ISU CENTRAL TÉCNICO
INSTITUTO SUPERIOR UNIVERSITARIO

PRÁCTICA EXPERIMENTAL Y EVALUACIÓN DE TÉCNICAS FRENTE A ATAQUES DDOS, EN UN ENTORNO DE LABORATORIO BASADO EN KALI LINUX

Electrónica

ESTRADA MEJIA GABRIEL ALEJANDRO

TUTOR:

DANIEL PATRICIO VINUEZA LOPEZ

2025 II

Contenido

TÍTULO DEL PROYECTO

Práctica experimental y evaluación de técnicas frente a ataques de Denegación de Servicio Distribuido (DDos), en un entorno de laboratorio basado en Kali Linux.

PLANTEAMIENTO DEL PROBLEMA

En el estado actual de la tecnología, la ciberseguridad representa un requisito fundamental para las organizaciones de los sectores público y privado a nivel mundial. Los peligros de seguridad digital están en aumento, y los ataques de Denegación De Servicio Distribuido (DDoS) se encuentran entre las amenazas más comunes y riesgosas para los dispositivos tecnológicos. Este tipo de amenazas busca reducir la capacidad de los servidores y las plataformas en línea aumentando él envió de paquetes o de información para que el sistema colapse, provocando la interrupción de servicios críticos que afectan a gobiernos o empresas. Las consecuencias van desde importantes pérdidas financieras hasta daños a la reputación de la empresa y la vulneración de información de los clientes. Ante este panorama, es necesario formar profesionales que comprendan cómo funcionan estas amenazas y puedan desarrollar estrategias de defensa.

Para la formación de Tecnólogos en electrónica del Instituto Superior Universitario Central Técnico, comprender y aplicar los principios de la ciberseguridad es una algo esencial en el panorama tecnológico actual. Los dispositivos electrónicos, las redes de comunicación y servicios web están conectados a través de internet, lo que los convierte en objetivos potenciales de ataques. Los estudiantes participan en el diseño e implementación de sistemas que interactúan no solo con dispositivos físicos, sino también con sitios web y los entornos digitales. Por lo tanto, es importante conocer las vulnerabilidades de estas plataformas, identificar los métodos de ataque y dominar los métodos de seguridad para formar a diversos profesionales capaces de encontrar soluciones seguras desde cero.

Los estudiantes de electrónica necesitan experiencia práctica en la identificación y eliminación de estas amenazas en un entorno de pruebas supervisado. Simular escenarios utilizando máquinas virtuales como Kali Linux y softwares especializados que ayudan a los estudiantes a comprender el funcionamiento de estos ataques, evaluar su impacto en los sitios web y desarrollar habilidades prácticas para implementar mecanismos de defensa como firewalls de aplicaciones web, sistemas de control de velocidad de conexión y monitorización del tráfico del Protocolo de transferencia de Hipertexto (HTTP).

PLANTEAMIENTO DE OBJETIVOS

General

Ejecutar una práctica experimental y evaluación de técnicas frente ataques de Denegación De Servicio Distribuido (DDOS) mediante un entorno basado en Kali Linux, para preparar a los estudiantes de la carrera de Tecnología en Electrónica en medidas de mitigación.

Específicos

Diseñar y configurar un servidor web mediante un sistema operativo Kali Linux el cual estará en red, que soporte HTTP, para ser usado en prácticas de laboratorio y pruebas controladas.

Evaluar las principales técnicas de ataques de Denegación De Servicio Distribuido (DDoS) y aplicar las medidas de mitigación apropiadas en respuesta, mediante ensayos controlados para elevar la seguridad informática

JUSTIFICACIÓN

El proyecto de práctica experimental sobre ataques DDoS es parte importante para los estudiantes del área de electrónica en el ISUCT ya que en la actualidad los ataques de denegación de servicio distribuido(DDoS) son una de las amenazas más frecuentes que afectan a las instituciones tanto públicas como privadas por lo cual , Es importante formar a los estudiantes a cerca de estos temas para que sepan identificar, mitigar estos ataques que no solo les ayuda en su formación como profesionales sino que también los prepara para el mundo laboral.

En este sistema de laboratorio controlado permitirá a los estudiantes entender de manera eficaz cómo funcionan los ataques DDoS, sus métodos y como afectan estos ataques a los servicios o sitios web, Al configurar un entorno simulado en Kali Linux y un servidor web con HTTP, los estudiantes podrán observar cómo funciona el ataque desde el lugar de la persona que lo ejecuta como también podrán observar cómo es ser víctima de estos ataques, es debido a esto que la práctica es importante para desarrollar las habilidades necesarias y así poder mitigar estos ataques.

Los estudiantes estarán capacitados para instalar las medidas de seguridad para proteger la integridad de las redes de instituciones públicas o privadas, así evitando irrupciones en los servicios que ofrecen estas entidades como lo son servicios de gestión académica o recursos en línea. Esta preparación también reduce la vulnerabilidad del ISUCT ante amenazas cibernéticas.

ALCANCE

El proyecto abarcará la implementación y evaluación de un entorno de laboratorio controlado para analizar cómo funcionan los ataques DDoS, manteniendo el foco en la configuración de cómo son ejecutados y en la manera de mitigar estos ataques maliciosos. Las actividades que se emplea es la configuración de un servidor web, implementación de herramientas de ataque desde Kali Linux y como implementar medidas de seguridad en los servidores. Este tema busca que los estudiantes de la carrera de electrónica tengan una experiencia práctica y didáctica que a la vez entiendan como pueden realizar ataques como también como defenderse de estos ataques DDoS.

Este proyecto se lo realizara en las instalaciones de la carrera de electrónica del ISUCT, implementando equipos tecnológicos con los cuales estas prácticas sean posibles de realizar y los estudiantes tengan un aprendizaje adecuado.

MARCO TEÓRICO

Servidor Web

Un Servidor Web es un sistema ya sea de hardware como de software que almacena y entrega la información que contiene una página web, un sitio web recibe la solicitud de una determinada página este la busca y procesa los archivos que contiene dicha página y los muestra en tu pantalla. Cada vez que se busca una dirección web o enlace el navegador envía solicitudes al servidor web para que posteriormente este reciba el contenido correspondiente o lo que necesitamos a través de los conocidos protocolos de comunicación estándar HTTP o HTTPS. En resumen, la función del servidor es recibir las solicitudes de los usuarios para poder buscar la información solicitada para finalmente mostrarte los resultados de esa búsqueda o solicitud en tu pantalla. Existe varios tipos de servidores como lo es el Servidor Físico o Servidor Dedicado,

que es un equipo exclusivo para centro de datos, se usa general mente en empresas o proyectos con alto tráfico donde se requiere control, potencia y personalización que necesiten de mayor estabilidad y rendimiento. Servidor virtual privado servidor físico que se divide en diferentes máquinas virtuales, por lo cual es considerado un servidor flexible con varios recursos disponibles. Servidor compartido es utilizado por varios sitios web donde todos comparten los mismos recursos de un solo servidor físico. Uno de los servidores más utilizado es Apache debido a que es fácil, confiable y fácil de configurar, compatible con muchas tecnologías. (KeepCoding, 2025)

Sistema Operativo Linux

Linux es un sistema operativo basado en Unix,su Keernel fue desarrolladopor Linus Torvalds en 19911.Este sistema operativo es de código abierto de tal modo que cualquier persona puede conseguirlo totalmente gratis, de hecho muchas personas o empresas contribuyen al desarrollo y han creado sus propias distribuciones de Linux altamente personalizables y configurables. Existen muchas distribuciones de Linux que se utilza para una amplia variedad de dispositivos no solo en ordenadores, sino que también en servidores. (Allende, 2019)

Debian Linux

Es la distribución más estable y cuenta con repositorio, una gran comunidad, gestores de paquetes Servidores, usuarios que buscan máxima estabilidad, Debian también se caracteriza por tener flexibilidad y personalización. (Allende, 2019)

Ubuntu Linux

Ubuntu tiene una tienda de aplicaciones que permite que instalemos diferentes programas, Ubuntu es ideal para Principiantes, compatibilidad de hardware y desarrollo. (Allende, 2019)

Fedora Linux

Fedora es un software cuya distribución es impulsada por Red Hat que se lanzó en 2003. Fedora se destaca por ofrecer una opción popular para usuarios avanzados y desarrolladores, porque cuenta con las últimas implementaciones a nivel de tecnología. (Allende, 2019)

CentOS Linux

CentOS es una distribución basada en el código fuente de Red Hat Enterprise Linux (RHEL), pero es de código abierto y gratuito. Está diseñada para ser una opción estable para servidores y entornos empresariales. Se centra en la seguridad y la estabilidad, y proporciona actualizaciones de seguridad regularmente. (Allende, 2019)

Kali Linux

Kali Linux es una distribución de Linux basada en Debian, específicamente diseñada para temas de seguridad muy variados, como análisis de redes, ataques inalámbricos, Kali Linux se encuentra entre las distribuciones de seguridad de Linux más usadas, ya que es una de las

mejores, tanto para uso personal como profesional, proporcionando a los usuarios paquetes de herramientas como Foremost, Wireshark, Maltigo as-Aircrack-ng, Kismet y más. (ALTUBE, 2021)

Ataques de Denegación de Servicios Distribuidos (DDoS)

Este ataque es considerado muy peligroso ya que envía gran cantidad de paquetes o peticiones ficticias al servidor de la red. Con el fin de que la red se colapse, generando una sobrecarga en el servidor. Un ataque DDoS se lanza desde varios dispositivos regularmente estos dispositivos están repartidos globalmente formando una botnet. (IMPERVA, 2029)

Ataques basados en volumen

Los ataques basados en volumen que se basa en la inundación User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) entre otras que llenan a un servidor de paquetes falsos, con el objetivo de saturar el ancho de banda del sitio o servidor web y su magnitud se mide en bits por segundo(bps). (IMPERVA, 2029)

Ataques de Protocolo

Los ataques de protocolo SYN, ataques de paquetes fragmentados, ping de la muerte entre otros, este tipo de ataques consume recursos del servidor o del equipo como firewalls y balanceadores de carga este se mide en paquetes por segundo (Psp). (IMPERVA, 2029)

Ataques de capa

Los ataques de capa de aplicación son aquellos que incluyen ataques de baja velocidad, ataques dirigidos a vulnerabilidades de apache, Windows entre otros, se basa en solicitudes sin

ninguna mala intención sin embargo estos ataques buscan derribar el servidor, este se lo mide en solicitudes por segundo (RPS). (IMPERVA, 2029)

TIPOS DE INVESTIGACIÓN PLANTEADA

Los tipos de investigación se refieren a las categorías generales en las que se clasifican los estudios de acuerdo con sus objetivos, propósitos y enfoques. Los tipos de investigaciones aplicadas y ejecutadas en este proyecto son las investigaciones, bibliográfica y experimental con las cuales abordaremos la problemática que tienen las instituciones públicas como privadas al no contar con medidas de prevención en contra de estos Ataques de Denegación de Servicios Distribuidos.

Investigación Bibliográfica

Esta investigación se basa en parte teórica, debido a que gracias a esto podemos comprender qué son los ataques DDoS y cómo pueden ser prevenidos a tiempo y así proteger nuestros equipos. Para ello se revisaron varias fuentes como libros, artículos científicos, manuales técnicos y documentos de seguridad informática. A través de esta consulta se pudo determinar cómo es que los ataques DDoS funcionan, cuáles son sus principales ataques y estrategias que afectan a nuestros equipos. Además, se desarrollaron estrategias para poder detener estos ataques, analizando información sobre cómo configurar los protocolos de red y sistemas web con HTTPS.

Investigación Experimental

La Parte experimenta se la realizo en el área de electrónica del ISUCT, nos enfocamos en realizar simulaciones de ataques DDoS para observar cómo afectan al funcionamiento de un servidor web configurado con Ubuntu. Se realizo la parte experimental con la implementación de un monitor con sistema operativo Kali Linux en donde se ejecutó el ataque, para poder observar el rendimiento del servidor, la velocidad del mismo y como afectaba el ataque DDoS al consumo de recursos del servidor web durante y después del ataque, esta práctica permitió entender de manera directa cómo se comporta un sistema ante un ataque DDoS y cómo se pueden aplicar medidas de defensa efectivas, brindando una experiencia de aprendizaje más completa y cercana a los retos reales de la ciberseguridad

MÉTODOS DE INVESTIGACIÓN UTILIZADOS

Método hipotético deductivo

Se aplica este método para analizar cómo se comportan los ataques DDoS y verificar la efectividad de las medidas de seguridad en contra de estos ataques. este proyecto parte de suposiciones o hipótesis acerca de cómo funcionan estos ataques para luego poner aprueba y observar cómo es que los ataques DDoS pueden usar los recursos del servidor, del ancho de banda y causar daño en el mismo. Es fundamental entender las medidas de mitigación como aplicar límites de velocidad puede reducir un ataque sin afectar a los usuarios. Esta hipótesis se pone a prueba en el laboratorio mediante pruebas en las cuales nos pondremos en los zapatos del atacante como de la víctima. De esta manera el método ayuda a comprender de forma acertada

como los sistemas reaccionan ante los diferentes tipos de ataques, así fomentando al pensamiento crítico y analítico.

Método lógico inductivo

Este método se utiliza para obtener soluciones o conclusiones generales del problema a partir de la observación de la practica simulada de ataques DDoS en la cual observamos y determinamos el comportamiento de los servidores en cada caso: cuando el ataque consume recursos del servidor y como las medidas de seguridad que instalamos responden ante estos ataques. A través de estas observaciones se puede concluir o llegar a la solución de que método de mitigación es adecuado para cada servidor dependiendo su uso ya sea para un servidor en algún lugar local como un servidor en el ámbito público, determinaremos el grado de seguridad que tendrá cada servidor web.

Tabla 1:

Cronograma de actividades para la práctica experimental y evaluación de técnicas frente a ataques DDos, en un entorno de laboratorio basado en Kali Linux.

	25-sep-1 octu	1-octu-13	13-octu-6nov	7-nov	14-nov	14-nov-17 nov	17-nov 24 nov	25-nov-	26-nov	27-nov	28-nov	28-nov-30	30-nov
Análisis del Tema													
Recopilación De datos													
Elaboración del Perfil													
Revisión de perfil													
Práctica experimental													
Elaboración de tesis													
Compra de Cpu													
Resultados y análisis													
Conclusión y recomendación													
Conclusión y recomendación													

FUENTES DE INFORMACIÓN

Las fuentes de información son diversas y pueden clasificarse de diferentes maneras según sus características y la naturaleza de la información que proporcionan.

Fuentes Primarias

Las fuentes primarias son documentos que contienen información original que no ha sido editada, traducida o reestructurada, ejemplos libros, manuscritos o documentos. (PINCAY, 2017)(Tesis), (Holmes, 2019)(libro)

Fuentes Secundarias

Son aquellas que proporcionan información ya procesada ejemplos enciclopedias, reseñas, páginas web y monogramas:

JOSE ALBERT (Albert, 2025)

RECURSOS

En la siguiente Tabla se describe los componentes utilizados:

Tabla 2

Detalle	Unidad	Cantidad	Valor Unit.	Valor Total
Procesador: I5 10ma generación	Unidad	1	150.00	$ 150.00
Placa Madre: Asus Prime H510M-F	Unidad	1	60.00	$ 60.00
Memoria RAM: 16GB (3200MHz)	Unidad	1	30.00	$ 30.00
Almacenamiento: HDD 1T	Unidad	1	30.00	$ 30.00
Fuente de Alimentación:450 W	Unidad	1	40.00	$ 40.00
Monitor	Unidad	1	50.00	$ 50.00
TOTAL:				**360.00 $**

Cotización

Nota: se detalla la cotización de los componentes, facilitando la planificación del presupuesto y optimizando recursos.

Elaborado por: Estrada Mejia Gabriel Alejandro

Tabla 2

Categorización de Actividades

	Recursos humanos	Cargo	Actividades
1	ALEJANDRO ESTRADA	Estudiante	Práctica experimental y evaluación de técnicas frente a ataques DDos, en un entorno de laboratorio basado en Kali Linux
	DANIEL PATRICIO VINUEZA	Tutor	Revisión del avance del proyecto

Nota: Se muestra la asignación de roles y tareas del proyecto, asegurando una ejecución eficiente y organizada. Elaborado *por*: Estrada Mejia Gabriel Alejandro.

REFERENCIAS

Bibliografía

Albert, J. (2025). Desdelinux. Obtenido de Desdelinux: https://blog.desdelinux.net/novedades-linuxverso-semana-45-2025/

Allende, S. L. (2019). SISTEMA OPERATIVO. Ciudad Autónoma de Buenos Aires.

ALTUBE, R. (2021). Kali Linux: Qué es y características principales. En R. ALTUBE, Kali Linux: Qué es y características principales. España. Obtenido de https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

Holmes, D. (2019). Protección DDoS de F5. En securityandtechnology, Protección DDoS de F5: (pág. 41). Seattle. Obtenido de https://securityandtechnology.org/wp-content/uploads/2021/04/F5-DDoS-Protection-ES.pdf

IMPERVA. (2029). Definición de ataque de denegación de servicio distribuido (DDoS). En Exabeam. Obtenido de https://www-imperva-com.translate.goog/learn/ddos/ddos-attacks/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wa

KeepCoding. (2025). Servidor Web: Guía esencial para elegir el mejor servidor para tu sitio. España. Obtenido de https://keepcoding.io/

PINCAY, J. L. (2017). EVALUACIÓN DE LOS ATAQUES DENEGACIÓN DE SERVICIOS (DDoS),. En J. L. PINCAY, EVALUACIÓN DE LOS ATAQUES DENEGACIÓN DE SERVICIOS (DDoS), (pág. 105). Manabí, Ecuador. Obtenido de https://repositorio.unesum.edu.ec/bitstream/53000/841/1/UNESUM-ECU-COMPR-18.pdf

CARRERA: ELECTRÓNICA

FECHA DE PRESENTACIÓN: 23 01 2026

DÍA MES AÑO

APELLIDOS Y NOMBRES DEL EGRESADO: ESTRADA MEJIA GABRIEL ALEJANDRO

APELLIDOS NOMBRES

TITULO DE LA PROPUESTA TECNOLÓGICA: PRÁCTICA EXPERIMENTAL Y EVALUACIÓN DE TÉCNICAS FRENTE A ATAQUES DDOS, EN UN ENTORNO DE LABORATORIO BASADO EN KALI LINUX

PLANTEAMIENTO DEL PROBLEMA:	CUMPLE	NO CUMPLE
• OBSERVACIÓN Y DESCRIPCIÓN	x	
• ANÁLISIS	x	
• DELIMITACIÓN.	x	
• PROBLEMÁTICA	x	
• FORMULACIÓN PREGUNTAS/AFIRMACIÓN	x	

PLANTEAMIENTO DE OBJETIVOS:

GENERALES:

REFLEJA LOS CAMBIOS QUE SE ESPERA LOGRAR CON LA INTERVENCIÓN DE LA PROPUESTA TECNOLÓGICA

	SI	NO
	X	

ESPECÍFICOS:

GUARDA RELACIÓN CON EL OBJETIVO GENERAL PLANTEADO

	SI	NO
	X	

JUSTIFICACIÓN:	CUMPLE	NO CUMPLE
IMPORTANCIA Y ACTUALIDAD	X	
BENEFICIARIOS	X	
FACTIBILIDAD	X	

ALCANCE:	CUMPLE	NO CUMPLE
ESTA DEFINIDO	X	

MARCO TEÓRICO:

FUNDAMENTACIÓN TEÓRICA	SI	NO
DESCRIBE LA PROPUESTA TECNOLÓGICA A REALIZAR	X	

TEMARIO TENTATIVO:	CUMPLE	NO CUMPLE
ANTECEDENTES, FUNDAMENTACIÓN TEÓRICA	X	
ANÁLISIS Y SOLUCIONES PARA LA PROPUESTA TECNOLÓGICA	X	
APLICACIÓN DE SOLUCIONES	X	
EVALUACIÓN DE LAS SOLUCIONES	X	

TIPO DE INVESTIGAIÓN PLANTEADA:

OBSERVACIONES: La investigación es aplicad. Se enfoca en resolver un problema concreto mediante una Práctica experimental. La Evaluación de la práctica permitirá evaluar la eficiencia de seguridad informática.

MÉTODOS DE INVESTIGACIÓN UTILIZADAS

OBSERVACIONES

Método hipotético-deductivo: Se formularán hipótesis relacionadas con el comportamiento del sistema, las cuales serán contrastadas mediante pruebas y resultados obtenidos durante el desarrollo del estudio.

Método lógico inductivo: A partir de la observación de casos particulares y resultados específicos, se establecerán conclusiones generales sobre el funcionamiento y desempeño del sistema.

CRONOGRAMA:

OBSERVACIONES: El cronograma incluye con las siguientes fases

Análisis del Tema (mes 1 -2)

Elaboración del Perfil (mes 1 - 2)

Revisión de perfil (mes 2)

Práctica experimental (mes 2)

Resultados y análisis (mes 2 -3)

Conclusión y recomendación (mes 2 -3)

FUENTES DE INFORMACIÓN: ----------
-

RECURSOS:	CUMPLE	NO CUMPLE
HUMANOS	x	
ECONÓMICOS	x	
	x	

MATERIALES

PERFIL DE PROPUESTA TECNOLÓGICA

Aceptado [x]

Negado [ ] el diseño de propuesta tecnológica por las siguientes razones:

a) ----------

---

b) ----------

---

c) ----------

ESTUDIO REALIZADO POR EL ASESOR:

NOMBRE Y FIRMA DEL ASESOR: DANIEL PATRICIO VINUEZA LÓPEZ

02 02 2026

DÍA MES AÑO

FECHA DE ENTREGA DE INFORME