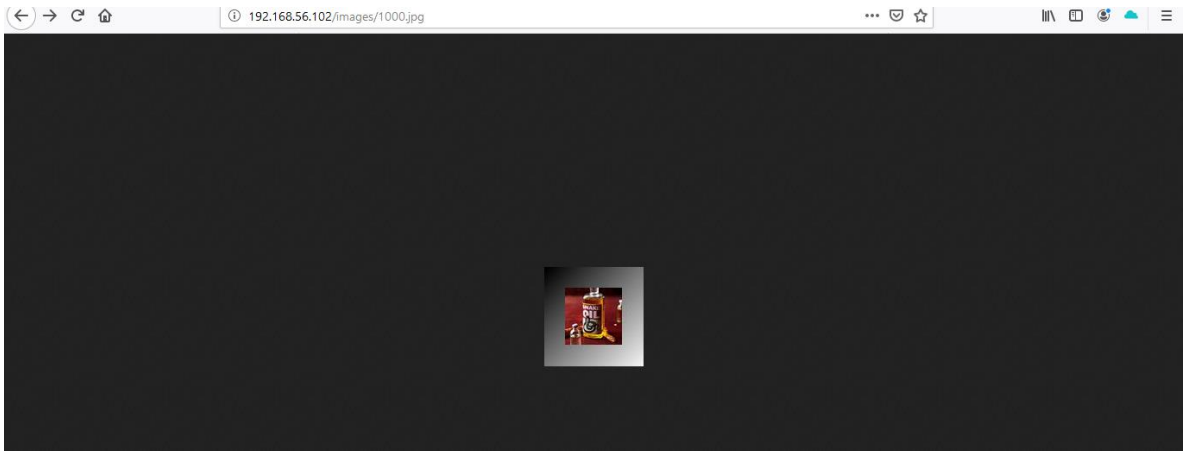


Ilustración 95 Acceso a las imágenes del sistema mediante ataque de directory transversal

Ilustración 96 Acceso al archivo de configuración del sistema mediante ataque de directory transversal

CONCLUSIONES

Mediante la ejecución de este proyecto se logró diseñar e implementar el mejoramiento de una infraestructura de red de datos haciendo uso de entornos virtualizados que permitieron el aseguramiento de los procesos y la información del caso de estudio de la empresa XYZ. De igual manera, se adquirieron diversos conocimientos acerca de nuevas tecnológicas de seguridad perimetral y pentesting, y mecanismos para la mitigación de vulnerabilidades para de esta manera, otorgar niveles de seguridad óptimos que le permiten a la compañía mantener la continuidad del negocio a la vanguardia de la tecnológica.

La creación de entornos virtualizados para el caso de estudio de la empresa XYZ permitió el mejoramiento de la seguridad de la infraestructura de la red de datos contribuyendo en el aprovechamiento de los recursos de la organización proporcionando una disminución en tiempos de administración y costos de implementación que contribuyen con los objetivos de la organización, garantizando la seguridad tecnológica y de la información.

La implementación de dispositivos de seguridad perimetral en la infraestructura de red de datos como Mikrotik, permitió elevar el nivel de aseguramiento de los procesos y la información, gracias a que esta tecnología ofrece una unificación de elementos de la red y de esta manera la compañía del caso de estudio logro la centralización de recursos y servicios como routers, firewalls, conexiones VPN, redes inalámbricas, controles de accesos y administración de anchos de banda, generando beneficios enfocados a la seguridad de la información y rendimiento de la red, de forma que se garantice la integridad, confidencialidad y disponibilidad de la información durante los procesos de transmisión de datos entre cada una de las sedes.

La ejecución de pruebas de pentesting para el software que soporta los proceso de la empresa (Badstore) permitió la identificación de vulnerabilidades presuntamente causadas por malas prácticas de desarrollo por parte del proveedor del aplicativo, que al ser explotadas, conlleva a la materialización del riesgo ya que se está comprometiendo la información sensible de la organización, lo cual puede desencadenar en pérdidas económicas, operativas y estratégicas, y a su vez, la generación de nuevas amenazas en la seguridad perimetral de toda la compañía y la red de datos.

Para la disminución de las brechas de seguridad que presenta la herramienta Badstore y la infraestructura de red de datos, es recomendable la utilización de diversas soluciones de aseguramiento como un WAF, el cual permitirá controlar y monitorear la información entrante y saliente de la red durante la operación del aplicativo; todo esto apoyado de buenas prácticas de documentación relacionada con la prevención de las vulnerabilidades y procedimientos de contingencia ante la presencia de amenazas.

RECOMENDACIONES

Para aumentar el nivel de seguridad en una red que haga uso de tecnología Mikrotik, se pueden configurar elementos adicionales de forma perimetral en la red como un firewall que realice un filtro inicial de las entradas y salidas, además utilizar herramientas de monitoreo que permitan la generación de alertas de seguridad de manera preventiva.

No se recomienda que los servidores de una compañía estén centralizados en un solo punto, ya que ante un ataque cibernético o un desastre natural difícilmente se podría colocar en marcha un plan de continuidad del negocio.

Es importante mantener actualizados los manuales y procedimientos que den cumplimento a la política de seguridad informática en las organizaciones, ya que esto contribuye en el aseguramiento de la infraestructura y la información, al genera buenas prácticas de seguridad informática.

Para implementaciones bajo tecnología Mikrotik que esté orientada a compartir recursos se recomienda, contar con un adecuado ancho de banda de internet que garantice estos procesos, optimizando tiempos y facilitando la labor de los funcionarios.

Se recomienda la creación de backups periódicos de cada uno de los dispositivos que permita el restablecimiento del sistema en caso de que ocurra algún incidente que comprometa el funcionamiento físico y lógico de este elemento. Se sugiere que esta copia de seguridad sea almacenada en un entorno distinto al de la empresa para asegurar la disponibilidad de los mismos.

Es recomendable la contratación de soporte técnico por parte del proveedor de la tecnología o consultores certificados en Mikrotik para lograr un mantenimiento confiable de los dispositivos que genere beneficios adicionales a la compañía tales como: capacitación del personal en el diseño, implementación y mantenimientos de redes.

Se recomienda la implementación de una DMZ (zona desmilitarizada) que aislé los servicios web de la organización evitando las intrusiones por accesos a través de estos medios y la explotación de vulnerabilidades relacionadas con fallos de seguridad que se puedan encontrar.

Es aconsejable la realización constante de actualizaciones al sistema operativo RouterOS para la aplicación de parches de seguridad que permitan dar solución a las diferentes vulnerabilidades que se puedan detectar en el sistema operativo y que pueden ser explotadas por las vulnerabilidades.

Se sugiere el cambio de la configuración por defecto que estos dispositivos traen de fabrica como lo es el usuario administrador y contraseña, que por lo general es Admin y no tiene contraseña. Es necesario la sustitución de estos por unas credenciales más seguras donde se utilicen diversos caracteres alfanuméricos y contenga una longitud mínima de 8 elementos.

Para otorgar una mayor seguridad a los dispositivos Mikrotik y a la red en general de una compañía se recomienda desactivar los servicios que no se vayan a utilizar, ya que si esto no se realiza, la red se está exponiendo a ser afectada por alguna amenaza que utilice este recurso como vía de acceso.

En el uso de dispositivos Mikrotik, se aconseja desactivar la función Neighbor Discovery la cual se puede utilizar para evitar que el equipo Mikrotik sea visualizado en la red para establecer la interfaz de conexión con el aplicativo Winbox.

Para mantener la seguridad en la red y en los dispositivos Mikrotik, es sugiere implementar configuraciones para limitar el número de conexión a usuarios, esto con el fin de prevenir conexiones no autorizadas en la red que puedan provocar riesgos en el funcionamiento de la misma.

Se recomienda la realización de auditorías a los dispositivos Mikrotik para evaluar las configuraciones de seguridad establecidas en el mismo. Esto se puede realizar haciendo uso de herramientas como Scapy, Hping3, Wireshark, entre otras.

Para mejorar la seguridad y el funcionamiento de la infraestructura de red de la compañía, se recomienda realizar manuales de instalación y configuración de cada uno de los dispositivos de red para garantizar que siempre se mantenga en correcto funcionamiento cada uno de estos elementos ante cambio de personal, remplazo de los elementos, entre otros.

Para garantizar el control del uso de los recursos tecnológicos de seguridad como lo es el Web Application Firewall (WAF) se recomienda crear formatos para la realización de bitácoras que permitan realizar un seguimiento a cada una de las modificaciones que se realicen en la reglas de protección que este tenga configurado y evitar fallos de seguridad por malas configuraciones.

BIBLIOGRAFIA

3CX. [En línea]. ¿Qué es la telefonia IP?. [Citado 05, diciembre, 2019]. Disponible en: https://www.3cx.es/voip-sip/telefonia-ip/

ACUNETIX. [En línea]. What is a Directory Traversal attack? [Citado 04, septiembre, 2019]. Disponible en: https://www.acunetix.com/websitesecurity/directory-traversal/#targetText=Directory%20traversal%20or%20Path%20Traversal,Root%20directory

ANDREU, Fernando;PELLEJERO,Izaskun;LESTA, Amaia. [En línea]. Fundamentos y aplicaciones de seguridad en redes WLAN. [Citado 20, octubre, 2018]. Disponible en: https://books.google.es/books?hl=es&lr=&id=k3JuVG2D9lMC&oi=fnd&pg=PA1&dq=RED+WLAN&ots=8Ftd_ziXdJ&sig=rCt6XJqQlaI1nPoZS5MDsFejia0#v=onepage&q&f=false

ANDREU,Joaquin. [En línea]. *Servivios en red*. [Citado 17, octubre, 2018]. Disponible en: https://books.google.com.co/books?id=vhit3ZmGQPsC&pg=PA213&dq=RED+WPAN&hl=es&sa=X&ved=0ahUKEwii5IeJiq_mAhUqqlkKHYmFBREQ6AEIKTAA#v=onepage&q=RED%20WPAN&f=false

CATORIA, Fernando. [En línea]. Consejos para evitar un ataque de denegación de servicio, 2012 . [Citado 04, septiembre, 2019]. Disponible en: https://www.welivesecurity.com/la-es/2012/03/28/consejos-ataque-denegacion-servicio/

CONEXIÓN ESAN. [En línea]. ¿Qué es y para que sirve la Norma ISO 27001?, 2016. [Citado 05, diciembre, 2019]. Disponible en: https://www.esan.edu.pe/apuntes-empresariales/2016/05/que-es-y-para-que-sirve-la-norma-iso-27001/

CONGRESO DE LA REPUBLICA DE COLOMBIA. [En línea]. LEY 1273 DE 2009, 2009. [Citado 04, noviembre, 2018]. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

CORPORACION COLOMBIA DIGITAL. [En línea]. ¿Cuáles son los sectores que más han avanzado en infraestructura tecnológica?, 2017. [Citado 21, octubre, 2018]. Disponible en: https://colombiadigital.net/actualidad/noticias/item/9608-cuales-son-los-sectores-que-mas-han-avanzado-en-infraestructura-tecnologica.html

GALLEGO, Jose. [En línea]. *Instalacion y mantenimiento de redes para transmision de datos*. [Citado 17, octubre, 2018]. Disponible en : https://books.google.com.co/books?id=qt_SCQAAQBAJ&pg=PA37&dq=Red+WWAN&hl=es&sa=X&ved=0ahUKEwj3t4ijha_mAhWoxVkKHVS7AwMQ6AEIQjAD#v=onepage&q=Red%20WWAN&f=false

GUTIERREZ, Camilo. [En línea]. *Tipos de redes VPN y cómo funcionan: ¿ya sabes cuál usar?, 2016*. [Citado 23, noviembre, 2018]. Disponible en: https://www.welivesecurity.com/la-es/2016/06/08/tipos-redes-vpn-como-funcionan/

IBM. [En línea]. Protocolos TCP/IP. [Citado 02, diciembre, 2019]. Disponible en: https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/network/tcpip_protocols.html

MICROSOFT. [En línea]. ¿Qué es virtualización? [Citado 04, noviembre, 2018]. Disponible en: https://azure.microsoft.com/es-es/overview/what-is-virtualization/

MIKROTIK. [En línea]. About us. [Citado 17, octubre, 2018]. Disponible en: https://mikrotik.com/aboutus

MOLARES, Estela. [En Linea]. Internet y Sociedad: Relación y compromiso de beneficios colectivos e individuales, 2004. [Citado 11, diciembre, 2019]. Disponible en: http://www.revista.unam.mx/vol.5/num8/art49/sep_art49.pdf

PANDA. [En línea]. Pentesting: Una herramienta muy valiosa para tu empresa, 2018. [Citado 11, diciembre, 2019]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

SGSI. [En línea]. ISO 27001: El método MAGERIT, 2015. [Citado 16, noviembre, 2018]. Disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

PRENAFETA, Javier. [En línea]. Tipos de Pentesting, 2018. [Citado 23, noviembre, 2018]. Disponible en: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/ de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080521_56.pdf

REFERENCIAS BIBLIOGRAFICAS

ACADEMY XPERTS. [En línea]. MTCTCE. [Citado 17, octubre, 2018]. Disponible en: http://www.academyxperts.com/index.php/cursos/certificaciones-de-fabrica/mikrotik/mtctce

ANCHONDO, Daniel. [En línea]. Mikrotik - Protocolos de comunicación para enlaces inalámbricos. [Citado 21, octubre, 2018]. Disponible en: https://soporte.syscom.mx/redes-inalambricas-enlaces/mikrotik/mikrotik-protocolos-de-comunicacion-para-enlaces-inalambricos

ANRRANGO, Rodrigo. [En línea]. Características Importantes de los Equipos Mikrotik, 2015. [Citado 17, octubre, 2018]. Disponible en: https://configurarmikrotikwireless.com/blog/caracteristicas-importantes-equipos-mikrotik.html

ANRRANGO, Rodrigo. [En línea]. Qué es Mikrotik RouterOS y para qué sirve, 2015 [Citado 17, octubre, 2018]. Disponible en: https://configurarmikrotikwireless.com/blog/mikrotik-routeros-para-que-sirve.html

ALARCO, Nancy. [En línea]. MikroTik - Características principales de RouterOS. [Citado 17, octubre, 2018]. Disponible en: http://soporte.syscom.mx/networking/mikrotik/mikrotik-caracteristicas-principales-de-routeros

ASTERISK.ORG. [En línea]. *Asterisk*. [Citado 23, noviembre, 2018]. Disponible en: https://www.asterisk.org/

CENTOS. [En línea]. *Centos.org*. [Citado 23, noviembre, 2018]. Disponible en: https://www.centos.org/download/

CORNEJO FLORES, Jairo Manuel; VAN HEMELRIJCK LUZA, Eduardo Bruno. [En línea]. Implementación de un hotspot wifi basado en mikrotik, 2012. [Citado 17, octubre, 2018]. Disponible en: http://www.academia.edu/16459310/Implementacion_Hotspot_Mikrotik

CRESPO, Adrian. [En línea]. Utilizan routers MikroTik para infectar equipos Windows, 2018. [Citado 17, octubre, 2018]. Disponible en: https://www.redeszone.net/2018/03/10/mikrotik-infectar-windows-malware/

Di Rienzo, Victor; PICA, Gustavo; ROCHE, Emilio. [En línea]. Implementación de una red para la empresa Royal Tech, 2008. [Citado 17, octubre, 2018]. Disponible en: https://es.scribd.com/doc/7700198/Proyecto-Usando-Mikrotik

DISTIVOIP. [En línea]. DistiVoIP. [Citado 17, octubre, 2018]. Disponible en: http://www.distrivoip.com/cart/34_mikrotik

DRAGONJAR. [En línea]. Video: Ataque de envenenamiento de cookies (Cookie-Poisoning). [Citado 04, septiembre, 2019]. Disponible en: https://www.dragonjar.org/video-ataque-de-envenamiento-de-cookies-cookie-poisoning.xhtml

DUARTE, Ernesto. [En línea]. ¿Qué Es Mikrotik RouterOS?, 2014 [Citado 17, octubre, 2018]. Disponible en: http://blog.capacityacademy.com/2014/04/09/que-es-mikrotik-routeros/

EXPRESSVPN. [En línea]. *¿Que es un PPTP?* [Citado 23, noviembre, 2018]. Disponible en: https://www.expressvpn.com/es/what-is-vpn/protocols/pptp

FERNANDEZ, Daniel. [En línea]. MikroTik arregla un fallo Zero-Day bajo ataque en tiempo récord. [Citado 17, octubre, 2018]. Disponible en: https://tecnonucleous.com/2018/04/25/mikrotik-arregla-un-fallo-zero-day-bajo-ataque-en-tiempo-record/

FERNANDEZ, Raul. [En línea]. *Cómo crear una VPN PPTP con Mikrotik y RouterOS, 2018*. [Citado 23, noviembre, 2018]. Disponible en: https://www.raulprietofernandez.net/blog/mikrotik/como-crear-una-vpn-pptp-con-mikrotik-y-routeros

FIS SOLUCIONES. [En línea]. FIS Soluciones. [Citado 17, octubre, 2018]. Disponible en: http://www.fisoluciones.com/

FLYNET. [En línea]. Casos de exito. [Citado 17, octubre, 2018]. Disponible en: http://flynetwifi.com/casosexito.html

GUTIERREZ, Angel. [En línea]. Cómo instalar Windows en VirtualBox, 2018. [Citado 23, noviembre, 2018]. Disponible en: https://www.aboutespanol.com/como-instalar-windows-en-virtualbox-3507786

HENRYRAUL. [En línea]. ¿Que es un ataque de tipo “Parameter Tampering” y como puede evitarse?, 2017. [Citado 04, septiembre, 2019]. Disponible en: https://henryraul.wordpress.com/2017/02/26/en-que-consisten-los-ataques-parameter-tampering-y-como-pueden-evitarse/

IDEONEOS.ORG. [En línea]. Redes Alambricas. [Citado 17, octubre, 2018]. Disponible en: http://idoneos.org/ovas/60/redes_alambricas.html

IDROVO, W. H. [En línea]. Analisis e implementacion de politicas de seguridad para WISP mediante equipos Mikrotik y elementos de red. [Citado 17, octubre, 2018]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/12127/1/UPS-CT006042.pdf

IEEE. [En línea]. EL ESTÁNDAR IEEE 802.11 . [Citado 17, octubre, 2018]. Disponible en: http://bibing.us.es/proyectos/abreproy/11138/fichero/memoria%252FCap%C3%ADtulo+3.pdf+

INTEGRAL COMUNICACIONES SRL. [En línea]. Solución de Cámaras Urbanas. [Citado 17, octubre, 2018]. Disponible en: http://www.integralcomunicaciones.com/site/casos-de-exito/

INTERNETWORK SOLUTION. [En línea]. Caso de exito: ptp 21km mikrotik, 2017. [Citado 17, octubre, 2018]. Disponible en: https://www.iws.ec/blog/caso-de-exito-ptp-21km-mikrotik

INTERNETWORK SOLUTION. [En línea]. Noticia #2: mikrotik en amazon datacenter, 2017 [Citado 17, octubre, 2018]. Disponible en: https://www.iws.ec/blog/noticia-2-mikrotik-en-amazon-datacenter

INTERNETWORK SOLUTION. [En línea]. Caso de exito: rt telecom. [Citado 17, octubre, 2018]. Disponible en: https://www.iws.ec/blog/caso-de-exito-rt-telecom

INTERNETWORK SOLUTION. [En línea]. Casos de exito. [Citado 17, octubre, 2018]. Disponible en: https://www.iws.ec/blog

MICROSOFT. [En línea]. seguridad y protección. [Citado 17, octubre, 2018]. Disponible en: https://msdn.microsoft.com/es-es/library/hh831778(v=ws.11).aspx

MICROSOFT. [En línea]. *Descargar imágenes de disco de Windows 7 (archivos ISO)*. [Citado 23, noviembre, 2018]. Disponible en: https://www.microsoft.com/es-mx/software-download/windows7

MIKROTIK COLOMBIA. [En línea]. Router OS. [Citado 17, octubre, 2018]. Disponible en: https://www.mikrotikcolombia.com.co/software.html

MIKROTIK. [En línea]. About us. [Citado 17, octubre, 2018]. Disponible en: https://mikrotik.com/aboutus

MIKROTIK. [En línea]. Manual:TOC. [Citado 17, octubre, 2018]. Disponible en: https://wiki.mikrotik.com/wiki/Manual:TOC

MIKROTIK. [En línea]. Schedule. [Citado 17, octubre, 2018]. Disponible en: https://mikrotik.com/training/

MIKROTIK PERU. [En línea]. Beneficios Soluciones Mikrotik. [Citado 17, octubre, 2018]. Disponible en: http://www.mikrotik.com.pe/index.php/10-mikrotik/25-beneficios-soluciones-mikrotik

MIKROTIK SOLUTIONS INTERNATIONAL. [En línea]. MikroTik Certified Wireless Engineer. [Citado 17, octubre, 2018]. Disponible en: http://www.mikrotiksolutions.com/certificaciones/mikrotik/mtcwe/

MKE SOLUTIONS. [En línea]. Actualización de seguridad en RouterOS, 2018. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/noticias/actualizacion-de-seguridad-en-routeros/

MKE SOLUTIONS. [En línea]. Consejo Profesional de Cs Económicas de Santa Fe. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/mke-solutions/casos-de-exitos/

MKE SOLUTIONS. [En línea]. Digital Herrera. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/mke-solutions/casos-de-exitos/

MKE SOLUTIONS. [En línea].. Integra. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/mke-solutions/casos-de-exitos/

MKE SOLUTIONS. [En línea]. SpeedyCom. [Citado 17, octubre, 2018]. Disponible en: de https://www.mkesolutions.net/mke-solutions/casos-de-exitos/

MKE SOLUTONS. [En línea]. Universidad Católica de Santiago del Estero. [Citado 17, octubre, 2018]. Disponible en: https://www.mkesolutions.net/mke-solutions/casos-de-exitos/

MIS PASOS MIKROTIK. [En línea]. *MikroTik - Configurar Firewall Basico, 2017*. [Citado 23, noviembre, 2018]. Disponible en: http://mispasosmikrotik.blogspot.com/2017/05/mikrotik-configurar-firewall-basico.html

MOLINA, Fransisco. [En línea]. *Instalación de Mikrotik en VirtualBox, 2018*. [Citado 23, noviembre, 2018]. Disponible en: https://www.franciscomolina.cl/instalacion-de-mikrotik-en-virtualbox/

NAT COLOMBIA. [En línea]. Construye y administra redes MikroTik & Ubiquiti. [Citado 17, octubre, 2018]. Disponible en: http://natcolombia.com/

NETPRO. [En línea]. Reparación de RouterBoards Mikrotik con NETINSTALL (bricked router). [Citado 17, octubre, 2018]. Disponible en: http://www.netpro-ar.com/reparacion-de-routerboards-mikrotik-con-netinstall-bricked-router/

NUSKOPE. [En línea]. Australia Lawful interception, 2008. [Citado 17, octubre, 2018]. Disponible en: https://forum.mikrotik.com/viewtopic.php?t=87763

PAZ, Dennis. [En línea]. CONCEPTOS Y TÉCNICAS DE RECOLECCIÓN DE DATOS EN LA INVESTIGACIÓN. [Citado 17, octubre, 2018]. Disponible en: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080521_56.pdf

PCFIX. [En línea]. Casos de Éxito. [Citado 17, octubre, 2018]. Disponible en: http://www.pcfix.cl/casos-de-exito.php

PROZCENTER. [En línea]. MikroTik Certified Routing Engineer. [Citado 17, octubre, 2018]. Disponible en: http://www.prozcenter.com/cursos/mtcre/

REDHAT. [En línea]. ¿Qué es la virtualización? Recuperado el 04 de noviembre de 2018, de https://www.redhat.com/es/topics/virtualization/what-is-virtualization

SALTOS.ORG. [En línea]. *Creación de la máquina virtual para instalar CentOS 7*. [Citado 23, noviembre, 2018]. Disponible en: http://www.saltos.org/portal/es/wiki/view/358/instalar-centos-7-en-virtualbox

SINNAPS. [En línea]. METODOLOGÍA DE UN PROYECTO. [Citado 17, octubre, 2018]. Disponible en: https://www.sinnaps.com/blog-gestion-proyectos/metodologia-de-un-proyecto

SOLUTEK INFORMATICA. [En línea]. MIKROTIK COLOMBIA. [Citado 17, octubre, 2018]. Disponible en: http://mikrotik.solutekcolombia.com/

SYMANTEC. [En línea]. Postmortem of a Compromised MikroTik Router, 2018. [Citado 17, octubre, 2018]. Disponible en: https://www.symantec.com/blogs/threat-intelligence/hacked-mikrotik-router

TECNOLOGIAS. [En línea]. *Instalacion de asterisk en maquina virtual*, 2012. [Citado 23, noviembre, 2018]. Disponible en: http://tecnologianue.blogspot.com/2012/11/instalacion-de-asterisk-en-la-maquina.html

TELADATA. [En línea]. Casos de Éxito. [Citado 17, octubre, 2018]. Disponible en: http://www.teledata.la/exitos.html

TREND MICRO. [En línea]. Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign. [Citado 17, octubre, 2018]. Disponible en: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/over-200-000-mikrotik-routers-compromised-in-cryptojacking-campaign

UBIQUITI NETWORKS. [En línea]. Bienvenido al sitio de cables y redes WiFi. [Citado 17, octubre, 2018]. Disponible en: http://wifi.cablesyredes.com.ar.

UNICEN. [En Linea]. El modelo OSI. [Citado 27, noviembre, 2019]. Disponible en: http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

VELASCO, R. [En línea]. 170.000 routers MikroTik convertidos en una botnet y utilizados para minar criptomonedas por un fallo 0-day, 2018. [Citado 17, octubre, 2018]. Disponible en: https://www.redeszone.net/2018/08/02/routers-mikrotik-botnet-minar-monedas/

VELASCO, R. [En línea]. Un exploit permite conseguir permisos de root en cualquier router MikroTik, 2018. [Citado 17, octubre, 2018]. Disponible en: https://www.redeszone.net/2018/10/09/exploit-root-router-mikrotik/

WNI MEXICO. [En línea]. Licencia de Software RouterOS Nivel 4, WISP, 2018. [Citado 17, octubre, 2018]. Disponible en: https://wni.mx/index.php?page=shop.product_details&flypage=flypage_new.tpl&product_id=568&cate%20gory_id=79&option=com_virtuemart&Itemid=53

ANEXOS

Anexo 1

Se anexa video del funcionamiento de la conexión existente entre las sedes de la empresa XYZ, la cual le permitirá compartir los recursos que la empresa disponga. https://youtu.be/5pyk60_S69o

De igual forma se anexa el video en donde se realiza la explotación de 8 vulnerabilidades identificadas en el software Badstore: https://www.youtube.com/watch?v=hOXUPdQdBPw&t=22s

Anexo 2

PROPUESTA DE ASEGURAMIENTO PARA HERRAMIENTA BADSTORE

Dada la importancia que la herramienta Badstore representa para las operaciones comerciales y operacionales de la compañía, es necesario adoptar medidas de aseguramiento que permitan reducir las vulnerabilidades que este software pueda contener y que puedan afectar la seguridad de los procesos o la información, así como generar riesgos sobre cada uno de los recursos que interactúen con el aplicativo para la consulta de clientes y de esta manera se pueda ver afectada la infraestructura de la red de datos de la compañía.

Para cumplir con el aseguramiento de la herramienta Badstore y demás elementos de la red de datos de la empresa XYZ, se propone llevar a cabo las siguientes medidas:

Identificación de activos

La empresa XYZ debe realizar una identificación de activos que componen la red de datos, con el fin de individualizar las posibles vulnerabilidades que se encuentren en cada uno de sus componentes.

TIPO DE ACTIVO	NOMBRE ACTIVO	DESCRIPCIÓN DEL ACTIVO
INFORMACIÓN	Base de datos de clientes	Información referente a datos personales y financieros de los clientes
	Base de datos de empleados	Información de los empleados que se encuentran en cada una de las sucursales de la entidad
DATOS/ INFORMACIÓN	Datos de configuración	Manual y procedimiento para la configuración de servidores
	Contraseñas	Credenciales de autenticación para el acceso a servidores y al software Badstore
FÍSICO	Equipo Servidor en rack PowerEdge R440, Intel®	Equipo servidor web donde se encuentra alojado el sistema

	Xeon® escalables de 2, RAM 64 G, 5TB	Badstore y su respectiva base de datos
LÓGICO	Sistema operativo TRINUX,	Sistema operativo que soporta la herramienta Badstore
	Software BADSTORE	Solución Badstore que se encuentra desplegada en el servidor web.
HUMANO	Personal de recuperación de cartera	Empleados y colaboradores de la empresa que operan el sistema para la consulta de clientes y sus estados de cuenta
	Profesionales de tecnologías e información	Profesionales del área de tecnología e información que tienen a cargo el soporte de la aplicación

Vulnerabilidades que pueden afectar la herramienta badstore

A continuación, se relacionan las vulnerabilidades identificadas en el aplicativo web Badstore, a nivel físico, lógico y humano, las cuales puede afectar la funcionalidad de los activos que se mencionan en la siguiente tabla:

TIPO DE ACTIVO	NOMBRE ACTIVO	VULNERABILIDAD
INFORMACIÓN	Base de datos de clientes	Ataque SQL Injection
		Denegación de servicios
		Elevación de privilegios
	Base de datos de empleados	Ataque SQL Injection
		Denegación de servicios
		Elevación de privilegios
DATOS/ INFORMACIÓN	Datos de configuración	Alteración de la configuración
	Contraseñas	Robo de credenciales
FÍSICO	Equipo Servidor en rack PowerEdge R440, Intel® Xeon® escalables de 2, RAM 64 G, 5TB	Instalaciones físicas inadecuadas.
		Ausencia de control de acceso para personal no autorizado
LÓGICO	Sistema operativo TRINUX	Mantenimiento inadecuado
		Denegación de servicios
		Inexistencia de antivirus

	Software BADSTORE	Ataque XSS
		Modificación de cookies
		Ataque de navegación forzada
		Ataque de tampering de parámetros
		Ataque de cookie snooping
		Ataque de denegación de servicio
		Ataque de directory transversal
HUMANO	Personal de recuperación de cartera	Falta de restricciones para descarga de aplicaciones
		Los puertos USB no se encuentran bloqueados
		Falta de capacitación en cuanto a amenazas informáticas
	Profesionales de tecnologías e información	El personal que está a cargo del servidor web donde se encuentra la herramienta Badstore no está capacitado, en configuraciones de seguridad
		El personal de tecnologías e información se cambia constantemente

Medidas de aseguramiento para la mitigación de las vulnerabilidades

Para evitar la materialización de las posibles vulnerabilidades que pueden afectar el software Badstore, se propone efectuar las siguientes medidas de aseguramiento para aumentar el nivel de seguridad y de esta manera proteger la información de los procesos que soporta la herramienta y al mismo tiempo garantice seguridad en otros activos informativos de la empresa XYZ.

- **Ataque SQL Injection**

- Definir los valores en las consultas de tal forma que, aun utilizando enteros, estos estén delimitados por comillas sencillas.
- Validar los datos que introduce el usuario, mediante la comprobación del tipo de datos que se espera, haciendo uso de la función ctype_digit() que muchos lenguajes de programación ofren.
- Implementar un firewall de base de datos con reglas orientadas a la restricción de peticiones no autorizadas.

- **Denegación de servicios**

  - Implementación de un Web Application Firewall (WAF), para el control del flujo de paquetes dirigidas al servidor web.
  - Crear una zona desmilitarizada (DMZ) para ubicar el servidor en este punto con el fin de evitar afectaciones en otros servicios y en la información de la entidad.
  - Implementar un sistema de detección de intrusos para monitoreo de las conexiones.

- **Elevación de privilegios**

  - Implementar sistemas de autenticación múltiple para el acceso a las bases de datos.
  - Definición de roles y responsabilidades dentro de una política orientada a la seguridad de la información.
  - Realizar la creación de una VLAN única para llevar cabo la administración de la base de datos.

- **Alteración de la configuración**

  - Implementar un sistema de detección de intrusos para monitoreo de las conexiones.
  - Definición de roles y responsabilidades dentro de una política orientada a la seguridad de la información.

- **Robo de credenciales**

  - Implementación, actualización, ejecución de una solución de antivirus para el monitoreo del sistema en busca de malware.
  - Implementar una directriz para el cambio periódico de contraseñas.
  - Implementar lineamientos para la creación segura de contraseña.

- **Instalaciones físicas inadecuadas.**

- Realizar instalación de un sistema de extracción de calor y refrigeramiento.
- Realizar instalación de un piso antiestático.
- Implementación adecuada de una UPS para la regulación del flujo eléctrico.
- Implementar sensores de detección de incendios.

- **Ausencia de control de acceso para personal no autorizado**

  - Instalación de sistemas de acceso biométricos para evitar el acceso de personal no autorizado que pueda ocasionar daños físicos o robos de información.

- **Mantenimiento inadecuado**

  - Realizar capacitaciones al personal del personal DTI para la ejecución de mantenimientos adecuados a sistemas operativos y servidores de la entidad.
  - Realizar o actualizar manuales y procedimientos para la configuración y manteamiento de la herramienta Badstore y demás elementos de la red de datos.
  - Diseñar una bitácora para el control en la realización de mantenimientos.

- **Inexistencia de antivirus**

  - Implementación, actualización y mantenimiento de un sistema de antimalware que pueda afectar los elementos de la red de datos de la entidad.

- **Ataque XSS**

  - Implementación de un Web Application Firewall (WAF), para el control del flujo de paquetes dirigidas al servidor web.
  - Realizar e implementar procedimientos para la actualización de navegadores

- **Modificación de cookies**

  - Realizar e implementar procedimientos para la actualización de navegadores
  - Ejecución de ataques de hacking ético para la identificación de vulnerabilidades respecto a cookies.

- **Ataque de navegación forzada**

- Implementación de un Web Application Firewall (WAF), para el control del flujo de paquetes dirigidas al servidor Web.
- Implementación de captcha en el direccionamiento a los diferentes contenidos del sitio web.

- **Ataque de tampering de parámetros y Ataque de cookie snooping**

  - Implementación de un Web Application Firewall (WAF), para el control del flujo de paquetes dirigidas al servidor web.

- **Falta de restricciones para descarga de aplicaciones**

  - Realizar configuraciones en cada uno de los equipos de los trabajadores para restringir la instalación de software no autorizado por la compañía

- **Los puertos USB no se encuentran bloqueados**

  - Realizar el bloqueo de puertos USB y bandejas de CD, haciendo uso de una solución de antivirus.

Falta de capacitación en cuanto a amenazas informáticas

- Realizar capacitaciones trimestrales en cada una de las áreas misionales enfocadas a la prevención de amenazas y ataques informáticas**.**

- **El personal que está a cargo del servidor web donde se encuentra la herramienta Badstore no está capacitado, en configuraciones de seguridad.**

  - Realizar capacitaciones trimestrales para el personal TI enfocadas a la prevención de amenazas y ataques informáticas, desde una perspectiva técnica.

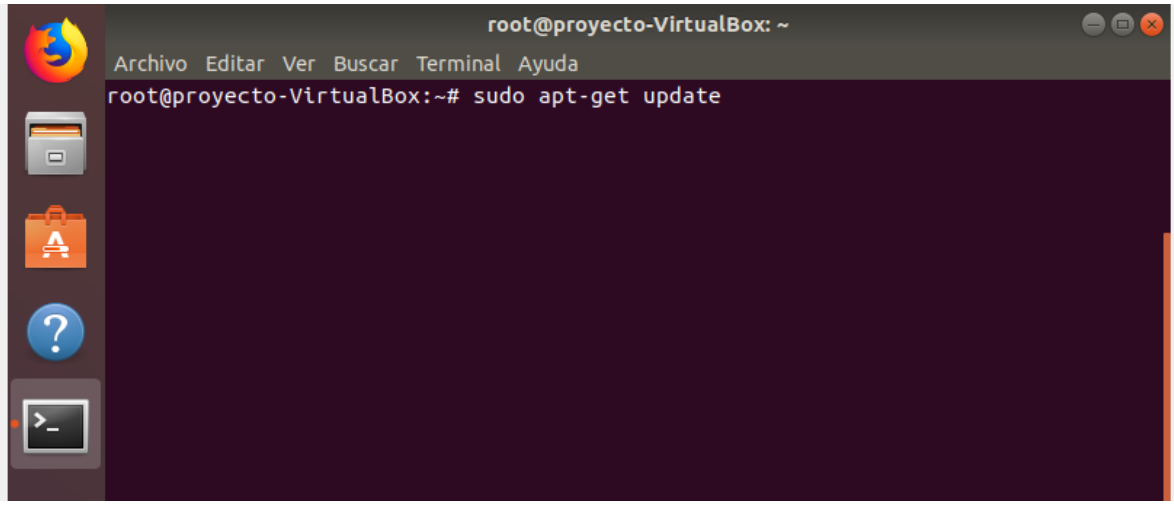
Anexo 3

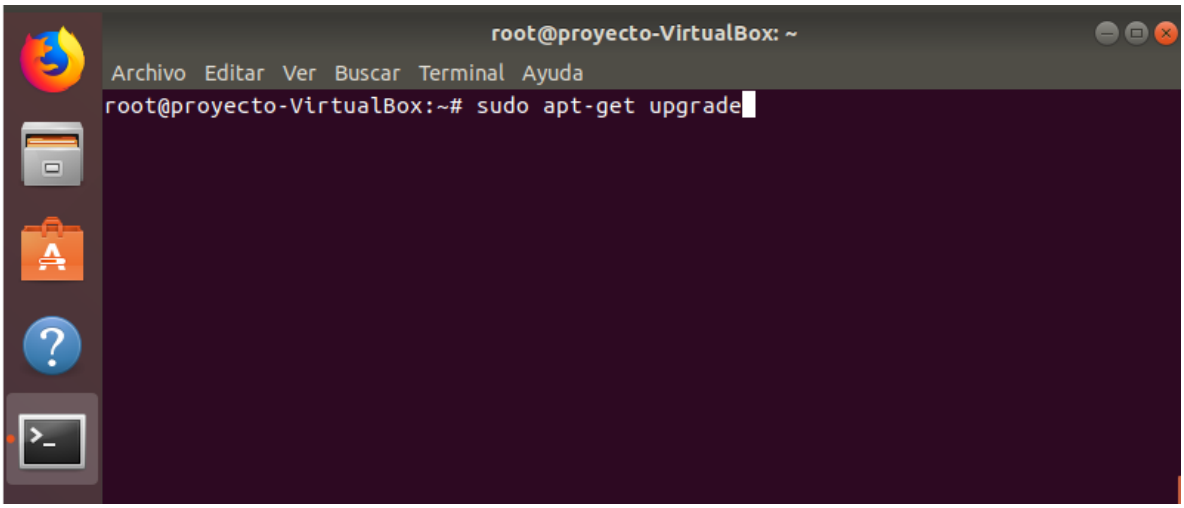
MANUAL DE INSTALACION Y CONFIGURACION DE UN WEB APPLICATION FIREWALL (WAF) PARA EL CASO DE ESTUDIO DE LA EMPRESA XYZ

A continuación, se realizará la explicación del proceso de instalación y configuración de un Web Application Firewall (WAF) de código abierto llamado ModSecurity sobre un sistema operativo Ubuntu, el cual está orientado a la protección de las vulnerabilidades encontradas en el aplicativo web Badstore del caso de estudio de la empresa XYZ.

Paso1: Actualización del sistema operativo

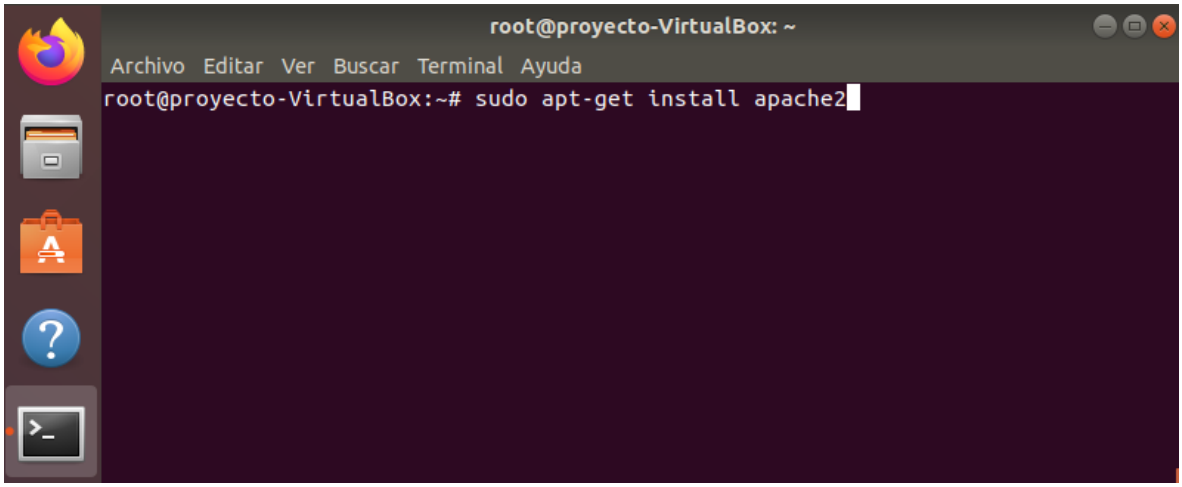
Como paso inicial, antes de realizar la instalación del WAF, se debe actualizar a su última versión el sistema operativo; para ello, en una terminal se deben escribir los comandos “sudo apt-get update” y “sudo apt-get upgrade”.





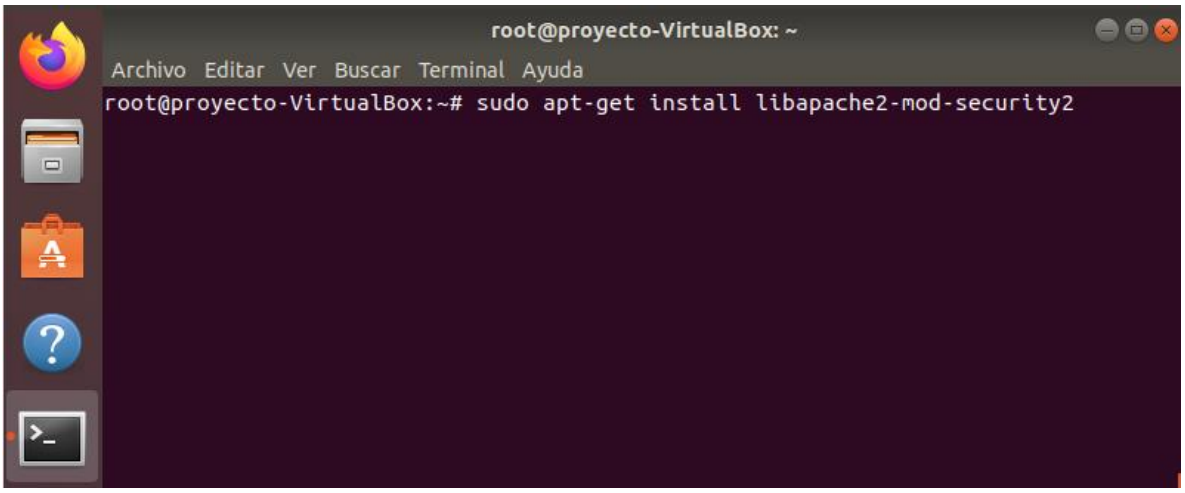
Paso 2: Instalación de Apache

Una vez finalizada la actualización, se procede a instalar Apache, el cual es un requisito para poder realizar la instalación del ModSecurity; para ello, en una terminal se debe escribir el comando “sudo apt-get install apache2”.



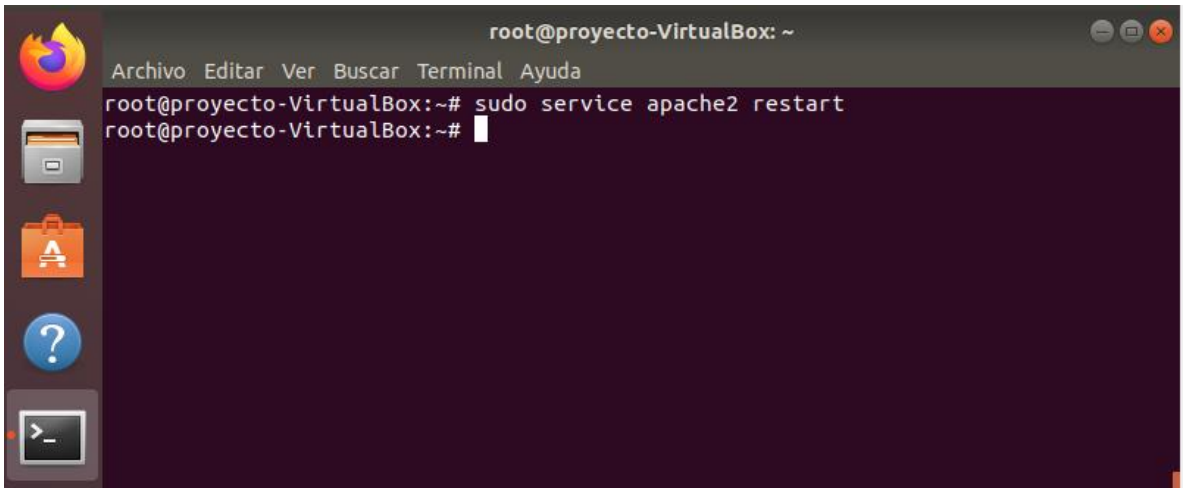
Paso 3: Instalación de ModSecurity

El siguiente paso corresponde a la instalación del WAF. En una terminal escribir el comando que visualiza en la siguiente imagen para ejecutar este procedimiento.



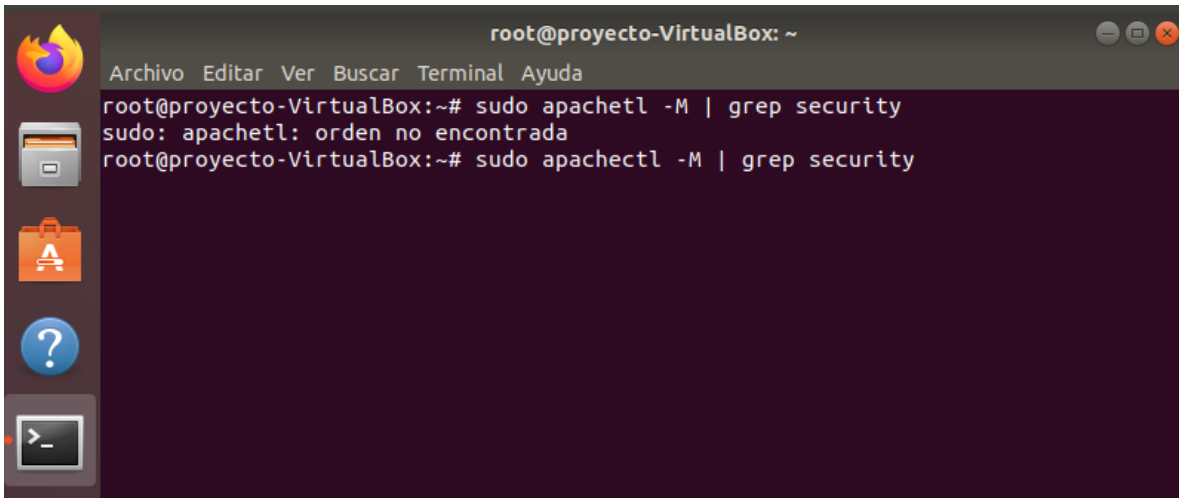
Paso 4: Reiniciar el servicio de Apache

A través del siguiente comando, se procede a reiniciar el servicio de Apache para que los cambios realizados durante la instalación de ModSecurity se efectúen.



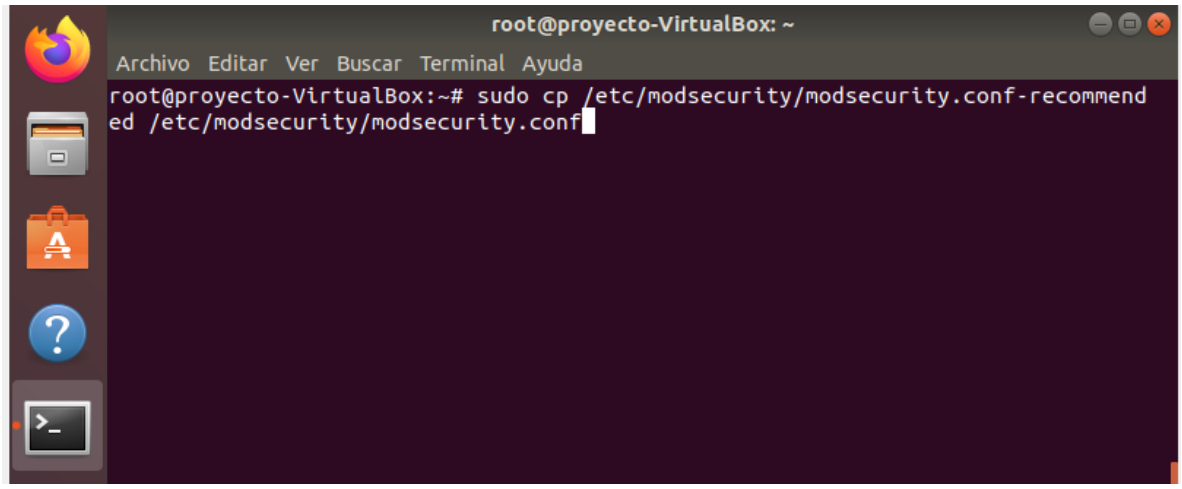
Paso 5: Verificación de la instalación

Con el comando que se visualiza en la siguiente imagen, se puede comprobar que ModSecurity se ha instalado correctamente; esto se comprueba mediante la visualización del mensaje que se ve en la segunda imagen



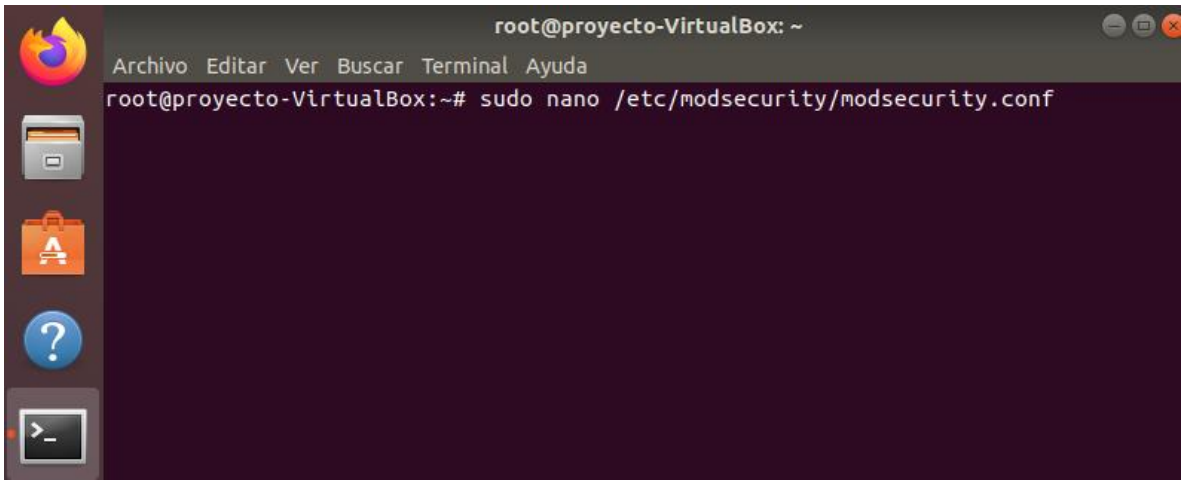
Paso 6: Copia archivo de configuración

Debido a que Modsecurirty para su funcionamiento requiere de la configuración de reglas para bloquear o permitir conexiones, se va a realizar la copia del archivo de configuración para su posterior edición.



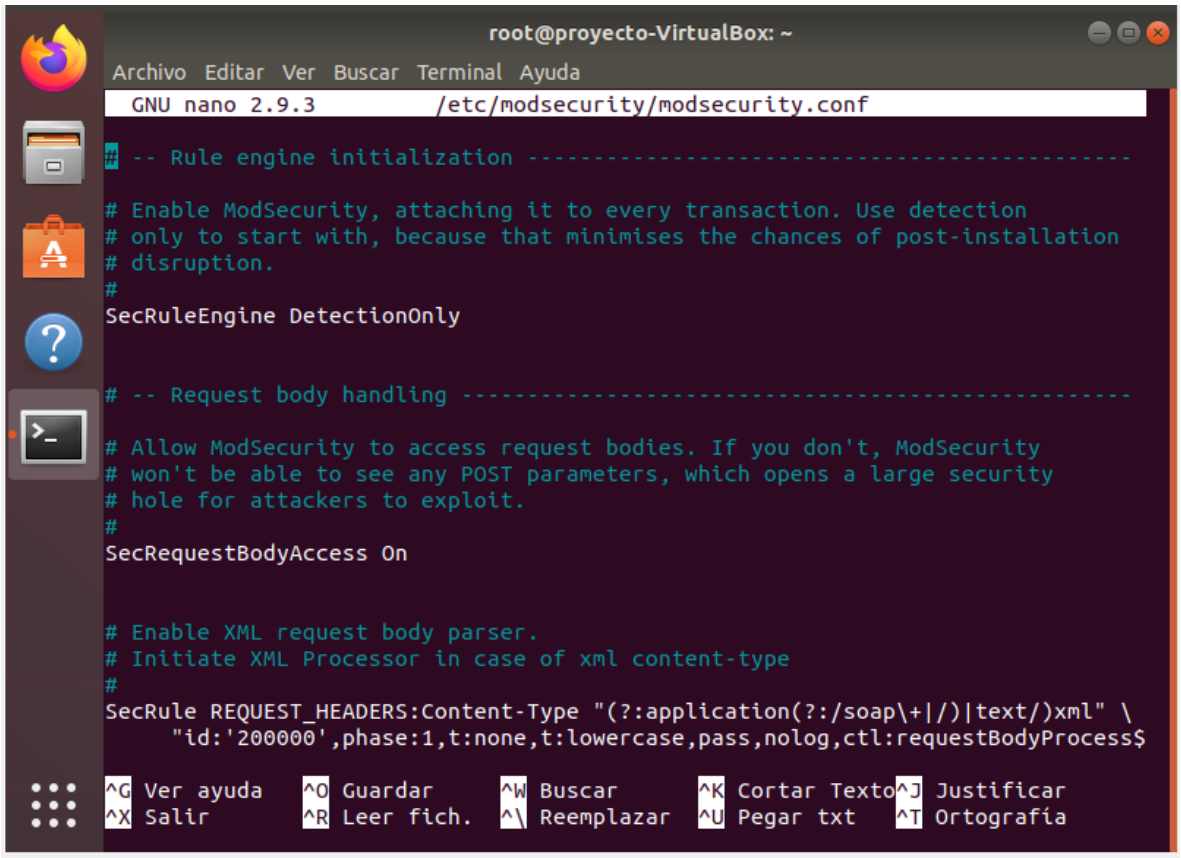
Paso 7: Ingreso al archivo de configuración

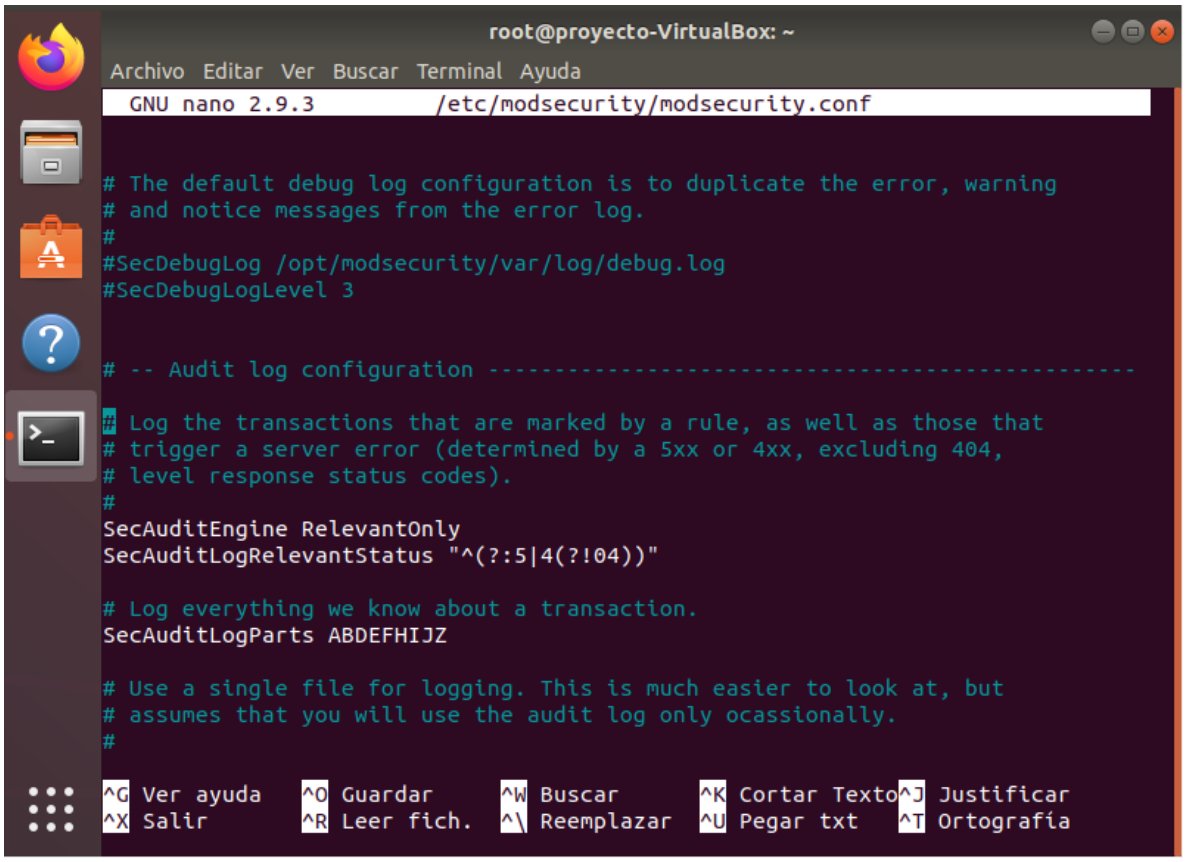
Realizado lo anterior, se procede a ingresar al archivo de configuración que fue copiado. Para esto se utilizará el editor de texto nano.



Paso 8: Validación de datos en el archivo de configuración

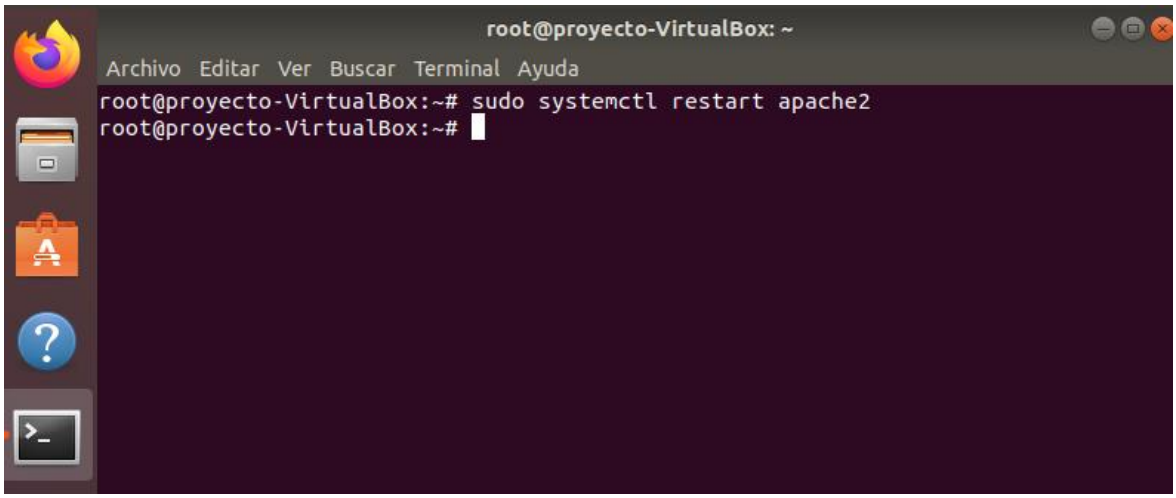
Una vez se haya ingresado al archivo de configuración, se valida que el parámetro “SecRequestBodyAccess” este en On y el campo “SecAuditLogParst” con tenga los datos que se aprecian en la segunda imagen. Hecho se guarda el archivo.


root@proyecto-VirtualBox: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3 /etc/modsecurity/modsecurity.conf
-- Rule engine initialization ----------
Enable ModSecurity, attaching it to every transaction. Use detection
only to start with, because that minimises the chances of post-installation
disruption.
#
SecRuleEngine DetectionOnly
-- Request body handling ----------
Allow ModSecurity to access request bodies. If you don't, ModSecurity
won't be able to see any POST parameters, which opens a large security
hole for attackers to exploit.
#
SecRequestBodyAccess On
Enable XML request body parser.
Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "(?:application(?:/soap\+|/)|text/)xml" \
"id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcess$
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía



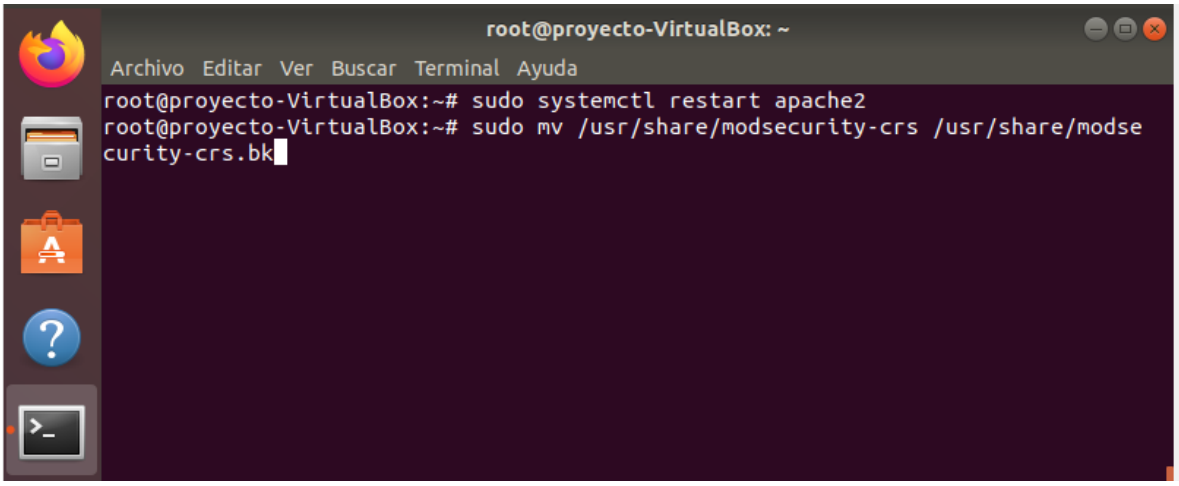
Paso 9: Reinicio del servicio de Apache

Se procede a realizar el reinicio del servicio de Apache para que se hagan efectivas las configuraciones realizadas



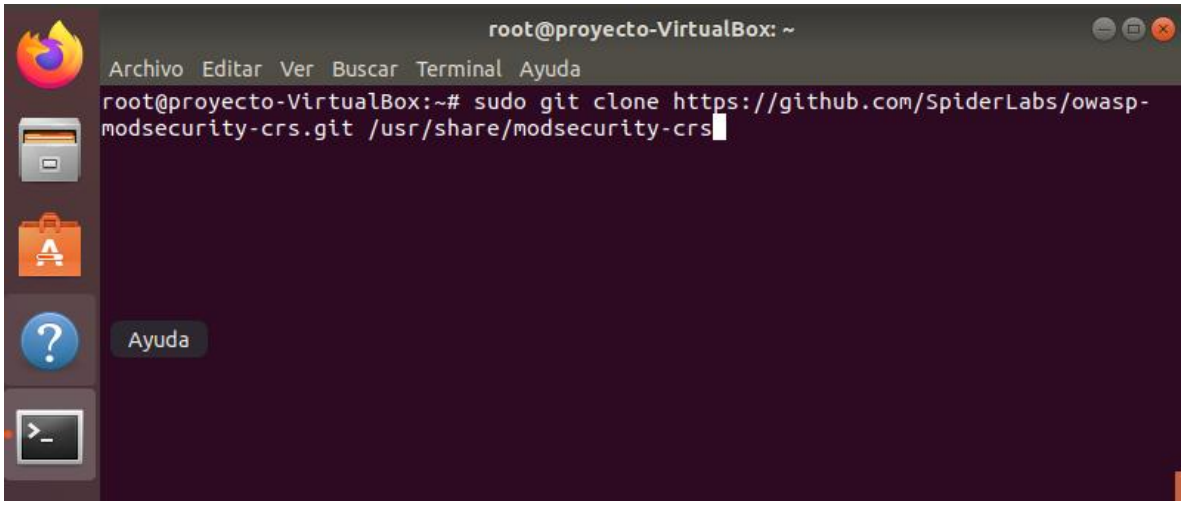
Paso 10: Renombrar archivo de configuración de reglas.

Para evitar daños en el funcionamiento del WAF, se procede a renombrar el archivo de configuración de reglas para su posterior creación



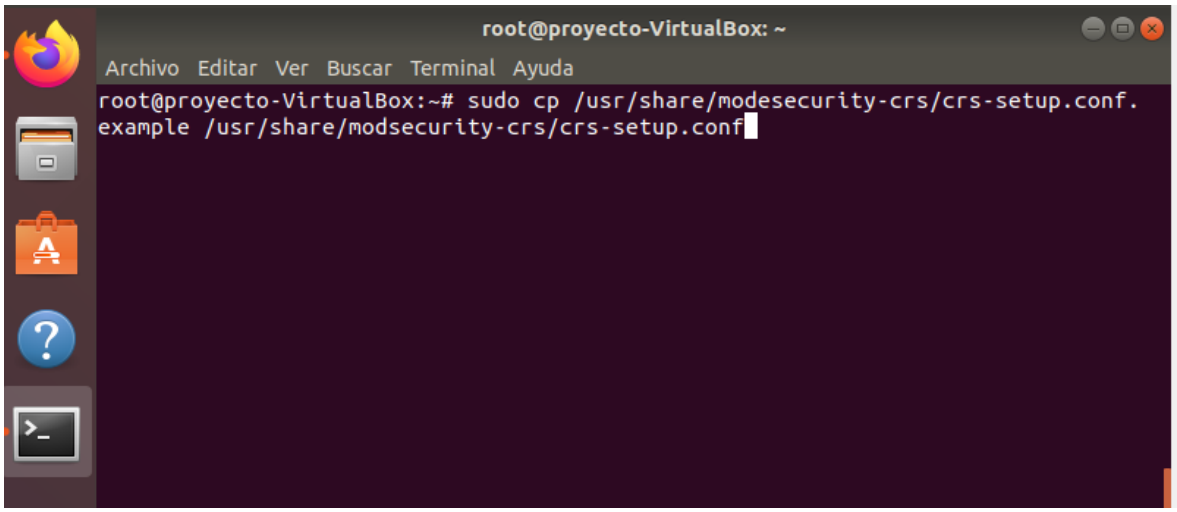
Paso 11: Descarga de reglas

OWASP (Proyecto abierto de seguridad en aplicaciones web) tiene a disposición un archivo de reglar orientado a Modsecurity, en el cual se incluyen reglas para la protección de las aplicaciones web ante ataques de tipo XSS, SQL Injection, navegación forzada, entre otros. Para hacer uso de este fichero, se procede a descargarlo desde los repositorios de Github



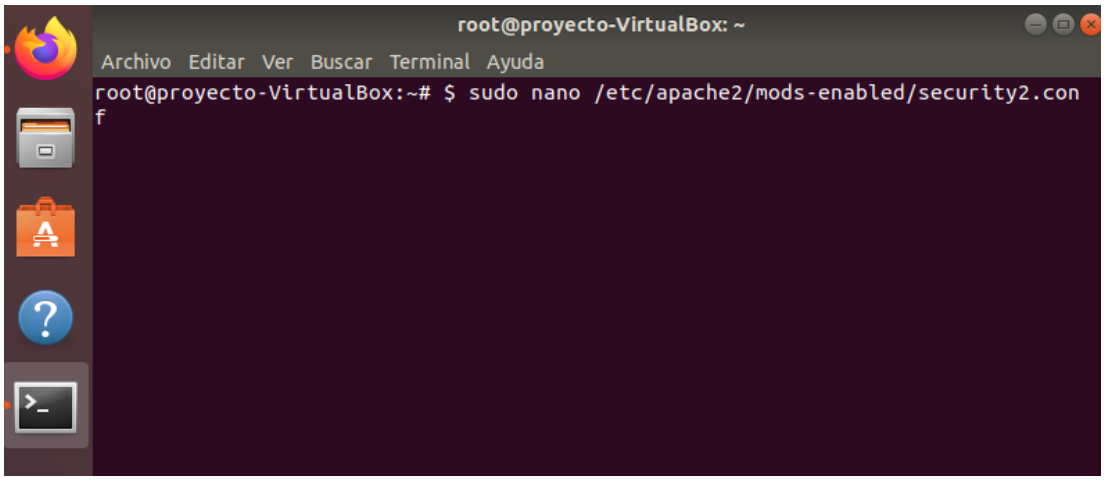
Paso 12: Copiar reglas

Se realiza la copia de la regla de seguridad descargada para su respectiva modificación



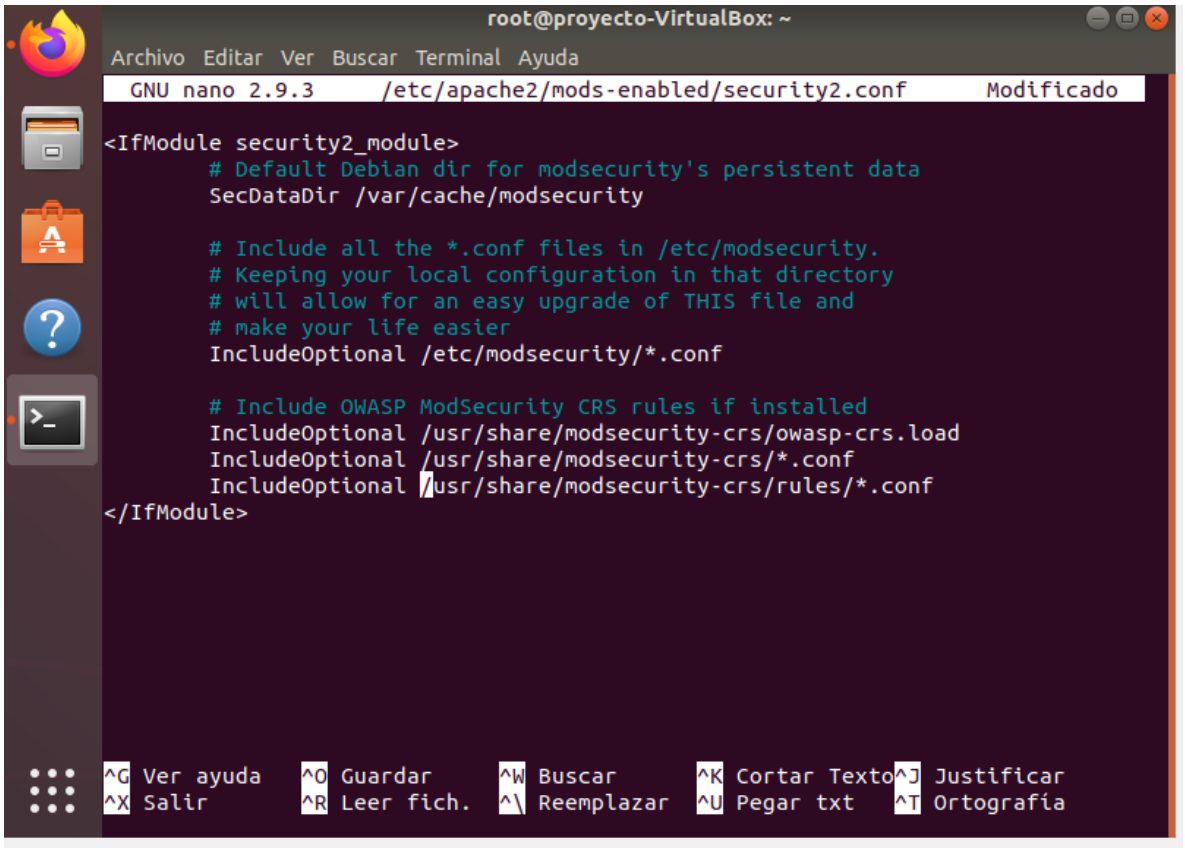
Paso 13: Ingreso al archivo de configuración de reglas

Con el comando nano, se procede a ingresar al archivo de configuración de reglas de Modsecurity



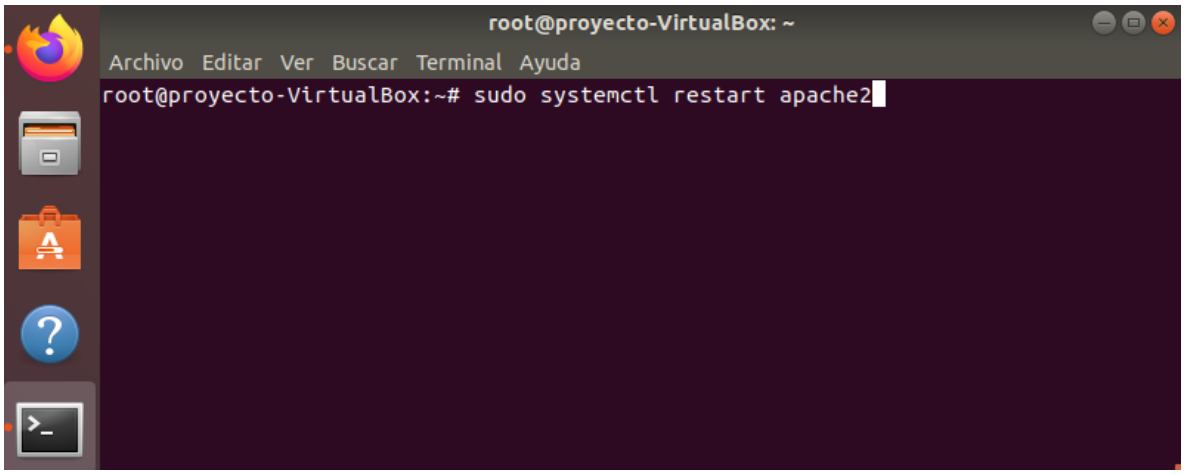
Paso 14: Editar el archivo de reglas

Una vez ingresado al archivo, se añaden las dos últimas líneas que se pueden apreciar en la siguiente imagen. Esto se realiza para indicarle a Modsecurity que reconozca el conjunto de reglas de seguridad anteriormente descargadas.



Paso 15: Reinicio del servicio de Apache y finalización del proceso

Guardo los cambios hechos en el archivo de configuración de reglas, se procede a realizar el reinicio del servicio de Apache. Si todo lo anterior se realizó de manera satisfactoria, el Web Application Firewall – Modsecurity habrá quedado instalado completamente.



Anexo 4

RESUMEN RAE

Fecha de Realización: 11/12/2016
Título: Diseño e implementación de una infraestructura de red de datos para el caso de estudio de la empresa XYZ a partir de un entorno virtualizado
Autor: Martínez Ripe, Harold Yesid; Bravo León, Mabel Rocío
Palabras Claves: Red, LAN, Mikrotik, servidor, entorno virtualizado, WAN, VPN, pentesting, Badstore, ataque, vulnerabilidad.
Descripción: El proyectos consiste en la implementación de una red de datos para el caso de estudio de la empresa XYZ, mediante entornos virtualizados que permitan el mejoramiento en materia de seguridad a nivel de hardware y software con tecnología Mikrotik y técnicas de pentesting.
Fuentes:
3CX. [En línea]. ¿Qué es la telefonia IP?. [Citado 05, diciembre, 2019]. Disponible en: https://www.3cx.es/voip-sip/telefonia-ip/
ACUNETIX. [En línea]. What is a Directory Traversal attack? [Citado 04, septiembre, 2019]. Disponible en: https://www.acunetix.com/websitesecurity/directory-traversal/#targetText=Directory%20traversal%20or%20Path%20Traversal,Root%20directory
ANDREU, Fernando;PELLEJERO,Izaskun;LESTA, Amaia. [En línea]. Fundamentos y aplicaciones de seguridad en redes WLAN. [Citado 20, octubre, 2018]. Disponible en: https://books.google.es/books?hl=es&lr=&id=k3JuVG2D9lMC&oi=fnd&pg=PA1&dq=RED+WLAN&ots=8Ftd_ziXdJ&sig=rCt6XJqQlaI1nPoZS5MDsFejia0#v=onepage&q&f=false
ANDREU,Joaquin. [En línea]. *Servivios en red*. [Citado 17, octubre, 2018]. Disponible en: https://books.google.com.co /books?id=vhit3ZmGQPsC&pg=PA213&dq=RED+WPAN&hl=es&sa=X&ved=0ahUKEwii5IeJiq_mAhUqqlkKHYmFBREQ6AEIKTAA#v=onepage&q=RED%20WPAN&f=false
CATORIA, Fernando. [En línea]. Consejos para evitar un ataque de denegación de servicio, 2012 . [Citado 04, septiembre, 2019]. Disponible en: https://www.welivesecurity.com/la-es/2012/03/28/consejos-ataque-denegacion-servicio/
CONEXIÓN ESAN. [En línea]. ¿Qué es y para que sirve la Norma ISO 27001?, 2016. [Citado 05, diciembre, 2019]. Disponible en:

https://www.esan.edu.pe/apuntes-empresariales/2016/05/que-es-y-para-que-sirve-la-norma-iso-27001/

CONGRESO DE LA REPUBLICA DE COLOMBIA. [En línea]. LEY 1273 DE 2009, 2009. [Citado 04, noviembre, 2018]. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

CORPORACION COLOMBIA DIGITAL. [En línea]. ¿Cuáles son los sectores que más han avanzado en infraestructura tecnológica?, 2017. [Citado 21, octubre, 2018]. Disponible en: https://colombiadigital.net/actualidad/noticias/item/9608-cuales-son-los-sectores-que-mas-han-avanzado-en-infraestructura-tecnologica.html

GALLEGO, Jose. [En línea]. *Instalacion y mantenimiento de redes para transmision de datos*. [Citado 17, octubre, 2018]. Disponible en : https://books.google.com.co/books?id=qt_SCQAAQBAJ&pg=PA37&dq=Red+WWAN&hl= es&sa=X&ved=0ahUKEwj3t4ijha_mAhWoxVkKHVS7AwMQ6AEIQjAD#v=onepage&q=Red%20WWAN&f=false

GUTIERREZ, Camilo. [En línea]. *Tipos de redes VPN y cómo funcionan: ¿ya sabes cuál usar?, 2016*. [Citado 23, noviembre, 2018]. Disponible en: https://www.welivesecurity.com/la-es/2016/06/08/tipos-redes-vpn-como-funcionan/

IBM. [En línea]. Protocolos TCP/IP. [Citado 02, diciembre, 2019]. Disponible en: https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/network/tcpip_protocols.html

MICROSOFT. [En línea]. ¿Qué es virtualización? [Citado 04, noviembre, 2018]. Disponible en: https://azure.microsoft.com/es-es/overview/what-is-virtualization/

MIKROTIK. [En línea]. About us. [Citado 17, octubre, 2018]. Disponible en: https://mikrotik.com/aboutus

MOLARES, Estela. [En Linea]. Internet y Sociedad: Relación y compromiso de beneficios colectivos e individuales, 2004. [Citado 11, diciembre, 2019]. Disponible en: http://www.revista.unam.mx/vol.5/num8/art49/sep_art49.pdf

PANDA. [En línea]. Pentesting: Una herramienta muy valiosa para tu empresa, 2018. [Citado 11, diciembre, 2019]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

SGSI. [En línea]. ISO 27001: El método MAGERIT, 2015. [Citado 16, noviembre, 2018]. Disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

PRENAFETA, Javier. [En línea]. Tipos de Pentesting, 2018. [Citado 23, noviembre, 2018]. Disponible en: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/ de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080521_56.pdf

Contenido del documento: Este proyecto se encuentra estructurado con el siguiente contenido

6. Ataque de cookie snooping
7. Ataque de denegación de servicio
8. Ataque de directory transversal

CONCLUSIONES

RECOMENDACIONES

BIBLIOGRAFIA

REFERENCIAS BIBLIOGRAFICAS

ANEXO

Anexo 1

Anexo 2

Anexo 3

Anexo 4

Metodología:

La metodología que se emplea para el desarrollo de este proyecto es la investigación aplicada, puesto que a partir del problema planteado en el caso de estudio se procede con la indagación de una temática específica y la implementación de la solución mediante la práctica, haciendo uso de tecnología Mikrotik y técnicas de pentesting.

Conceptos nuevos:

Ataque Tampering de parámetros: La manipulación de parámetros es un tipo de ataque que consiste en la modificación de los parámetros que se envían al servidor web, ya sean los que se encuentran en los formularios o en la URL.

Ataque directory transversal: Cuando un sistema de información tiene vulnerabilidades en el acceso al contenido web, permite el recorrido en el directorio permitiendo salir de la raíz hacia otros sistemas de archivos, al cual no se tiene acceso mediante permisos de usuario.

Conclusiones:

La creación de entornos virtualizados para el caso de estudio de la empresa XYZ permitió el mejoramiento de la seguridad de la infraestructura de la red de datos

contribuyendo en el aprovechamiento de los recursos de la organización proporcionando una disminución en tiempos de administración, costos de implementación y optimización de los tiempos de los procesos que se llevan a cabo día a día por parte de los empleados y que contribuyen con los objetivos de las organizaciones, garantizando la seguridad informática y de la información ya que estos dispositivos facilitan la administración de diferentes elementos de la red.

La implementación de dispositivos de seguridad perimetral en la infraestructura de red de datos como Mikrotik, permitió elevar el nivel de aseguramiento de los procesos y la información, gracias a que esta tecnología ofrece una unificación de elementos de la red y de esta manera la compañía del caso de estudio logro la centralización de recursos y servicios como routers, firewalls, conexiones VPN, redes inalámbricas, controles de accesos y administración de anchos de banda, generando beneficios enfocados a la seguridad de la información y rendimiento de la red, de forma que se garantice la integridad, confidencialidad y disponibilidad de la información durante los procesos de transmisión de datos entre cada una de las sedes.

La ejecución de pruebas de pentesting para el software que soporta los proceso de la empresa (Badstore) permitió la identificación de vulnerabilidades presuntamente causadas por malas practicas de desarrollo por parte del proveedor del aplicativo, que al ser explotadas, conlleva a la materialización del riesgo ya que se está comprometiendo la información sensible de la organización, lo cual puede desencadenar en pérdidas económicas, operativas y estratégicas, y a su vez, la generación de nuevas amenazas en la seguridad perimetral de toda la compañía y la red de datos.

Para la disminución de las brechas de seguridad que presenta la herramienta Badstore y la infraestructura de red de datos es recomendable la utilización de diversas soluciones de aseguramiento como un WAF, el cual permitirá controlar y monitorear la información entrante y saliente de la red durante la operación del aplicativo; todo esto apoyado de buenas prácticas de documentación relacionada con la prevención de las vulnerabilidades y procedimientos de contingencia antes la presencia de amenazas.

Mediante la ejecución de este proyecto se logró diseñar e implementar el mejoramiento de una infraestructura de red de datos haciendo uso de entornos virtualizados que permitieron el aseguramiento de los procesos y la información del caso de estudio de la empresa XYZ. De igual manera, se adquirieron diversos

conocimientos acerca de nuevas tecnológicas de seguridad perimetral y pentesting, y mecanismos para la mitigación de vulnerabilidades para de esta manera, otorgar niveles de seguridad óptimos que le permiten a la compañía mantener la continuidad del negocio a la vanguardia de la tecnológica.
AUTOR: Harold Yesid Martínez Ripe, ,Mabel Rocío Bravo León