DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED PARA LA INTERCONEXIÓN PARA CUATRO SEDES (CIUDADES) DEL CASO DE ESTUDIO DE LA EMPRESA DE COBRANZA XYZ

MILADY GÓMEZ YATE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PROYECTO DE SEGURIDAD INFORMÁTICA II
IBAGUÉ, TOLIMA
2019

DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED PARA LA INTERCONEXIÓN PARA CUATRO SEDES (CIUDADES) DEL CASO DE ESTUDIO DE LA EMPRESA DE COBRANZA XYZ

MILADY GÓMEZ YATE

Proyecto de grado Para optar al título de
Especialista en seguridad informática

Director
ALEXANDER LARRAHONDO NUÑEZ
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PROYECTO DE SEGURIDAD INFORMÁTICA II
IBAGUÉ, TOLIMA
2019

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Jurado

_____
Jurado

Ibagué Tolima, 24 Diciembre 2019

DEDICATORIA

A mi madre, por sus esfuerzos y dedicación, a mi padre por su apoyo y disciplina, a ellos por confiar siempre en mí, mostrándome su cariño.

A mi hermana por compartir momentos significativos, su compresión y disposición a escucharme y ayudarme en cualquier momento.

AGRADECIMIENTOS

A mi familia, que siempre han estado cerca de mi dándome su apoyo incondicional y demostrándome ser siempre fuerte.

A mis amigos, por acompañarme durante el camino, compartiendo conmigo buenos y malos momentos.

A mis compañeros de la facultad, que han compartido conmigo las enseñanzas.

A los maestros, por depositar en mí sus conocimientos.

CONTENIDO

pág.

LISTA DE ILUSTRACIONES

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

GLOSARIO

DOS: (sigla de Disk Operating System, "Sistema Operativo de Disco" y "Sistema Operativo en Disco") es un grupo de sistemas operativos usados en computadoras personales (PC).

COOKIE: Archivo que se crea y se almacena conteniendo información, que puede ser actividades realizadas por el usuario en un sitio web[1].

GATEWAY: El Gateway es un dispositivo situado entre aparatos o dispositivos, y tiene la función de ser una interfaz de conexión, además de compartir recursos entre dos o más computadoras[2].

IP: (Internet *Protocolo*) Protocolo de Internet. Es un estándar que se usa para el envío y recepción de información en las redes que reúne paquetes conmutados[3].

LAN: (Local Área Network) Red de Área Local, esta red realiza la representación de dispositivos físico pequeño, como puede ser una oficina o un edificio. La interconexión se realiza a través de un cable o de ondas.

SQL: (*Structured Query Language*) Lenguaje que gestiona las bases de datos de carácter relacional[4].

[1] González, Gabriela. Qué son las cookies de tu navegador y para qué sirven. s.l.: Blogthinkbig.com, septiembre de 2014. 19 p.

[2] Pantaleo, José. Redes informáticas II. s.l.: quizlet. Pequeño Diccionario de término de información. 19 p.

[3] Pérez Porto, Julián y Merino, María. DEFINICIÓN DE. 2019 19p.

[4] Rouse, Margaret. Base de datos relacional. s.l.: SearchDataCenter, 2015. 19 p.

RESUMEN

Las redes son en una empresa son de gran importancia pues a partir de ellas se puede transmitir información de una forma segura en tiempo real y a cualquier parte del mundo, reduciendo los envíos físicos, que suelen ser costoso y demorados.

Las VPN han tenido gran acogida ya que permiten a los usuarios acceder a desde otros sitios a la información necesaria en tiempo real sin tener que desplazarse hasta el sitio.

Los ataques a las aplicaciones web tienden a ser más comunes y diversos, en la actualidad las organizaciones invierten un capital para poder crear planes de aseguramiento que garanticen la protección a las aplicaciones, entre las amenazas más comunes se encuentran la inyección de código SQL, (*Cross Site Scripting*)[5], las debilidades pueden provocar errores críticos.

El presente proyecto tiene como propuesta el diseñar e implementar un prototipo de Red Virtual Privada VPN para interconectar las sedes de una empresa situados en diferentes cuidad (Bogotá, Medellín, Bucaramanga y Cali), las cuales necesitan estar conectadas a un cluster de Servidores que se encuentra ubicados en la cuidad de Bogotá; se realiza una arquitectura de red según las observaciones de la empresa la cual se implementara dicho proyecto, se deberá configurar el direccionamiento privado, los parámetros de IP públicas propios de cada proveedor de servicio de internet; además se realizar pruebas de posibles vulnerabilidades de una página web, el desarrollo del proyecto se crean las posibles soluciones a los ataques positivos, implementado planes de contingencia y barreras.

La metodología a ser desarrollada durante el desarrollo de la actividad es de tipo experimental donde se realizará en máquinas virtuales.

Palabras clave:
Ataque, Aplicaciones, Servidor web, Amenazas, Ataques.

[5] Pakala, Sangrita. Preguntas Frecuentes sobre seguridad en aplicaciones web (OWASP FAQ). s.l.: The Open Web Application Security Project, 25 de enero de 2005. 20 p.

ABSTRACT

The networks are in a company are of great importance because from them you can transmit information in a secure way in real time and anywhere in the world, reducing physical shipments, which are usually expensive and delayed.

VPNs have been well received because they allow users to access the necessary information from other sites in real time without having to navigate to the site.

Attacks to web applications tend to be more common and diverse, today organizations invest capital to be able to create insurance plans that guarantee protection to applications, among the most common threats are the injection of SQL code, (Cross Site Scripting), weaknesses can cause critical errors.

The purpose of this project is to design and implement a VPN Virtual Private Network prototype to interconnect the headquarters of a company located in different cities (Bogotá, Medellin, Bucaramanga and Cali), which need to be connected to a cluster of Servers that are It is located in the city of Bogotá; a network architecture is made according to the observations of the company which will implement said project, the private addressing, the public IP parameters of each internet service provider must be configured; In addition to testing possible vulnerabilities of a web page, the development of the project will create possible solutions to positive attacks, implemented contingency plans and barriers.

The methodology to be developed during the development of the activity is of an experimental type where it will be carried out in virtual machines.

1. INTRODUCCIÓN

En el presente trabajo se diseñará una Red Privada Virtual (VPN) para la interconexión de cuatro sedes de la empresa de cobranza “XYZ” además de análisis de vulnerabilidad y pruebas de penetración quienes están encargados de realizar las llamadas a los clientes que han sido reportados por los bancos, actualmente cada sede maneja sus propios protocolos, creando perdida de información y desorden.

Se requiere el diseño de una red que permita una comunicación segura, con el uso de VPN’s a través de internet; ya que se presenta la importancia de manejar la información de forma segura, en las diferentes sedes, la implementación de la red debe permitir que los sedes pueden enviar y trasmitir datos.

El tipo de investigación que vamos a desarrollar en el siguiente proyecto es de tipo cuasi-experimental.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Diseñar e implementar una infraestructura de red para la interconexión de cuatro sedes de la empresa de cobranza “XYZ” y Diseño e implementación de WEB APLICATION FILTER que permita proteger la aplicación web.

2.2 OBJETIVOS ESPECÍFICOS

- Diseño, configuración y desarrollo de infraestructura de red.
- Probar la infraestructura de red implementada, teniendo en cuenta conectividad entre sedes.
- Analizar las vulnerabilidades de la empresa, por medio del uso de herramientas para realizar ataques de seguridad en escenarios controlado.
- Realizar una propuesta de aseguramiento que permita mitigar los riesgos informáticos de la empresa.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICION DEL PROBLEMA

La empresa XYZ presta servicio de BPO y Contact Center a clientes corporativos quienes buscan contactarse con sus clientes para ofrecer los servicios de: Servicio al Cliente, Venta, Cobranzas, Mesa de Servicios, por medio de diferentes canales: telefónicos, virtuales y presenciales.

Con el gran crecimiento que ha tenido la empresa y sus clientes ha sido necesario que los agentes repartidos en las diferentes ciudades pueden tener acceso a clúster de servidores que cuenta la empresa en su totalidad, ya que a petición de los clientes quienes tienen también diferentes sede solicita que la información sea unificada; actualmente cada sede cuenta con su propio sistema de email, su propio servidor de telefonía IP, he incluso su propio aplicativo de gestión, causando que la información entre sede sea más complejo inclusive para los usuarios; se utilizan metodologías como transporte de información mediante Mail, Cd y medios de almacenamiento externo que hace insegura el manejo de la información.

Además de ello desean que se realice pruebas de vulnerabilidades y pruebas de penetración a los productos, donde se debe registrar todos los ataques de informática, evidenciando si la aplicación BADSTORE puede llegar a ser segura.

3.2 JUSTIFICACIÓN

La información de las sedes está siendo trasportada por vía correos electrónico, correo certificado, CD y medios de almacenamiento externo, lo que podría ocasionar perdida de información, ya que no se cuentan con las medidas de seguridad informáticas necesarias; es por ello que es necesario la implementación de una nueva infraestructura de red usando VPN para poder integrar la red interna de la empresa en una sola.

Las redes con VPN permiten la conexión de redes separadas físicamente, en ellas se puede trasmitir información de una forma segura.

La disminución de tiempos en él envió de información, además de poder transportar datos por redes virtuales, reduce considerablemente los costos de gestión de la empresa puesto que se evitarían los envió por correos certificados, inclusive los viáticos de los trabajadores quienes realizan funciones de envió y entrega de paquetes.

La concentración las redes permite para los administradores de la red mejorar el monitoreo de cada red, llevando un seguimiento de ello.

El presente trabajo se enfoca en estudiar las vulnerabilidades y penetraciones que puedan existir en la aplicación BadStore, ya que la empresa creadora desea saber qué tipo de seguridad tiene dicha aplicación, así mismos también se realiza una propuesta de aseguramiento que permita mitigar el riesgo que pueda presentar la aplicación.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Concepto de red

Las redes es una conexión que permite la transferencia electrónica de información entre usuarios, este grupo de usuario está conformado por dispositivos y computadores. Los dispositivos dentro de una red realizan la trasmisión de información de uno a otro, en grupos de impulsos eléctricos pequeños (conocidos como paquetes). Este paquete guarda la dirección del dispositivo transmisor (la dirección fuente) y la del dispositivo receptor (dirección de destino). El equipo situado dentro de la red usa esta información de la dirección para ayudar al paquete a llegar a su destino[6].”

La red se encarga que la información que se envía sea recibida[7] .

4.1.2 Tipos de red

Existen dos tipos de tecnologías de transmisión: Enlaces de difusión y enlaces de punto a punto.

Redes de área local (LAN): Redes de propiedad Privada que se encuentra en un mismo espacio, son usadas para conectar computadoras personales y estaciones de trabajo.

Redes de área metropolitana (MAN): Redes que se encuentra situadas en una ciudad como por ejemplo la red de televisión por cable.

Redes de área amplia (WAN): Redes que se situadas en una amplia geografía, como por ejemplo la red de teléfono.

Redes inalámbricas: Interconexión de sistemas[8].

---

[6] Almachi Oñate, Paúl Noé y Chiluisa Quimbita, Carlos Orlando. 2010. Implementación de una VPN con seguridades de la red inalámbrica y red externa para la empresa exportadora de flores GP FLOWERS. Latacunga, Ecuador: 2010. 26 p.

[7] López, Aguilera. Seguridad Informática. s.l.: Edite, pág. 147. 26 p.

[8] Tanenbaum, Andrew S. Redes de computadoras. México: Pearson, 2003. 26 p.

4.1.3 Red privada Virtual (VPN)

Extensión de una red privada que se enlaza en rede compartidas o públicas, allí se permite enviar datos entre dos computadoras por un enlace privado punto a punto[9]. Se pueden clasificar en

- Acceso remoto: Conexión de sitios remotos a través de internet a redes locales.
- Punto a punto: Conexión de redes completas a otras[10] (Ardila, 2015).

4.1.4 Seguridad en VPN

La VPN se caracteriza por tener una alta seguridad. La VPN requiere establecer un camino (túnel) en la red corporativa y la encriptación de los datos entre la PC del usuario y los servidores corporativos. Para llevar a cabo esta tarea hace uso de protocolos estándar de autenticación y encriptación los cuales hacen que se pueda ocultar los datos en entornos inseguros de internet, con la condición de que son accesibles a los usuarios corporativos[11].

4.1.5 Arquitectura de las VPN

La arquitectura de las redes VPN se planifican de según las necesidades que presenta en cada una de las organizaciones en la que se va a implementar, el tipo de red debe ser clasificada según la capacidad técnica y adecuación para mantener e instalar este tipo de red, garantizando la seguridad, la infraestructura de hardware y el número de usuarios que harán uso de las redes. Actualmente las arquitecturas de redes privadas más usadas son las siguientes:

- Basada en hardware: Son routers que encriptan, tienen como características que ofrecen gran rendimiento, esto es debido a que no malgastan ciclos de procesador haciendo funcionar un sistema operativo. Además, cuenta con un hardware muy rápido y de fácil instalación.
- Basada en cortafuegos: Son utilizados con software de cortafuegos (firewall). Entre las ventajas que tiene es que los mecanismos de seguridad que usan los cortafuegos además tienen el acceso restringido a la red interna, pueden realizan la traducción de direcciones (NAT). Permitiendo tener los

[9] Windows. Redes privadas virtuales: una visión general. Microsoft. [En línea] 12 de agosto de 2009. P26-27.

[10] Ardila, Óscar. Que es y cómo usar un VPN. [En línea] 2015. 27 p.

[11] Ñacato Gualotuña, Marco Antonio. Diseño e implementación de una red privada virtual para la empresa hato telecomunicaciones. Quito: s.n., 2007, págs. 45-46. 27 p.

requerimientos de autenticación fuerte. El rendimiento de este tipo decrece, ya que no se tiene hardware especializado de encriptación.

- Basadas en software: Esta arquitectura es necesaria cuando se presente los siguientes escenarios, los dos puntos de conexión de la VPN no son manipulados por la misma organización, otro escenario puede ser cuando los diferentes cortafuegos o routers no son usados por la misma organización. Este tipo ofrece el método más flexible en cuanto al manejo de tráfico de datos[12] .

4.1.6 Servidor de telefonía IP

La tecnología IP es una tecnología contigua a la de VoIP, es por ello por lo que se permite las llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares. Cuando realizamos una llamada telefónica por IP, nuestra voz es digitalizada, posteriormente se comprime y es enviado en paquetes de datos IP. El enrutamiento de una llamada es la actividad que en ruta la red hasta el punto final, seleccionando el Gateway VoIP más adecuado. Este enrutamiento se realiza según unas tablas de condiciones que se programan en distintos gateways VoIP denominados Servidores de Directorio cuando los paquetes son envidos a la persona con que se realiza la llamada, llegando a su destino, son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original, así mismo, un teléfono puede llamar a otro conectándose a un Gateway VoIP (directamente, a través de central telefónica o con llamada externa desde la calle) que digitalice y comprima la voz. Estos gateways VoIP soportan varios teléfonos/ conversaciones simultáneamente)[13].

4.1.7 Túneles

Los túneles son una conexión que existe entre dos máquinas por medio de un protocolo seguro, como puede ser un intérprete de ordenes seguras (SSH), en el podemos realizar conexiones no seguras o transferencias inseguras, que pasaran de este modo a ser seguras. Siendo la conexión segura el túnel por el cual enviamos nuestros datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos[14] .

---

[12] Ñacato Gualotuña, Marco Antonio. Diseño e implementación de una red privada virtual para la empresa hato telecomunicaciones. Quito: s.n., 2007, págs. 45-46. p 27-28.

[13] Huidobro, José. Tecnologías de información y comunicación. Madrid: s.n., 2007. 28 p.

[14] Montes de los santos, Andrés, Corona Carrión, Jocelyn Carolina y González Beltrán, Jorge. Propuesta de implementación de una VPN. México: s.n., 2012. 28 p.

4.1.8 Tipo de túneles

Los túneles puedes tener diferentes características esto difiere según como son creados:

- Túneles voluntarios: Un PC de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, el PC del usuario es un punto terminal del túnel y actúa como un cliente del túnel.
- Túneles obligatorios: Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con un túnel obligatorio, el PC del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre el PC del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente[15] del túnel.

4.1.9 Protocolos de Túneles

Los protocolos de enrutamiento punto a punto o de túnel, se clasifican en términos de los niveles de OSI. Los protocolos son los siguientes.

- PPTP: Microsoft crea un protocolo llamado PPTP el cual tiene la característica de realizar trasferencias seguras desde un punto inicial que es el cliente remoto hasta redes privadas, empleando para ello tanto líneas telefónicas conmutadas como internet.
- L2F: El protocolo L2F tiene como objetivo suministrar un mecanismo de túnel para el transporte de tramas a nivel de enlace. El proceso de túnel involucra tres protocolos diferentes: protocolo pasajero, protocolo encapsulador y protocolo portador.
- L2TP: El protocolo L2TP es una unión entre los protocolos L2F y PPTP, se caracteriza por establecer un túnel a través de varias de redes para el transporte de tráfico PPP.
- IPSec: El protocolo IPSec se puede usar sobre las maquinas o través de un túnel entre los dispositivos periféricos, denominados gateways de seguridad, que las conectan a través de internet[16].
- SSL: el objetivo de SSL es promover la privacidad y confiabilidad entre dos aplicaciones; este protocolo está compuesto por dos capas, la primera es el registro SSL quien se encarga de encerrar otros protocolos de más alto nivel y la segunda Handshake SSL permite tanto al cliente como al servidor autenticarse y realizar intercambios de algoritmo encriptado.

---

[15] Limari Ramírez, Víctor Humberto. Protocolos de seguridad para redes privadas virtuales. Valdivia: s.n., 2004. 29 p.

[16] Cosios Castillo, Eduardo Richard y Simbaña Loachamin, Wilson Xavier. Estudio y diseño de redes virtuales privadas. Quito: s.n., 2004. 29 p.

4.1.10 Métodos de Autenticación

En Extensible Authentication Protocol (EAP) los mensajes son transportados en claro, sin ningún tipo de autenticación por parte del servidor ni del cliente, esto identifica un alto nivel de vulnerabilidad. Se han realizado mejoras al protocolo, entre ellas se han incluido variantes que crean canales seguros entre el cliente y el servidor de autenticación: EAP-TLS, EAP-PEAP, y EAP-TTLS. EAP-TLS se trata de una variante de EAP donde se realiza convenio SSL con autenticación basada en certificado, tanto por parte del cliente como del servidor.

En los canales EAP-PEAP como de EAP-TTLS, la conexión segura se realiza a partir exclusivamente del certificado del servidor (sería el equivalente a HTTPS en web). En el caso del canal TLS, las credenciales son parte del certificado de cliente, mientras que en el de PEAP y TTLS éstas son comunicadas utilizando uno de los métodos ya comentados: MS-CHAP, PAP, etc. A nivel de usuario, en el primer caso (TLS) basta con tener el certificado de cliente instalado, mientras que en los otros (PEAP y TTLS) tendría que proporcionar las credenciales, por lo general un usuario/password[17] .

4.1.11 Tipos de ataques

Cisco Systems es una empresa global fundad en 1984 en san francisco (California) que tiene como actividad comercial la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones, ellos exponen cuatro clases de ataques principales a las redes:

- Reconocimiento: El atacante tiene el objetivo de analizar las vulnerabilidades para así obtener información de importancia, con ello pueden obtener el acceso a recurso informático sin la autorización respectiva.

1. Barridos de ping: Barrido de ping es un método de administración de red que supone un rango de direcciones está en uso en la red. Su nombre viene la utilidad ping, aunque ping estándar no proporciona la funcionalidad necesaria para un barrido de ping automático. Ping se identifica estrechamente con el protocolo de mensajes de Control de Internet y un barrido de ping explota los mismos elementos de ICMP ping utiliza[18].
2. Escaneos de puertos: uno de los primeros proceso por realizar por los hackers o personas que realizan ataques es un escaneo de puertos, un

[17] Castro, Rodrigo. Avanzando en la seguridad de las redes. 2005, Fundamento de redes. 30 p.

[18] Ubiquitour. ¿Qué es el barrido de Ping? ¿Qué es el barrido de Ping? [En línea] 27 de 01 de 2013. http://www.ubiquitour.com. 30 p.

portscan; a través de este ataque se puede observar una primera información del servicio que se está atacando, si se profundiza un poco más se puede obtener datos como el sistema operativo que tienen los host o incluso la arquitectura de red.[19]

- Acceso: El ataque denominado acceso consiste en que un tercero no autorizado logra acceder a un dispositivo donde no tiene ni usuario y contraseña, esto lo hace a través de comandos o herramientas de piratería informática a si puede ingresar sin ser autorizados, el usuario legitimo puede o no ser cociente de que está siendo atacado; Para nombrar algunos ataques de acceso se exponen los siguientes:

1. Ataque a la Contraseña: Las contraseñas de cuentas de usuario son robadas o encriptados generalmente para que el usuario no tenga acceso de la red, si las contraseñas cuentas con un mecanismo de seguridad se puede hacer uso de herramientas especiales del kit de herramientas de los hackers para romper el algoritmo[20].
2. Explotación de Confianza: es el ataque a un host a través de un cliente que tiene privilegios para usar un recurso en la máquina "víctima", por eso el concepto de confianza porque el host "confía" en un cliente al que le da ciertos privilegios y a través de este cliente se realiza el ataque[21] .

- Denegación de Servicio: El ataque de denegación de servicio es el cual realiza bloqueo un servidor no permitiéndole brindar el servicio que ofrece a los usuarios debido a que el ataque hace superar la capacidad de procesamiento debido al envió de un gran flujo de información, Entre los ataques de Denegación de Servicio se exponen los siguientes:

1. Ataque de DoS: Los ataques de DoS se caracterizan porque impiden que el usuario legítimo de un servicio haga uso de sus servicios. Por lo cual existen tres tipos de ataques DoS; estos son la destrucción o alteración de la configuración de información, destrucción o alteración de los componentes

[19] ibiblio. Escaneos de puertos. Escaneos de puertos. [En línea] 08 de 08 de 2003. www.ibiblio.org. 31 p.

[20] ehack. Ataques de contraseñas. Ataques de contraseñas. [En línea] 23 de 06 de 2017. http://ehack.info. 31 p.

[21] Muycomputerpro. La explotación de la confianza. La explotación de la confianza. [En línea] 16 de 09 de 2014. muycomputerpro.com. 31 p.

de red físicos y, finalmente, el consumo de recursos escasos, limitados o no renovables[22].

2. Ping de la Muerte: Ping es un comando encontrado en muchos sistemas operativos, usado principalmente por técnicos de redes para encontrar problemas en una red particular. Este comando envía una solicitud de respuesta a través del cable que incluye un paquete de datos de tamaño modificable; el servidor objetivo especificado en el comando responde con un mensaje de "Acá estoy". Desafortunadamente, el comando ping también es usado por personas con malas intenciones, y cuando se configura de cierta manera, este comando inunda el servidor objetivo con peticiones ping, en un ataque conocido como "Ping de la Muerte"[23].
3. Saturación SYN: Este ataque utiliza la forma de conexión del TCP, de tal forma que sí el cliente envía un paquete SYN, el objetivo responde, pero no recibe confirmación por parte del cliente, el objetivo guardará la conexión en memoria. De este modo, el objetivo va almacenando en memoria las conexiones que se van generando hasta llegar al límite establecido y ya no pueda recibir más conexiones entrantes, haciendo que los demás usuarios no puedan acceder al servicio. Además, el cliente maligno utilizaría menos tiempo para generar la solicitud de conexión y no gastaría recursos de memoria para almacenar la conexión generada
4. DDoS: Un ataque “Distribute Denial of Service” (DDoS por sus siglas en Ingles), también conocido como “SMURF”, es una evolución del DoS que tiene como objetivo eliminar la conexión entre los usuarios legítimos y un servicio. Su funcionamiento se basa en un grupo de computadoras que envían flujos de paquetes al servicio, esto ocasiona que el servicio consuma recursos clave. Cuando el ataque se realiza satisfactoriamente ocasiona que los usuarios que deberían utilizar el servicio queden inhabilitados de hacerlo o que el atacante pueda ingresar al computador de la víctima pudiendo hacer daños arbitrarios[24].

- Virus Gusano y Caballo de Troya: El software malicioso es ejecutado en un host para alterar dañar o dejar inutilizable el sistema, en muchos de los casos una vez que logran penetrar en un computador se propagan en toda la red generando negación de los servicios o lentitud de las operaciones.

[22] pandasecurity. Que es un ataque DoS. Que es un ataque DoS. [En línea] 26 de 05 de 2018. www.pandasecurity.com. 32 p.

[23] techlandia. Pin de la muerte. Pin de la muerte. [En línea] 01 de 01 de 2004. techlandia.com. 32 p.

[24] Florián Otoya, Cesar Augusto. Implementación de una aplicación móvil para monitoreo de contenido y disponibilidad de servicios web. Lima: M, 2015. 32 p.

1. SSH: Protocolo de interconexión entre los ordenadores, con el propósito de interconectar y permitir el acceso de un usuario al ordenador[25]. Ataques de denegación de servicio normalmente se ejecuta bajo los protocolos TCP/IP, el problema con este protocolo es baja capacidad de tolerancia a fallo es por ello por lo que un ataque puede provocar:
    - SYN Flood. Inundar el Servidor con este tipo de mensajes
    - TCP RST, bogus ICMP. Existen mensajes de tipo ICMP y TCP que pueden inhabilitar la conexión entre el Cliente y Servidor.
    - TCP desynchronization and Hijacking. Cambio de la sincronización y flujo normal de los paquetes, inyectando octetos de bytes lo cual se traduce en inyectar tráfico durante una conexión[26].

4.1.12 Protocolo TCP/IP

TCP hacer referencia a trasmisión control protocolo o transmisión por paquetes; el TCP realiza la conmutación por paquetes, ya sea divididos en bloques o paquetes, Cada mensaje a trasmitir tiene una cabecera donde contiene información básica[27].

- TCP e IP son los protocolos de gran significativos. Su nombre corresponde a la familia de protocolos que son parte de los cinco niveles o capas:
- Aplicación. Protocolos SMTP, para el correo electrónico; FTP, para las transferencias de archivos; TELNET, para la conexión remota, y HTTP, Hypertext Transfer Protocol.
- Transporte. Se comprende a los protocolos TCP y UDP, que se ocupan del manejo y el transporte de los datos.
- Internet. Se ubica en el nivel de la red para enviar los paquetes de información.
- Físico. Es el análogo al nivel físico del OSI.
- Red. Es el correspondiente a la interfaz de la red[28].

[25] Pinto, Cristhian, Reascos, Jorge y Torres, Alejandro. experimental, Evaluación de ataques de tipo Forck empleando entornos virtuales como plataforma. s.l.: Departamento de ciencias de la computación. 33 p.

[26] León Rodríguez, José David. ACCIONES DE HARDENING PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN CUANDO SE USAN LOS SERVICIOS DE HTTP, LDAP, SSH Y SMTP. Ibagué: s.n., 2018. 33 p.

[27] Gómez, Fernández. Conocimientos y aplicaciones tecnológicas para la dirección comercial. Madrid: ESIC, 2004. 33 p.

[28] Estrada Corona, Adrián. PROTOCOLOS TCP/IP DE INTERNET. 2004, Revista Digital Universitaria, págs. 4-7. 33 p.

Protocolo FTP Protocolo de transferencias de archivos a una red TCP, donde es usada la arquitectura Cliente – Servidor[29]; funciona de la siguiente manera un usuario ejecuta un programa cliente FTP para conectarse con otro ordenador que tiene un programa servidor FTP, al establecer correctamente la conexión se puede realizar el intercambio de archivos[30].

El ordenador del usuario se denomina maquina local mientras que el otro ordenador, el servidor ficheros, se denomina maquina remota[31].

4.1.13 Servidor FTP

Servicio de administración de ficheros que permite subirlos, renómbralos, moverlos, crear carpetas, borrar, etc., independientemente de los sistemas de archivos sean distintos, por defecto usa el puerto TCP20 para transferir datos y el puerto TCP21 para el control[32].

FTP tiene la ventaja de tener separado la conexión existente de control y las de transferencia de datos. Mientras que las primeras se mantienen abiertas permanentemente, las segundas se abren y se cierran en función de si hay datos que enviar al otro extremo o no[33].

4.1.14 Servidor WEB

El servidor WEB se define como un programa el cual implementa el protocolo HTTP (hypertext transfer protocolo). Este protocolo hace parte de la capa de aplicación del modelo OSI y el cual está diseñado para transferir lo que llamamos hipertextos, páginas web o páginas[34].

---

[29] Joaquín Andreu. Servicios en red. Madrid: Editex S.A, 2002. 34 p.

[30] González Castañeda, Ricardo. IMPLEMENTACIÓN Y EJECUCIÓN DE UN PROTOCOLO DE TRANSFERENCIA. Pereira: s.n., 2012. 34 p.

[31] Cobo Yera, Ángel Luis. Protocolo de trasferencia de archivos (FTP). Pueblo Nuevo: Innovación y experiencias educativas, 2009. 34 p.

[32] Andreu, Joaquín. Servicios de red. Protocolo de trasferencia de ficheros FTP (File Tranfer Protocol). s.l.: editex, pág. 82. 34 p.

[33] David Melendi, Xabiel G. Pañeda, Member, IEEE, Roberto García, Member, IEEE, Víctor García. Sistema para la realización y evaluación de. 2009. 34 p.

[34] (Peq)

Usan modelo Cliente/servidor; Los principales servidores web usan apache, internet Información Server (IIS) de Microsoft y nginx (que se pronuncia engine X) de NGNIX[35].

Almacenamiento de servicio en una estructura similar a un diccionario, donde se define la llave con el nombre del atributo y el valor, el valor del atributo[36].

4.1.15 Seguridad en red

Las organizaciones deben planear la seguridad de sus datos, revisando las prácticas, desarrollando planes de mejoras, es decir administrando su sistema. Para implementar un esquema de seguridad se debe tener una administración definida del sistema[37].

Los riegos de la información están presentes en un sistema cuando dos elementos, Amenaza y vulnerabilidad se unen, la vulnerabilidad es una debilidad en los procesos de la información, una amenaza es una situación que puede afectar la organización[38].

Los ataques de seguridad generalmente son realizados por los más conocidos piratas informáticos, algunos los conocen como “Hackers”. Es por ello por lo que los administradores de red deben conocer los principales ataques de internet, para tomar decisión acerca de los equipos de seguridad, y conocer los posibles riesgos[39].

4.1.16 Políticas de seguridad

Las políticas de seguridad informática es una descripción de lo que se desea proteger, para ellos describe unas técnicas de seguridad empleando sanciones, y comportamientos de usuarios; Entre sus elementos encontramos: el objetivo de las políticas, definición de violencia, responsabilidad y alcances de las políticas[40].

---

[35] Rouse, Margaret. Servidor Web. [En línea] diciembre de 2016. 35 p.

[36] Florián Otoya, Cesar Augusto. Implementación de una aplicación móvil para monitoreo de contenido y disponibilidad de servicios web. Lima: M, 2015. p 31-35.

[37] FI, Ingeniería. Mecanismo de seguridad en red. 2015. 35 p.

[38] Tarazona T., Cesar H. Amenazas informáticas y seguridad de la información. 2015. 35 p.

[39] Pineda Mejillones, Daniel Afren y Leyton, Edgar. Gestión de seguridad en redes de comunicaciones: Análisis de seguridad en la red de datos de la FIEC. 2004. 35 p.

[40] Bello, Claudia E. Manual de seguridad en redes. s.l.: Coordinación de emergencia en redes teleinformáticas. 35 p.

El análisis de riesgos es identificar los posibles medios de ataques a la red, es por ello por lo que se debe asignar a cada recurso uno de los tres niveles de riesgo:

- Sistemas de bajo riesgo, no afectaría a gran escala las ramificaciones económicas y legales de una organización, se puede recuperar rápidamente la información.
- Los sistemas de riesgo medio, se causaría una interrupción a baja escala en la organización, requiriendo un esfuerzo pequeño para la restauración.
- Sistemas de alto riesgo, causaría un gran daño, afectado todo el sistema.

Los equipos como los son switches, routers, servidores DNS y servidores DHCP, son elementos de riesgo moderado o alto en la red, para mantener una red segura se debe prevenir los ataques, es por ellos que se divide los cambios en la seguridad y supervisión de la supervisión de la red[41].

4.1.17 Mikrotik

Empresa funda en 1996 con el objetivo de desarrollar enrutadores y sistemas ISP inalámbricos. Actualmente comercializa hardware y software para la conectividad a internet[42].

Es un sistema operativo basado en Kernel de Linux 2.6, contiene su propio S.O, este sistema operativo puede ser instalado en computador con todas las características necesarias: firewall, routing, punto de acceso, Servidor VPN, etc.; RoureOS se puede configurar en varios métodos:

- Acceso local vía teclado y monitor
- Consola serial con una terminal
- Acceso vía Telnet y SSH vía una red
- Una interfaz gráfica llamada WinBox
- Una API para el desarrollo de aplicaciones propias para la configuración
- En caso de no tener un acceso local y existe una complicación con las direcciones IP RouterOS las cuales soporta una conexión basada en direcciones MAC usando las herramientas customizadas Mac-Telnet y herramientas de Winbox[43].

[41] Seguridad en las comunicaciones. s.l.: Universidad de Oviedo Ingeniería de sistemas y automática. 36 p.

[42] Mikrotik. [En línea] https://mikrotik.com/. 36 p.

[43] Duarte, Eugenio. ¿Qué Es Mikrotik RouterOS? Abril: Information Tecnology Academy, 2014. 36 p.

4.1.18 VPN

RouterOS admite varios métodos de VPN y protocolos de túnel:

- Ipsec: túnel y modo de transporte, certificado o PSK, AH y ESP protocolos de seguridad
- Túnel punto a punto (OpenVPN, PPTP, PPPoE, L2TP)
- Funciones avanzadas de PPP (MLPPP, BCP)
- Túneles simples (IPIP, EoIP)
- Soporte de túnel 6to4 (IPv6 sobre red IPv4)
- VLAN - IEEE802.1q Soporte de LAN virtual, Q-in Soporte Q
- VPNs basadas en MPLS

4.1.19 Cortafuegos

Se implementa el filtrado de paquetes, lo cual se utiliza para administrar el flujo de datos hacía, desde y a través del enrutador[44].

4.1.20 Origen de internet

El internet se origina en la década de los sesenta del siglo XX, dentro de la red ARPA (*Advanced Research Project Agency*) usada militarmente en USA, que tenía como objetivo poder acceder a la información si existía un ataque soviético. En 1969 se crea una red para el mundo académico nombrada ARPANET al inicio solo se componía de 4 ordenadores, tiempo después se crea NSFNET una red científica y académica que absorbe a ARPANET[45].

En 1989 CERN (centro Europeo de Investigación Nuclear) comparte una forma para la vinculación e intercambio de información, nombrado Gestión de la información.

4.1.21 Protocolo HTTP

A comienzo de las décadas de 1990 se crea una nueva aplicación *World Wide Web*, es una aplicación que permite el enlace de la información, donde se pueden encontrar imágenes, archivos, etc. Las páginas web se componen de objetos, y se puede alcanzar a través de URL (*uniform Resourse locator*)[46].

---

[44] Mikrotik. RouterOS official mickotik distributor. [En línea] 2016. 37 p.

[45] Talledo San Miguel, José. Implantación de aplicaciones web en entornos internet, intranet y extranet. España: Paraninfo, 2015. 37 p.

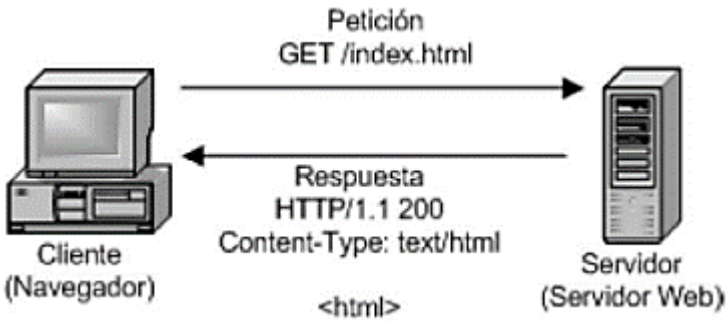
[46] Gómez Montoya, Carlos Eduardo, Candela Uribe, Christian Andrés y Sepúlveda Rodríguez, Luis Eduardo. Seguridad en la configuración del Servidor Web Apache. Armenia: INGE CUC, Vol. 9, N° 2, pp 31-38, diciembre, 2013, 29 de abril de 2013. 37 p.

Las especificaciones del protocolo HTTP se encuentra en el RFC 1945, es un protocolo que funciona también en los entornos UNIX.

Existe una variable HTTPS que utiliza el protocolo de seguridad SSL, se usa para poder cifrar la información que se trasmite y recibe entre el cliente y el servidor.

"El funcionamiento esquemático de HTTP es el siguiente; el cliente establece una conexión TCP hacia el servidor, hacia el puerto HTTP (o el indicado en la conexión), envía un comando HTTP de petición de un recurso (junto con algunas cabeceras informativas) y por la misma conexión el servidor responde con los datos solicitados, así como algunas cabeceras informativas, en la figura 1 se detalla el esquema grafico del funcionamiento del protocolo HTTP"[47].

Figura 1 Funcionamiento del Protocolo HTTP



Fuente: Jessica Nataly Castillo Fiallos

4.1.22 Tipos de ataques informáticos

4.1.22.1 Detección de vulnerabilidades en los sistemas

Análisis de las posibles vulnerabilidades de los sistemas informáticos para posteriormente explotarlas herramienta "exploits".

4.1.22.2 Modificación del contenido y secuencia de los mensajes transmitidos

Realización de reenvíos de mensajes y documentación con contenido maliciosos.

[47]Castillo Fiallos, Jessica Nataly. ESTUDIO COMPARATIVO DEL RENDIMIENTO DE SERVIDORES WEB DE VIRTUALIZACION SOBRE LA PLATAFORMA WINDOWS SERVER 2008. Ecuador: ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO, 2012. 38 p.

4.1.22.3 Análisis de tráfico

Análisis de los datos en la red, identificación del tipo de tráfico transmitido, las redes que utilizan *switches* son más propensas a tener ataques conocida como "*MAC flooding*"

4.1.22.4 Ataques de suplantación de la identidad

IP Spoofing: Modificación de la cabecera de los paquetes enviados, simulando que se envían de un equipo distinto al original, para poder evitarlo se pueden utilizar filtros para que las redes asocien una dirección IP desde el tráfico de origen.

DNS Spoofing: realización de direccionamiento erróneo, para ello se hace uso de un servidor DNS legítimo que permite información incorrecta, con esto se inyecta información errónea.

4.1.22.5 Conexión no autorizada a equipos y servidores

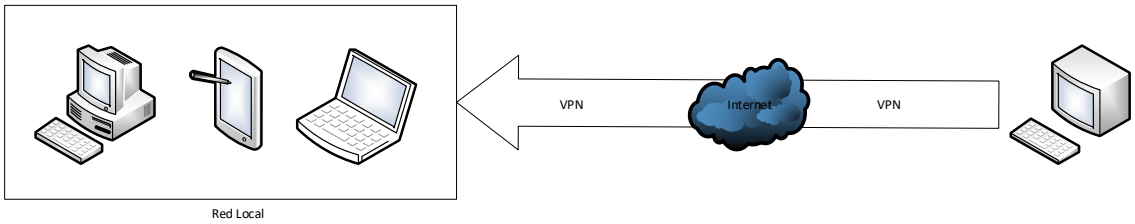
Entre los ataques de este tipo se encuentra las siguientes, Violaciones de control de accesos a los sistemas, *Backdoors, rootkis*[48].

[48] Gómez Vieites, Álvaro. TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS. s.l.: Profesor de la Escuela de Negocios Caixanova. 39 p.

4.2 MARCO CONCEPTUAL

VPN son las iniciales de Virtual Private Network o red privada virtual, la cual te permite interconectar los equipos sin necesidad que estén conectado físicamente, sino a través de internet; permitiendo él envió y recesión de datos sobre redes compartidas o públicas, en la figura 2 se observa un diagrama básico de conexión VPN desde una red externa a otra.

Figura 2 Red VPN

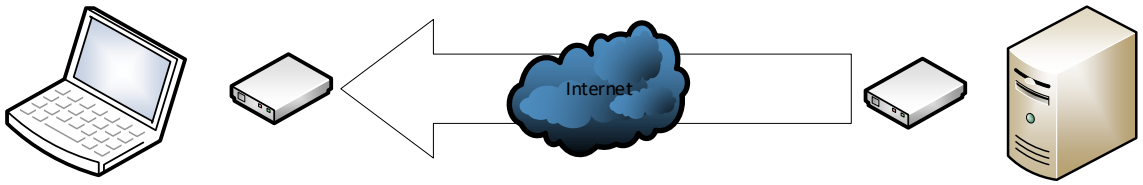


Fuente: Autor

4.2.1 Servicios VPN

- VPN de enrutador a enrutador: En la figura 3 se observa canal de seguridad Protocolo de internet (IPsec) entre los enrutadores.

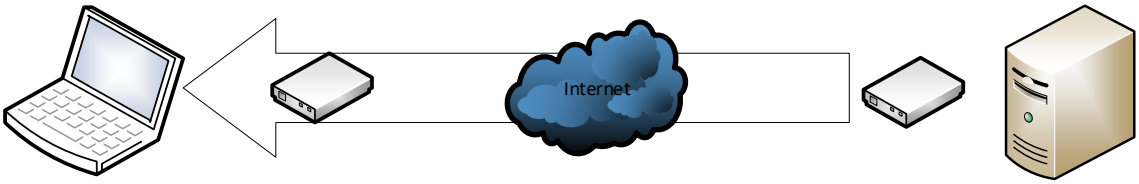
Figura 3 Conexión de VPN enrutador a enrutador



Fuente: Autor

- VPN de cliente a enrutador: En la figura 4 se observa los administradores se pueden conectar al enrutador a través de la VPN.

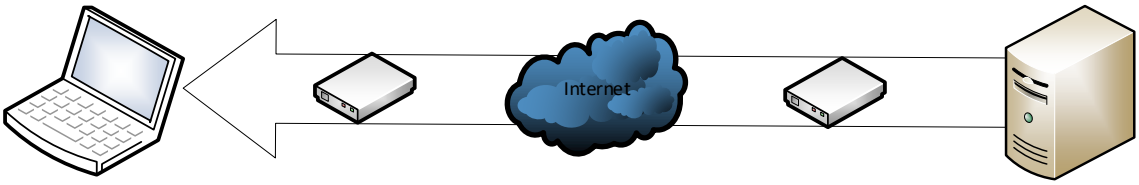
Figura 4 Conexión de una VPN de cliente a enrutador



Fuente: Autor

- Servidor de acceso a la red de cliente a VPN: En la figura 5 se observa la puerta de enlace del servidor de acceso a la red[49].

Figura 5 Servidor de acceso a la red de cliente a VPN



Fuente: Autor

4.2.2 Protocolos de comunicación VPN

Los protocolos VPN definen la forma en que se enrutan desde nuestro dispositivo hasta el servidor VPN

a. IPsec: Extensión de protocolo IP que promueve una comunicación privada y segura mediante el servicio de seguridad criptográfica.
b. L2TP: (Layer 2 Tunneling Protocol) líneas virtuales, es un protocolo de encapsulación basado en protocolo de criptografía; es fácil de configurar, aunque puede ser fácil de bloquear por algunos proveedores de internet.
c. PPTP: (Point-to-Point Tunneling Protocol) es un protocolo VPN desarrollado como una extensión del PPP (Point-to-Point Protocolo, encapsula los protocolos IP en datagramas del PPP, posteriormente el servidor de encapsulación realizas las comprobaciones; tiene la ventaja de ser unos de los protocolos de mayor velocidad en las conexiones aunque ha sido criticado por su inseguridad.
d. L2F: Layer 2 Forwarding.

[49] Microsoft. Servicios VPN. 2018. 41 p.

4.2.3 RouterOS L4

MikroTik RouterOS™ es un sistema operativo para routers el cual para transformar cualquier PC en un router dedicado[50].

4.2.4 ATAQUES en servidores web

Tabla 1 Matriz de trazabilidad de ataques, vulnerabilidades y técnicas[51]

ATAQUE	VULNERABILIDAD	TÉCNICA PARA DETECCIÓN DE VULNERABILIDADES
INYECCIÓN SQL	Inyección	Análisis estático de código
		Análisis dinámico de código
		Pruebas de penetración
ATAQUE DE FIJACIÓN DE SESIONES	Perdida de autenticación y manejo de sesión	Utilización de estándar de manejo de sesiones
ATAQUE XSS	Secuencia de comandos en sitios cruzados XSS	Análisis estático de código
		Pruebas de penetración
PHISING	Redirección y reenvíos no válidos	Análisis estático de código
		Análisis estático de código

[50] Mikrotik. [En línea] https://mikrotik.com/. p 36-42.

[51]Hernández Saucedo, Ana Laura y Mejía Miranda, Jezreel. Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. s.l.: Computación e informática, febrero de 2015. 42 p.

4.2.5 WEB APLICATION FILTER

WAF	CARACTERÍSTICAS	VENTAJAS	DESVENTAJAS
NAXSI	Cortafuego de aplicaciones WEB, diseñado para servidores *Nginx*	• Uso de reglas simples usando un sistema basado en puntajes. • Creación de reglas blancas • Poco uso de recursos del servidor	• Sobrecarga al usar el modo de aprendizaje • Solo sirve para sistema Nginx
MODSECURITY	Cortafuego de aplicaciones WEB, diseñado para servidores Apache, IIS, Nginx, etc.	• Integra un conjunto de reglas básicas que bloquea ataques comunes. • Soporta parches virtuales.	• No permite simplificación de reglas • Uso de recursos elevado.

4.3 MARCO LEGAL

Con el gran unos de las nuevas tecnologías de la información y las telecomunicaciones, se ha formado un nuevo mundo, el ciberespacio, allí se producen problemas, conflictos y agresiones, además de crearse la ciberamenazas que atentaran con la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La ley 1341 de 2009 determina el marco general para la formulación de las políticas públicas que regirán en el sector de las tecnologías de la información y las comunicaciones, la cual marca un momento importante en la política pública sectorial ya que, a través de ella, el estado reconoce que:

La promoción del acceso, uso y apropiación de las tecnologías de la información y las comunicaciones, como lo establece en el artículo 68 con temas relacionados con las licencias y permisos autorizados para los proveedores de redes y servicios de telecomunicaciones. El artículo 6 deduce que las personas naturales o jurídicas, públicas o privadas que son responsables de la gestión de una red en virtud de un permiso para el uso de frecuencias para su uso exclusivo, deben inscribirse en el registro, tal como expresamente lo señala el artículo 5 del decreto 4948 del año 2009. El despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, como lo establece el artículo 4 autorizando al estado obligar a los proveedores de redes y servicios de telecomunicaciones la implementación de base de datos a cargo de ellos, por razones de defensa nacional y seguridad pública. Esta obligación de implementación de la base fue ratificada por el artículo 106 de la ley 1453 de 2011.

La formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y el conocimiento, impactando en el mejoramiento de la inclusión social y de la competitividad del país; dejando de lado la distinción y regulación por tipos de servicios de telecomunicaciones, lo cual no implica que técnica y comercialmente no tenga diferencias.

Con el uso masivo de las tecnologías de la información, se crea un nuevo espacio llamado ciberespacio en el cual al igual que en el contexto físico existen amenazas, que pretende atacar el estado de bienestar de la sociedad, también pretendiendo atentar con la seguridad nacional.

Las normas que rigen la tecnología en Colombia son las siguientes.

Normas que rigen la Propiedad Intelectual del software en Colombia

- Decisión Andina 486 de 2000: Con respecto a la protección de la propiedad industrial, cada País Miembro concederá a los nacionales de los demás miembros de la Comunidad Andina, de la Organización Mundial del Comercio y del Convenio de París para la Protección de la Propiedad Industrial, un trato no menos favorable que el que otorgue a sus propios nacionales, a reserva de lo previsto en los artículos 3 y 5 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), y en el artículo 2 del Convenio de París para la Protección de la Propiedad Industria[52]l.
- Decisión Andina 351 de 1993: Las disposiciones de la presente Decisión tienen por finalidad reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino[53].
- Ley 23 de1982: Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta ley a los intérpretes o ejecutantes, a los productores de fonogramas y a los organismos de radiodifusión, en sus derechos conexos a los del autor[54].
- Ley 1450 del 16 de junio de 2011: El Plan Nacional de Desarrollo 2011-2014: Prosperidad para Todos, que se expide por medio de la presente ley, tiene como objetivo consolidar la seguridad con la meta de alcanzar la paz, dar un gran salto de progreso social, lograr un dinamismo económico regional que permita desarrollo sostenible y crecimiento sostenido, más empleo formal y menor pobreza y, en definitiva, mayor prosperidad para toda la población[55].
- Ley 1273 De 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de 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[56].

---

[52] DECISION 486. TITULO I DISPOSICIONES GENERALES Articulo 1. s.l.: LA COMISION DE LA COMUNIDAD ANDINA. 45 p.

[53] DECISIÓN 351. CAPITULO I DEL ALCANCE DE LA PROTECCION Articulo 1. s.l.: El Artículo 30 del Acuerdo de Cartagena y la Propuesta 261 de la Junta. 45 p.

[54]CONGRESO DE LA REPUBLICA. LEY NÚMERO 23 DE 1982 CAPÍTULO I Disposiciones generales Articulo 1. 45 p.

[55] CONGRESO DE LA REPUBLICA. LEY 1450 DE 2011 TITULO 1 DISPOSICIONES GENERALES ARTICULO 1. 45 p.

[56] CONGRESO DE COLOMBIA. LEY 1273 DE 2009 CAPITULO PRIMERO De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. 45 p.

4.4 MARCO ESPACIAL

El proyecto de implantación se desarrolla en un ambiente virtual controlado, haciendo uso de máquinas virtuales que simulen el tráfico de información de la aplicación.

4.5 MARCO METODOLÓGICO

Metodología

La investigación que se usara tipo cuasi-experimental; ya que por medio de este tipo de investigación los resultados se aproximan a una investigación experimental en la que no es posible tener el control y manipulación de las variables.

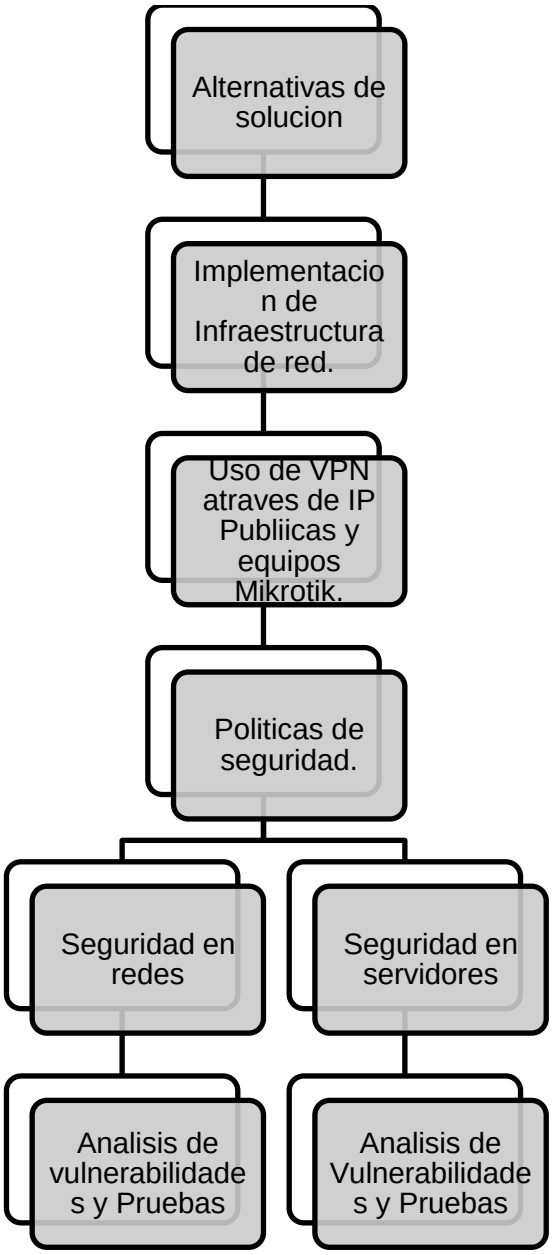
El tipo de investigación que se aplica en el presente trabajo es de tipo Cualitativa-Cuantitativa.

Etapas

Para el desarrollo del proyecto aplicado se tendrán en cuenta las siguientes etapas:

- Realización de investigación bibliográfica de conceptos relacionados al tema del proyecto, se investiga proyectos actualmente existentes.
- Se realiza ataques de vulnerabilidades y penetración realizando documentación de toda la información obtenida.
- Se buscarán alternativas de qué tipo de aplicaciones se podrán utilizar, teniendo en cuenta las observaciones realizadas por la empresa.
- Realizar los diseños de infraestructura de red.
- Desarrollar el puesto en marcha del proyecto.
- Se realiza pruebas de aseguramiento al aplicativo BADSTORE.
- Se harán evaluaciones y validaciones del rendimiento del proyecto.
- Desarrollo de un manual de instalación de WAF.

4.6 DIAGRAMA DE SOLUCION



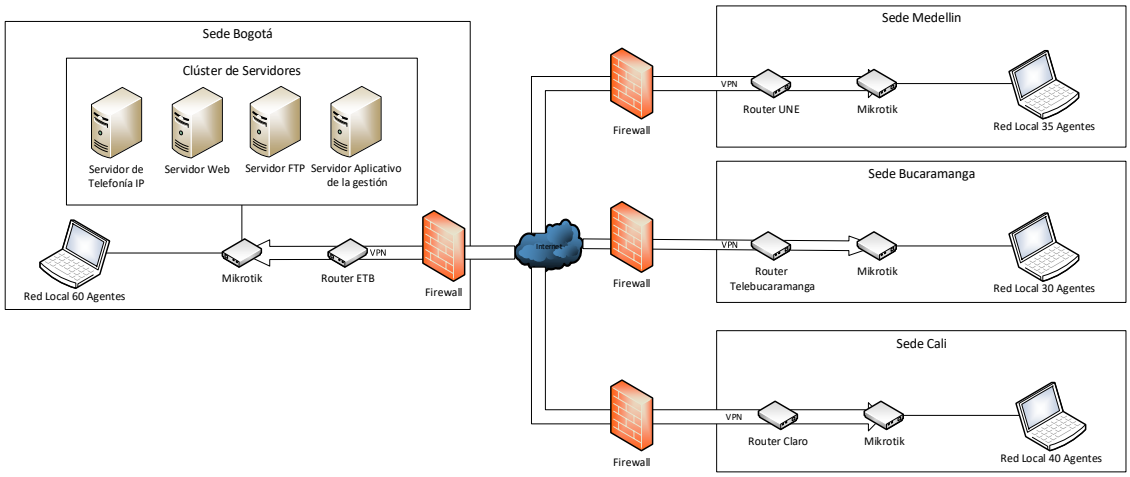
5. RESULTADOS

5.1 INFRAESTRUCTURA DE RED PARA LA INTERCONEXIÓN PARA CUATRO SEDES DE LA EMPRESA DE COBRANZA “XYZ”.

Se realiza la infraestructura de la empresa de cobranzas “XYZ” de las cuatro Sedes que forman parte de la empresa (Bogotá, Medellín, Bucaramanga y Cali) ver figura 6. Cada una de las sedes cuenta con un número específico de agentes (Bogotá: 60; Bucaramanga: 30; Cali: 40 y Medellín: 35), los cuales están encargados de realizar las llamadas a los clientes que han sido reportados por los bancos, con el fin de realizar la respectiva recuperación de cartera.

Para el acceso a Internet, la empresa XYZ ha contratado en cada ciudad con el proveedor de servicios que cuenta con la mejor referencia de conectividad, de la siguiente forma: Bogotá, Medellín, Bucaramanga y Cali han contratado el servicio de internet con ETB, UNE, Tele Bucaramanga y Claro respectivamente. Los anchos de banda contratados para cada sede son los siguientes: (Bogotá: 50MB; Bucaramanga: 20MB; Cali: 30MB y Medellín: 30MB).

Figura 6 Topología de red implementada en la empresa XYZ



Fuente: Autor

5.1.1 Equipos usados

Se usan en cada sede las siguientes routerboard:

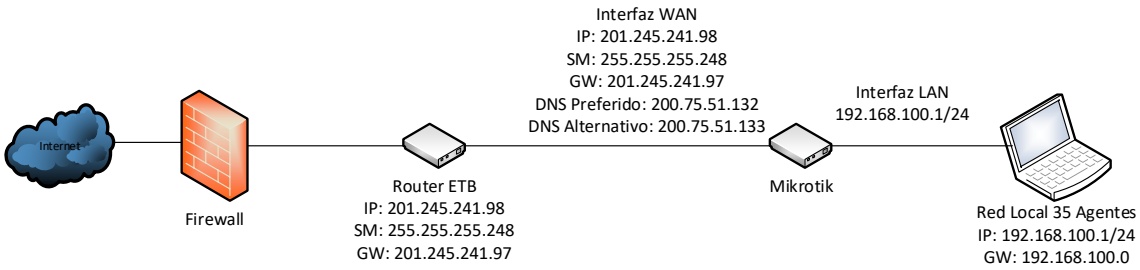
Tabla 2 Características de Routerboard

Sede	Routerboard	Imagen
Bogotá	RB2011iL-IN • Dimensiones 214x86mm • Tamaño de la memoria RAM 64 MB • Tamaño de almacenamiento 128 MB • Tipo de almacenamiento NAND • 10/100 puertos Ethernet 5 • 10/100/1000 puertos Ethernet 5	
Medellín	RB951ui-2nd • CPU QCA9531 @ 650 MHz • RAM 64 MB • Ethernet 5 Puertos 10/100 Ethernet • Estándar Inalámbrico 2.4 GHz - 802.11b/g/n, Cadena dual. • Antena 1.5 dBi • Salida PoE Ether 5 • Energía 6-30 V DC o PoE Pasivo • Máximo Consumo de Potencia 5 W • Dimensiones 113 x 89 x 28 mm • Sistema Operativo RouterOS L4	
Bucaramanga	RB951ui-2nd • CPU QCA9531 @ 650 MHz • RAM 64 MB • Ethernet 5 Puertos 10/100 Ethernet • Estándar Inalámbrico 2.4 GHz - 802.11b/g/n, Cadena dual. • Antena 1.5 dBi • Salida PoE Ether 5 • Energía 6-30 V DC o PoE Pasivo • Máximo Consumo de Potencia 5 W • Dimensiones 113 x 89 x 28 mm • Sistema Operativo RouterOS L4	
Cali	RB951ui-2nd • CPU QCA9531 @ 650 MHz • RAM 64 MB • Ethernet 5 Puertos 10/100 Ethernet • Estándar Inalámbrico 2.4 GHz - 802.11b/g/n, Cadena dual. • Antena 1.5 dBi • Salida PoE Ether 5 • Energía 6-30 V DC o PoE Pasivo • Máximo Consumo de Potencia 5 W • Dimensiones 113 x 89 x 28 mm • Sistema Operativo RouterOS L4	

5.1.2 Definición de direccionamiento

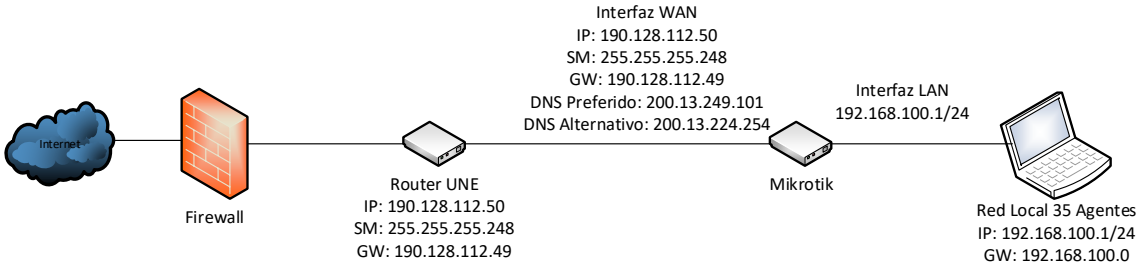
En las Figuras 7, 8, 9 y 10 se detallan la configuración de IP de las cuatro sedes de la empresa d cobranza XYZ.

Figura 7 Direccionamiento Sede Bogotá



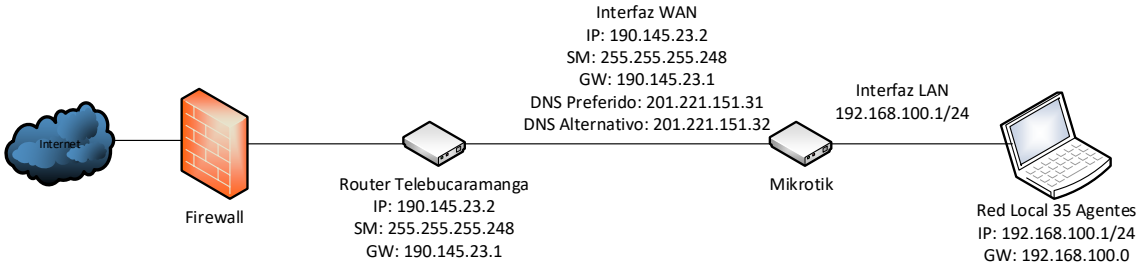
Fuente: Autor

Figura 8 Direccionamiento Sede Medellín



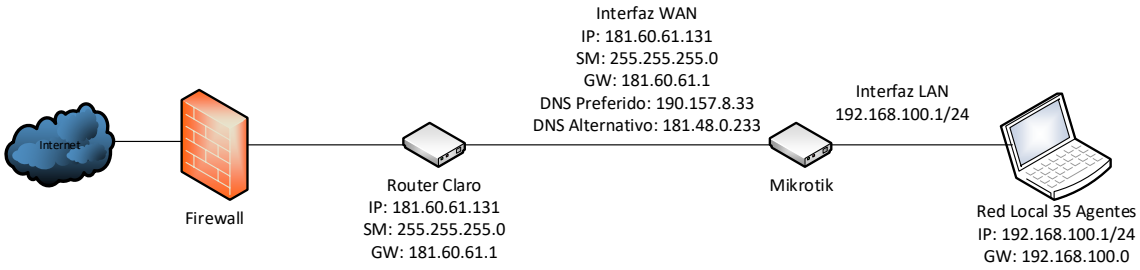
Fuente: Autor

Figura 9 Direccionamiento Sede Bucaramanga



Fuente: Autor

Figura 10 Direccionamiento Sede Cali



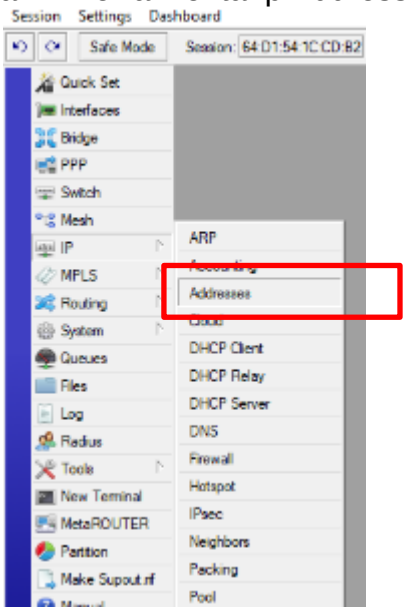
Fuente: Autor

5.1.3 Configuración de IP PÚBLICA en MIKROTIK

Para la configuración de la IP Publicas en cada sede se realiza los siguientes pasos:

- Primero configuramos la IP pública para ellos, damos clic en IP y luego Addresses, en la figura 11 se muestra gráficamente el proceso a realizar.

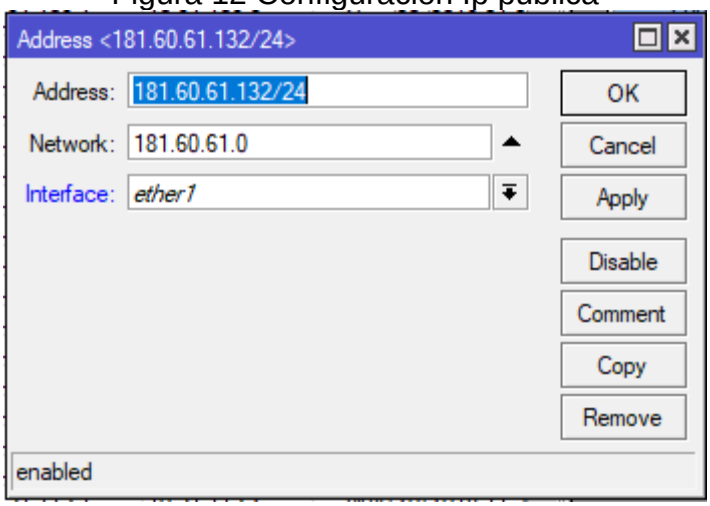
Figura 11 Herramienta Ip Addresses



Fuente: Autor

- Como se puede observar en la figura 12 se identifica la configuración de la IP publica con su respectiva mascara de red.

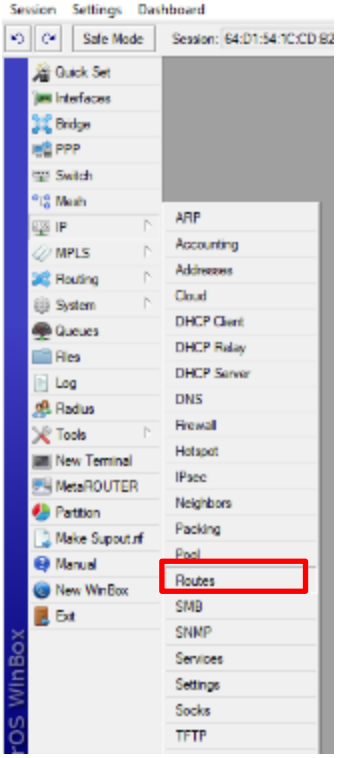
Figura 12 Configuración Ip pública



Fuente: Autor

- Luego configuramos la puerta de enlace, damos clic en IP y luego Router, en la figura 13 se observa gráficamente el proceso.

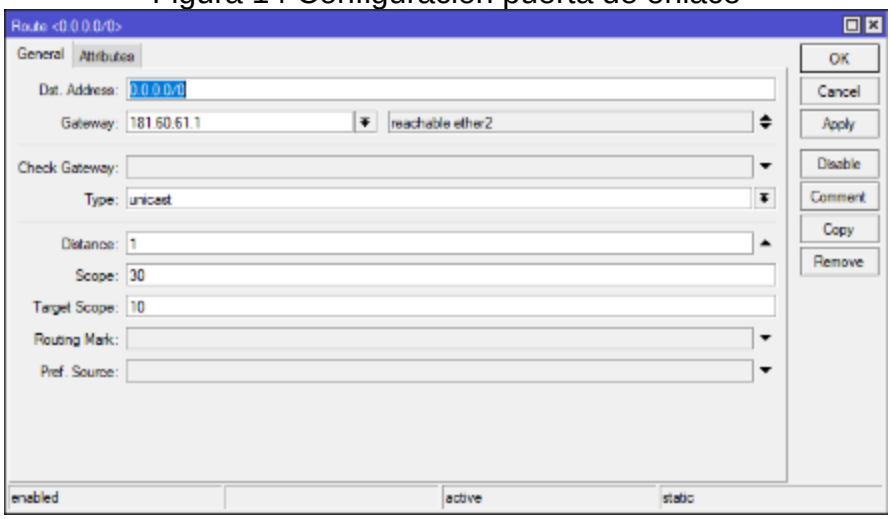
Figura 13 Herramienta Routes



Fuente: Autor

- Como se puede observar en la figura 14 la configuración de la puerta de enlace.

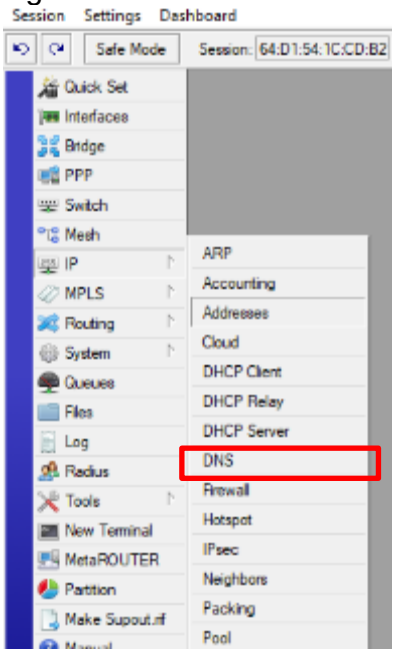
Figura 14 Configuración puerta de enlace



Fuente: Autor

- Como se puede observar en la figura 15 se muestra la configuración de los dns, damos clic en IP y luego en DNS.

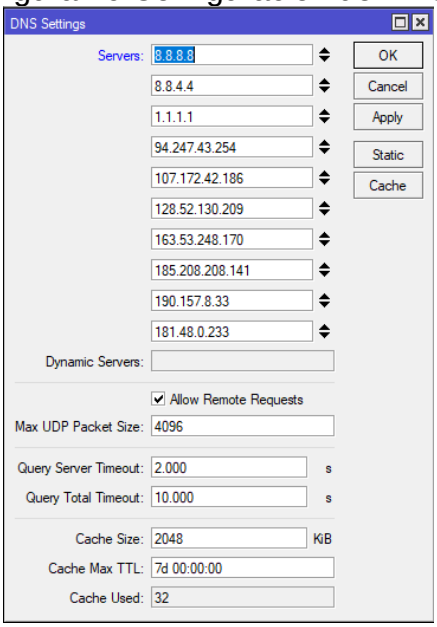
Figura 15 Herramienta DNS



Fuente: Autor

- Configuramos los dns, en la figura 16 se puede observar los resultados de la operación.

Figura 16 Configuración de DNS



Fuente: Autor

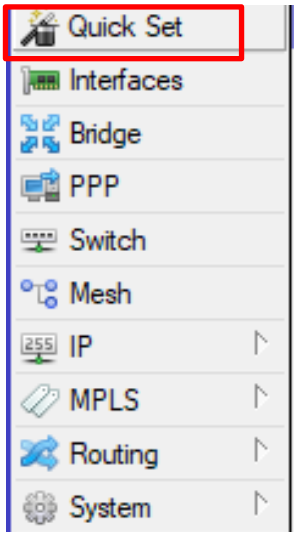
5.1.4 Creación de VPN

Se selecciona el protocolo de VPN L2TP, puesto que es un protocolo seguro y fácil de configurar, además que se encuentra disponible en todos los dispositivos y sistemas operativos modernos.

En la RouterBoard de la sede Bogotá sede principal se realiza las configuraciones de las VPN.

- Configuración de las VPN, En la figura 17 se ve la herramienta PPP.

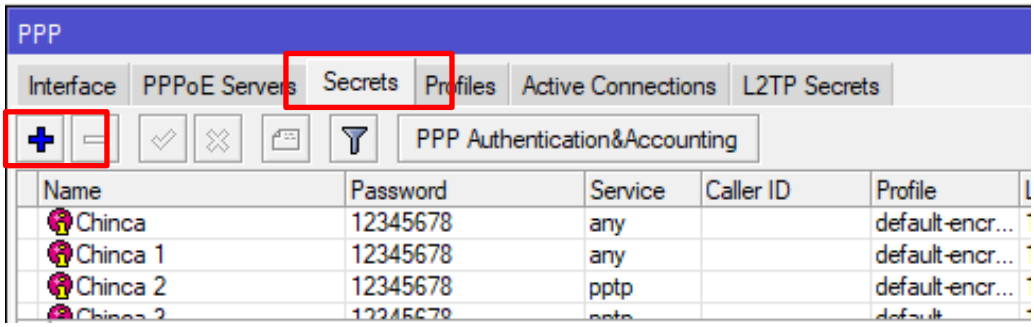
Figura 17 Herramienta PPP



Fuente: Autor

- Seleccionamos la pestaña Secrets y damos clic en el símbolo más, en la figura 18 se especifica el proceso.

Figura 18 Configuración de VPN



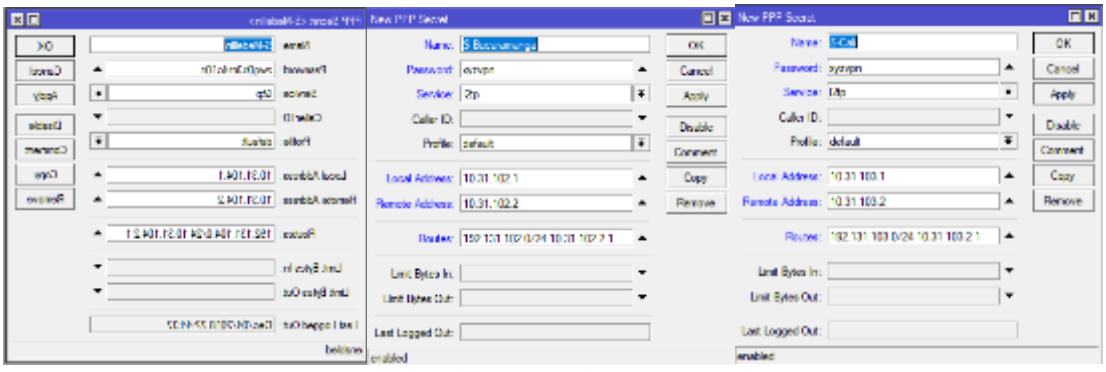
Fuente: Autor

- Allí elegimos los usuarios, contraseña, service, local address, remote address, en la figura 19 se observa la configuración que debe realizarse a cada router.

Tabla 3 Configuración de IP por sede

SEDE	USUARIO	CONTRASEÑA	SERVICE	LOCAL ADDRESS	REMOTE ADDRESS	ROUTER
MEDELLÍN	S-Medellín	Xyzvpn	l2tp	10.31.104.1	10.31.104.2	192.131.104.0/24 10.31.104.2 1
BUCARAMANGA	S-Bucaramanga	Xyzvpn	l2tp	10.31.102.1	10.31.102.2	192.131.102.0/24 10.31.102.2 1
CALI	S-Cali	Xyzvpn	l2tp	10.31.103.1	10.31.103.2	192.131.103.0/24 10.31.103.2 1

Figura 19 Configuración de VPN routerboard principal

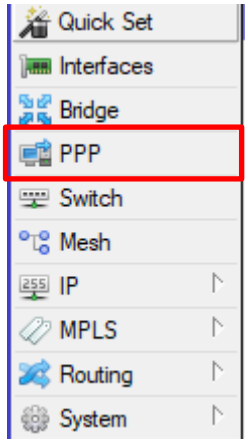


Fuente: Autor

En cada Sede se realiza la configuración de la VPN.

- Configuración de las VPN´s, vamos a la herramienta PPP, en la figura 20 se muestra la herramienta PPP.

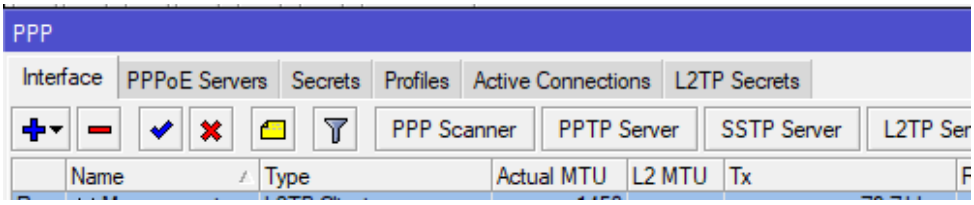
Figura 20 Herramienta PPP en RouterBoard



Fuente: Autor

- Seleccionamos la pestaña Interface y damos clic en el símbolo más (+), en la figura 21 se observa la interface PPP.

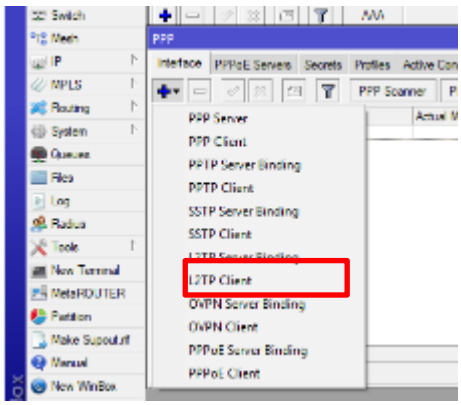
Figura 21 Pestaña Interface



Fuente: Autor

- En la figura 22 se observa la selección del tipo de protocolo en este caso elegiremos el protocolo L2TP Client.

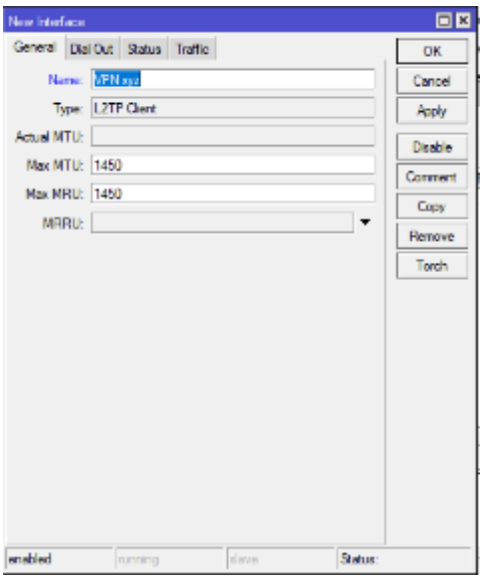
Figura 22 Protocolos de VPN



Fuente: Autor

- Como se puede observar en la figura 23 el nombramiento de la VPN.

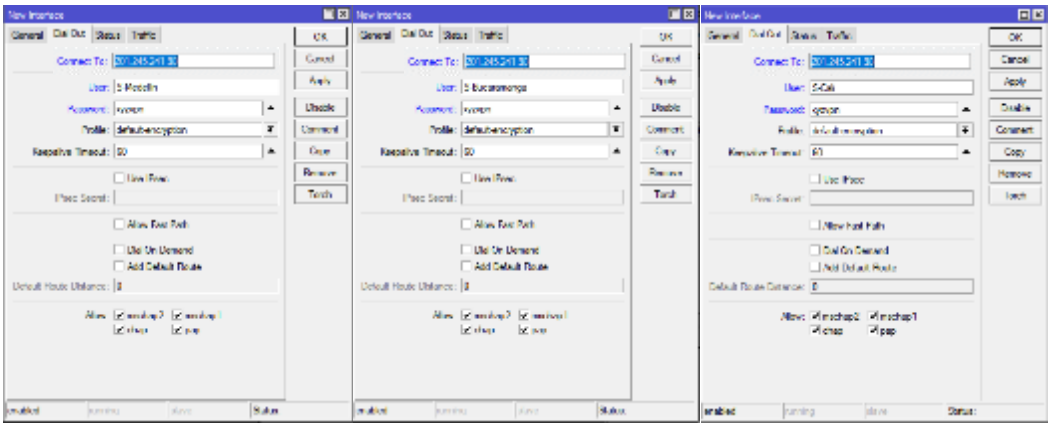
Figura 23 Configuración de VPN en RouterBoard Sede



Fuente: Autor

- Configuramos la IP pública donde están asociado las VPN, con sus respectivos Usuarios y Contraseña, en la figura 24 se observa el resultado de la operación.

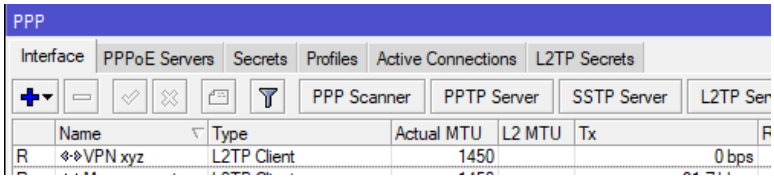
Figura 24 Configuración de VPN routerboard en cada Sede



Fuente: Autor

- Verificamos conexión con la RouterBoard Principal, en la figura 25 se indica dónde está la herramienta *PPP > interface.*

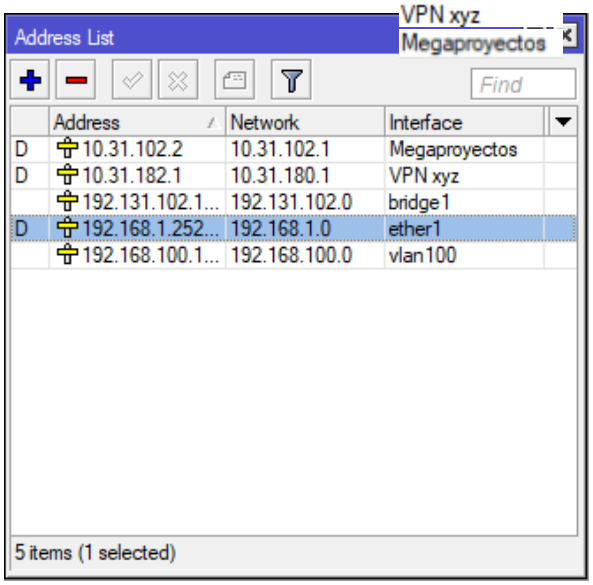
Figura 25 Pestaña Interface en la herramienta PPP



Fuente: Autor

En la figura 26 se observa la activación de la ip remota.

Figura 26 Obtención de IP Remota

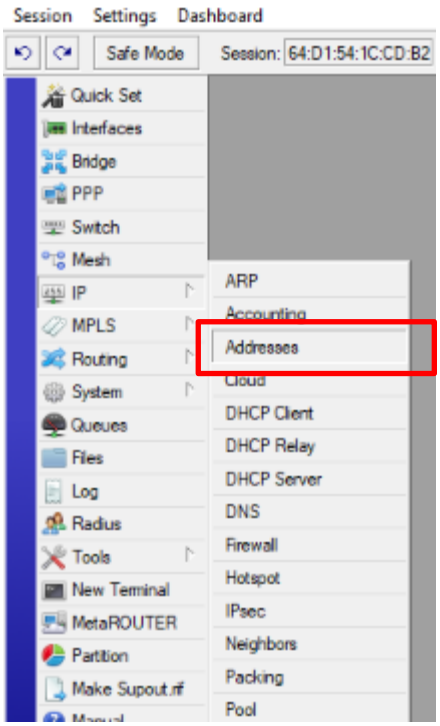


Fuente: Autor

5.1.5 Configuración de red local en la RouterBoard de las sedes

- Primero configuramos la IP publica para ellos, damos clic en IP y luego Addresses, seguir pasos de la figura 27.

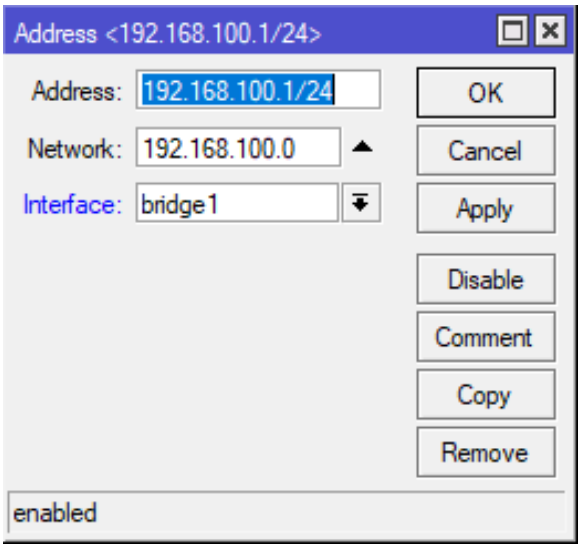
Figura 27 Herramienta IP Addresses



Fuente: Autor

- En la figura 28 se observa la IP local con su respectiva mascara de red

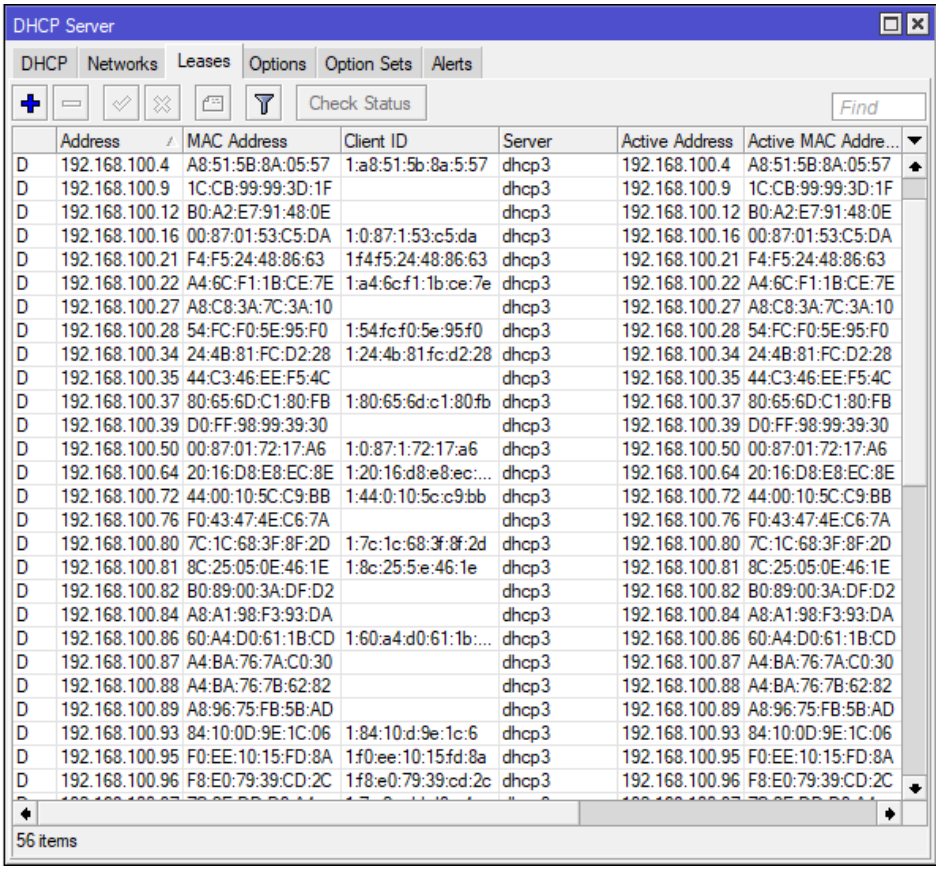
Figura 28 Configuración de IP Local para agentes



Fuente: Autor

- En la figura 29 se muestra la herramienta para verificar los Agentes conectados.

Figura 29 IP Local de los agentes

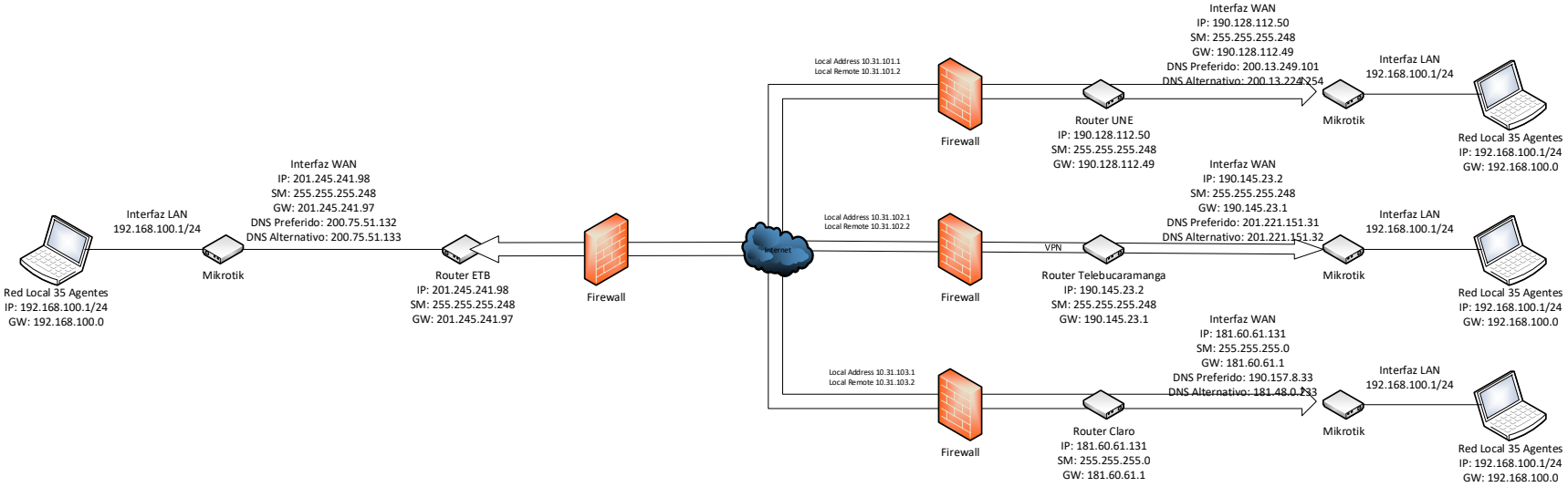


Fuente: Autor

5.1.6 Topología de red empresa XYZ

En la figura 30 se detallada la infraestructura de red de la empresa de cobranza XYZ, con sus respectivas IP.

Figura 30 Infraestructura de red para la interconexión para cuatro sedes (ciudades) de la empresa de cobranza "xyz

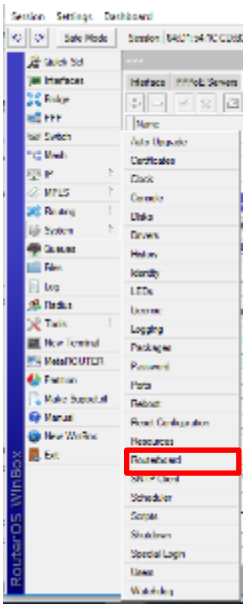


Fuente: Autor

5.1.7 Políticas de seguridad aplicadas

- Cambio de Usuario para el ingreso de las RouterBoards, para ello se ingresa a las herramientas System->Users, evitar usar nombre de usuarios como admin, root, administrator, seguir indicaciones de la figura 31.

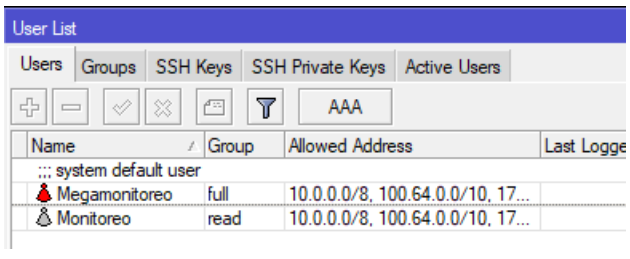
Figura 31 Herramienta Users



Fuente: Autor

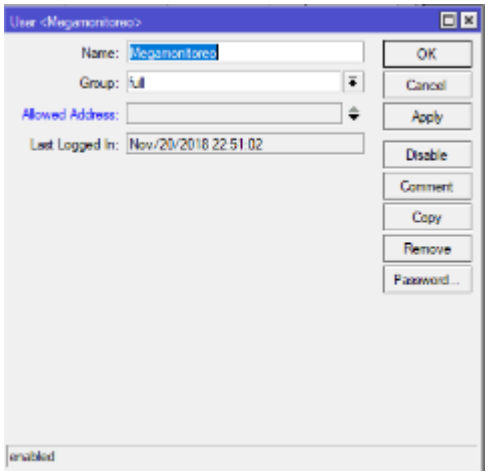
- Damos doble clic sobre el usuario que deseamos cambiar el nombre, seguir indicaciones figura 32 y 33.

Figura 32 Usuarios existentes en la RouterBoard



Fuente: Autor

Figura 33 Herramienta cambio de Nombre de Usuario

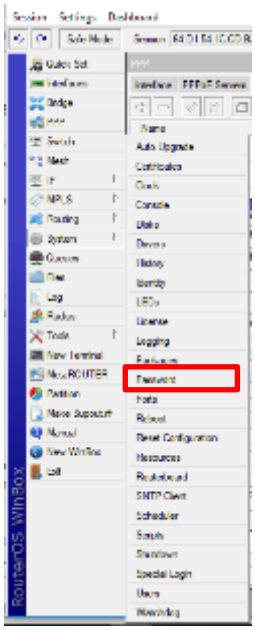


Fuente: Autor

Se recomienda tener dos usuarios uno que contenga todos los privilegios quien será usado por el administrador de la red, y otro usuario de lectura para realizar el monitoreo de la Red

- Cambio de contraseña, para el cambio de contraseña de los usuarios se dirige a la herramienta System > Password como lo indica en la figura 34.

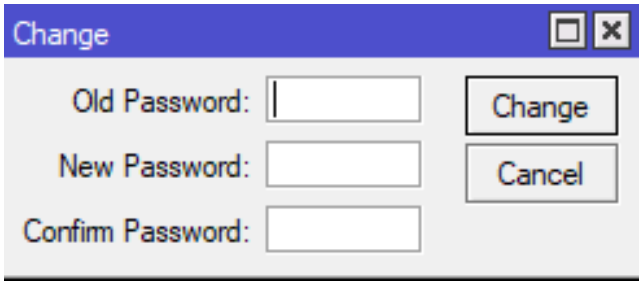
Figura 34 Herramienta Password



Fuente: Autor

- Se debe asignar una contraseña ya que por defecto viene en blanco, la pestaña Change es como se muestra en la figura 35.

Figura 35 Ventana Change

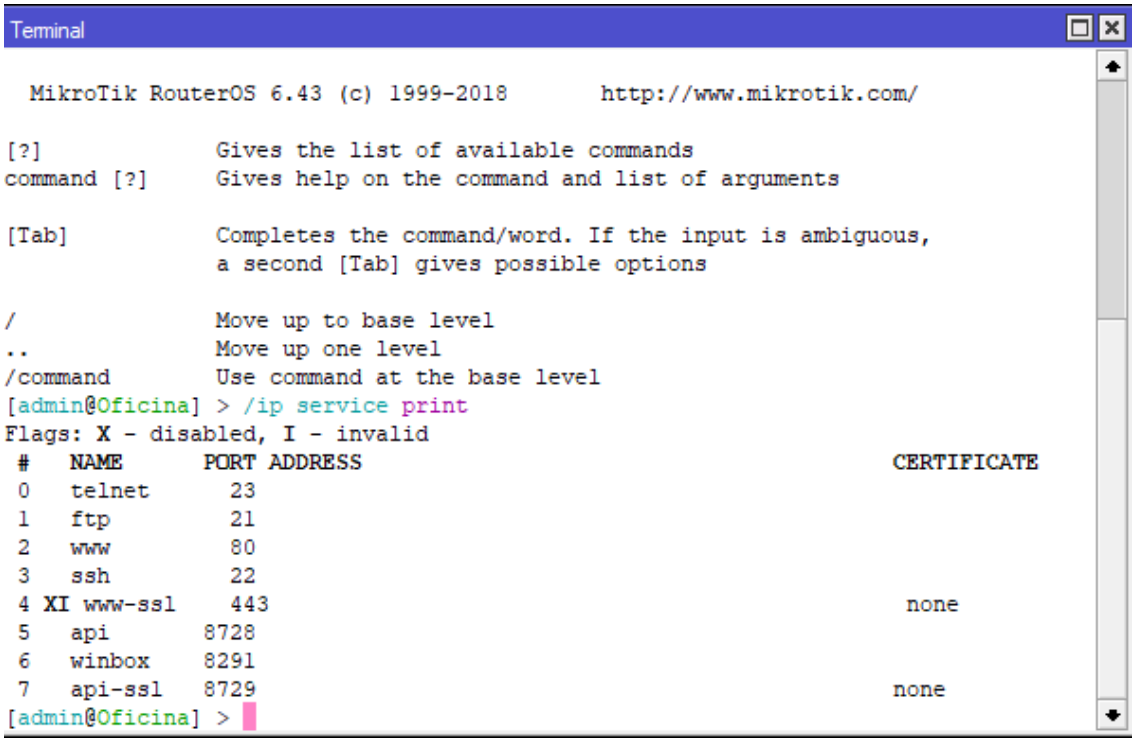


Fuente: Autor

- Deshabilitar protocolo y cambiar puertos

Con el comando /ip service print, encontramos todos los protocolos activados, debemos ingresar a la herramienta terminal donde se ejecutará el comando como se indica en la figura 36.

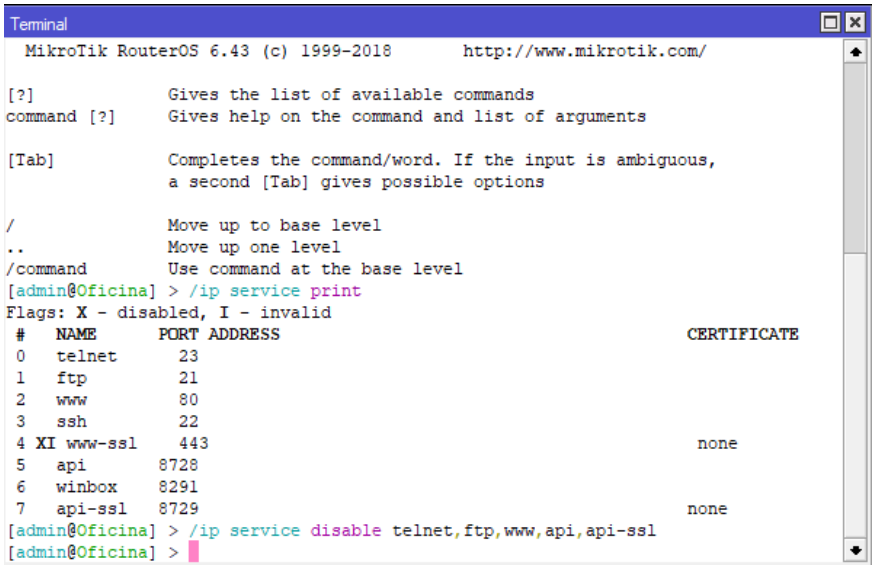
Figura 36 Protocolos activados



Fuente: Autor

En la figura 37 se observa el uso del comando /ip service disable telnet, ftp, www, api, api-ssl, el cual deshabilitara los protocolos que no se usaran y son menos seguros.

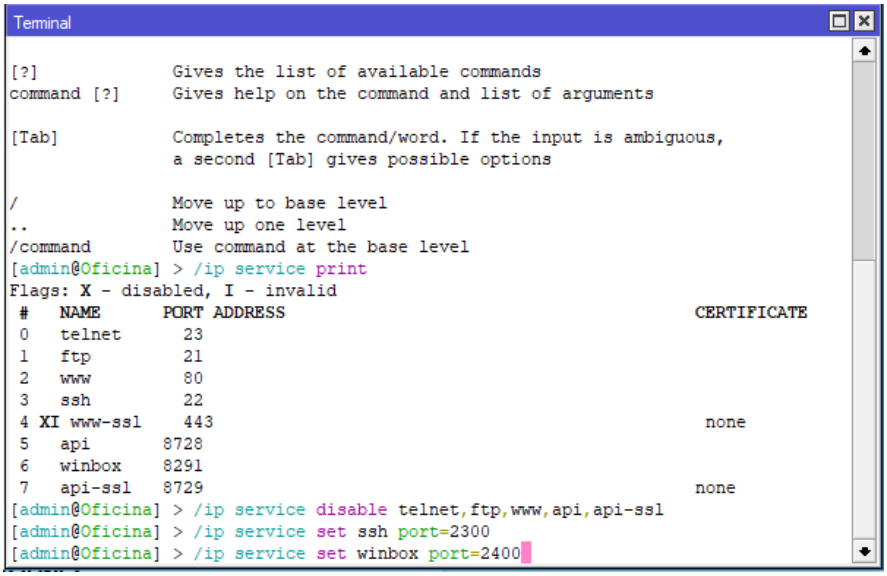
Figura 37 Desactivación de protocolos



Fuente: Autor

Se cambia los puertos de conexión de SSH y de Winbox para evitar los ataques de fuerza bruta, ver figura 38.

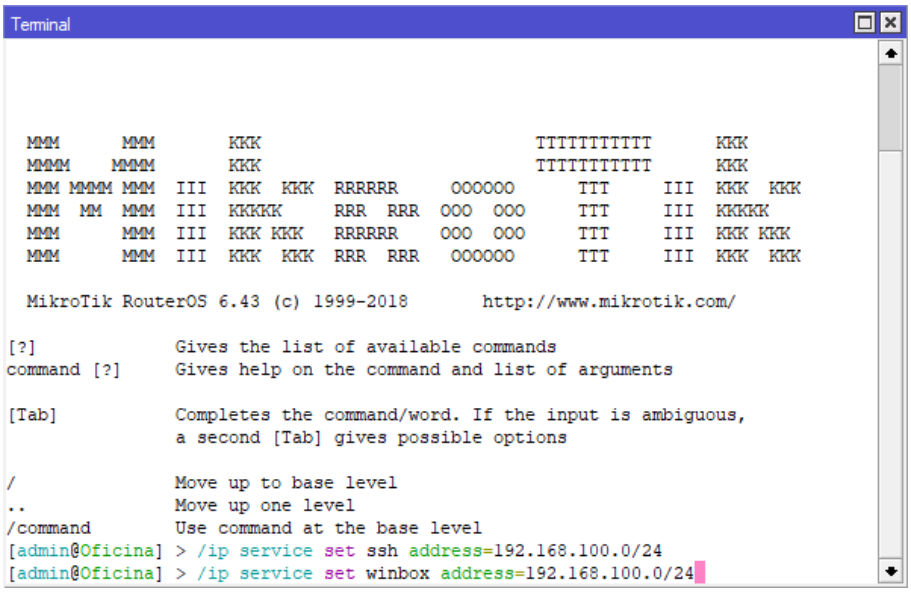
Figura 38 Cambio de Puertos



Fuente: Autor

Se establece un rango de IP o subnet para accesos de IP's asignadas, ver figura 39.

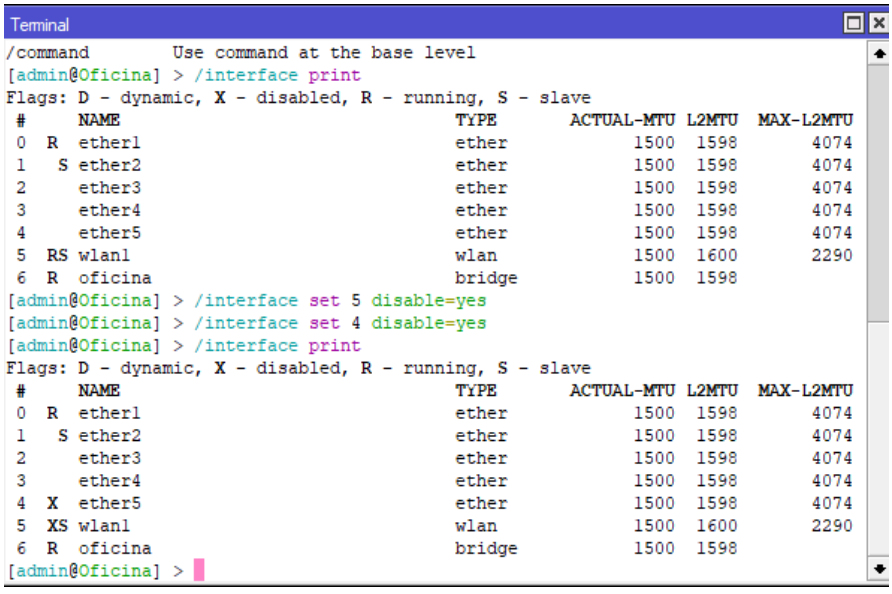
Figura 39 Rango de IP para conexión



Fuente: Autor

- En la figura 40 se observa cómo se deshabilita las interfaces no usadas, esto evita que terceros se conecte a nuestros equipos.

Figura 40 Desactivar interface

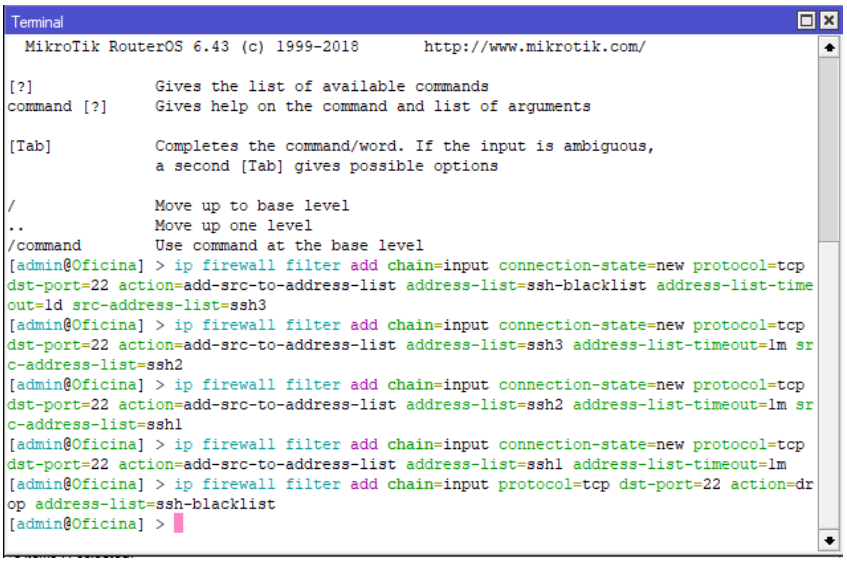


Fuente: Autor

- Limitación de acceso por SSH

Las limitaciones de acceso por SSH impiden ataques de fuerza bruta, se permitirán solo tres intentos de acceso posteriormente se bloqueará la RouterBoard por 1 Día, en la figura 41 se observa el comando a ser usado.

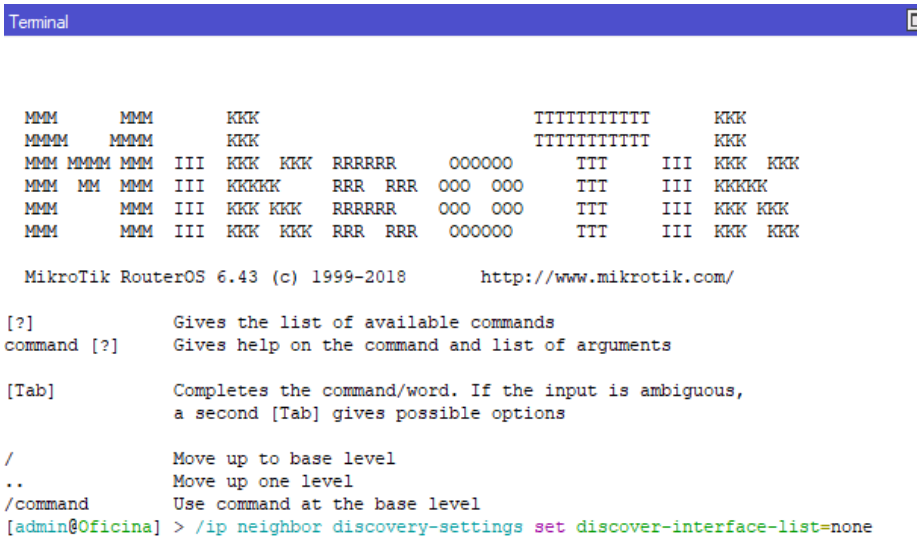
Figura 41 Limitaciones de acceso por SSH



Fuente: Autor

- Desactivar protocolo de reconocimientos de equipos en la red, ver figura 42.

Figura 42 Desactivar reconocimiento de otros equipos en la red

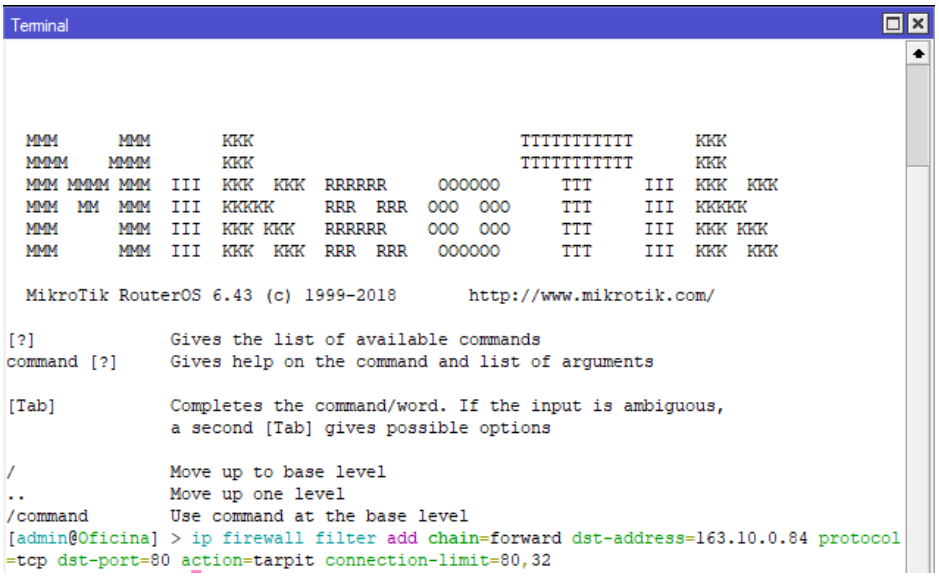


Fuente: Autor

- Uso de estrategia tarpit

La herramienta tarpit impide los ataques de DoS, permite que haya transferencia de datos, pero deja que se generen las conexiones. Permitir 79 conexiones simultáneas por IP con destino al servidor web y aplicar tarpit a partir de la conexión 80, en la figura 43 se observa el comando usado.

Figura 43 Herramienta Tarpit



Fuente: Autor

5.1.8 Síntesis de las vulnerabilidades

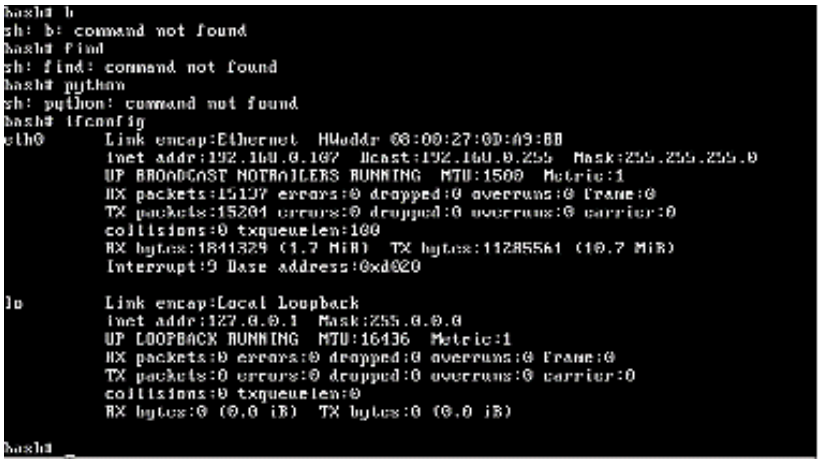
Elemento	Prueba Realizada	Vulnerabilidad Encontrada	Identificador asociado a la vulnerabilidad (CVE)
BadStore	Cross Site Scripting (XSS)	insertar código HTML en el servidor WEB	CVE-2019-8391
BadStore	Ataque por inyección de código SQL	Ataque a la base de datos del servidor WEB	CVE-2019-6491
BadStore	Denegación de servicio	Pérdida de la conectividad del usuario real	CVE-2009-1441
BadStore	Cookie snooping	Decodificación de información privada de usuarios	CVE-2018-1484
BadStore	Modificación de cookies	Modificación de datos de compras de los usuarios	CVE-2010-4333
BadStore	Tampering de parámetros y formularios	Modificación de los parámetros en la aplicación web	CVE-2009-1583
BadStore	Directory transversal	Acceso a nivel privilegiado a usuario no autorizado	CVE-2004-1862
BadStore	Navegación forzada	Visualización de elementos y archivos importantes para la empresa	CVE-2008-1045

5.1.9 Análisis de vulnerabilidad y prueba de penetración de prueba.

5.1.9.1 Cross Site Scripting (XSS)

- Luego de instalar BadStore en la máquina virtual VM VirtualBox, se ejecuta el comando IFCONFIG para conocer la dirección IP, ver ilustración 1.

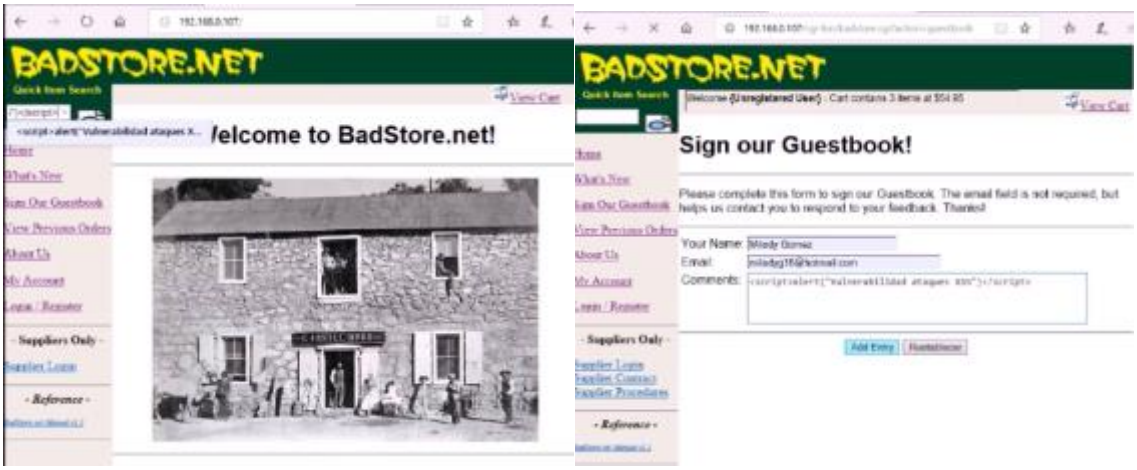
Ilustración 1 Dirección IP BadStore



Fuente: Autor

- En la ilustración 2 se describe el ingreso de datos en los campos de búsqueda la petición “<script>alert("Vulnerabilidad ataques XSS")</script>

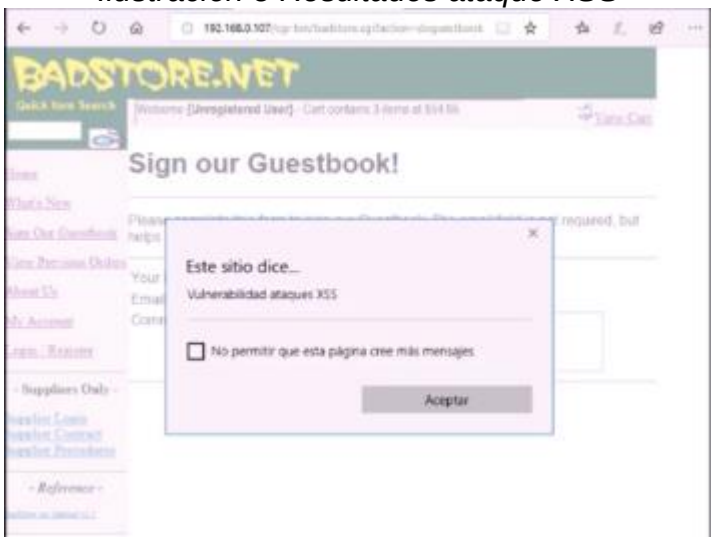
Ilustración 2 Uso de la petición <script>alert ("Vulnerabilidad ataques XSS") </script>”



Fuente: Autor

- En la ilustración 3 se evidencia el resultado de la vulnerabilidad.

Ilustración 3 Resultados ataque XSS

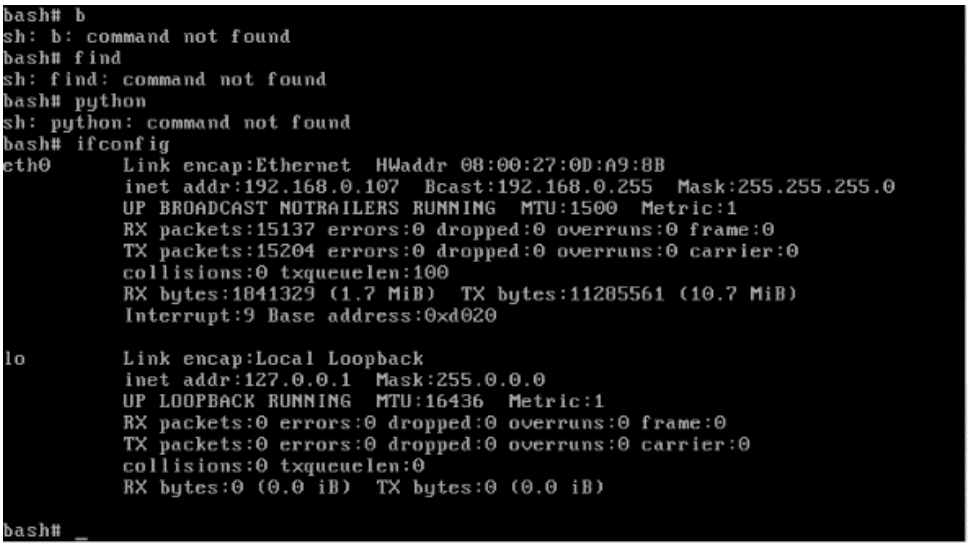


Fuente: Autor

5.1.9.2 Ataque por inyección de código SQL

- Luego de instalar *BadStore* en la máquina virtual *VM VirtualBox*, se ejecuta el comando *IFCONFIG* para conocer la dirección IP, ver ilustración 4.

Ilustración 4 Dirección IP BadStore



Fuente: Autor

- En la ilustración 5 se ve la dirección asignada es 192.168.0.107, se realiza verificación del funcionamiento del servidor web se ingresa la dirección IP a través de un navegador web.

Ilustración 5 Verificación de funcionamiento servidor web

Fuente: Autor

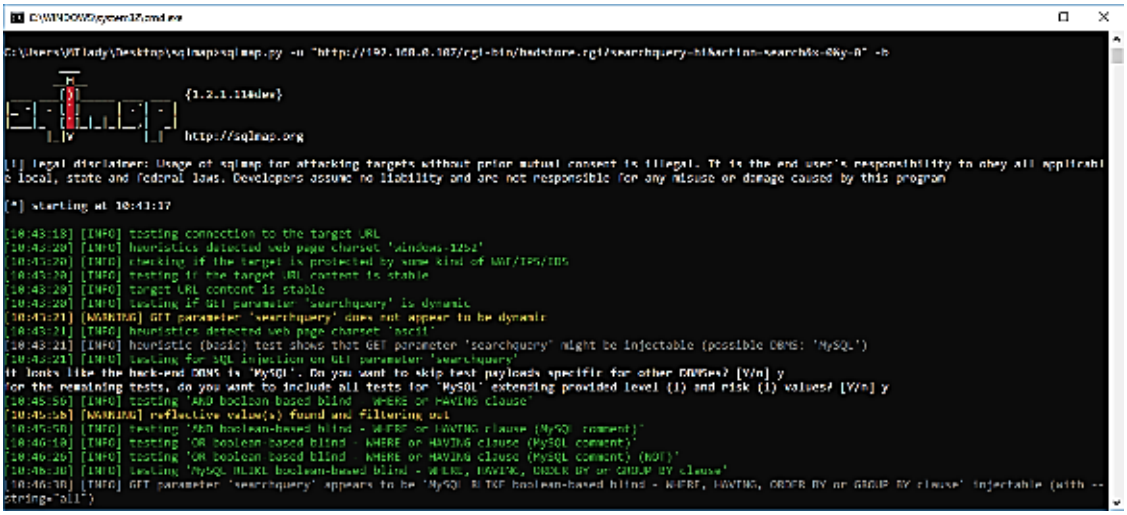
- Al verificar el funcionamiento del servidor web, se procede a analizar las primeras vulnerabilidades del servidor identificando las variables de la URL, en la ilustración 6 se verifica que el comando común en *“action”.*

Ilustración 6 Verificación de similitud en variables

Fuente: Autor

- Se ejecuta el comando *sqlmap.py -u "http://192.168.0.107/cgi-bin/badstore.cgi?searchquery=hi&action=search&x=0&y=0" –b,* como se observa en la ilustración 7, este punto se realiza si ya se conoce una variable de programación de la página en este caso es las variables *action.*

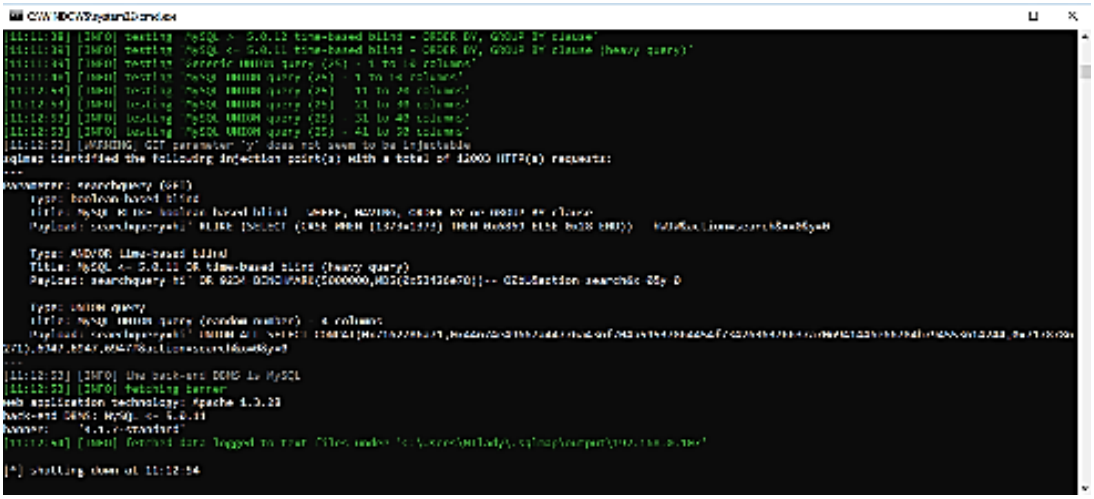
Ilustración 7 Ejecución del sqlmap



Fuente: Autor

- Al finalizar el análisis se observa la versión de apache y *Mysq*l usados en el servidor web, este resultado se puede ver en la ilustración 8.

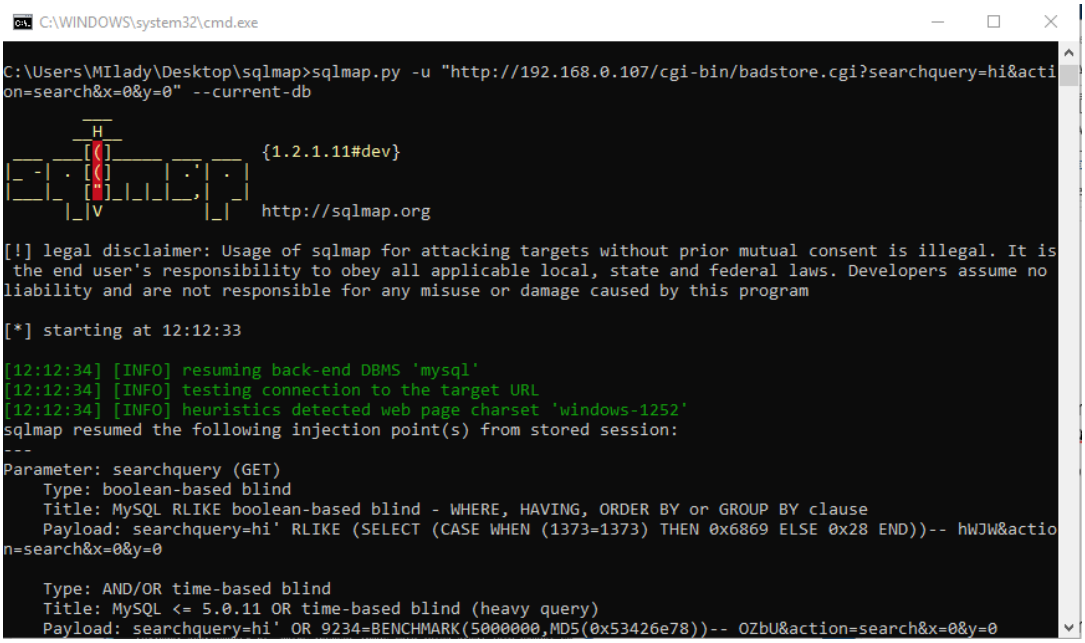
Ilustración 8 Resultados del análisis sqlmap



Fuente: Autor

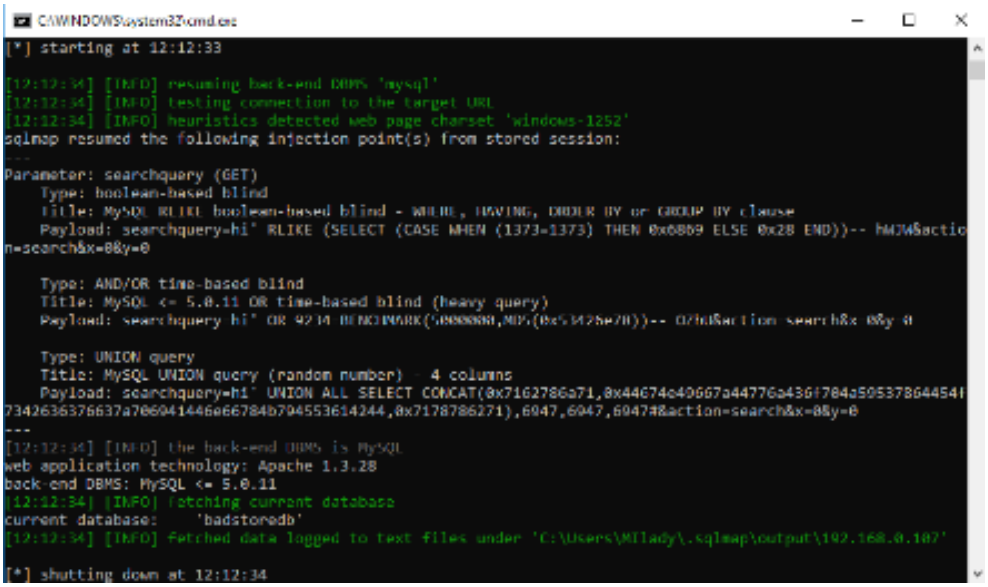
- Se obtiene el nombre de la base de datos a través del comando *--current-db*, el resultado se observa en las ilustraciones 9 y 10.

Ilustración 9 Obtención nombre de base de datos servidor web badstore



Fuente: Autor

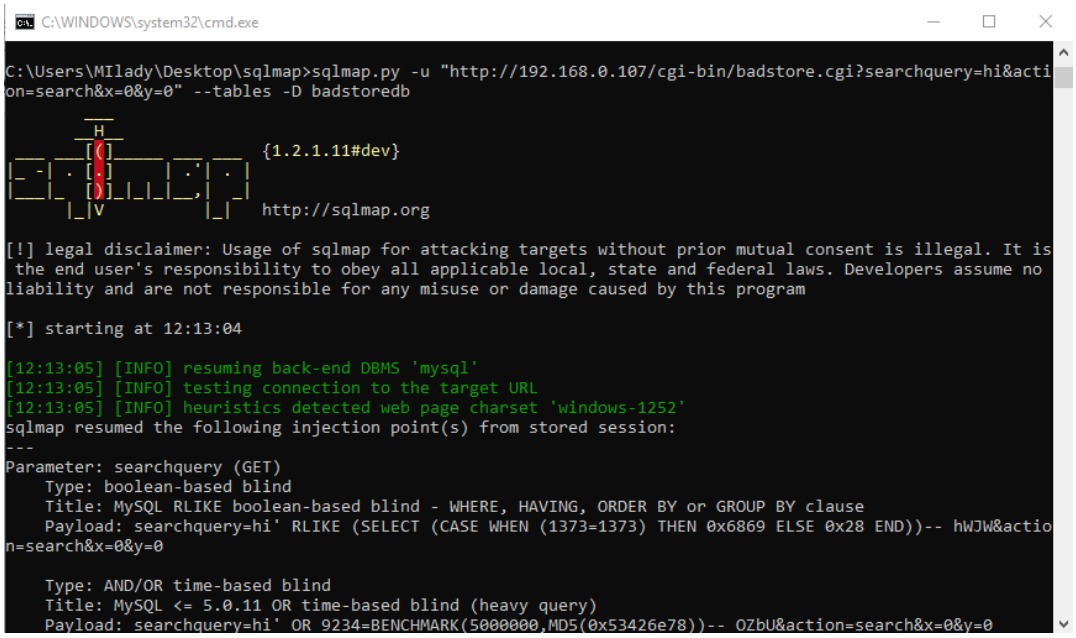
Ilustración 10 Nombre de base de datos servidor web badstore



Fuente: Autor

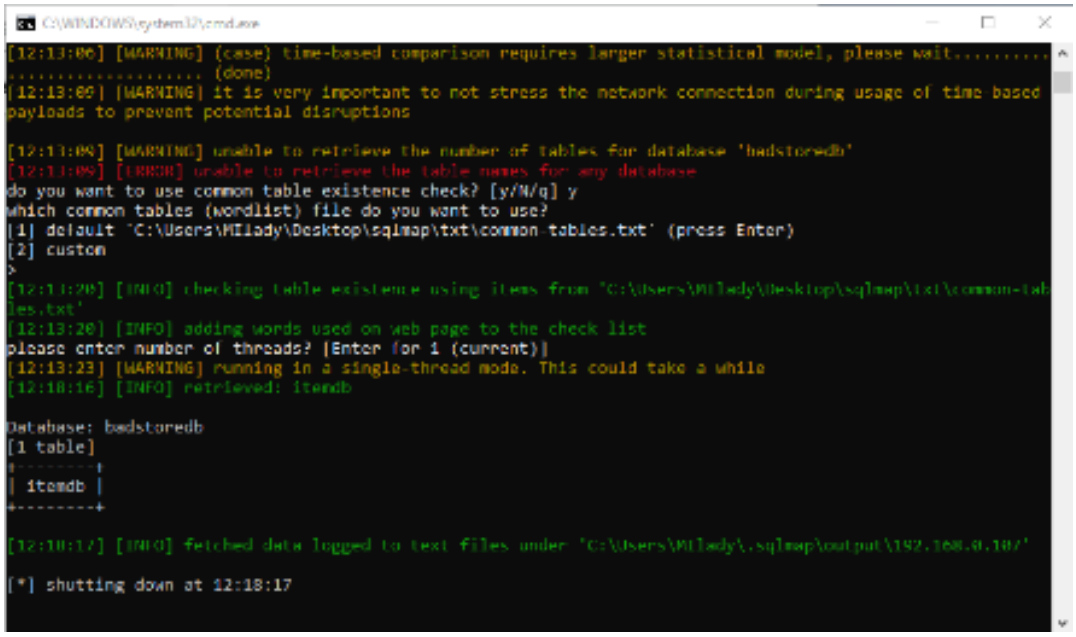
- Se obtiene el listado de tablas a través del comando *–tables –D badstoredb, ver resultados en las ilustraciones 11 y 12.*

Ilustración 11 Obtención Listado de tablas de base de datos servidor web badstore



Fuente: Autor

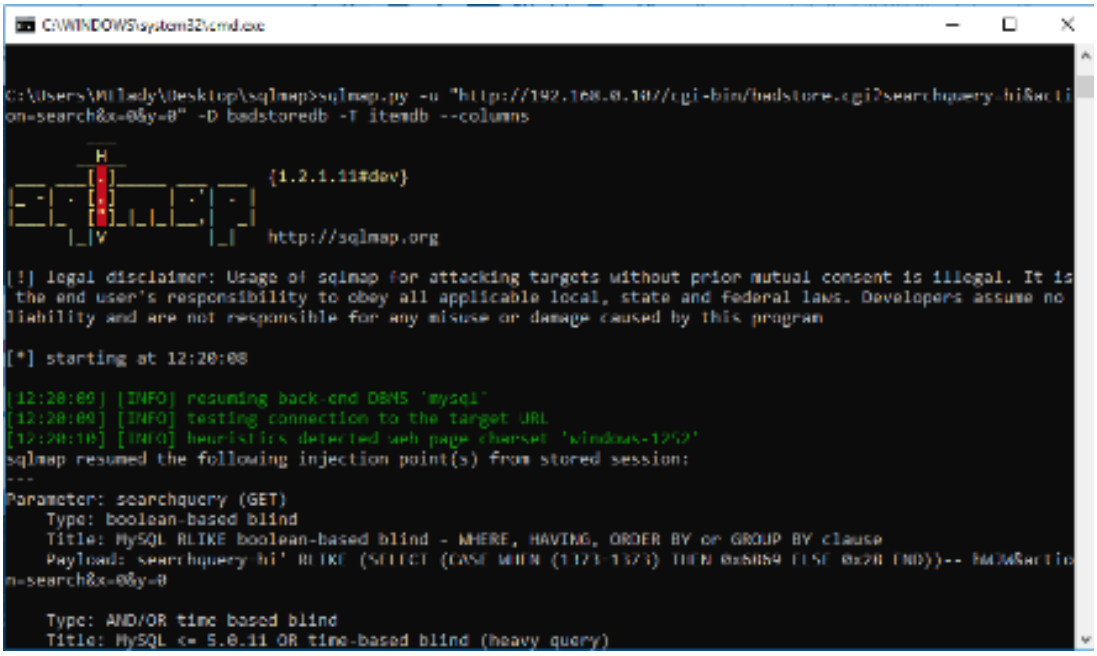
Ilustración 12 Listado de tablas de base de datos servidor web badstore



Fuente: Autor

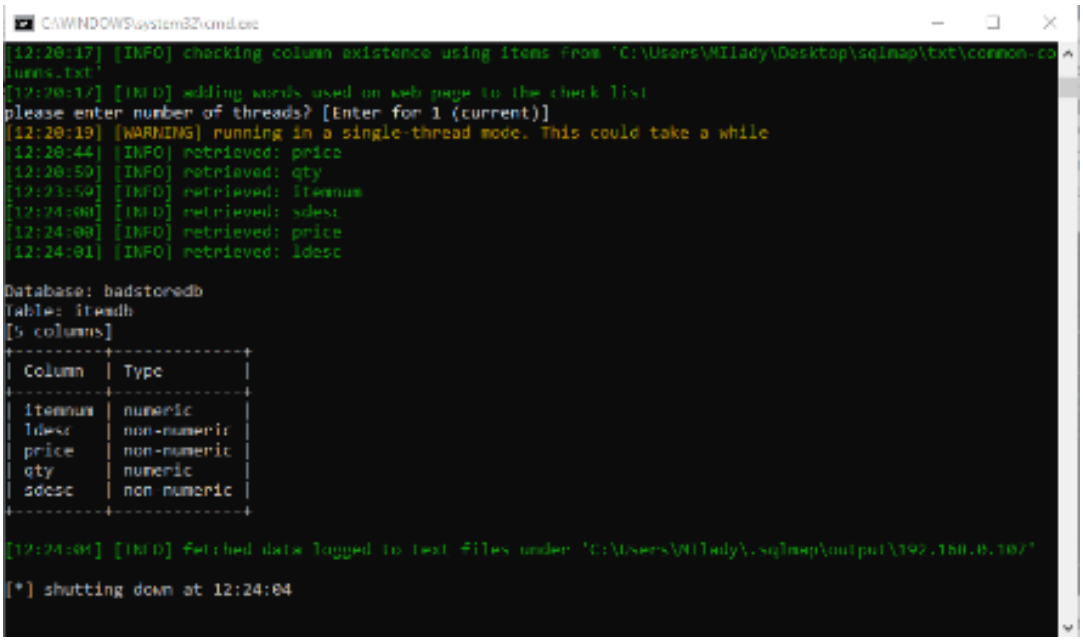
- Se obtiene el listado de columnas con el comando *–D badstoredb –T itemdb –columns, ver resultados en las ilustraciones 13 y 14.*

Ilustración 13 Obtención Listado de columnas base de datos servidor web badstore



Fuente: Autor

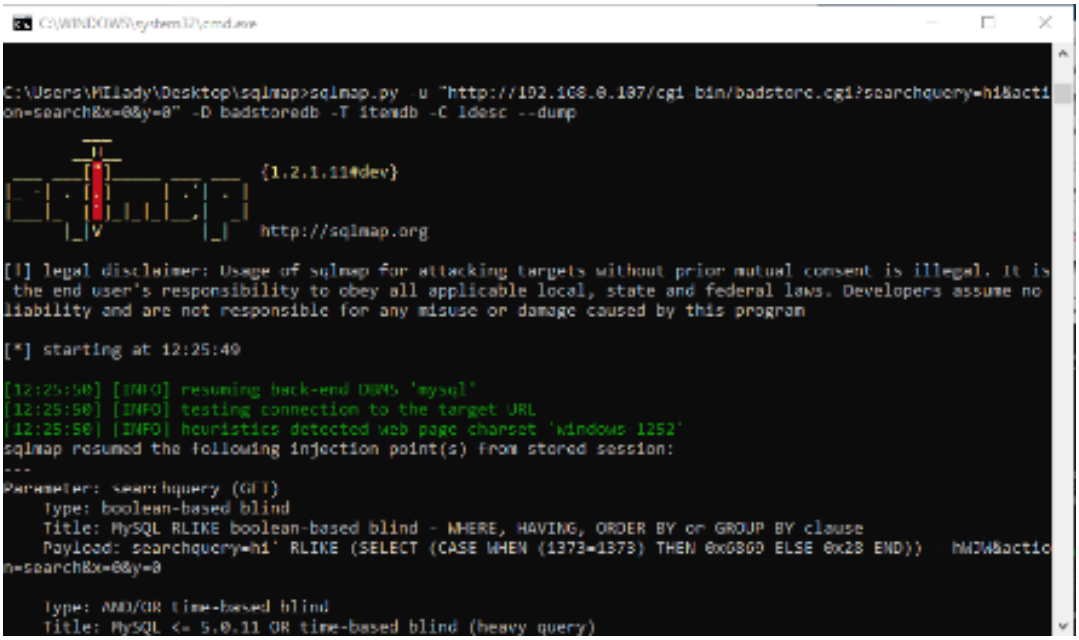
Ilustración 14 Listado de columnas base de datos servidor web badstore



Fuente: Autor

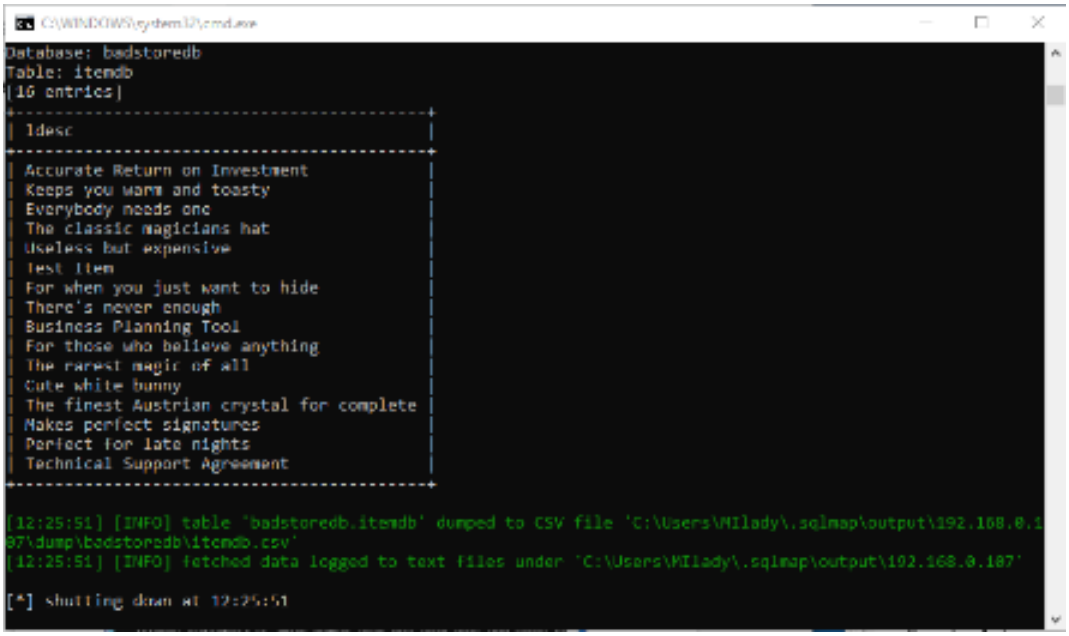
- Finalmente se analiza los datos almacenados en la tabla, ver resultados en las ilustraciones 15 y 16.

Ilustración 15 Obtención Visualización de datos almacenados servidor web badstore



Fuente: Autor

Ilustración 16 Visualización de datos almacenados servidor web badstore

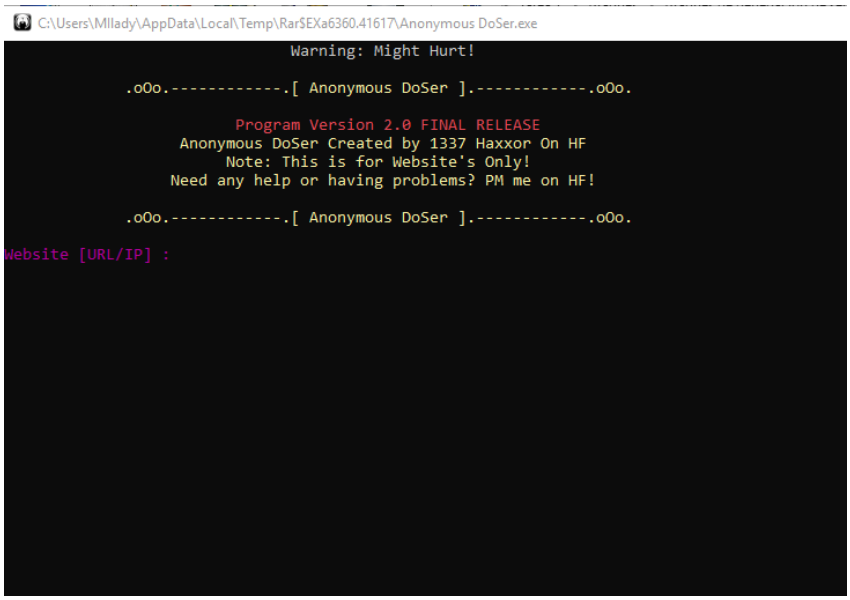


Fuente: Autor

5.1.9.3 DENEGACIÓN DE SERVICIO

- Uso de la herramienta Anonymous Doser, en la ilustración 17 se puede verificar la plataforma de la herramienta.

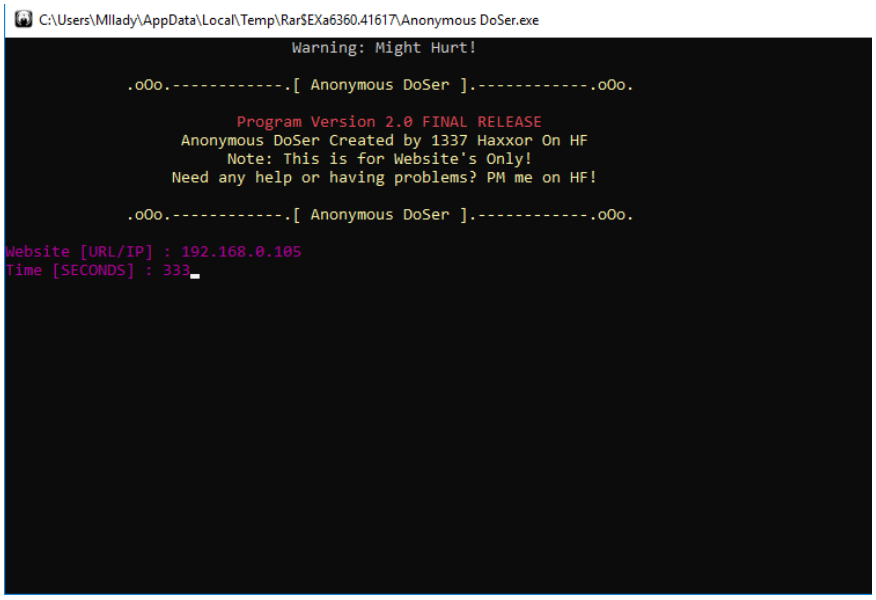
Ilustración 17 Herramienta Anonymous Doser



Fuente: Autor

- Se escribe en la herramienta la IP de página web y los paquetes en este caso son 333 paquetes como se muestra en la ilustración 18.

Ilustración 18 IP de página web



Fuente: Autor

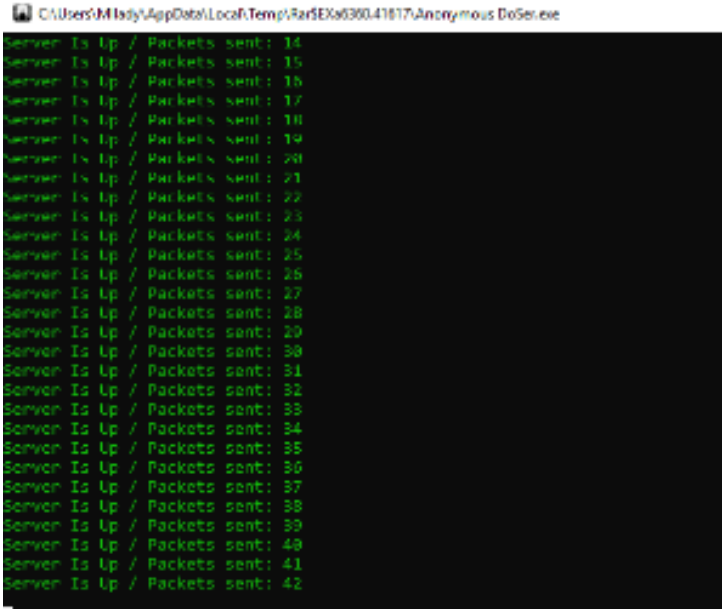
- Verificación del funcionamiento de página web en la figura 19.

Ilustración 19 Funcionamiento de página web

Fuente: Autor

- Funcionamiento de herramienta *Anonimo Doser* enviando múltiples peticiones a la página web en la ilustración 20.

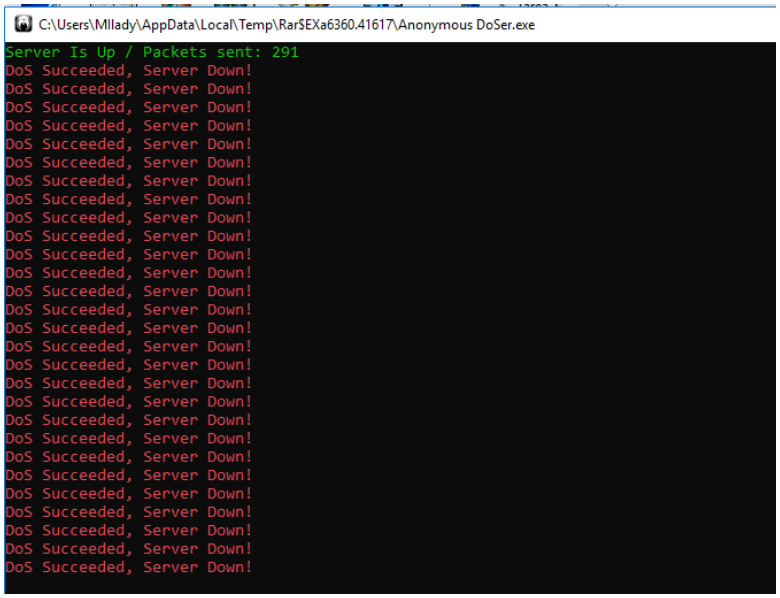
Ilustración 20 Envió de peticiones



Fuente: Autor

- Bloqueo de la página web después de recibir 291 peticiones, en la ilustración 21 se observa el código de error.

Ilustración 21 Error en envió de peticiones



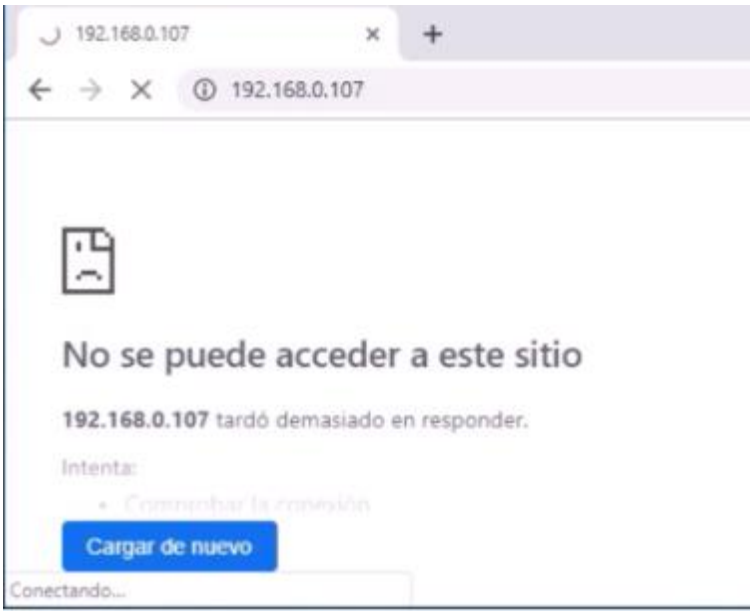
Fuente: Autor

- Verificación del bloqueo de la página web, en las ilustraciones 22 y 23 se observa el resultado del ataque.

Ilustración 22 Verificación de funcionamiento página web

Fuente: Autor

Ilustración 23 Bloqueo de página web



Fuente: Autor

5.1.9.4 Cookie snooping

- Se realiza verificación de conexión de BadStore, ver ilustración 24.

Ilustración 24 Conexión BadStore

Fuente: Autor

- Se realiza registro de Usuario, ver ilustración 25.

Ilustración 25 Registro de Usuario

Fuente: Autor

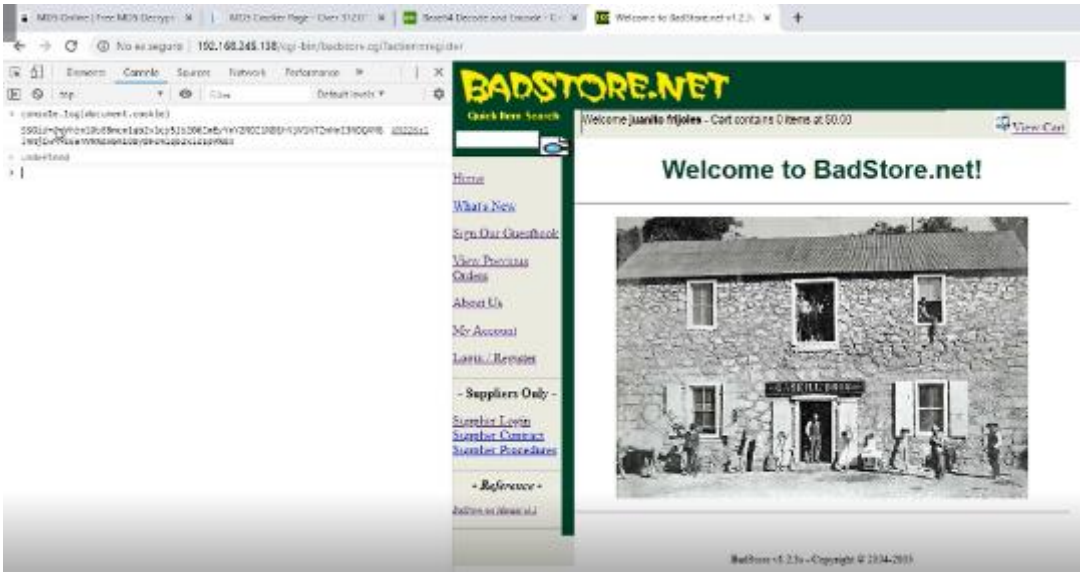
- Se ejecuta la Herramientas de desarrollo, como se observa en la ilustración 26.

Ilustración 26 Herramienta de desarrollo

Fuente: Autor

- Se obtiene las cookies asociados, como se observa en la ilustración 27.

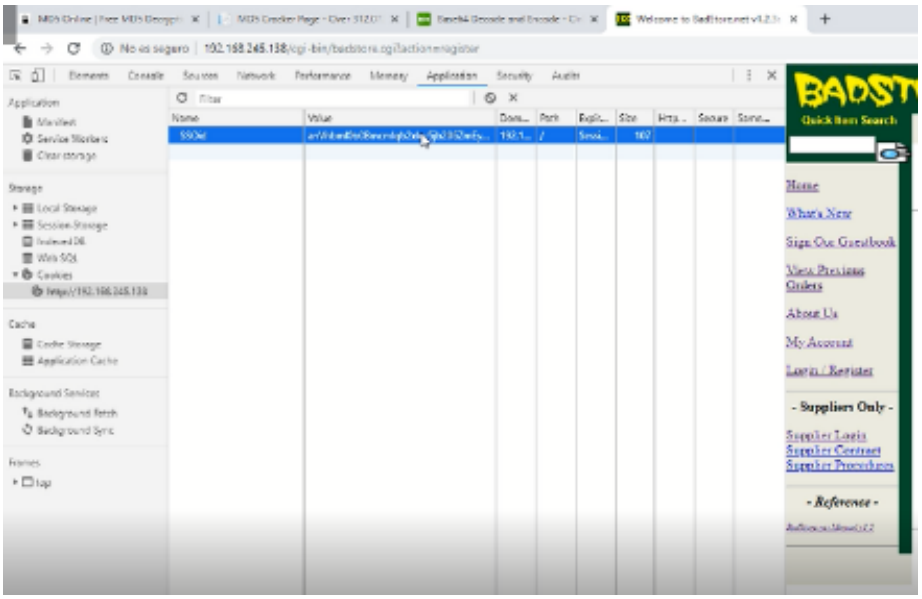
Ilustración 27 Cookies Asociados



Fuente: Autor

- Ver la ilustración 28 como se copia las cookies para su decodificación.

Ilustración 28 Copia de las cookies asociados



Fuente: Autor

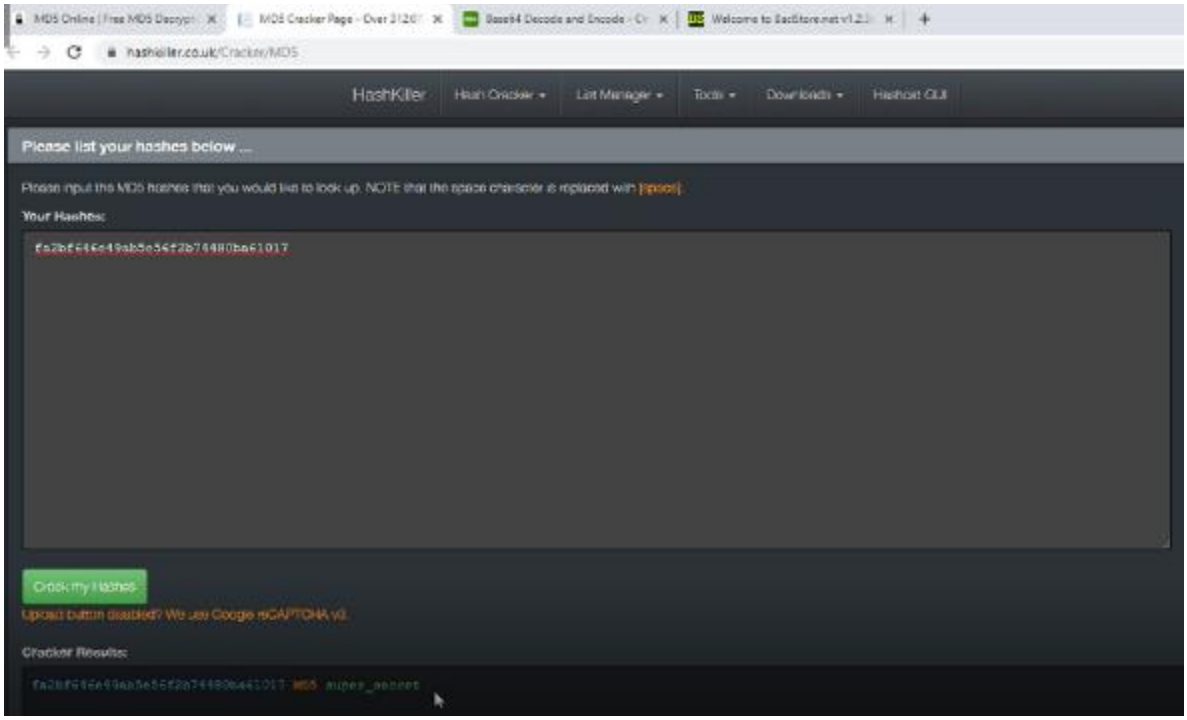
- Se realiza Codificación en base24, como se observa en la ilustración 29.

Ilustración 29 Codificación en base24

Fuente: Autor

- Se realiza codificación en MD5, en la ilustración 30 se verifica la herramienta usada.

Ilustración 30 Codificación en MD5



Fuente: Autor

5.1.9.5 Modificación de cookies

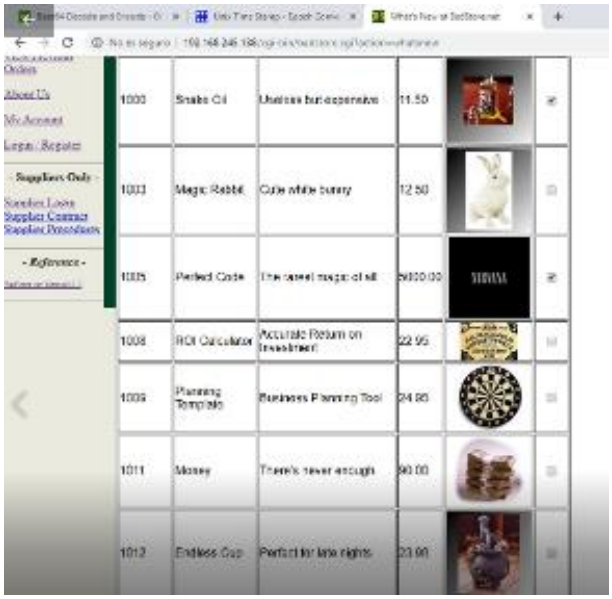
- Se realiza registro en la WEB, ver ilustración 31.

Ilustración 31 Registro de usuario

Fuente: Autor

- Seleccionamos los productos a comprar, ver ilustración 32.

Ilustración 32 Productos seleccionados



Fuente: Autor

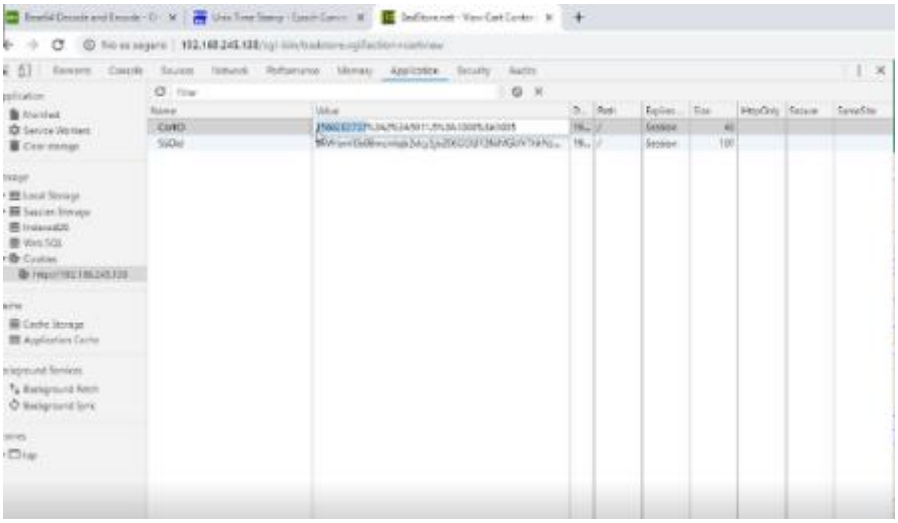
- Verificamos el valor de la compra en este caso es de 5011.50, este valor se puede verificar en la ilustración 33.

Ilustración 33 Valor de compra

Fuente: Autor

- Verificamos el cookie asociado, en la ilustración 34 se verifica el cookie que se va a modificar.

Ilustración 34 Cookies asociado



Fuente: Autor

- En la ilustración 35 se observa el cookie; el primer valor del cookies hace referencia a la fecha, el siguiente a la cantidad de producto seleccionado, el siguiente valor es el precio de la compra, y los últimos valores hace referencia a los productos seleccionados.

Ilustración 35 Descripción de cookie

Fuente: Autor

- Al realizar la modificación de los cookies se realiza modificación de la cantidad y valor de la compra, ver ilustración 36.

Ilustración 36 Resultado de modificación de cookies

Fuente: Autor

5.1.9.6 Tampering de parámetros y formularios

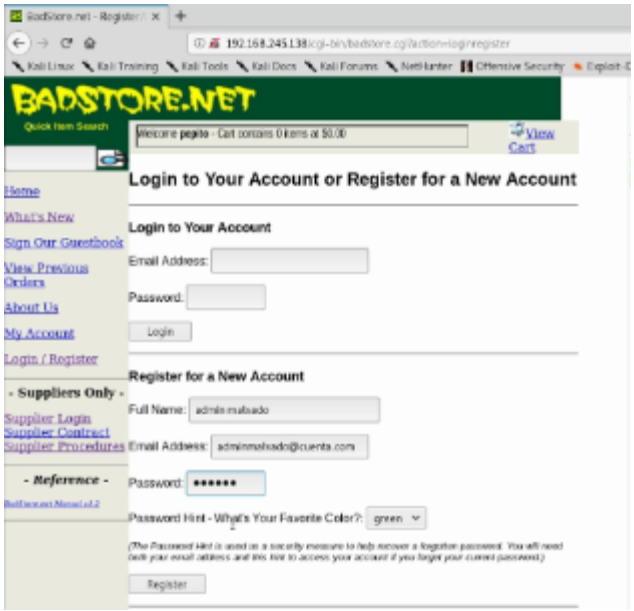
- Luego de instalar BadStore en la máquina virtual VM VirtualBox, se ejecuta el comando *IFCONFIG* para conocer la dirección IP, se verifica la conexión con la página web, ver figura 37.

Ilustración 37 Conexión página web BadStore

Fuente Autor

- Se realiza registro de Usuario, como se observa en la ilustración 38.

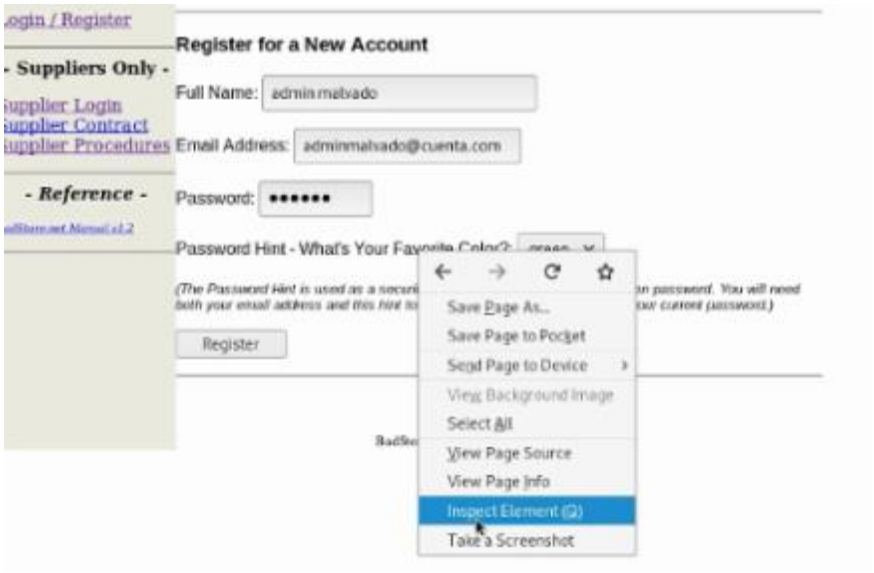
Ilustración 38 Registro de Usuario



Fuente: Autor

- Se ejecuta la herramienta Inspección de elementos, en la ilustración 39 se observa la herramienta a ejecutar.

Ilustración 39 Herramienta Inspección de elementos



Fuente: Autor

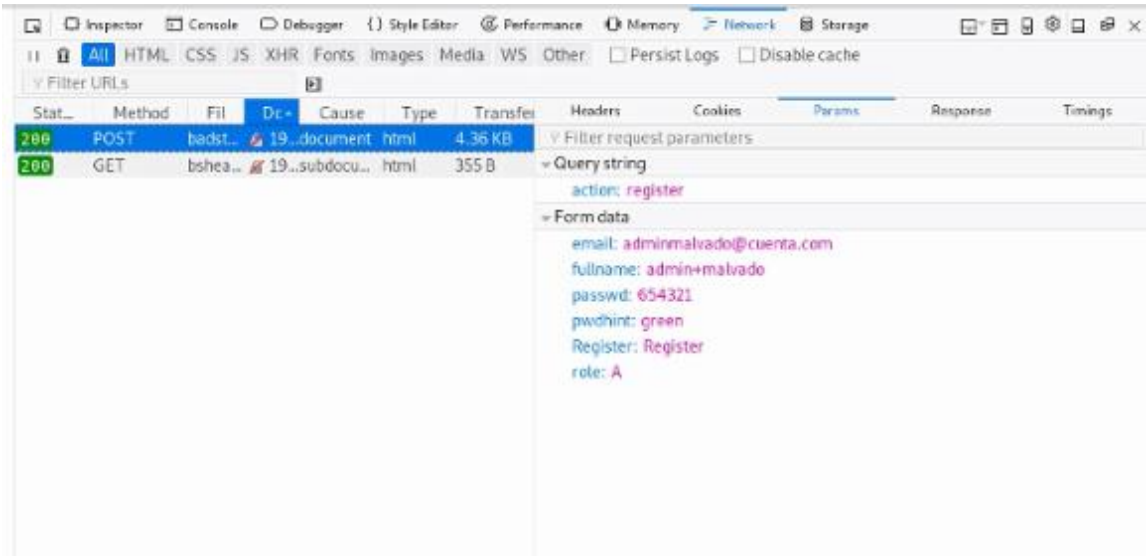
- Se realiza cambio del parámetro Value del name, el cual por defecto está en U por A, que en este caso es un usuario de administrador, ver ilustración 40.

Ilustración 40 Cambio de parámetro Value en Name

Fuente: Autor

- En la ilustración 41 se verifica que el cambio se realice en la herramienta de inspección de elemento Método Post.

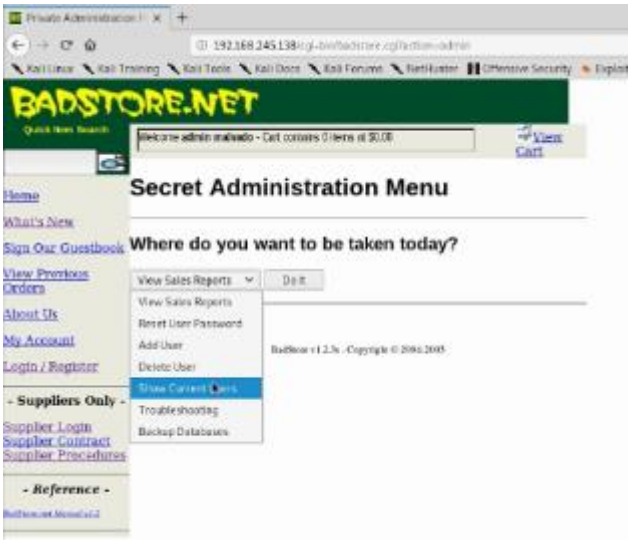
Ilustración 41 Método Post



Fuente: Autor

- Se ingresa al link 192.168.254.138/cgi-bin/badstore.cgi?action=admin, se selecciona la opción Show Current Users, en la ilustración 42 se observa el proceso a realizar.

Ilustración 42 Conexión link 192.168.254.138/cgi-bin/badstore.cgi?action=admin



Fuente: Autor

- Con ello se puede observar los datos personales de los usuarios de la página Web, ver ilustración 43.

Ilustración 43 Datos personales Usuarios

Fuente: Autor

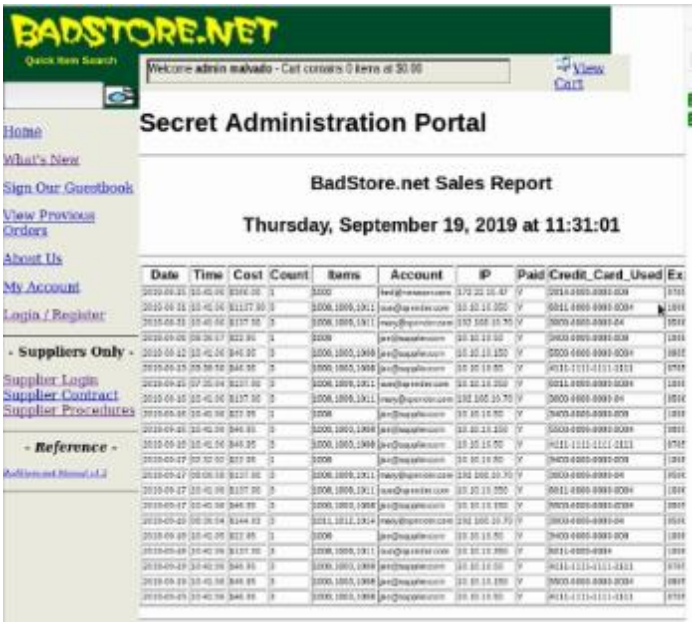
- Si seleccionamos la opción View Sales Reports, como se muestra en la ilustración 44.

Ilustración 44 Opción View Sales Reports

Fuente: Autor

- Se observa los datos de la tarjeta de créditos, se puede ver los resultados en la ilustración 45.

Ilustración 45 Datos de Tarjeta de crédito



Fuente: Autor

5.1.9.7 Directory transversal

- Se verifica la conexión con la página web BadStore, ver ilustración 46.

Ilustración 46 Verificación de conexión de página web

Fuente: Autor

- Se ejecuta el comando "1'='0' UNION SELECT 1,1,1, LOAD FILE('/ETC/PASSWD')#", como se muestra en la ilustración 47.

Ilustración 47 Comando para obtener link

Fuente: Autor

- Se copia el link obtenido, como se muestra en la ilustración 48.

Ilustración 48 Link obtenido de la prueba

Fuente: Autor

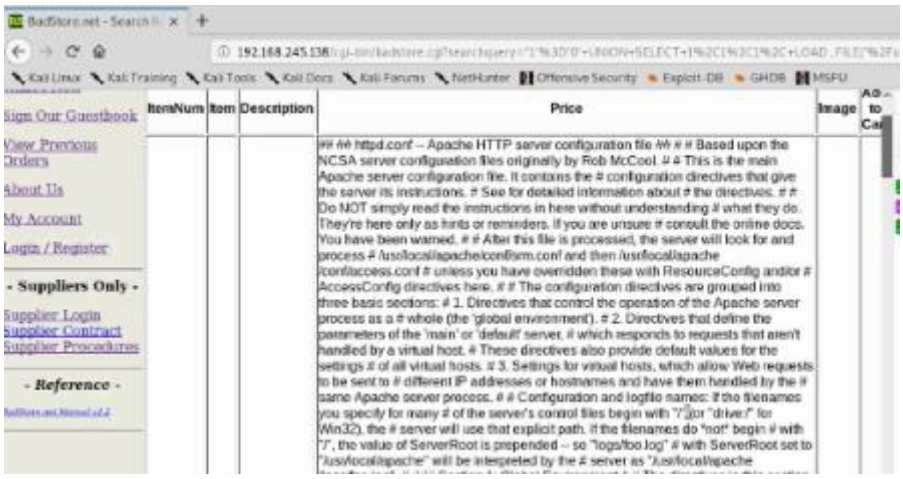
- En la ilustración 49 se observa cómo se realiza el cambio del dato etc/passwd del link obtenido por usr/local/apache/conf/httpd.conf

Ilustración 49 Cambio de valores en el link obtenido

Fuente: Autor

- Se obtiene los resultados, como se observa en la ilustración 50.

Ilustración 50 Resultado de Directory Transversal



Fuente: Autor

5.1.9.8 Navegación forzada

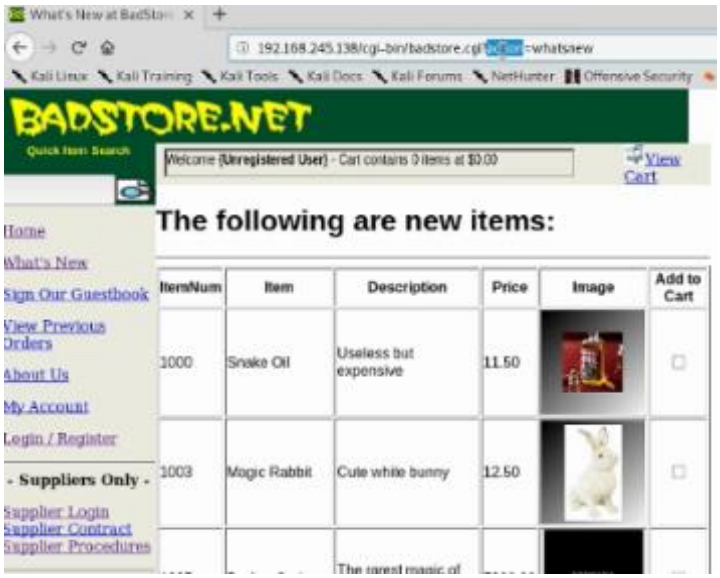
- Se verifica la conexión con la página web BadStore, ver ilustración 51.

Ilustración 51 Verificación de conexión de página web

Fuente: Autor

- Se realiza navegación en el sitio web se encuentra que se repite varias veces la acción “action”, como se observa en la ilustración 52.

Ilustración 52 Verificación de acción "Action"



Fuente: Autor

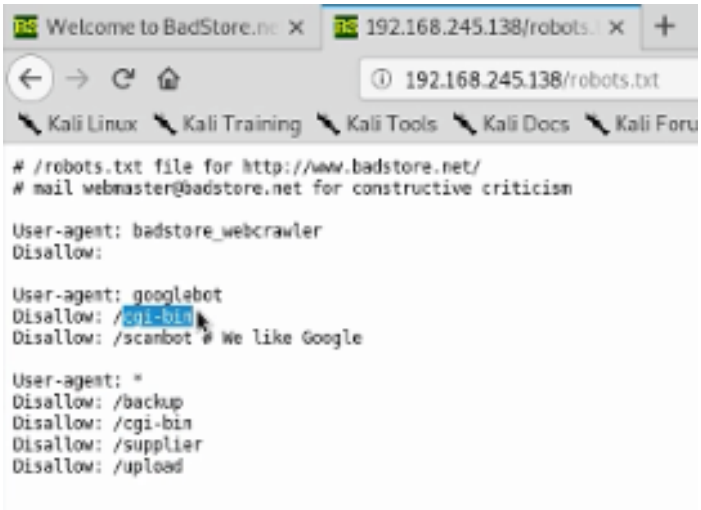
- En la ilustración 53 se observa cómo se realiza cambio en la URL agregando la palabra “admin”, como resultado nos abre una página de administrador.

Ilustración 53 Verificación de modificación de URL

Fuente: Autor

- Se digita el comando robots para verificar los archivos, ver ilustración 54.

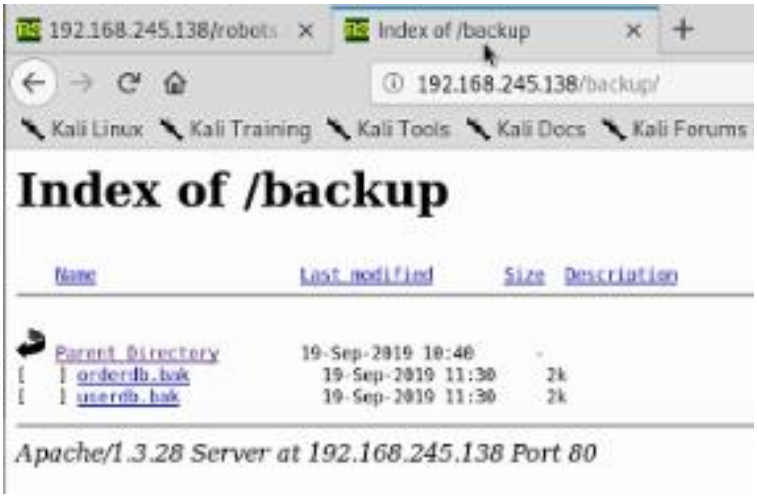
Ilustración 54 Comando Robots



Fuente: Autor

- Se realiza verificación de ingreso con el archivo “backup”, donde se verifica que allí están almacenado las copias de seguridad de la página web, ver resultados en la ilustración 55.

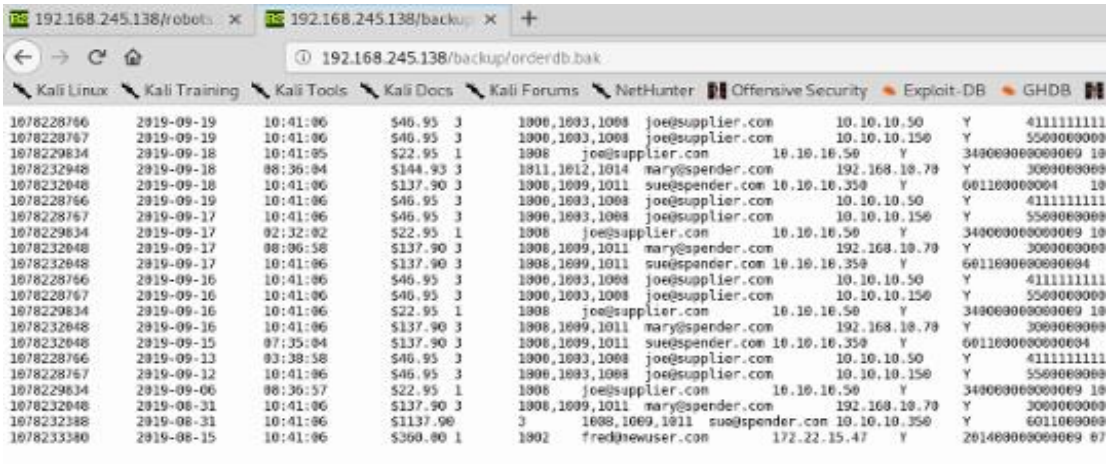
Ilustración 55 Copias de seguridad página web



Fuente: Autor

- Se verifica el primer link obtenidos en las copias de seguridad donde se verifica números de orden de pedido, precio, ip del cliente, etc, ver ilustración 56.

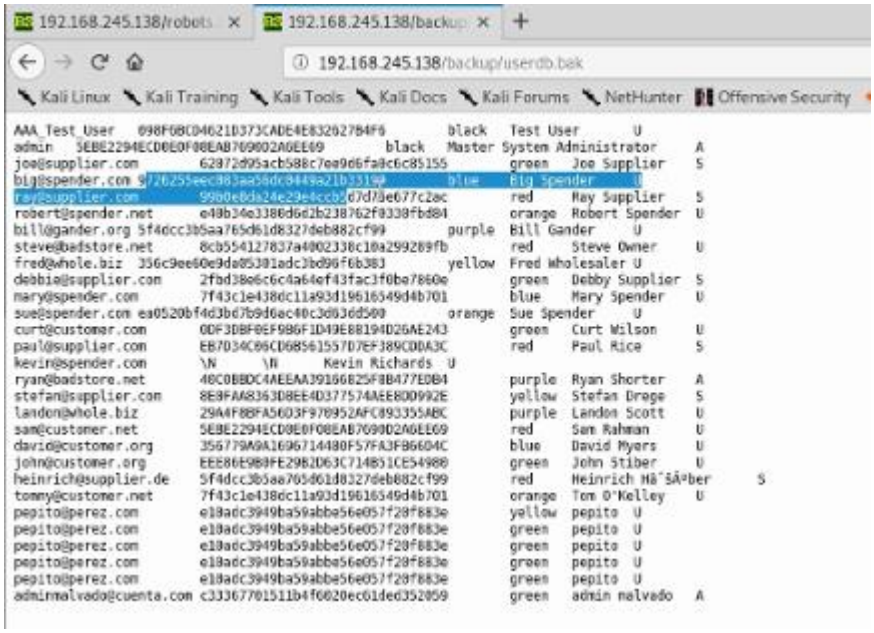
Ilustración 56 Datos obtenidos en las copias de seguridad.



Fuente: Autor

- Se verifica el segundo link obtenidos en las copias de seguridad donde se verifica los datos personales de los clientes, ver resultados en la ilustración 57.

Ilustración 57 Datos obtenidos en las copias de seguridad.



Fuente: Autor

5.2 PROPUESTA DE ASEGURAMIENTO

Es de vital importancia conocer las vulnerabilidades y riesgos con que cuenta la plataforma de servicio web, es por ellos que se plantea el uso de metodologías de aseguramiento donde se encuentre almacenada los procedimientos e instrucciones a llevar a cabo para garantizar la seguridad del servidor web.

En el área de sistemas en la seguridad deben garantizarse aspectos como: Control de acceso, autenticación, seguridad en el uso de la información.

5.2.1 Políticas de seguridad

5.2.1.1 Organización

La empresa de cobranzas “XYZ” es una organización encargados de realizar las llamadas a los clientes que han sido reportados por los bancos, con el fin de realizar la respectiva recuperación de cartera.

5.2.1.2 Políticas de seguridad informática en red privada virtual de la empresa de cobranza xyz

Los resultados obtenidos en el análisis de la seguridad de la implementación de la VPN en la empresa de cobranzas “XYZ”, dan como recomendación el uso de prácticas para la mitigación de vulnerabilidades y amenazas.

5.2.1.3 Análisis de riesgos

La metodología usada es MAGERIT, en la ilustración 58 se muestra los activos y valoración cualitativa. En la ilustración 59 se muestra la valoración cuantitativa y en la ilustración 60 se muestra las amanezcas y el plan de tratamiento.

MATRIZ DE INVENTARIO; PROBABILIDAD, IMPACTO Y VALORACIÓN DEL RIESGO DE ACTIVOS DE INFORMACIÓN

METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN MAGERIT

PROBABILIDAD DEL RIESGO

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

VALORACIÓN DEL RIESGO

IMPACTO						
	MA					
	A					
	M					
	B					
	MB					
RIESGO		MB	B	M	A	MA
		PROBABILIDAD				

VALORACIÓN DEL RIESGO

	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Ilustración 58 Activos y Valoración Cualitativa

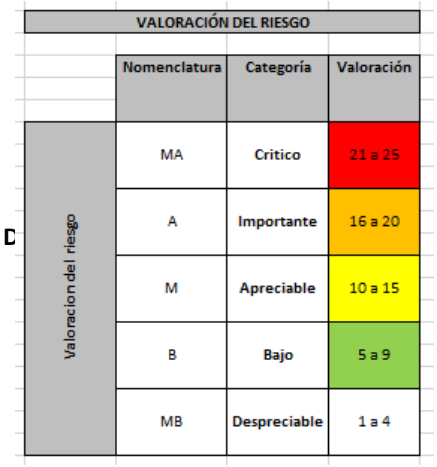
INFORMACIÓN DE LOS ACTIVOS																														
	DATOS DEL ACTIVO DE INFORMACION			TIPO										DIMENSION					ATRIBUTOS										UBICACIÓN	
No.	Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DATOS	[K] CLAVES CRIPTOGRAFICAS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMIENTO INFORMATICO	[COM] REDES DE COMUNICACIONES	[Media] SOPORTE DE INFORMACION	[AUX] EQUIPAMIENTO AUXILIAR	[L] INSTALACIONES	[P] PERSONAL	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencilidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser estringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativame			Físico	Electrónico
																										Leve	Importa	Grave		
1	Servidor de Base de Datos	Departamento de	Área de Desarroll			x								MA	M	MA	A	MA	SI	SI	SI	SI	SI	SI			X		X
2	Switch Firewall, VLAN	Departamento de	Área de Desarroll					x						B	B	B	MA	MA	SI	SI	SI	SI	SI	SI			X		X
3	Servidor Monitoreo de Equipos	Departamento de Sistemas	Área de Desarrollo					x						B	B	B	A	A	SI	NO	NO	SI	NO	NO		X		X	
4	FTP, VPN, Terminal	Departamento de	Área de Desarroll						x					A	MA	A	MA	MA	SI	SI	SI	SI	SI	SI		X			X

Fuente: Autor

Ilustración 59 Valoración Cuantitativa

Resumen de Valoración de Riesgos de los Activos

METODOLOGIA DE MAGERIT: VALORACION DEL RIESGO - APROBADA POR EL D



VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
Servidor de Base de Datos	CRITICO	25	15	25	20	25	22
Switch Firewall, VLAN	APRECIABLE	9	9	9	25	25	15
Servidor Monitoreo de Equipos	APRECIABLE	9	9	9	20	20	13
FTP, VPN, Terminal Server	CRITICO	20	25	20	25	25	23

Fuente: Autor

Ilustración 60 Amenazas - Plan de tratamiento

MATRIZ DE ANALISIS Y TRATAMIENTO DE RIESGOS														
IDENTIFICACIÓN DE AMENAZAS, VULNERABILIDADES, ANALISIS DE RIESGOS, ESTRATEGIA DE CONTROLES Y PLAN DE TRATAMIENTO A APLICAR														
INFORMACIÓN DE LOS ACTIVOS DE INFORMACION														
GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS														
Activos de Informacion	**No. De Amenazas y Vulnerabilidades**	**Nombre del activo de información**	**VALORACIÓN DEL RIESGO DE LOS ACTIVOS**	**Amenazas Metodologia Magerit**	**Vulnerabilidades**	**Probabilidad de vulneraáón** (1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 practicamente seguro)	**Calculo del riesgo neto** (Valoracion del riesgo * probabilidad de vulneración)	**Criticidad neta** (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))	**Calificación de Gestión** (1 control no existe, 2 existe pero no efectivo, 3 efectivo pero no documentado, 4 efectivo y documentado)	**Si la opción es 2 - 3 o 4 Indique el Control aplicado actual**	**Riesgo residual** (riesgo neto dividido entre la calificación de gestión)	**Criticidad residual** (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))	**Niveles de aceptación del riesgo** (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I))
[S] SERVICIOS	1	Servidor de Base de	22	[I6] Corte del suministro eléctrico		5	110	C	1		110	C	I
[HW] EQUIPAMENTO INFORMÁTICO	2	Switch Firewall, VLAN	15	[I6] Corte del suministro eléctrico		27	405	C	23		18	I	I
[HW] EQUIPAMENTO INFORMÁTICO	3	Servidor Monitoreo de Equipos	13	[I6] Corte del suministro eléctrico		28	364	C	24		15	A	I
[HW] EQUIPAMENTO INFORMÁTICO	4	FTP, VPN, Terminal Server	23	[I6] Corte del suministro eléctrico		29	667	C	25		27	C	I

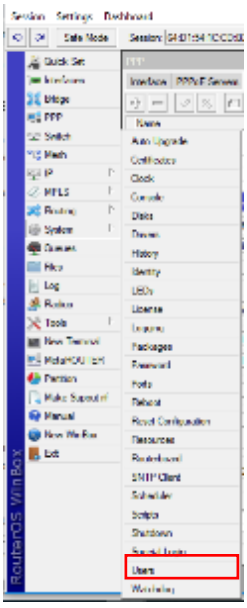
Fuente: Autor

5.2.2 Implementación de soluciones de seguridad

5.2.2.1 Cambios de usuarios y contraseña a equipos de la red

1. En la figura 44 se puede observar cómo se realiza el cambio de Usuario para el ingreso de las RouterBoards, para ello se ingresa a las herramientas System->Users, evitar usar nombre de usuarios como admin, root, administrator.

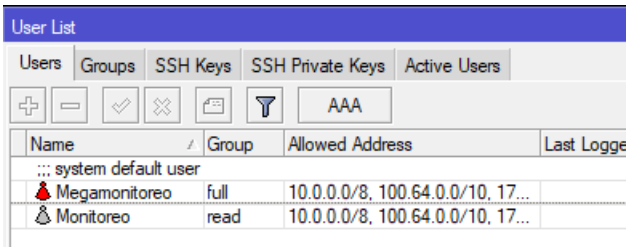
Figura 44 Herramienta Users



Fuente: Autor

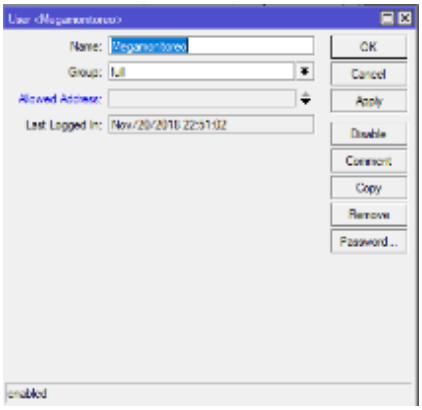
Damos doble clic sobre el usuario que deseamos cambiar el nombre, ver figura 46 y 47.

Figura 45 Usuarios existentes en la RouterBoard



Fuente: Autor

Figura 46 Herramienta cambio de Nombre de Usuario

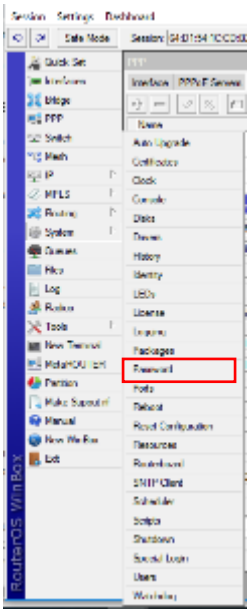


Fuente: Autor

Se recomienda tener dos usuarios uno que contenga todos los privilegios quien será usado por el administrador de la red, y otro usuario de lectura para realizar el monitoreo de la Red

2. En la figura 48 se observa la herramienta de cambio de contraseña.

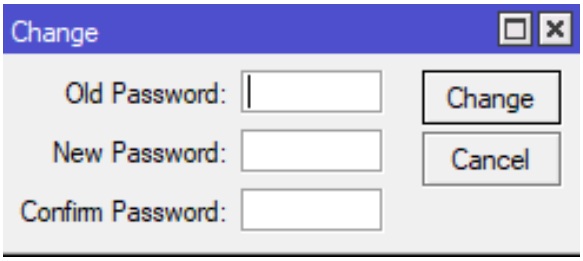
Figura 47 Herramienta Password



Fuente: Autor

Se debe asignar una contraseña ya que por defecto viene en blanco, ver figura 49.

Figura 48 Ventana Change



Fuente: Autor

5.2.2.2 Deshabilitación de protocolo y cambios de puerto de conexión a los equipos.

1. Deshabilitar protocolo y cambiar puertos

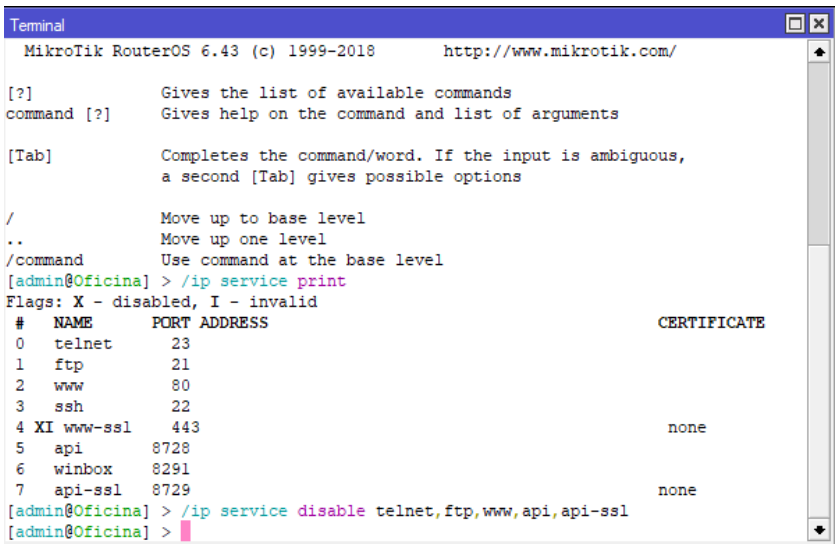
En la figura 50 se muestra el comando /ip service print, el cual permite encontrar todos los protocolos activados

Figura 49 Protocolos activados

Fuente: Autor

Con el comando /ip service disable telnet, ftp, www, api, api-ssl, desactivamos los protocolos que no se usaran y son menos seguros, ver figura 51.

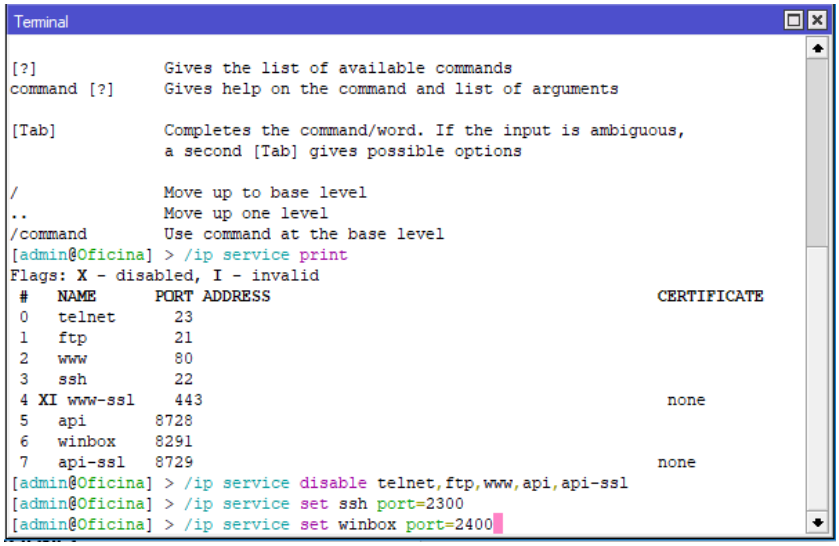
Figura 50 Desactivación de protocolos



Fuente: Autor

Se cambia los puertos de conexión de SSH y de Winbox para evitar los ataques de fuerza bruta, como se muestra en la figura 52.

Figura 51 Cambio de Puertos

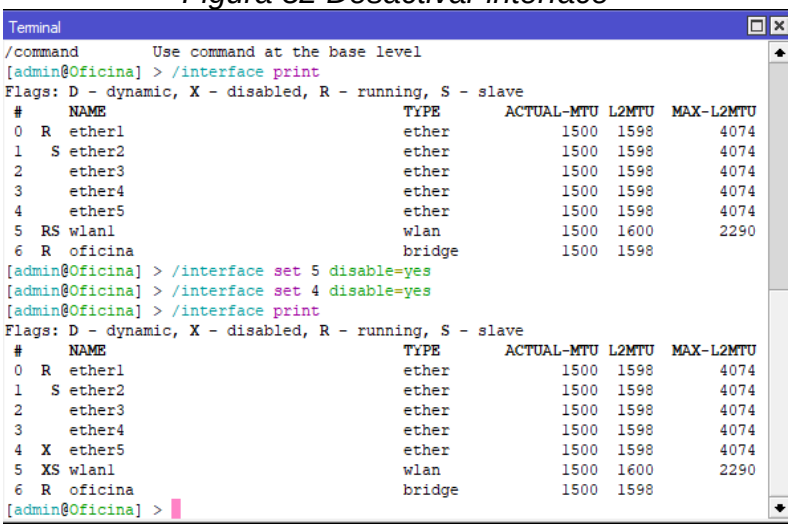


Fuente: Autor

5.2.2.3 Limitación de conexión por Ethernet

1. Deshabilitar interfaces no usados, esto evita que terceros se conecte a nuestros equipos, como se muestra en la figura 53.

Figura 52 Desactivar interface



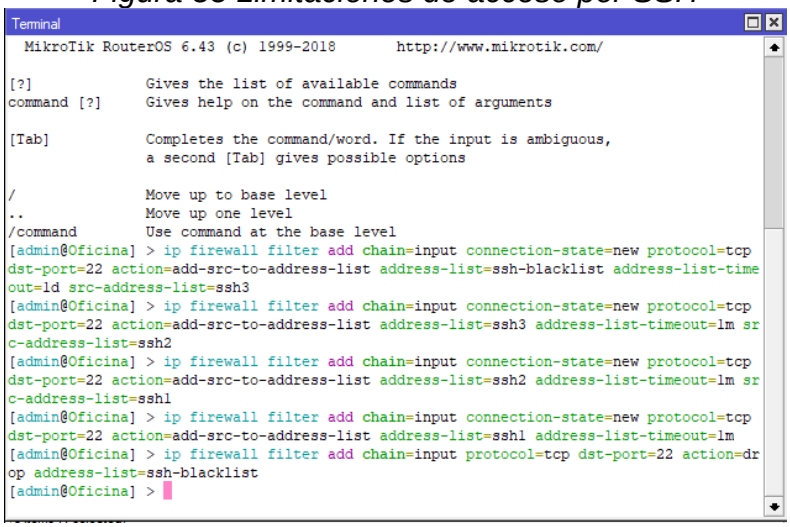
Fuente: Autor

5.2.2.4 Controles de acceso

1. Limitación de acceso por SSH

Las limitaciones de acceso por SSH impiden ataques de fuerza bruta, se permitirán solo tres intentos de acceso posteriormente se bloqueará la RouterBoard por 1 Día, en la figura 54 se observa los comandos a hacer usados.

Figura 53 Limitaciones de acceso por SSH

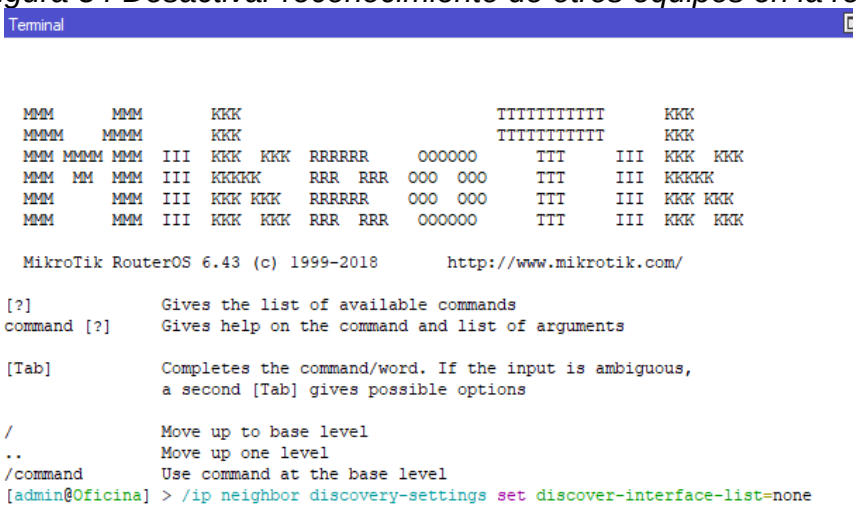


Fuente: Autor

5.2.2.5 Limitación de visualización de equipos en la red

1. Desactivar protocolo de reconocimientos de equipos en la red, ver figura 55.

Figura 54 Desactivar reconocimiento de otros equipos en la red



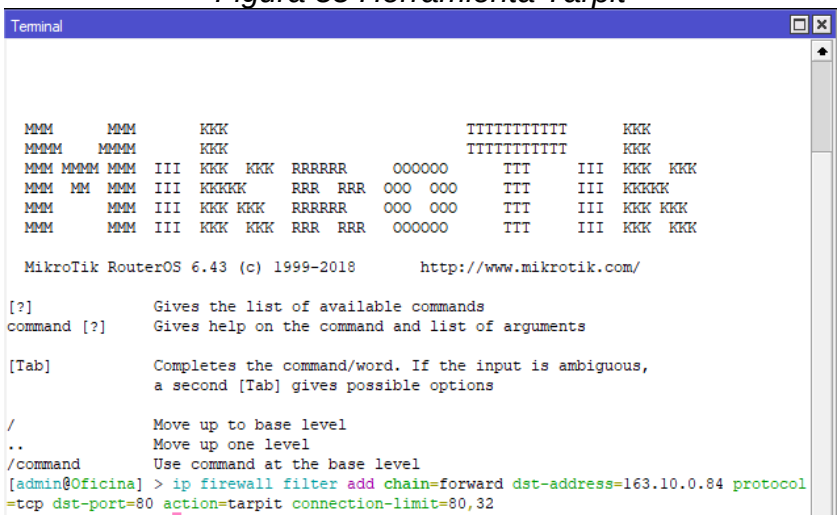
Fuente: Autor

5.2.2.6 Evitar ataques de DoS

1. Uso de estrategia tarpit

La herramienta tarpit impide los ataques de DoS, permite que haya transferencia de datos pero deja que se generen las conexiones. Permitir 79 conexiones simultáneas por IP con destino al servidor web y aplicar tarpit a partir de la conexión 80, en la figura 56 se observa el comando.

Figura 55 Herramienta Tarpit



Fuente: Autor

5.2.3 Auditoria de seguridad

- Validación de acceso: Los componentes de las aplicaciones web tienen una ubicación la cual se identifica con la URL, es por ello que es de vital importancia validar el usuario que ingresa a cada módulo, con ello se especifica las restricciones que contiene cada usuario.
- Encriptación de contraseña: el uso de encriptación de contraseña permite que este no sea de fácil acceso a usuarios no privilegiados.
- Bloqueo de puertos: Es necesario el bloqueo de puertos como son las más comunes 80, 3306 y 21.

5.2.4 Análisis de vulnerabilidades

- Cross Site Scripting (XSS): Para evitar ataques de XSS de debe realizar filtrado de caracteres específicos en los campos abiertos como lo son: #, [,], {, }, ~, Limitación de caracteres de entrada.
- Ataque por inyección de código SQL: En este tipo de ataque se debe bloquear el uso de caracteres como comillas dobles, las comillas simples, también se puede realizar delimitación de los valores de la consulta.
- Denegación de Servicio: Para evitar este tipo de ataque se recomienda control de la tasa de tráfico de los hosts.
- Cookie snooping: Cambiar el sistema de encriptado por uno más nuevo y eficiente.
- Modificación de cookies: en el proceso de solicitud de pedido se debe contrastar la información con la base de datos no determinar el precio por la información en la cookie.
- Tampering de parámetros y formularios: Se debe eliminar la opción de crear usuarios admins de esa manera, los usuarios admin solo deben crearse por usuarios admin.
- Directory transversal: Filtrado de caracteres específicos en el URL, con ello se evita el acceso a directorios privados.
- Navegación forzada: bloquear el acceso a documentos delicados.

5.3 WEB APPLICATION FIREWALL

*ModSecuritye*s un firewall de aplicaciones Web bajo la licencia de GNU, ofrece en su catálogo protección contra diversos ataques, como XSS, SQL Injection, robots, troyanos, etc., entre su portafolio ofrece una consola de administración que permite el registro de monitorización y alertas.

Fue lanzada en noviembre del 2002, en el 2006 se lanzó la versión 2 *ModSecurity* 2.0, siendo la última versión *ModSecurity* 3.0[57].

5.3.1 Funcionalidades

ModSecurity es una herramienta que tiene el objetico de detección y prevención de ataques de aplicaciones WEB[58].

Funcionalidades de los módulos:

5.3.1.1 Filtrado de Peticiones

Las peticiones entrantes son analizadas por el módulo *mod_security* antes de pasarlas al servidor web, y a su vez son comparadas con unas reglas.

5.3.1.2 Técnicas Anti-evasión

En este módulo las rutas y los parámetros son normalizados antes del análisis para evitar técnicas de evasión; en este módulo se eliminan barras, decodificación de URL.

5.3.1.3 Comprensión del protocolo HTTP

Filtrados específicos y granulares.

5.3.1.4 Post Payload análisis

Intercepta y analiza el contenido transmitido a través del método POST.

---

[57] ModSecurity. [En línea] 2004-2019. http://www.modsecurity.org/. 112 p.

[58] Ristiæ, Iván. MODSECURITY HANDBOOK The Complete Guide to the Popular Open Source Web Application Firewall. s.l.: Feisty Duck Londo, 03 de junio de 2013. 112 p.

5.3.1.5 Audit Logging

Es posible loguear para un posterior análisis.

5.3.1.6 HTTPS Filtering

Al estar embebido como módulo tiene acceso a los datos después de que estos hayan sido desencriptados.

5.3.1.7 Compressed content Filtering

Tiene acceso a los datos después de la descompresión.

5.3.1.8 Byte range verification

Sirve para detectar y bloquear *shellcodes*.

5.3.2 Características

Permite la protección contra varios ataques de aplicaciones web, realiza monitoreo de tráfico HTTP, su funcionalidad es similar a un sistema de detección de intrusos (IDS), pero en este caso trabaja en el nivel de HTTP, entre sus técnicas encontramos[59]:

- Modelo de seguridad negativo.
- Modelo de seguridad positivo.
- Vulnerabilidades y debilidades conocidas.

5.3.3 Ventajas

- Es gratuito.
- Fácil de configuración.
- Creación de reglas específicas, para el rendimiento del programa.
- Compatible con casi todos los sistemas operativos.
- Detecta y bloquea ataques antes de la interacción con la aplicación web.
- Realiza monitoreo de tráfico HTTP.

[59]Mischel, Magnus. ModSecurity 2.5 Securing your Apache installation and web applications Prevent web application hacking with this easy-to-use guide. s.l.: Packt Publishing BIRMINGHAM - MUMBAI, 2009. 114 p.

5.3.4 Desventajas

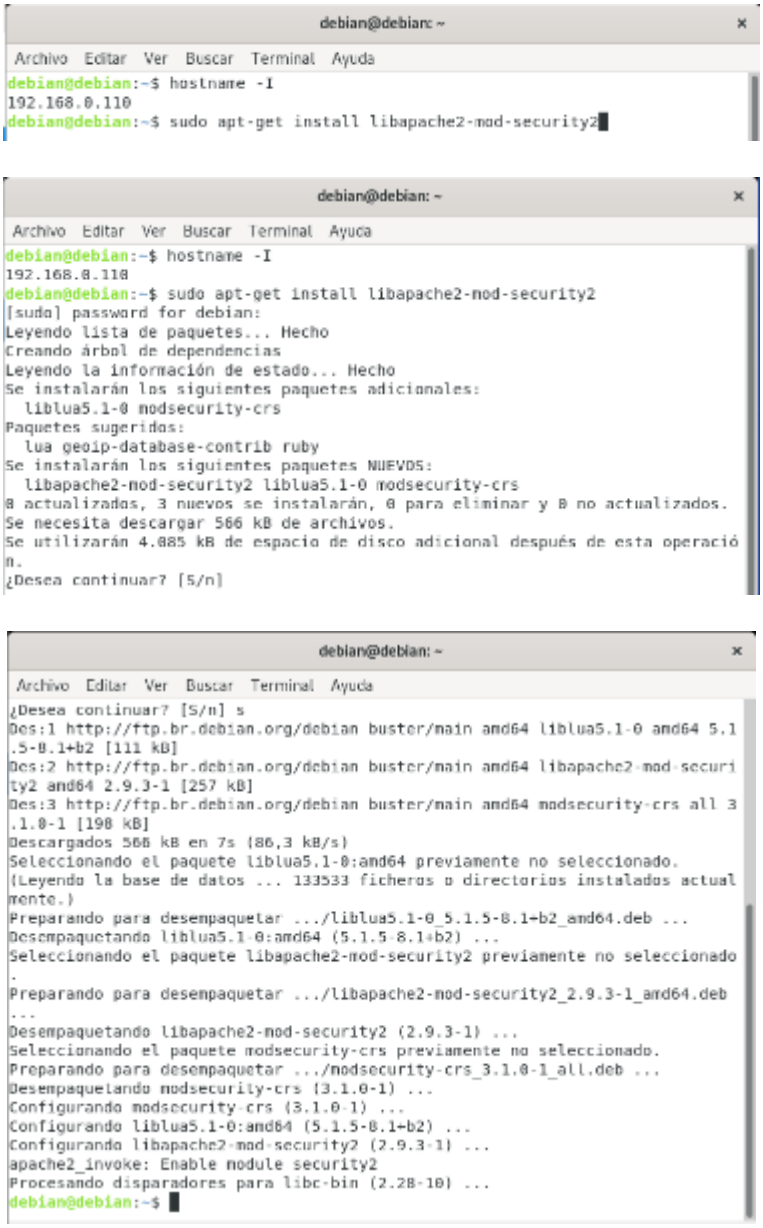
- Si se cae el proxy perdemos el servidor.
- Después de su implementación puede que algunas funciones del servidor WEB deje de funcionar, esto se le llama falso positivos y falsos negativos.
- Contante actualización del proxy.
- Consumo elevado de recursos, Procesador, RAM.

5.3.5 Instalación

Instalación de ModSecurity en debian.

- Para la instalación del módulo ModSecutiy se debe instalar apache.
  En la herramienta terminal como se muestra en la ilustración 61, se ejecuta el siguiente comando sudo apt-get install libapache2-mod-security2, antes de ejecutar el comando se debe realiza las actualizaciones.

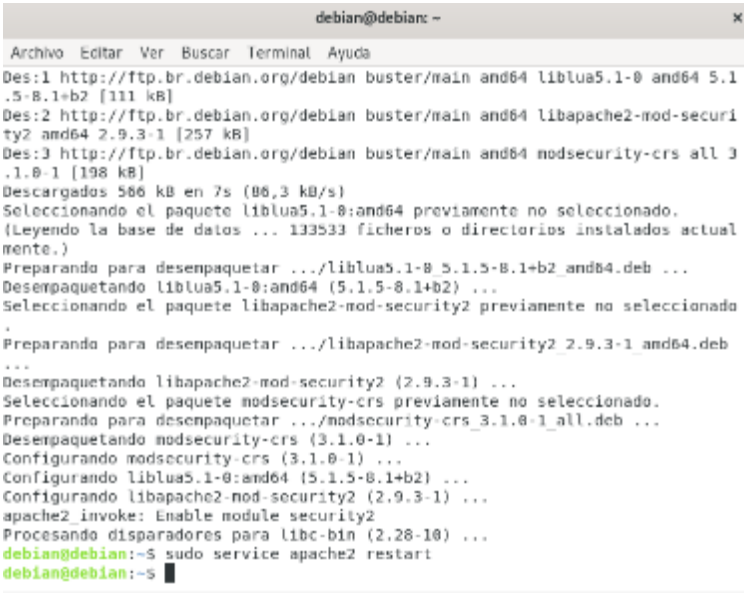
Ilustración 61 Instalación de Modsecurity



Fuente: Autor

- Se realiza reinicio de apache, ver ilustración 62.

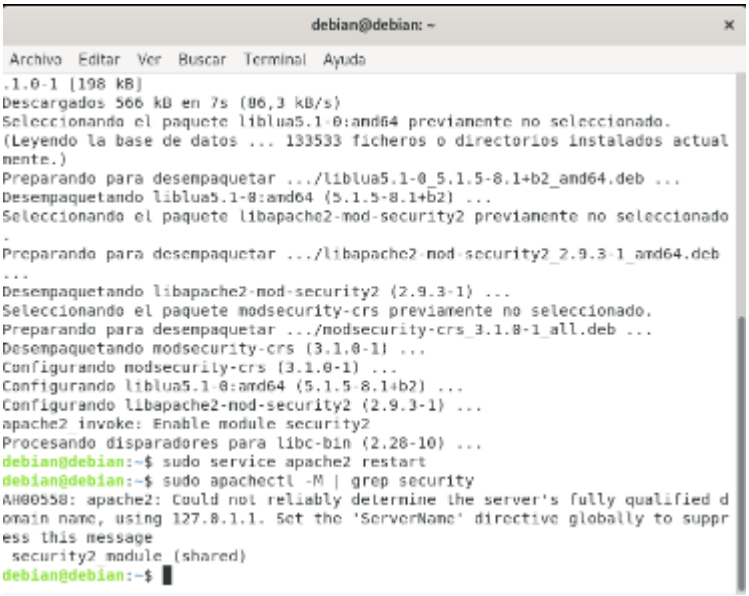
Ilustración 62 Reinicio del servidor Apache



Fuente: Autor

- Se verifica el estado del módulo, ver ilustración 63.

Ilustración 63 Verificación del estado del Módulo Modsecurity

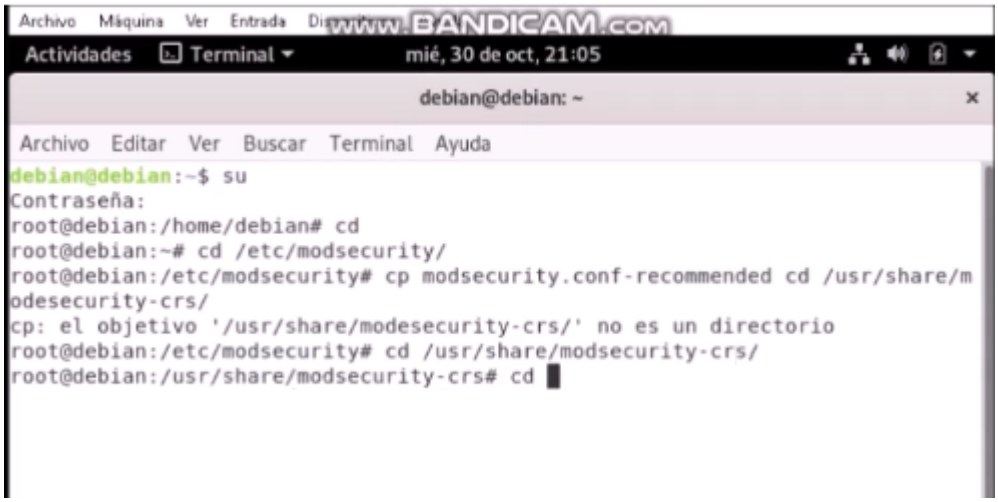


Fuente: Autor

Configuración del módulo ModSecurity

- Primero se debe ingresar a la carpeta crs, como se observa en la ilustración 64, para ellos se ejecuta los siguientes comandos, se ingresa como usuario administrador, cd /etc/modsecurity/, luego se ejecuta el comando cd /usr/ share/modsecurity-crs/.

Ilustración 64 Ingreso a la carpeta crs del módulo Modsecurity



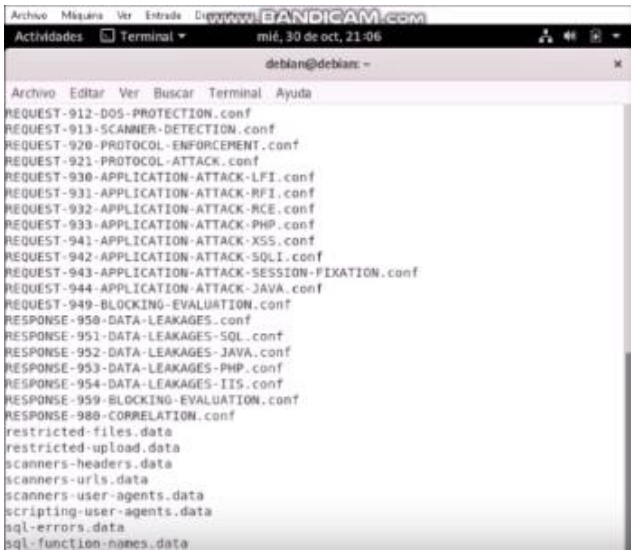
Fuente: Autor

- Se ingresa a rules y se ejecuta el comando ls el cual muestra un listado con los archivos y directorios, como se muestra en las ilustraciones 65 y 66.

Ilustración 65 Rules ModSecurity

Fuente: Autor

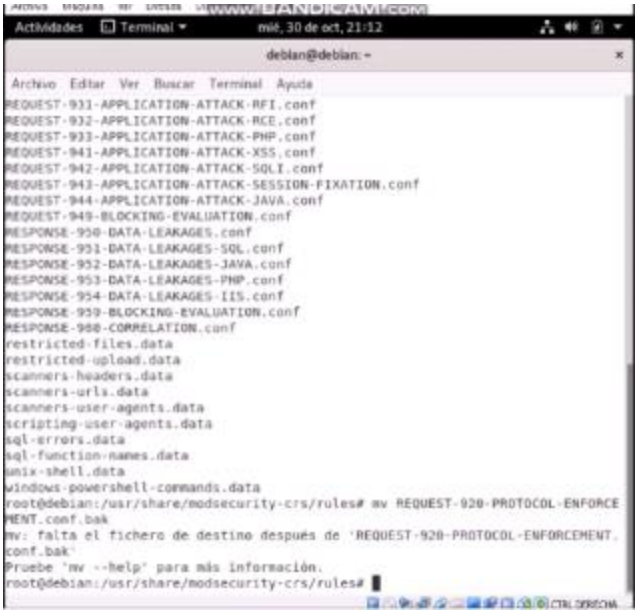
Ilustración 66 Archivos y directorios



Fuente: Autor

- Se realiza modificación de la regla REQUEST-920PROTOCOL-ENFORCEMENT.conf por REQUEST-920PROTOCOL-ENFORCEMENT.conf.bak, en la ilustración 67 se observa la ejecución de la regla.

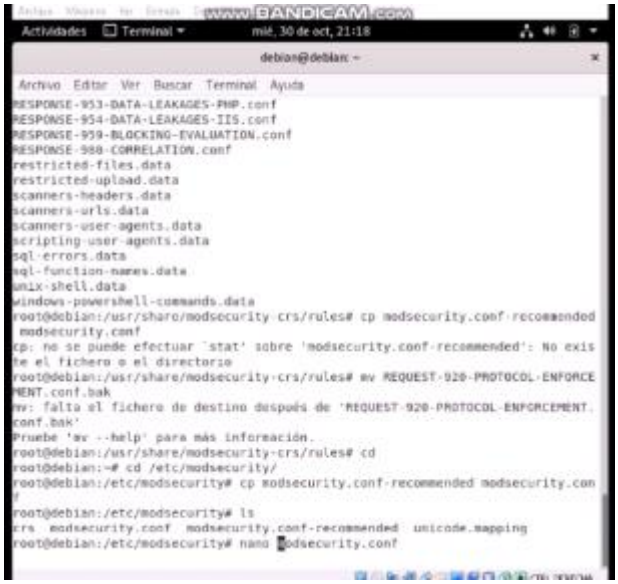
Ilustración 67 Modificación de la regla REQUEST-920PROTOCOL-ENFORCEMENT.conf



Fuente: Autor

- Ahora se ingresará un SecRuleEngine para ello se ejecuta el comando cp modsecurity.conf-recommended modsecurity.conf, revisamos los archivos que contiene y se modifica el archivo modsecurity.conf, como se muestra en la ilustración 68.

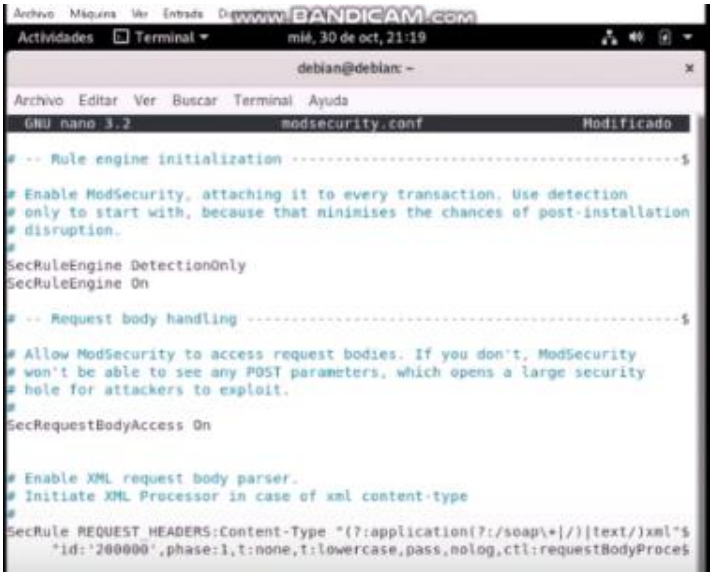
Ilustración 68 Ingreso archivo modsecurity.conf.



Fuente: Autor

- Se agrega la línea SecRuleEngine On, ver ilustración 69.

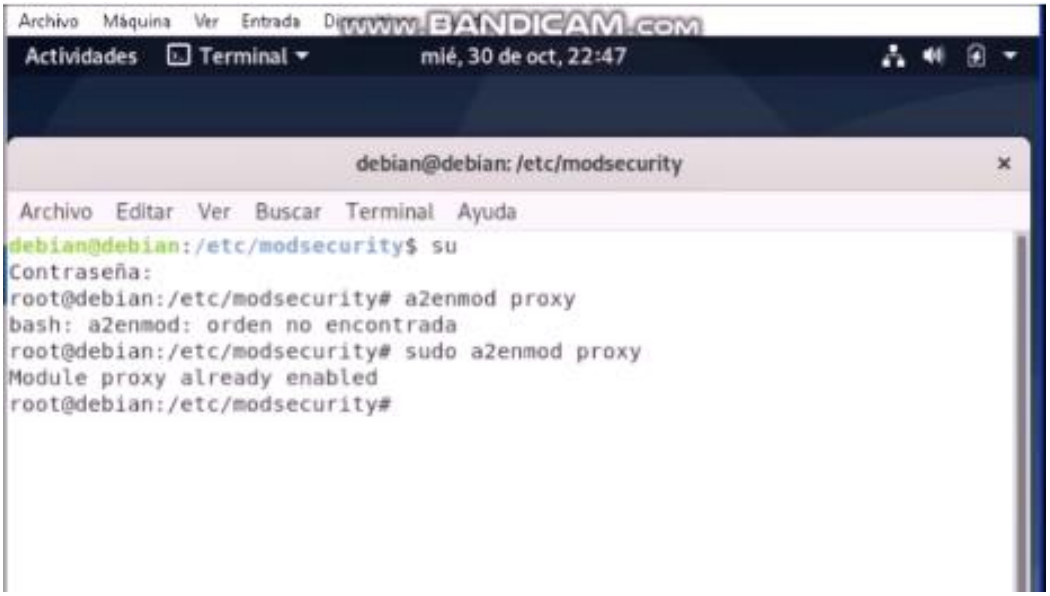
Ilustración 69 Modificación archivo modsecurity.conf.



Fuente: Autor

- Como se muestra en la ilustración 70 se verifica el estado del Módulo.

Ilustración 70 Verificación de estado del modulo



Fuente: Autor

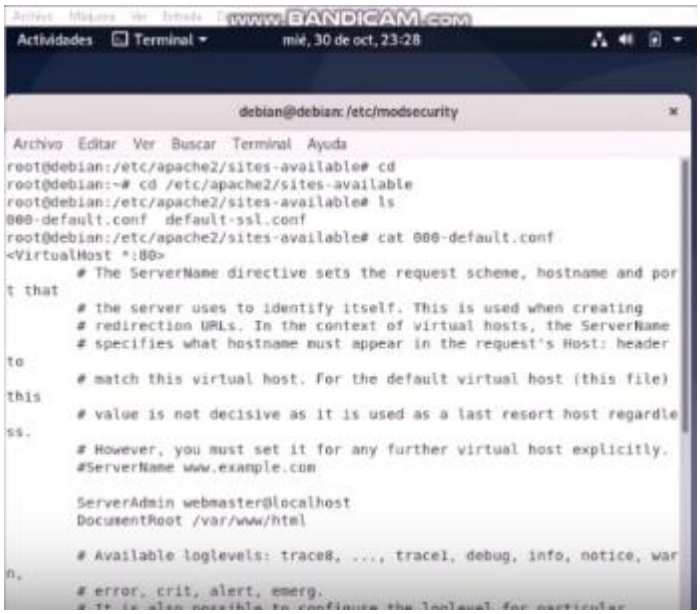
- Se procede a modificar el siguiente fichero /etc/apache2/site-available – 000-default.conf, ver ilustración 71.

Ilustración 71 fichero /etc/apache2/site-available – 000-default.conf.

Fuente: Autor

- Como es la primera vez que se instala Modsecurity este archivo estará vaciado se procede a cambiarlo, como se observa en la ilustración 72.

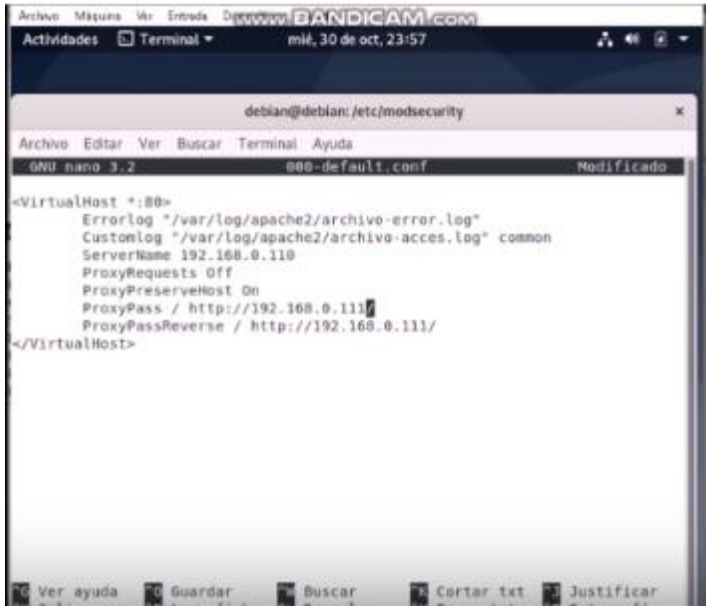
Ilustración 72 Contenido 000-default.conf.



Fuente: Autor

- Se escribirá la IP del servidor apache y el servidor Badstore, ver ilustración 73

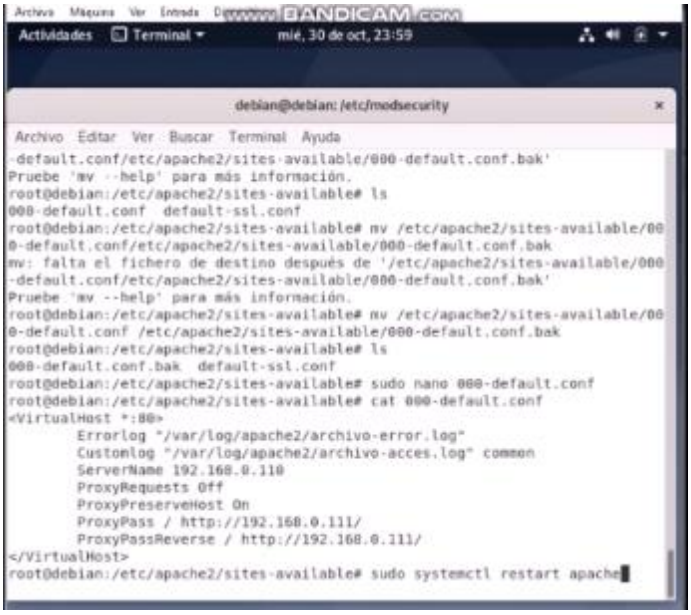
Ilustración 73 VirtualHost



Fuente: Autor

- Cuando se realiza la modificación se procede a verificar que los cambios se guardaron y se reinicia el servidor apache, el resultado debe ser como se muestra en la ilustración 74.

Ilustración 74 Verificación de modificaciones



Fuente: Autor

5.3.6 Prueba de penetración CON WAF.

5.3.6.1 Cross Site Scripting (XSS)

- Ingresamos al servidor BadStore con la IP configurada, ver ilustración 75.

Ilustración 75 Servidor BadStore

Fuente: Autor

- En la ilustración 76 se muestra el ingreso en los campos de búsqueda la petición “<script>alert("Vulnerabilidad ataques XSS")</script>

Ilustración 76 Uso de la petición <script>alert ("Vulnerabilidad ataques XSS") </script>”

Fuente: Autor

- Se evidencia el resultado de la vulnerabilidad, los resultados se muestran en la ilustración 77.

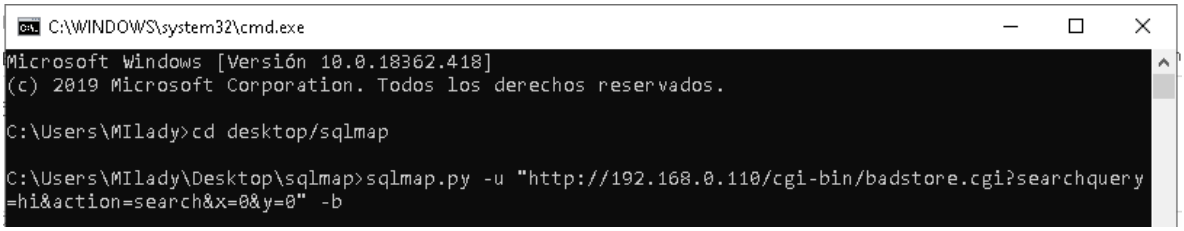
Ilustración 77 Resultados ataque XSS

Fuente: Autor

5.3.6.2 Ataque por inyección de código SQL

- Se abre la consola de comando de Windows como se observa en la ilustración 78, luego se ingresa a la carpeta sqlmap, y se el comando sqlmap.py -u "http://192.168.0.110/cgi-bin/badstore.cgi?searchquery=hi&action=search&x=0&y=0" –b, en él nos mostrara si el servidor web puede ser atacado por inyección de código SQL.

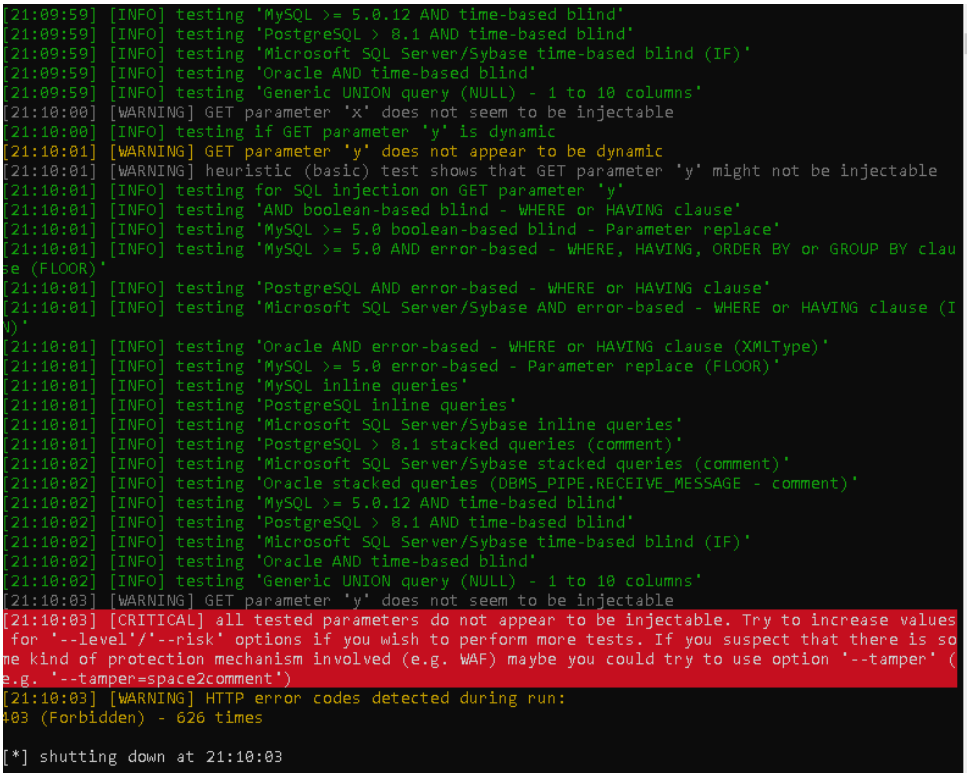
Ilustración 78 Comando de consola Windows



Fuente: Autor

- Como resultado nos indica que el servidor tiene protección, ver ilustración 79.

Ilustración 79 Resultado Ataque de inyección SQL

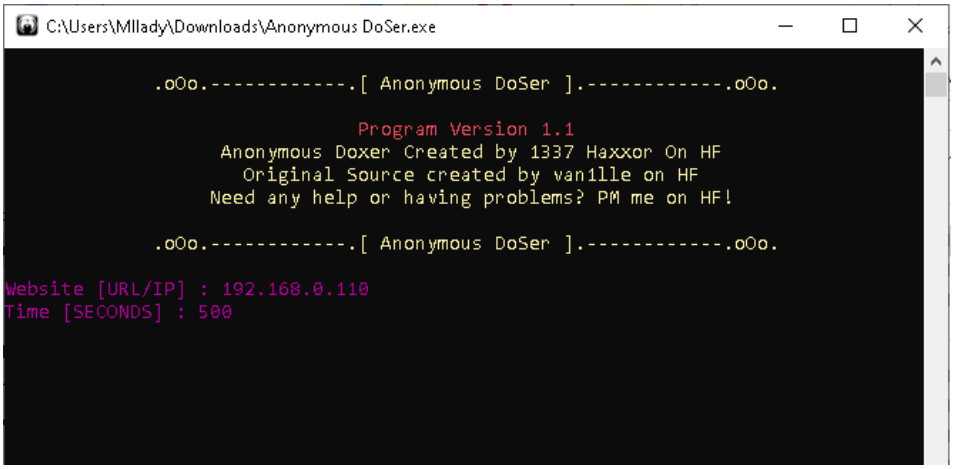


Fuente: Autor

5.3.6.3 DENEGACIÓN DE SERVICIO

- Se escribe en la herramienta la IP de página web, en este caso se usa la herramienta de la ilustración 80 *anónimo Doser*.

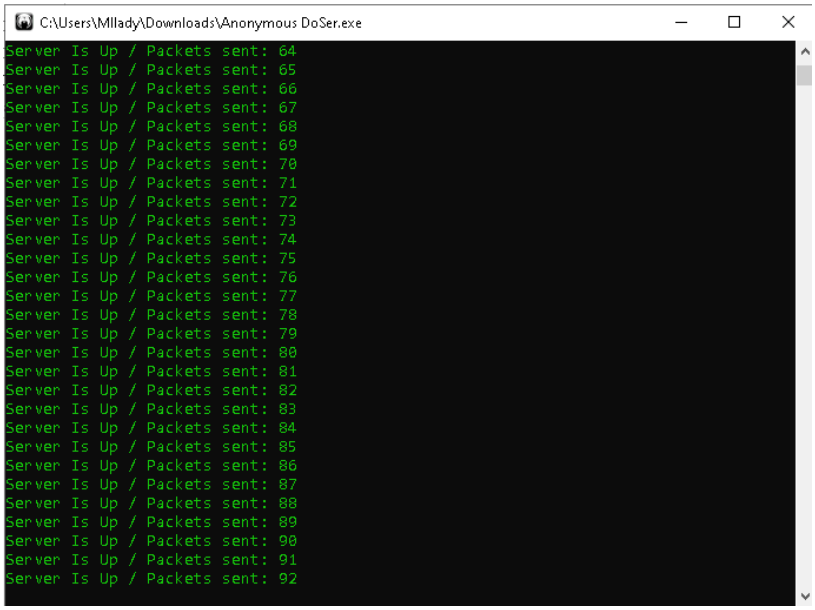
Ilustración 80 IP de página web



Fuente: Autor

- Funcionamiento de herramienta *Anonimo Doser* enviando múltiples peticiones a la página web, como se observa en la ilustración 81.

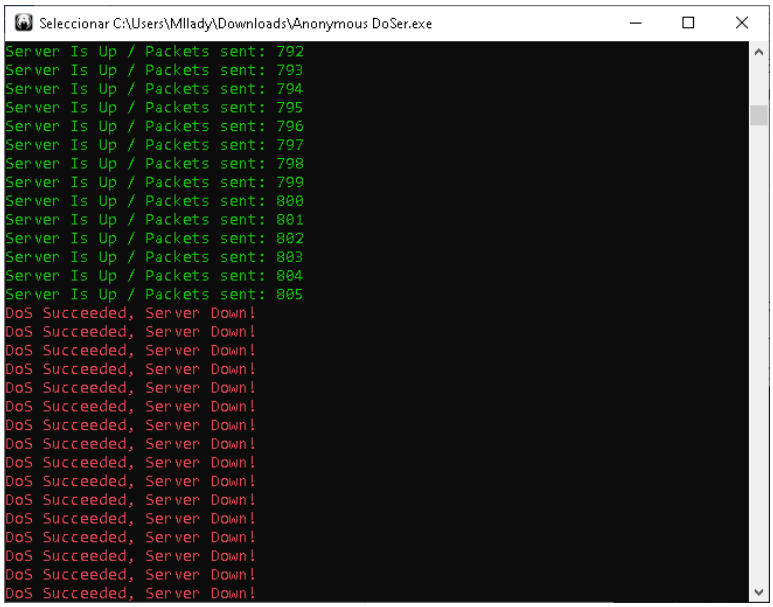
Ilustración 81 Envió de peticiones



Fuente: Autor

- Bloqueo de la página web después de recibir 805 peticiones sin el WAF el bloqueo sucedía a las 291 peticiones, ver resultado en la ilustración 82.

Ilustración 82 Error en envió de peticiones

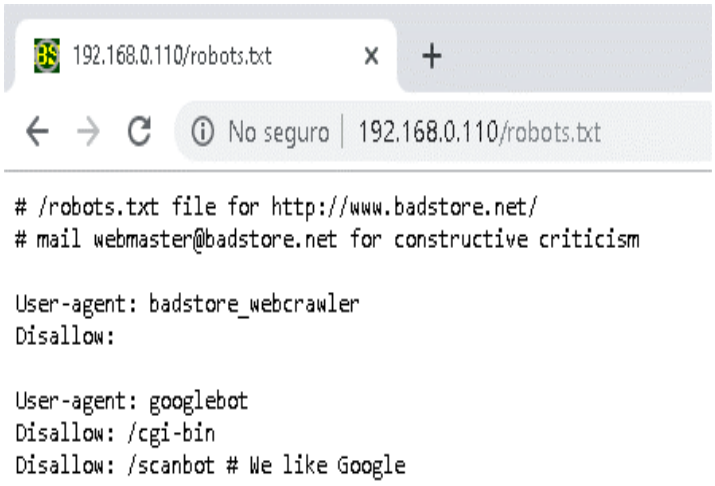


Fuente: Autor

5.3.6.4 Navegación forzada

- Se digita el comando robots para verificar los archivos, ver ilustración 83.

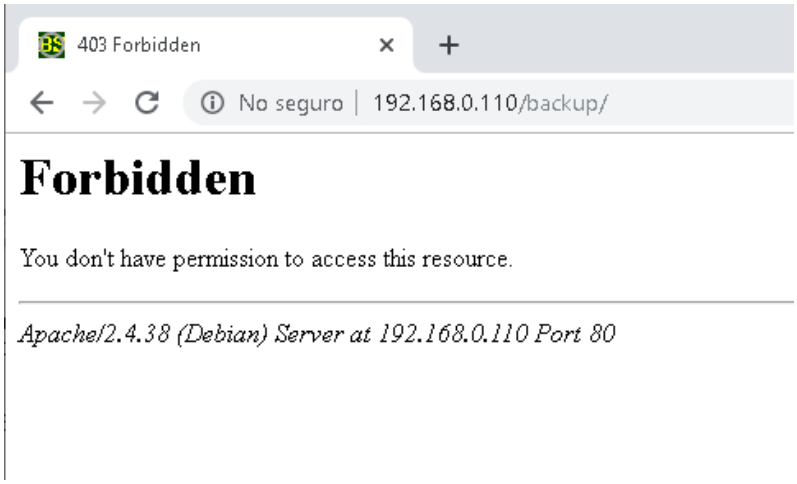
Ilustración 83 Comando Robots



Fuente: Autor

- Se realiza verificación de ingreso con el archivo “backup”, donde se verifica que allí están almacenado las copias de seguridad de la página web, como se muestra en la ilustración 84.

Ilustración 84 Copias de seguridad página web



Fuente: Autor

5.3.7 Síntesis de las vulnerabilidades

Elemento	Prueba Realizada	Vulnerabilidad Encontrada	Identificador asociado a la vulnerabilidad (CVE)	Solución
BadStore	Cross Site Scripting (XSS)	insertar código HTML en el servidor WEB	CVE-2019-8391	Uso de WAF
BadStore	Ataque por inyección de código SQL	Ataque a la base de datos del servidor WEB	CVE-2019-6491	Uso de WAF
BadStore	Denegación de servicio	Pérdida de la conectividad del usuario real	CVE-2009-1441	Uso de WAF
BadStore	Cookie snooping	Decodificación de información privada de usuarios	CVE-2018-1484	Cifrado de Cookie
BadStore	Modificación de cookies	Modificación de datos de compras de los usuarios	CVE-2010-4333	Cifrado de Cookie
BadStore	Tampering de parámetros y formularios	Modificación de los parámetros en la aplicación web	CVE-2009-1583	Creación limitada de usuarios administradores. Cambio de forma de crear Usuarios.
BadStore	Directory transversal	Acceso a nivel privilegiado a usuario no autorizado	CVE-2004-1862	Uso de filtrado de usuarios.
BadStore	Navegación forzada	Visualización de elementos y archivos importantes para la empresa	CVE-2008-1045	WAF

CONCLUSIONES

- Con la implementación de la infraestructura de red en la empresa de cobranza “xyz”, se logra interconectar entre si las cuatro Sedes que forman parte de la empresa.
- La comunicación por VPN entre RouterBoard es efectiva independientemente de la red física existente
- Al finalizar el análisis de las vulnerabilidades del servidor web se puede concluir que es un servidor fácil de manipular, y no solo sucede con el servidor web de prueba sino con servidores que están en la red son propenso a ataques por su baja seguridad, pero también existen muchas herramientas que pueden ayudar a proteger.
- Es fundamental contar con un firewall WEB, la herramienta Mod_security es fácil de configurar y sencillas de usar.

RECOMENDACIONES

- Se recomienda garantizar en un 100% el servicio de conectividad para evitar caídas entre los túneles.
- Se recomienda que el personal encargado de la supervisión de la red garantice las políticas de seguridad, siguiendo un plan de seguridad.
- Se recomienda realizar backups de las configuraciones de los equipos, para permitir dar solución rápidamente si se presenta fallas.
- Se recomienda revisar el consumo de procesador de los equipos constantemente, esto evita que los equipos se sobrecalienten o bloqueen.
- Se recomienda monitorear los consumos de ancho de banda.
- Se recomienda a la empresa CAPSULE CORP S.A.S hacer uso de políticas de seguridad, que mitigue los ataques al servidor con ello elevarían las ventas de los nuevos productos.

BIBLIOGRAFÍA

Almachi Oñate, Paúl Noe y Chiluisa Quimbita, Carlos Orlando. 2010. *Implementación de una VPN con seguridades de la red inalámbrica y red externa para la empresa exportadora de flores GP FLOWERS.* Latacunga, Ecuador: 2010. 26 p.

Andreu, Joaquin. Servicios de red. *Protocolo de trasnferencia de ficheros FTP (File Tranfer Protocol).* s.l. : editex, pág. 82. 34 p.

Ardila, Osacr. Que es y como usar un VPN. [En línea] 2015. 27 p.

Castro, Rodrigo. *Avanzando en la seguridad de las redes.* 2005, Fundamento de redes. 30 p.

Bello, Claudia E. *Manual de seguridad en redes.* s.l. : Coordinacion de emergencia en redes teleinformaticas. 35 p.

Castillo Fiallos, Jessica Nataly. ESTUDIO COMPARATIVO DEL RENDIMIENTO DE SERVIDORES WEB DE VIRTUALIZACION SOBRE LA PLATAFORMA WINDOWS SERVER 2008. Ecuador : ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO, 2012. 38 p.

Cobo Yera, Angel Luis. *Protocolo de trasnferencia de archivos (FTP).* Pueblo Nuevo : Innivacion y experiencias educativas, 2009. 34 p.

CONGRESO DE COLOMBIA. LEY 1273 DE 2009 CAPITULO PRIMERO De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. 45 p.

Cosios Castillo, Eduardo Richard y Simbaña Loachamin, Wilson Xavier. *Estudio y diseño de redes virtuales privadas.* Quito : s.n., 2004. 29 p.

David Melendi, Xabiel G. Pañeda, Member, IEEE, Roberto García, Member, IEEE, Víctor García. *Sistema para la realización y evaluación de.* 2009. 34 p.

DECISIÓN 351. *CAPITULO I DEL ALCANCE DE LA PROTECCION Articulo 1.* s.l. : El Artículo 30 del Acuerdo de Cartagena y la Propuesta 261 de la Junta. 45 p.

DECISION 486. *TITULO I DISPOSICIONES GENERALES Articulo 1.* s.l. : LA COMISION DE LA COMUNIDAD ANDINA. 45 p.

CONGRESO DE LA REPUBLICA. LEY 1450 DE 2011 TITULO 1 DISPOSICIONES GENERALES ARTICULO 1. 45 p.

CONGRESO DE LA REPUBLICA. LEY NÚMERO 23 DE 1982 CAPÍTULO I Disposiciones generales Articulo 1. 45 p.

Duarte, Eugenio. *¿Qué Es Mikrotik RouterOS?* Abril : Information Tecnology Academy, 2014. 36 p.

ehack. Ataques de contraseñas. *Ataques de contraseñas.* [En línea] 23 de 06 de 2017. http://ehack.info. 31 p.

Estrada Corona, Adrian. *PROTOCOLOS TCP/IP DE INTERNET.* 2004, Revista Digital Universitaria, págs. 4-7. 33 p.

FI, Ingenieria. *Mecanismo de seguridad en red.* 2015. 35 p.

Florian Otoya, Cesar Augusto. *Implementacion de una aplicacion movil para monitoreo de contenido y disponibilidad de servicios web.* Lima: M, 2015. p 32-35.

Gómez Montoya, Carlos Eduardo, Candela Uribe, Christian Andres y Sepúlveda Rodríguez, Luis Eduardo. Seguridad en la configuración del Servidor Web Apache.

Armenia : INGE CUC, Vol. 9, N° 2, pp 31-38, Diciembre, 2013, 29 de Abril de 2013. 37 p.
Gómez Vieites , Álvaro. TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS. s.l. : Profesor de la Escuela de Negocios Caixanova. 39 p.
Gomez, Fernandez. *Conocimientos y aplicaciones tecnologicas para la direccion comercial.* Madrid : ESIC, 2004. 33 p.
Gonzalez Casrañeda, Ricardo. *IMPLEMENTACIÓN Y EJECUCIÓN DE UN PROTOCOLO DE TRANSFERENCIA.* Pereira : s.n., 2012. 34 p.
Gonzalez, Gabriela. Qué son las cookies de tu navegador y para qué sirven. s.l. : Blogthinkbig.com, Septiembre de 2014. 19 p.
Hernández Saucedo, Ana Laura y Mejia Miranda, Jezreel. Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. s.l. : Computacion e informatica, Febrero de 2015. 42 p.
Huidobro, José. *Tecnologias de informacion y comunicacion.* Madrid: s.n., 2007. 28 p.
ibiblio. Escaneos de puertos. *Escaneos de puertos.* [En línea] 08 de 08 de 2003. www.ibiblio.org. 31 p.
Joaquin Andreu. *Servicios en red.* Madrid : Editex S.A, 2002. 34 p.
Leon Rodriguez, Jose David. *ACCIONES DE HARDENING PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN CUANDO SE USAN LOS SERVICIOS DE HTTP, LDAP, SSH Y SMTP.* Ibague : s.n., 2018. 33 p.
Limari Ramirez, Victor Humberto. *Protocolos de seguridad para redes privadas virtuales.* Valdivia : s.n., 2004. 29 p.
Lopez, Aguilera. Seguridad Informatica. s.l. : Edite, pág. 147. 26 p.
Microsoft. Servicios VPN. 2018. 41 p.
Mikrotik. [En línea] https://mikrotik.com/. p 36-42.
Mikrotik. RouterOS official mickotik distributor. [En línea] 2016. 37 p.
Mischel, Magnus. ModSecurity 2.5 Securing your Apache installation and web applications Prevent web application hacking with this easy-to-use guide. s.l. : Packt Publishing BIRMINGHAM - MUMBAI, 2009. 114 p.
ModSecurity. [En línea] 2004-2019. http://www.modsecurity.org/. 112 p.
Montes de los santos, Andres, Corona Carrion , Jocelyn Carolina y Gonzalez Beltran, Jorge. *Propuesta de implementacion de una VPN.* Mexico: s.n., 2012. 28 p.
Muycomputerpro. La explotacion de la confianza. *La explotacion de la confianza.* [En línea] 16 de 09 de 2014. muycomputerpro.com. 31 p.
Ñacato Gualotuña, Marco Antonio. *Diseño e implementacion de una red provada virtual para la empresa hato telecominucaciones.* Quito: s.n., 2007. p 27-28.
Pakala, Sangrita. Preguntas Frecuentes sobre seguridad en aplicaciones web (OWASP FAQ). s.l. : The Open Web Application Security Project, 25 de Enero de 2005. 20 p.
pandasecurity. Que es un ataque DoS. *Que es un ataque DoS.* [En línea] 26 de 05 de 2018. www.pandasecurity.com. 32 p.
Pantaleo, Jose. Redes informáticas II. s.l. : quizlet. *Pequeño Diccionario de termino de informacion. 19 p.*
Pérez Porto, Julian y Merino, Maria. DEFINICIÓN DE. 2019. 19 p.

Pineda Mejillones, Daniel Afren y Leyton, Edgar. *Gestion de seguridad en redes de comunicaciones: Analisis de seguridad en la red de datos de la FIEC.* 2004. 35 p.
Pinto, Cristhian, Reascos, Jorge y Torres, Alejandro. *experimental, Evaluación de ataques de tipo Forck empleando entornos virtuales como plataforma.* s.l. : Departamento de ciencias de la computacion. 33 p.
Ristiæ, Ivan. MODSECURITY HANDBOOK The Complete Guide to the Popular Open Source Web Application Firewall. s.l. : Feisty Duck Londo, 03 de Junio de 2013. 112 p.
Rouse, Margaret. Base de datos relacional. s.l. : SearchDataCenter, 2015. 19 p.
Rouse, Margaret. Servidor Web. [En línea] Diciembre de 2016. 35 p.
Seguridad en la comunicaciones. s.l. : Universidad de Oviedo Ingenieria de sistemas y automatica. 36 p.
Talledo San Miguel, Jose. Implantacion de aplicaciones web en entornos internet, intranet y extranet. España : Paraninfo, 2015. 37 p.
Tanenbaum, Andrew S. *Redes de computadoras.* Mexico : Pearson, 2003. 25 p.
Tarazona T., Cesar H. *Amenazas informaticas y seguridad de la informacion.* 2015. 35 p.
techlandia. Pin de la muerte. *Pin de la muerte.* [En línea] 01 de 01 de 2004. techlandia.com. 32 p.
Ubiquitour. ¿Qué es el barrido de Ping? *¿Qué es el barrido de Ping?* [En línea] 27 de 01 de 2013. http://www.ubiquitour.com. 30 p.
Windows. Redes privadas virtuales: una visión general. *microsoft.* [En línea] 12 de Agosto de 2009. 27 p.

ANEXOS

Anexo A. Video

https://www.youtube.com/watch?v=t8XdF1fMrEM&feature=youtu.be
https://www.youtube.com/watch?v=T7hHTE_lhxY&feature=youtu.be
https://www.youtube.com/watch?v=1cjEVkN9b8A&feature=youtu.be