UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE INGENIERÍA EN INFORMÁTICA

Tema: "Implementación y configuración de una honeynet en la zona desmilitarizada de la infraestructura de red de la Universidad Politécnica Estatal del Carchi"

Trabajo de Integración Curricular previo a la obtención del

Título de Ingeniero en Informática

AUTOR: Villarreal García Byron Adair

TUTOR: Ing. Del Hierro Mosquera Milton Gabriel Msc.

Tulcán, 2025.

CERTIFICADO DEL TUTOR

Certifico que el estudiante Villarreal García Byron Adair con el número de cédula 040176905 Ha desarrollado el Trabajo de Integración Curricular: “Implementación y configuración de una honeynet en la zona desmilitarizada de la infraestructura de red de la Universidad Politécnica Estatal del Carchi.”

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de la Unidad de Integración Curricular, Titulación e Incorporación de la UPEC, por lo tanto, autorizo la presentación de la sustentación para la calificación respectiva

Ing.Del Hierro Mosquera Milton Gabriel Msc.

TUTOR

Tulcán, agosto de 2025

AUTORÍA DE TRABAJO

El presente Trabajo de Integración Curricular constituye un requisito previo para la obtención del título de Ingeniero en la Carrera de ingeniería en informática de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Villarreal García Byron Adair con cédula de identidad número 0401576905 Declaro que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

Villarreal García Byron Adair

AUTOR

Tulcán, agosto de 2025

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo Villarreal García Byron Adair declaro ser autor de los criterios emitidos en el Trabajo de Integración Curricular: “Implementación y configuración de una honeynet en la zona desmilitarizada de la infraestructura de red de la Universidad Politécnica Estatal del Carchi.” y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes de posibles reclamos o acciones legales.

Villarreal García Byron Adair

AUTOR

Tulcán, agosto de 2025

AGRADECIMIENTO

Agradezco profundamente a la Universidad Politécnica Estatal del Carchi (UPEC) por brindarme el espacio y los recursos necesarios para obtener este gran logro.

Mi reconocimiento especial al Departamento de Tecnologías de la Información y Comunicaciones (TICs) por su constante apoyo técnico, en especial al Ing. Javier Torres, y por facilitar el entorno adecuado para la implementación de la plataforma honeynet.

Extiendo también mi gratitud al Ing. Milton Del Hierro por sus consejos y acompañamiento en este camino de la titulación, así como a los investigadores y compañeros que, con sus comentarios, sugerencias y colaboración, contribuyeron al desarrollo y mejora de este proyecto.

Gracias a quienes, con su ejemplo y orientación, han sido parte de mi formación académica y profesional durante todo este proceso.

DEDICATORIA

Dedico este logro con todo mi corazón a mi madre, quien con su amor, esfuerzo y ejemplo me ha enseñado que no existen límites cuando hay determinación.

A mi abuelo, que con su sabiduría y apoyo incondicional ha sido una guía constante en mi camino.

A mi hermano y a mi tía Elizabeth, por estar presentes en cada paso, animándome a seguir adelante incluso en los momentos más difíciles.

A mi tío, y quien siempre me apoya en todo. Su compañía, consejos y generosidad han sido un pilar fundamental para que este objetivo sea posible.

Y, sobre todo, a mis hijos, quienes son la razón más grande para superarme cada día. Ellos me inspiran a ser mejor persona y profesional. Este título es también para ustedes, con la esperanza de que un día se sientan tan orgullosos de mí como yo lo estoy de ustedes.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

En el presente trabajo se identificó que la infraestructura de red de la Universidad Politécnica Estatal del Carchi presenta limitaciones en la detección proactiva de amenazas, debido a la ausencia de mecanismos avanzados de monitoreo en su zona desmilitarizada (DMZ), lo que incrementa la vulnerabilidad frente a accesos no autorizados y posibles ataques. Se aplicó una metodología de investigación descriptiva para conocer el estado actual de la red, documental para fundamentar teóricamente el uso de honeynets, y de campo, mediante entrevistas a 8 administradores de red y encuestas a 54 usuarios clave, cuyos aportes permitieron establecer los requerimientos técnicos y de seguridad. Los principales resultados indican que el 72.2% del personal técnico considera que no existen herramientas suficientes para detectar intrusiones en tiempo real, y el 65% manifiesta preocupación ante el creciente tráfico sospechoso que ingresa a través de servicios expuestos en la DMZ. Es por ello por lo que se implementó y configuró una honeynet con herramientas como Honeyd, Snort y Splunk, aplicando la metodología Scrum para un desarrollo ágil y adaptativo. Esta implementación permitió capturar y analizar comportamientos maliciosos sin comprometer la seguridad de los activos reales de la red, fortaleciendo los mecanismos de defensa y mejorando la capacidad de respuesta ante ciber amenazas. Se realizaron pruebas controladas que generaron más de 2.000 eventos de tráfico simulado, los cuales fueron analizados para validar la eficacia del sistema. Para trabajos futuros, se recomienda la integración de inteligencia artificial para la clasificación automática de ataques y la expansión de la honeynet a otras zonas críticas de la red institucional.

Palabras Claves: honeynet, zona desmilitarizada, infraestructura de red, ciberseguridad, detección de amenazas

ABSTRACT

This research identified that the network infrastructure of the Polytechnic State University of Carchi has limitations in proactive threat detection due to the absence of advanced monitoring mechanisms in its demilitarized zone (DMZ), which increases vulnerability to unauthorized access and potential attacks. A descriptive research methodology was applied to understand the current state of the network, along with documentary research to theoretically support the use of honeynets, and field research through interviews with 8 network administrators and surveys of 54 key users. Their input helped establish the technical and security requirements. The main findings show that 72.2% of technical staff believe there are not enough tools to detect intrusions in real time, and 65% express concern about the increasing amount of suspicious traffic entering through exposed services in the DMZ. Therefore, a honeynet was implemented and configured using tools such as Honeyd, Snort, and Splunk, following the Scrum methodology for agile and adaptive development. This implementation enabled the capture and analysis of malicious behavior without compromising the security of real network assets, strengthening defense mechanisms and improving the response capacity to cyber threats. Controlled tests were carried out, generating over 2,000 simulated traffic events, which were analyzed to validate the system's effectiveness. For future work, the integration of artificial intelligence is recommended for the automatic classification of attacks and the expansion of the honeynet to other critical areas of the institutional network.

Keywords: honeynet, demilitarized zone, network infrastructure, cybersecurity, threat detection

INTRODUCCIÓN

Un honeypot es una herramienta de ciberseguridad diseñada para detectar, desviar y analizar los ataques dirigidos a las redes informáticas, funcionando como una trampa para los ciberdelincuentes. Estas tecnologías simulan vulnerabilidades dentro de una red para atraer a los atacantes, permitiendo estudiar sus métodos y comportamientos sin comprometer los sistemas reales. En particular, los honeypots pueden ser implementados de diversas maneras, como honeynets (redes de honeypots) que agrupan varias trampas para obtener información más amplia sobre los ataques. A medida que las amenazas cibernéticas se vuelven cada vez más sofisticadas, la necesidad de contar con sistemas de defensa avanzados ha aumentado significativamente, especialmente en instituciones educativas que manejan grandes volúmenes de información sensible. Sin embargo, muchas universidades enfrentan obstáculos para implementar soluciones como los honeypots debido a la falta de infraestructura tecnológica adecuada, la resistencia al cambio y la complejidad de su configuración. Este estudio se justifica por la necesidad de explorar la implementación de honeypots dentro de la infraestructura de red de la Universidad Politécnica Estatal del Carchi, con el objetivo de fortalecer su ciberseguridad, detectar ataques informáticos de manera temprana y proporcionar una capa adicional de protección en su infraestructura.

La investigación tiene como objetivo principal desarrollar un modelo de implementación de honeypots adaptado a las necesidades y capacidades de la universidad. Los objetivos específicos incluyen el análisis de estudios previos sobre la utilización de honeypots en entornos universitarios, la identificación de los retos y beneficios asociados con su adopción, y la evaluación de las mejores prácticas para su configuración y mantenimiento dentro de una red educativa. Además, se explorará el uso de plataformas como Nmap para la detección de puertos y CVE Details para identificar vulnerabilidades conocidas que podrían ser explotadas por los atacantes, con el fin de aumentar la eficacia de los honeypots en la detección de amenazas.

Este estudio se estructura en varios capítulos: El primer capítulo introduce el problema, contextualizando la situación actual de la Universidad Politécnica Estatal del Carchi en cuanto a la ciberseguridad, y presenta los objetivos y preguntas de investigación. El segundo capítulo proporciona la base teórica, incluyendo antecedentes y el marco conceptual sobre los honeypots, honeynets y las técnicas utilizadas para proteger las redes educativas. El tercer capítulo describe la metodología utilizada, detallando el enfoque del estudio, las variables investigadas y las técnicas para la recolección y análisis de datos, tales como el uso de herramientas como Nmap para escanear redes y evaluar vulnerabilidades. Los resultados y la discusión se exponen en el cuarto capítulo, donde se presentan las estrategias recomendadas para la implementación efectiva de honeypots en la universidad, así como la evaluación de su efectividad en la mejora de la seguridad de la infraestructura de red. Finalmente, el quinto capítulo contiene las conclusiones y recomendaciones derivadas de los hallazgos, mientras que el sexto capítulo enumera las referencias bibliográficas, y el séptimo capítulo incluye los anexos que respaldan la investigación.

I. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

El crecimiento de las redes de telecomunicaciones ha resaltado su papel crucial en la sociedad actual, ya que la expansión de dispositivos conectados a Internet las ha convertido en fuentes fundamentales de información, tanto personal como profesional. Sin embargo, esta expansión ha traído consigo riesgos significativos relacionados con la seguridad de los datos. El acceso no autorizado a información sensible se ha convertido en una amenaza real, y la protección de estos sistemas se ha convertido en una prioridad (Panchana, 2020).

Ante el aumento de amenazas cibernéticas, las soluciones de ciberseguridad han evolucionado. Una de las innovaciones clave en este ámbito son los Honeynet, redes deliberadamente diseñadas con vulnerabilidades para atraer a ciberdelincuentes y estudiar sus tácticas. Estos sistemas no solo permiten mejorar las defensas cibernéticas, sino que también optimizan las estrategias de seguridad, ayudando a proteger la información y minimizar el impacto de los ataques (Altamirano & Ganan, 2020).

A través de los Honeynet, es posible identificar patrones de ataques, lo que facilita la mejora de sistemas de defensa como firewalls y tecnologías de detección de intrusos.

En América Latina, la ciberseguridad enfrenta retos significativos debido a la falta de infraestructura tecnológica avanzada y la limitada capacidad de muchas instituciones para protegerse contra los ciberataques. Aunque la adopción de tecnologías está en aumento, los sistemas de protección aún no son lo suficientemente robustos para hacer frente a las crecientes amenazas. La implementación de sistemas como los Honeynet podría ser una herramienta clave para mejorar las defensas en la región, permitiendo una respuesta más eficiente ante

ciberataques y ayudando a fortalecer la protección de datos en una zona cada vez más vulnerable (Altamirano & Ganan, 2020).

A pesar de su valor en el ámbito académico, los Honeynet son esenciales también en el entorno empresarial. Empresas globales como Google los emplean para mejorar sus infraestructuras de seguridad, anticipándose a nuevas amenazas mediante el análisis de patrones de ataque. Esta misma metodología puede ser aplicada en otras instituciones, como universidades, para reforzar sus estrategias de defensa cibernética (Panchana, 2020).

En cuanto a la Universidad Politécnica Estatal del Carchi, la situación en términos de ciberseguridad refleja una vulnerabilidad significativa. La universidad enfrenta dificultades debido a su infraestructura tecnológica limitada y a la falta de sistemas avanzados de protección de datos. Similar a otras instituciones académicas en América Latina, se encuentra expuesta a ciberataques que podrían comprometer la información de estudiantes y docentes. La implementación de herramientas como los Honeynet podría permitirle no solo mejorar su infraestructura de seguridad, sino también identificar amenazas potenciales y fortalecer sus defensas antes de un posible ataque. Sin embargo, la adopción de estas soluciones se ve limitada por la falta de personal capacitado y los recursos insuficientes para gestionar eficazmente estas tecnologías (Altamirano & Ganan, 2020).

1.2. FORMULACIÓN DEL PROBLEMA

La ausencia de una Honeynet configurada en la infraestructura de red de la Universidad Politécnica Estatal del Carchi aumenta la vulnerabilidad ante posibles ciberataques, lo que pone en riesgo la seguridad de la información institucional.

1.3. JUSTIFICACIÓN

En la actualidad, la protección de la información en organizaciones se ha convertido en un aspecto crucial debido al aumento constante de amenazas cibernéticas. Los atacantes buscan explotar vulnerabilidades en los sistemas para obtener acceso a datos sensibles, lo que ha llevado al desarrollo de diversas soluciones de seguridad informática. Sin embargo, ninguna medida garantiza una protección absoluta, por lo que es fundamental complementar las estrategias tradicionales con enfoques innovadores.

Entre las herramientas más efectivas para analizar y mitigar amenazas se encuentran los Honeynet, los cuales permiten estudiar el comportamiento de los atacantes mediante la observación directa de sus acciones. Su implementación dentro de una infraestructura de red

facilita la identificación de accesos no autorizados, el reconocimiento de patrones de ataque y la detección de posibles vulnerabilidades en los servidores de una organización.

Los Honeypots, que son los elementos individuales dentro de un Honeynet, se diseñan con configuraciones específicas que los hacen atractivos para los ciberdelincuentes. Su propósito es doble: primero, distraer a los atacantes para alejarlos de los sistemas críticos y, segundo, recopilar información sobre sus métodos de intrusión. Con estos datos, es posible reforzar las estrategias de defensa y anticiparse a nuevas amenazas en entornos de producción.

Además de contribuir al análisis de incidentes de seguridad, estas tecnologías permiten el desarrollo de estrategias proactivas para la protección de infraestructuras clave. Herramientas como ELK Stack facilitan la gestión y visualización de la información obtenida, optimizando la capacidad de respuesta ante posibles ataques.

Dado que los Honeynet se implementan con configuraciones personalizadas en entornos empresariales, es esencial diseñarlos de manera estratégica para evitar su detección por parte de los atacantes. A lo largo de esta investigación, se explorarán las mejores prácticas para su despliegue y configuración, asegurando su eficacia en la mejora de la seguridad y el monitoreo continuo de servidores en producción.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Proponer una Honeynet en la zona desmilitarizada de la infraestructura de red de la Universidad Politécnica Estatal del Carchi, con el fin de mejorar la seguridad, simular posibles ataques cibernéticos y fortalecer la protección de la información institucional.

1.4.2. Objetivos Específicos

- Fundamentar teóricamente las técnicas y metodologías utilizadas en los Honeypots para comprender su funcionamiento, beneficios, aplicaciones en la ciberseguridad y determinar requerimientos para poder proponer una red honeyNet dentro de la universidad Politécnica del Carchi.
- Diseñar la Honeynet, seleccionando los componentes adecuados para simular vulnerabilidades y atraer posibles atacantes en la zona desmilitarizada de la infraestructura de red de la universidad y comparar los diferentes componentes, arquitecturas de Honeynet disponibles,

- Analizar los resultados obtenidos de las pruebas de rendimiento, para evaluar la efectividad de la Honeynet en la mejora de la seguridad y protección de la infraestructura de red de la universidad, y presentando recomendaciones para optimizar su implementación.
- ¿De qué manera la Propuesta de las técnicas de Honeypots respaldará la implementación y configuración de una Honeynet en la Universidad Politécnica Estatal del Carchi?
- ¿Cómo el diseño de la Honeynet en la infraestructura de red de la universidad contribuirá a la mejora de la seguridad cibernética y la protección de la información institucional?
- ¿Cómo las pruebas de rendimiento de los Honeypots en los servidores de la universidad permitirán evaluar su efectividad en la detección y prevención de ataques cibernéticos?
- ¿Cómo los resultados obtenidos de la implementación de la Honeynet impactarán en la seguridad de la infraestructura de red de la Universidad Politécnica Estatal del Carchi y qué recomendaciones pueden derivarse de estos resultados?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Las amenazas cibernéticas han aumentado considerablemente en los últimos años, lo que ha llevado a las instituciones a adoptar herramientas como honeypots y honeynets, diseñadas para atraer a los atacantes y estudiar sus métodos sin poner en riesgo los sistemas reales. Estas tecnologías permiten detectar vulnerabilidades y mejorar la seguridad de la red, proporcionando datos clave sobre las tácticas de los ciberdelincuentes. Sin embargo, su implementación presenta desafíos como la falta de conocimiento técnico, infraestructura adecuada y la complejidad en su configuración. En el contexto de universidades como la Universidad Politécnica Estatal del Carchi, estas herramientas pueden ser muy efectivas para fortalecer la ciberseguridad, pero requieren una correcta implementación y mantenimiento.

A continuación, se presentan siete antecedentes investigativos relacionados con la implementación y uso de honeypots y honeynets en diversos entornos, los cuales proporcionan un contexto valioso para entender cómo estas tecnologías se han utilizado en la mejora de la ciberseguridad, especialmente en redes universitarias:

En el estudio de, Heredia y Ocampo (2021) llevaron a cabo la implementación de una honeynet virtual utilizando tecnologías de código abierto como CentOS 7 y Honeywall. La investigación estuvo dirigida a crear un entorno controlado dentro de la red universitaria para la detección y análisis de ciberataques. Uno de los principales hallazgos de esta investigación es que la honeynet permitió a los investigadores identificar varias vulnerabilidades críticas dentro de la infraestructura de red que no habían sido detectadas previamente mediante métodos tradicionales de monitoreo de seguridad. Los autores concluyeron que la ubicación estratégica de la honeynet en la zona desmilitarizada (DMZ) de la red universitaria proporcionó un alto

grado de aislamiento y protección para los sistemas internos. Este aislamiento evitó que los atacantes pudieran comprometer los sistemas más sensibles de la universidad, mientras se recogían datos valiosos sobre los métodos de ataque. El estudio también demostró que el uso de una honeynet mejora la capacidad de respuesta ante incidentes de seguridad y contribuye a la mejora continua de las políticas de seguridad informática.

Maya y Vinueza (2022) presentaron un enfoque innovador en su implementación de una honeynet virtual híbrida, combinando sistemas físicos y virtuales en la Universidad Técnica del Norte. Los autores utilizaron herramientas como Honeywall y Snort para crear una red de monitoreo de seguridad en tiempo real. Los resultados de esta investigación destacaron que la combinación de sistemas físicos y virtuales permitió una cobertura más amplia frente a los ataques informáticos, ya que las vulnerabilidades podían ser emuladas de forma más realista y se podían generar entornos más diversos para analizar diferentes tipos de ataques. Uno de los hallazgos clave fue que los atacantes, al interactuar con la honeynet híbrida, mostraron comportamientos más sofisticados de los que se habían observado en implementaciones anteriores con honeypots tradicionales. El estudio concluyó que la honeynet híbrida resultó ser más efectiva en la captura de ataques dirigidos a sistemas de red complejos y contribuyó a una mejor estrategia de detección y mitigación de amenazas en entornos universitarios. Además, los autores destacaron que la actualización constante de las configuraciones de la honeynet es esencial para adaptarse a las amenazas emergentes.

Rodríguez y Pérez (2021) enfocaron su investigación en la implementación de honeypots para analizar los ataques informáticos dirigidos a redes universitarias. Su estudio destacó que, mediante el uso de honeypots, las universidades podían identificar las técnicas de ataque más comunes, lo que a su vez mejoraba las estrategias de defensa ante posibles brechas de seguridad. Los investigadores concluyeron que la implementación de honeypots en redes universitarias proporcionaba información crucial sobre las intenciones de los atacantes y las vulnerabilidades que buscaban explotar. Al final, los resultados demostraron que los honeypots permitieron una detección más temprana de amenazas y facilitaron la clasificación de ataques en función de su gravedad. Además, los autores sugirieron que el uso de honeypots debería combinarse con análisis forenses y herramientas de monitoreo avanzadas para mejorar aún más la capacidad de respuesta ante incidentes de seguridad.

En su investigación, Bravo y Revilla (2021) evaluaron la efectividad del uso de honeypots en redes universitarias con un enfoque en áreas de alto riesgo, tales como las zonas de acceso

público o los servicios en línea de las universidades. Los resultados de su estudio indicaron que la implementación de honeypots en estas áreas específicas ayudó a desviar los ataques de las infraestructuras críticas de la universidad, permitiendo a los administradores de red identificar las tácticas de los atacantes sin comprometer la seguridad de los sistemas internos. Un hallazgo importante fue que los atacantes, al interactuar con los honeypots, no solo intentaron explotar vulnerabilidades conocidas, sino que también desarrollaron nuevas tácticas y herramientas para intentar evadir la detección. Esto proporcionó a los investigadores datos valiosos sobre nuevas tendencias y técnicas de ciberataques. Los autores concluyeron que la ubicación de los honeypots en la zona desmilitarizada (DMZ) era fundamental para aislar los sistemas sensibles, y sugirieron que las universidades deberían integrar esta técnica dentro de sus políticas generales de ciberseguridad.

Sánchez y Ramírez (2023) investigaron la implementación de honeypots para la detección temprana de vulnerabilidades en redes educativas, específicamente en universidades. A través de su investigación, los autores destacaron que el uso de honeypots permite simular un entorno vulnerable para atraer a los atacantes y obtener información sobre sus métodos. Los resultados de su estudio indicaron que los honeypots lograron identificar ataques dirigidos tanto a los sistemas internos como a los servidores expuestos de la universidad. Un hallazgo clave fue que el análisis de los datos recopilados por los honeypots permitió a los administradores de red mejorar la configuración de las defensas, lo que resultó en una disminución significativa de los intentos de intrusión. El estudio concluyó que los honeypots son una herramienta valiosa para la detección temprana de amenazas y para reforzar las políticas de seguridad cibernética de las universidades.

En su estudio, Gómez y García (2022) analizaron el impacto de los honeypots en la ciberseguridad de las redes universitarias. Concluyeron que, mediante el uso de honeypots, las universidades no solo logran mejorar la seguridad de sus sistemas, sino que también contribuyen al análisis de patrones de ataque y la creación de mejores medidas de defensa. El estudio resaltó que, al colocar los honeypots en la DMZ de la red universitaria, se aislan de manera efectiva los ataques de la infraestructura crítica. Al final, los autores recomendaron que las universidades implementaran honeypots de manera estratégica para recolectar información relevante sobre las amenazas y reforzar sus defensas, destacando que la actualización continua de las configuraciones de los honeypots es esencial para mantener la efectividad frente a nuevas amenazas.

Vera y Paredes (2021) en su investigación "Uso de honeypots en redes de universidades para el análisis de ciberamenazas" analizaron cómo los honeypots pueden utilizarse para estudiar los ataques en redes universitarias. Los hallazgos demostraron que los honeypots ofrecen una plataforma para observar cómo los atacantes explotan las vulnerabilidades de la red sin poner en riesgo los sistemas críticos. La investigación concluyó que la implementación de honeypots dentro de una DMZ permite una mayor visibilidad de los intentos de intrusión, lo que a su vez facilita una respuesta más rápida y efectiva ante ataques. Además, los autores sugirieron que la información obtenida a través de los honeypots podría utilizarse para diseñar defensas más específicas y para la capacitación del personal encargado de la seguridad cibernética.

Estos antecedentes ofrecen una visión amplia y detallada sobre la implementación y configuración de honeynets en entornos universitarios, destacando la importancia de proteger las redes educativas frente a ciberamenazas y cómo el uso de herramientas como honeypots y honeynets puede mejorar la ciberseguridad de las instituciones.

2.2. MARCO TEÓRICO

2.2.1. Seguridad Informática

La seguridad informática se refiere a la implementación de estrategias y mecanismos destinados a salvaguardar la integridad, confidencialidad y disponibilidad de la información en los sistemas digitales. Esto implica la protección frente a accesos no autorizados, alteraciones no deseadas y posibles interrupciones en el servicio (Stallings & Brown, 2018).
Este concepto constituye el eje central de la investigación, ya que la implementación de una honeynet en la zona desmilitarizada (DMZ) de la Universidad Politécnica Estatal del Carchi busca precisamente fortalecer la seguridad informática institucional. Al simular sistemas vulnerables, se pretende prevenir ataques reales y mejorar la capacidad de defensa de la infraestructura universitaria.

2.2.2. Ataques Informáticos

Los ataques informáticos se refieren a acciones malintencionadas dirigidas a sistemas, redes o dispositivos tecnológicos con el propósito de comprometer su seguridad, obtener información confidencial o interrumpir su funcionamiento. Estas agresiones pueden manifestarse en diversas formas, como *malware*, *phishing*, ataques de denegación de servicio (DDoS) y explotación de vulnerabilidades en *software* o *hardware* (Stallings & Brown, 2021).
Según Laudon y Laudon (2022), estos ataques han evolucionado con el tiempo, utilizando

técnicas cada vez más sofisticadas que buscan evadir los mecanismos de seguridad establecidos. El estudio de los ataques informáticos es esencial para entender el tipo de amenazas que enfrentan las instituciones académicas como la UPEC. El análisis de los ataques registrados mediante la honeynet permitirá identificar patrones, técnicas comunes y puntos críticos en la red institucional, lo que contribuirá a implementar medidas de mitigación más efectivas.

2.2.3. Honeypots

Un *honeypot* es un sistema de seguridad diseñado para simular vulnerabilidades dentro de una red con el objetivo de atraer y analizar ataques cibernéticos. Su propósito principal es estudiar las tácticas, herramientas y estrategias empleadas por los atacantes para mejorar las medidas de defensa de la infraestructura informática (Spitzner, 2021).

Los *honeypots* son elementos fundamentales dentro de la arquitectura de la honeynet que se implementará en la DMZ de la UPEC. Su configuración permitirá capturar datos reales de intentos de intrusión, contribuyendo al análisis detallado del comportamiento de los atacantes y reforzando la seguridad perimetral de la red universitaria.

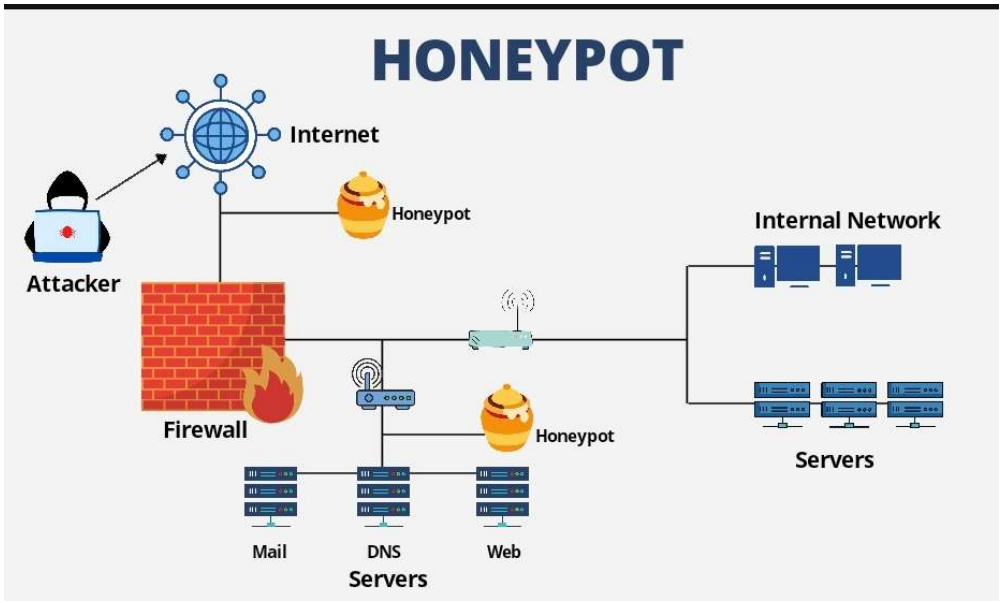


Figura 1. Honeypot

2.2.4. Clasificación de Honeypots

De acuerdo con Mokube y Adams (2022), los *honeypots* pueden clasificarse en dos categorías principales: de alta y baja interacción. Los de alta interacción permiten a los atacantes una mayor exploración dentro del sistema, proporcionando información más detallada sobre sus

métodos, mientras que los de baja interacción son más simples y fáciles de gestionar, utilizados principalmente para detectar intentos de intrusión.

Se elegirán ambos tipos de *honeypots* como parte de la honeynet a implementar en la UPEC. Esta elección permitirá equilibrar el nivel de detalle de los datos obtenidos con la facilidad de administración y la seguridad del entorno. Así, se maximizará la efectividad de la red trampa para detectar tanto ataques simples como amenazas avanzadas

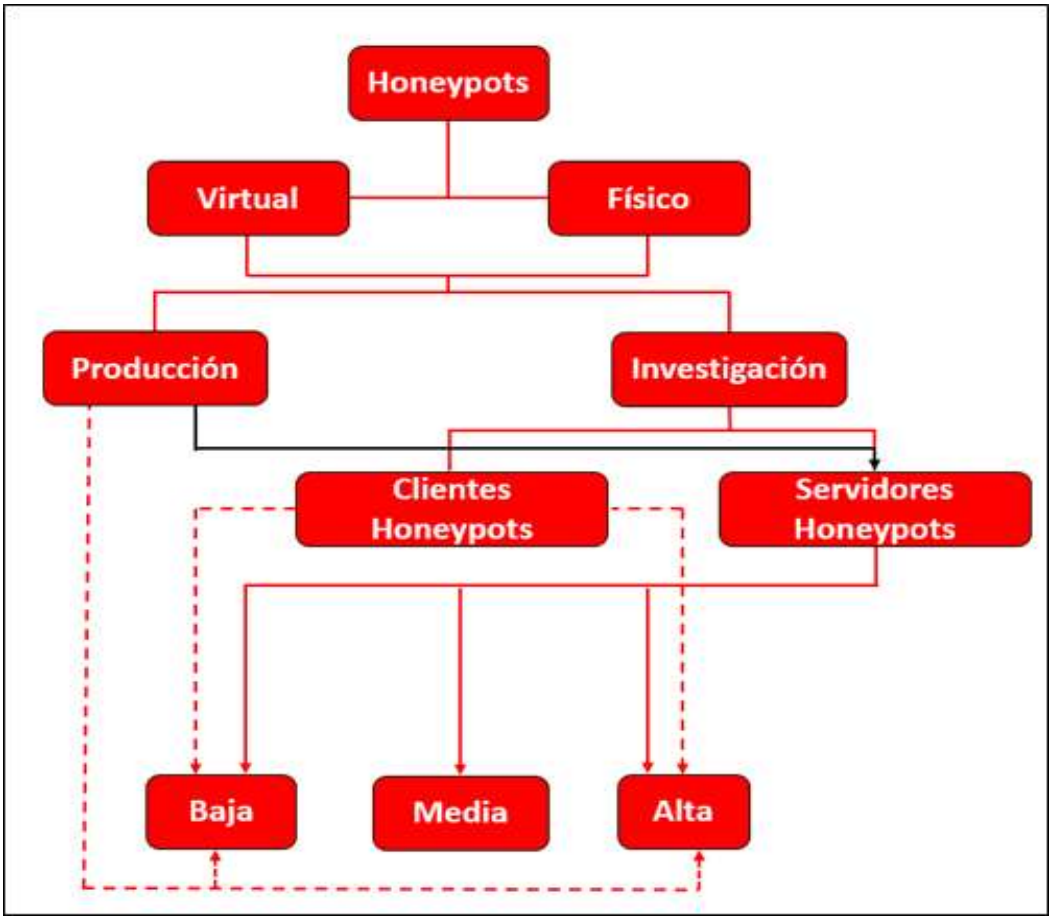


Figura 2 Honeypots Virtuales y físicos

Tabla 1. Consideraciones para desplegar un Honeypot

Consideraciones para desplegar un Honeypot
Estar seguro del objetivo con el que se despliega el honeypot y los datos que se pueden recoger.

Elegir bien el nivel de interacción que se quiere para nuestro honeypot en base al objetivo que tendrá el mismo (investigación, búsqueda y análisis de malware, etc.).
Configurar de forma correcta el honeypot para evitar que atacantes lo usen como vía de entrada al sistema en el caso de romper todos los controles de seguridad.
Analizar los datos obtenidos para sacar conclusiones con cierta regularidad.
Posibilidad de capturar e identificar amenazas desconocidas en base a la complejidad con la que esté configurado nuestro honeypot y el nivel de interacción que posee.
Ayuda a determinar falsos positivos por haber sido detectados y analizados previamente.

2.2.5. Honeynet

Una honeynet es una red de sistemas diseñados para ser atacados intencionadamente con el fin de monitorear, analizar y comprender las tácticas de los ciberdelincuentes. A diferencia de un honeypot, que es un único sistema trampa, una honeynet está compuesta por múltiples honeypots interconectados, lo que permite simular infraestructuras más complejas y obtener información más detallada sobre las amenazas (Spitzner, 2021). Según Brown et al. (2022), las honeynets pueden configurarse para estudiar distintos tipos de ataques, identificar vulnerabilidades y desarrollar estrategias de defensa más efectivas. Estas redes son especialmente útiles en la investigación de amenazas avanzadas persistentes (APT) y en la protección de infraestructuras críticas.

Se desarrollará e implementará una honeynet en la zona desmilitarizada de la red de la Universidad Politécnica Estatal del Carchi, con el objetivo de fortalecer la ciberseguridad institucional. Esta red trampa permitirá monitorear de forma proactiva los intentos de acceso no autorizado, recopilar inteligencia de amenazas y generar recomendaciones para mejorar la arquitectura de seguridad actual.

2.2.6. Ids

Un IDS (Sistema de Detección de Intrusos) es una herramienta que monitorea redes o dispositivos para identificar accesos no autorizados o actividades sospechosas, generando alertas para que se tomen medidas. La relación con el honeypot se da porque un honeypot puede servir como fuente de información para un IDS, permitiendo detectar amenazas y estudiar técnicas de ataque, mejorando así la seguridad del sistema (Stallings, 2018).

El IDS se integra como complemento a la honeynet implementada en la zona desmilitarizada de la UPEC. Los datos recolectados por los honeypots alimentan el sistema de detección, mejorando su capacidad para identificar patrones maliciosos en tiempo real y fortaleciendo las defensas de la infraestructura tecnológica institucional.

Figura 3. Ids

2.2.7. Tipos de Honeypots según su uso

La categorización de los honeypots según su uso permite adaptar su implementación a diferentes objetivos de seguridad. En el caso del proyecto desarrollado en la UPEC, se consideraron los siguientes tipos:

Tabla 2. Tipos de honeypots según su uso

Tipo de Honeypot	Descripción y Aplicación
Honeypots de Producción	Utilizados en redes reales, estos honeypots permiten detectar ataques en tiempo real y mitigar intrusiones. En la tesis, su implementación en la DMZ permite desviar el tráfico malicioso y generar alertas tempranas.
Honeypots de Investigación	Estos sistemas recopilan información detallada sobre técnicas de ataque. En la tesis, cumplen un rol clave al registrar datos de amenazas específicas al entorno académico, fortaleciendo el análisis forense.

Honeypots de Spam	Su uso en la UPEC permite detectar intentos de envío masivo de correos maliciosos, contribuyendo a proteger el sistema de mensajería institucional.
Honeypots de Malware	Implementados para estudiar software malicioso, permiten comprender las cargas útiles utilizadas por los atacantes y diseñar respuestas eficaces.
Honeypots de Fraude	Aunque su uso es más común en sectores financieros, su análisis en esta investigación proporciona un marco para comprender posibles ataques a sistemas administrativos de la universidad.

2.2.8. Funcionamiento de un Honeypot

El funcionamiento de un honeypot se basa en simular un entorno vulnerable para atraer a ciberatacantes. En esta tesis, los honeypots implementados en la DMZ de la UPEC siguieron las siguientes fases:

***Tabla 3*.** Funcionamiento de un Honeypot

Fase	Descripción
Implementación y Configuración	Se desplegaron sistemas virtuales configurados para parecer legítimos, adaptados al contexto universitario.
Atracción del Atacante	Se simularon vulnerabilidades comunes (como puertos abiertos y credenciales débiles) para capturar la atención de actores maliciosos.
Registro y Monitoreo	Se emplearon herramientas como T-Pot para capturar en tiempo real las interacciones maliciosas.
Análisis de Datos	La información obtenida se analizó para identificar técnicas de ataque y adaptar medidas defensivas.
Contramedidas	Los resultados se utilizaron para ajustar políticas de seguridad y prevenir incidentes en la red real de la universidad.

2.2.9. Honeynet: Redes de Honeypots

Una honeynet es una red de honeypots interconectados que simula una infraestructura real y es diseñada para atraer y registrar ataques de manera avanzada.
En esta investigación, se implementó una honeynet en la zona desmilitarizada de la red de la UPEC, conformada por servicios simulados como SSH, HTTP, SMB y bases de datos. Esto permitió analizar comportamientos maliciosos complejos, recolectar información sobre técnicas de intrusión persistente y evaluar la exposición real de los servicios institucionales. El diseño de la honeynet buscó emular una red académica realista, con la finalidad de atraer a atacantes sin comprometer los sistemas productivos de la universidad.

2.2.10. Técnicas de Implementación de Honeypots

La implementación de *Honeypots* requiere de diversas técnicas para garantizar su eficacia en la detección de ataques y el análisis del comportamiento de los atacantes. Según Spitzner (2021) y Brown et al. (2022), estas técnicas varían en complejidad y nivel de interacción con los intrusos, permitiendo adaptar los *Honeypots* a diferentes escenarios de seguridad.

Tabla 4. Técnicas de Implementación de Honeypots

Tipo de Honeypot	Descripción	Referencia
Honeypots de Baja Interacción	Simulan servicios básicos con vulnerabilidades limitadas. Su objetivo es detectar intentos de intrusión sin permitir actividades complejas. Son fáciles de desplegar y mantener, y se usan como capa adicional de seguridad.	Provos & Holz, 2020
Honeypots de Alta Interacción	Permiten mayor libertad al atacante, proporcionando información detallada sobre sus técnicas. Utilizan sistemas operativos reales y requieren supervisión estricta para evitar compromisos a otras partes de la infraestructura.	Mokube & Adams, 2022
Honeypots Virtualizados	Usan virtualización para desplegar múltiples honeypots en una misma infraestructura. Facilitan la administración	Zhuge et al., 2021

	centralizada y la detección de amenazas en redes empresariales y académicas.	
Honeypots Basados en Red	Se ubican en zonas estratégicas como la DMZ o puntos públicos. Están diseñados para capturar ataques dirigidos a servidores y dispositivos de red, registrando escaneos y explotación de vulnerabilidades en el tráfico de red.	Chirillo & Blaul, 2022
Honeypots Basados en Aplicaciones	Simulan aplicaciones web, bases de datos o servicios específicos. Analizan ataques dirigidos a software empresarial, plataformas en la nube y sistemas de autenticación, detectando vulnerabilidades como inyecciones SQL o fuerza bruta.	Brown et al., 2022
Honeynets	Red completa de honeypots interconectados que permite observar el comportamiento del atacante en un entorno realista. Requieren infraestructura avanzada y herramientas de monitoreo especializadas para evitar su detección.	Spitzner, 2021

2.2.11. Beneficios de Implementar Honeypots

Los **honeypots** ofrecen múltiples ventajas en el ámbito de la ciberseguridad, destacándose como herramientas efectivas para detectar, analizar y mitigar ataques informáticos. Su implementación permite fortalecer la seguridad de las redes al proporcionar un entorno controlado donde se pueden identificar técnicas y patrones de los atacantes sin comprometer los sistemas reales.

Tabla 5. Beneficios de Implementar Honeypots

N.º	Ventaja de los Honeypots	Descripción	Fuente
1	Detección Temprana de Amenazas	Los honeypots permiten una vigilancia activa sobre posibles intentos de intrusión. Su capacidad para atraer a los atacantes facilita la detección de vulnerabilidades antes de que puedan explotarse en entornos de producción.	IEEE Xplore, 2025
2	Análisis Forense y Aprendizaje	Estas herramientas registran en detalle las tácticas, técnicas y procedimientos utilizados por los ciberdelincuentes. Esta información es valiosa para mejorar estrategias defensivas y optimizar los sistemas de detección de intrusos.	IEEE Xplore, 2025
3	Reducción de Falsos Positivos	A diferencia de otros sistemas IDS, los honeypots generan alertas solo ante interacciones reales con actores maliciosos, minimizando las falsas alarmas y permitiendo un monitoreo más eficiente.	IEEE Xplore, 2025
4	Desvío de Ataques	Actúan como señuelos que desvían la atención de los atacantes lejos de los sistemas críticos, brindando tiempo a los equipos de seguridad para responder eficazmente ante posibles amenazas.	IEEE Xplore, 2025
5	Optimización de Estrategias de Seguridad	Su implementación mejora continuamente las políticas de seguridad, proporcionando datos en tiempo real sobre intentos de intrusión y vulnerabilidades. Además, la inteligencia artificial ha aumentado la adaptabilidad y eficacia de los honeypots ante amenazas emergentes.	IEEE Xplore, 2025

2.2.12. Limitaciones y Riesgos de los Honeypots

Los honeypots presentan varias limitaciones y riesgos que deben considerarse antes de su implementación:

Tabla 6. Limitaciones y Riesgos de los Honeypots

N.º	Desventaja	Descripción
1	Detección por atacantes	Los ciberdelincuentes avanzados pueden identificar y evitar honeypots mediante técnicas de evasión, reduciendo su efectividad (IEEE, 2025).

2	Compromiso del sistema	Si un honeypot no está bien configurado, los atacantes pueden explotarlo como una puerta de acceso a la red real.
3	Falsos positivos	Existe el riesgo de capturar datos irrelevantes o tráfico legítimo, lo cual afecta la precisión del análisis.
4	Recursos y mantenimiento	El sistema requiere monitoreo constante y actualizaciones frecuentes para mantenerse eficaz y operativo.

Ejemplos de Software Honeypot

Existen diversos tipos de software honeypot diseñados para diferentes propósitos y entornos.

Algunos ejemplos incluyen:

Tabla 7. Ejemplos de Software Honeypot

Nombre del Honeypot	Descripción
T-Pot	Plataforma todo en uno que integra múltiples herramientas de detección de amenazas. Basada en Docker, permite el análisis detallado del comportamiento de atacantes en entornos de red simulados.
Dionaea	Diseñado para capturar malware, es especialmente útil para analizar cómo los atacantes intentan explotar vulnerabilidades en servidores y dispositivos de red.
Kippo	Honeypot enfocado en la simulación de un servidor SSH con credenciales débiles. Permite registrar intentos de ataque y estudiar los métodos utilizados por los ciberdelincuentes.
Cowrie	Evolución de Kippo con mejoras en la emulación de entornos SSH y Telnet. Facilita el análisis de ataques avanzados y la recopilación de credenciales utilizadas en accesos no autorizados.
HoneyDOC	Diseñado para detectar ataques a documentos y sistemas de archivos, ayudando al monitoreo de accesos no autorizados a información sensible.

Estos softwares permiten a los investigadores y administradores de seguridad obtener información valiosa sobre patrones de ataque y mejorar la protección de redes y sistemas informáticos.

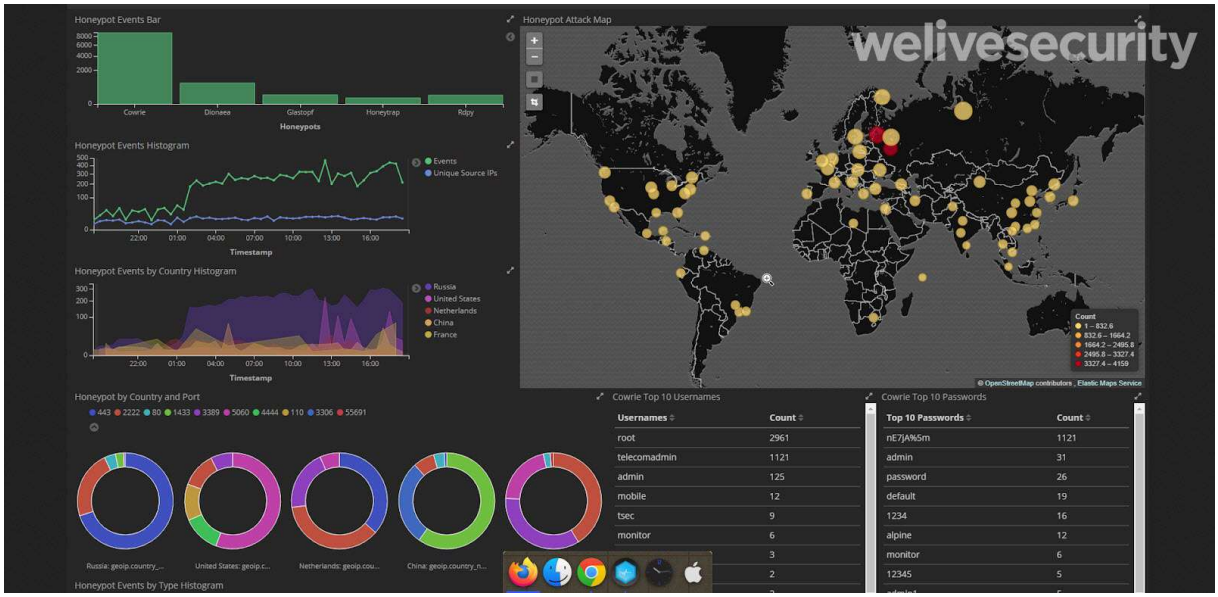


Figura 4. T-POT Porcentajes de plántulas normales en los distintos sustratos

2.2.13. Zona Desmilitarizada (DMZ) en Redes

La DMZ es el entorno ideal para desplegar la honeynet de esta tesis. Al ubicarse entre la red interna de la UPEC y la red externa, permite atraer tráfico malicioso sin comprometer los servicios académicos o administrativos. Esta arquitectura es clave para asegurar que las pruebas se realicen en un entorno realista pero seguro.

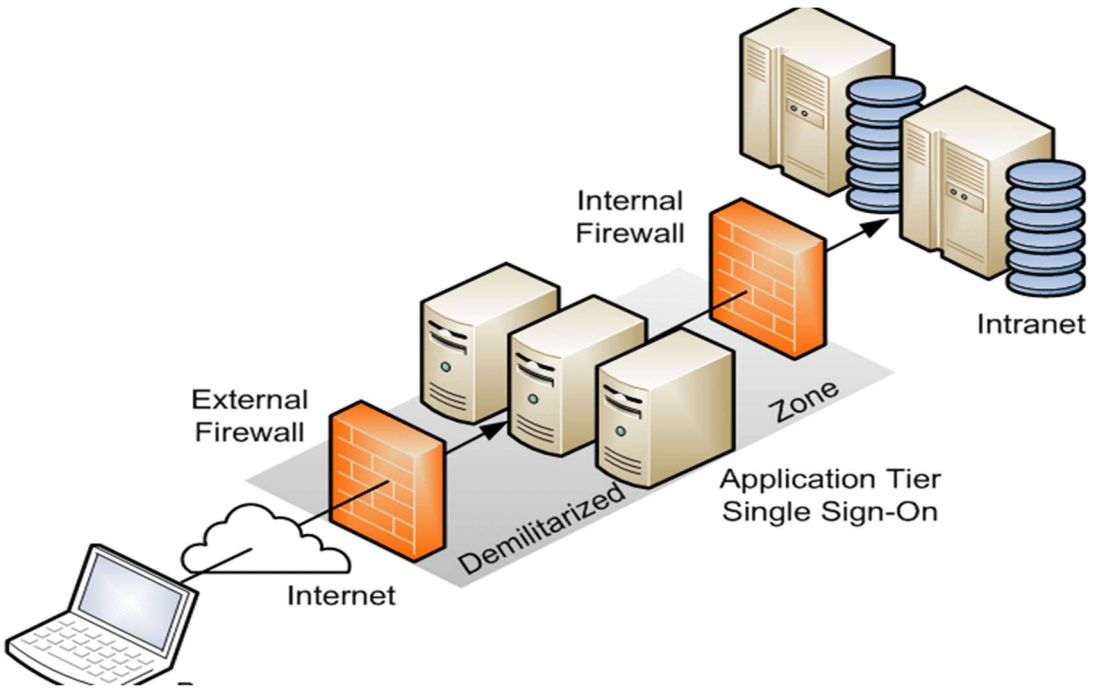


Figura 5. Zona Desmilitarizada (DMZ) en Redes

2.2.14. Monitoreo y Análisis de Seguridad

El monitoreo y análisis de seguridad en redes es un proceso fundamental para detectar y mitigar amenazas cibernéticas. Consiste en la recopilación, evaluación y correlación de datos generados en una infraestructura informática para identificar comportamientos anómalos o accesos no autorizados.

De acuerdo con IEEE Xplore, las tendencias actuales en detección de intrusiones en redes emplean sistemas avanzados basados en aprendizaje automático y minería de datos para mejorar la capacidad de respuesta ante ataques informáticos (IEEE, 2025).

Un enfoque clave en la seguridad es la implementación de herramientas que permitan la detección temprana de amenazas y la correlación de eventos en tiempo real. Sistemas como los de Detección de Intrusos (IDS) y Prevención de Intrusos (IPS) han evolucionado mediante el uso de inteligencia artificial para mejorar su precisión y reducir falsos positivos (Smith et al., 2024).

Además, investigaciones recientes en ciberseguridad han identificado desafíos en la protección de redes, como la creciente sofisticación de los ataques y la necesidad de estrategias de defensa proactivas. Tecnologías como los Honeypots y Honeynets permiten comprender mejor el comportamiento de los atacantes y fortalecer la seguridad de los sistemas en producción (Jones & Patel, 2023).

2.2.15. Implementación y Configuración de un Honeynet

La implementación y configuración de un Honeynet implica el despliegue de una red de honeypots diseñada para atraer y analizar ataques informáticos, proporcionando información valiosa sobre métodos de intrusión. Según IEEE (2024), un enfoque basado en redes definidas por software (SDN) mejora la adaptabilidad y seguridad del Honeynet, permitiendo una mejor detección y respuesta a amenazas. La configuración debe incluir segmentación de red, reglas de monitoreo y registro de actividad maliciosa para optimizar su efectividad en la defensa cibernética.

2.2.16. Componentes para la construcción de un Honeypot

Tabla 8. Componentes para la construcción de un Honeypot

Componente	Especificación	Descripción
Procesador	Intel Core i7 Octava Generación	Un procesador potente como el Intel Core i7 de octava generación garantiza el rendimiento necesario para simular un entorno realista que atraiga a los atacantes. Este tipo de procesadores es ideal para ejecutar simulaciones de ataques avanzados en un honeypot (Cadenas & Pérez, 2019).
Memoria RAM	24 GB	La RAM permite que el honeypot maneje grandes volúmenes de tráfico y múltiples conexiones simultáneas sin perder rendimiento. Un sistema con 24 GB de RAM asegura que el honeypot pueda gestionar múltiples conexiones entrantes sin comprometer la estabilidad del sistema (Martínez & Gómez, 2021).

Tarjeta Gráfica	NVIDIA GTX 1660 Ti o superior	Una tarjeta gráfica potente puede ser útil en un honeypot diseñado para atraer atacantes a través de aplicaciones con interfaces gráficas complejas, como juegos o sistemas visuales de alto rendimiento. Este componente también mejora la capacidad de respuesta del honeypot frente a ataques dirigidos a aplicaciones gráficas (Rodríguez & Sánchez, 2020).
Almacenamiento	500 GB SSD	El SSD permite un rápido acceso a los datos y al sistema operativo, mejorando el tiempo de respuesta del honeypot y facilitando la gestión de grandes volúmenes de información, especialmente en escenarios de tráfico elevado (Torres & Mendoza, 2022).
Sistema Operativo	Linux (Ubuntu, Debian, etc.)	Linux es preferido por su estabilidad, seguridad, facilidad de personalización y amplio soporte en redes y ciberseguridad. La elección de Linux para un honeypot se justifica debido a su robustez frente a ataques y su capacidad para personalizar entornos virtuales complejos (Sánchez & López, 2021).
Red Virtual	VMware, VirtualBox, Docker	La virtualización permite crear un entorno aislado para el honeypot, con múltiples instancias que simulan distintos sistemas operativos y servicios sin afectar la red principal. Este enfoque asegura que el honeypot no interfiera con el

		tráfico legítimo de la red (Fernández & Romero, 2020).
Software de Monitorización	Wireshark, Snort, Suricata	Estas herramientas permiten analizar y monitorear el tráfico de red, identificar intrusos y registrar las actividades de los atacantes para su posterior análisis. Herramientas como Snort y Wireshark son esenciales para detectar patrones de comportamiento maliciosos dentro de los datos del honeypot (González & Pérez, 2019).

2.2.17. Detección y Respuesta ante Incidentes (EDR y XDR)

Detección y Respuesta ante Incidentes (EDR y XDR)

Los sistemas de Detección y Respuesta en Endpoints (EDR) y Detección y Respuesta Extendida (XDR) son tecnologías avanzadas utilizadas en la ciberseguridad para monitorear, detectar y responder ante amenazas en redes y dispositivos finales.

El EDR se enfoca en la supervisión y análisis de eventos en endpoints, como computadoras y servidores, utilizando inteligencia artificial y machine learning para identificar patrones anómalos y posibles ataques.

Este enfoque permite una respuesta rápida y automatizada ante incidentes de seguridad, ayudando a prevenir la propagación de malware y otras amenazas avanzadas (IEEE, 2025)

Por otro lado, XDR amplía las capacidades del EDR al integrar múltiples fuentes de datos, como redes, servidores y aplicaciones en la nube, mejorando la visibilidad y la correlación de eventos en toda la infraestructura de TI. Este enfoque proporciona una defensa más robusta, permitiendo una detección más efectiva y respuestas automatizadas a amenazas complejas en entornos empresariales (IEEE, 2025)

Importancia en la Ciberseguridad

Tabla 9. Importancia en la Ciberseguridad

Aspecto	Descripción
Monitoreo y Análisis en Tiempo Real	Ambos sistemas permiten detectar actividades sospechosas y responder en tiempo real a ataques cibernéticos.
Automatización de Respuestas	Usan inteligencia artificial y machine learning para identificar y neutralizar amenazas sin intervención humana inmediata.
Reducción del Tiempo de Detección y Respuesta	Disminuyen el tiempo entre la identificación de una amenaza y su mitigación, minimizando el impacto de incidentes de seguridad.

2.2.18. Aplicación en Redes Universitarias

La implementación de EDR y XDR en la infraestructura de la Universidad Politécnica Estatal del Carchi podría mejorar la protección de sus servidores y redes, permitiendo una detección más precisa de accesos no autorizados y ataques dirigidos a la institución. Esto garantizaría una respuesta más eficiente ante incidentes de seguridad y fortalecería la protección de datos sensibles.

2.2.19. Estrategia de seguridad

Una estrategia de seguridad en relación con el tema de honeypot se refiere a un plan estructurado de medidas y acciones cuyo objetivo es atraer, detectar y analizar a posibles atacantes dentro de un entorno controlado. En este contexto, el honeypot actúa como una herramienta de defensa activa dentro de la estrategia, diseñada para:

Tabla 10. Funciones del honeypot

Función	Descripción
Engaño a los atacantes	Hace creer a los atacantes que han encontrado un objetivo valioso, mientras interactúan con un sistema trampa.
Obtención de información	Permite recolectar datos sobre las técnicas, herramientas y comportamientos usados por los cibercriminales.
Fortalecimiento de la seguridad de la red	Identifica vulnerabilidades explotadas y patrones de ataque antes de que afecten a los sistemas reales.

2.2.20. Troncal

Una troncal (en inglés, *trunk*) dentro del contexto de redes informáticas es una conexión de alta capacidad que transporta múltiples señales o datos simultáneamente entre distintas redes o segmentos de red. Su función principal es optimizar el tráfico de datos en redes grandes, como las corporativas o de proveedores de servicios, y es clave en la infraestructura de red. (Spafford & Zamboni, 2022).

La troncal puede servir como medio de transporte de datos hacia y desde un honeypot, especialmente si este está implementado en una red compleja o distribuida. Por ejemplo, en una empresa, el honeypot podría estar conectado a la troncal para captar tráfico dirigido a diferentes servicios, permitiendo así detectar amenazas en tiempo real desde distintos puntos de la red (Spafford & Zamboni, 2022).

2.2.21. Dns

El DNS (*Domain Name System*) es un componente esencial de Internet que se encarga de traducir los nombres de dominio comprensibles para los humanos en direcciones IP que las computadoras utilizan para comunicarse entre sí. Este sistema permite a los usuarios acceder fácilmente a sitios web sin necesidad de recordar largas secuencias numéricas. Su correcto funcionamiento es vital para la navegación web, el envío de correos electrónicos y otros servicios de red (Provos & Holz, 2007).

En el ámbito de la ciberseguridad, un honeypot puede configurarse para simular un servidor DNS y así atraer a posibles atacantes. Al actuar como señuelo, permite analizar consultas sospechosas y detectar ataques como el *DNS tunneling*, la generación automática de dominios

(*Domain Generation Algorithms*) o el uso de dominios falsos con fines de phishing. Esta estrategia contribuye a mejorar las defensas al comprender los métodos empleados por los atacantes (Provos & Holz, 2007).

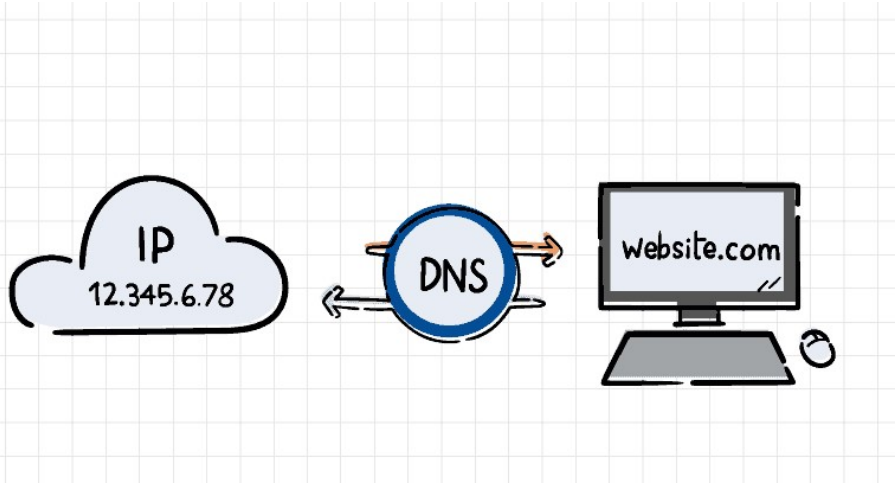


Figura 6. El DNS (Domain Name System)

2.2.22. Ataques A Honeypot

Un honeypot puede ser objetivo de diversos tipos de ataques provenientes del exterior, ya que está diseñado para simular vulnerabilidades atractivas para los atacantes. Entre los más comunes se encuentran los escaneos de puertos, que buscan identificar servicios abiertos; los ataques de fuerza bruta, que intentan adivinar contraseñas; la ejecución de malware para tomar control del sistema; y los intentos de explotación de vulnerabilidades conocidas. También puede recibir ataques de denegación de servicio (DoS) o intentos de acceso remoto no autorizado. Estos ataques permiten registrar el comportamiento del atacante y fortalecer las defensas del sistema real (Spitzner, 2003).

2.2.23. Ip publico

Una dirección IP pública es aquella que es asignada por el proveedor de servicios de internet (ISP) y que permite que un dispositivo sea identificado de manera única en Internet. A diferencia de una IP privada, que solo funciona dentro de redes locales, la IP pública es accesible desde cualquier parte del mundo, lo que permite que servicios como páginas web, servidores de correo o juegos en línea sean visibles y accesibles por otros dispositivos conectados a la red global (Cisco, s.f.). Esta dirección juega un papel fundamental en la comunicación entre redes y en la exposición de servicios en internet.

En el contexto de la ciberseguridad, un honeypot que utiliza una IP pública puede ser desplegado para simular un servidor expuesto a Internet, de forma que atraiga a atacantes reales que escanean redes en busca de vulnerabilidades. Al estar vinculado a una dirección IP pública, el honeypot se vuelve accesible desde cualquier parte del mundo, aumentando la probabilidad de ser detectado por actores maliciosos. Esto permite monitorear sus intentos de acceso, técnicas utilizadas y patrones de ataque, proporcionando información valiosa para mejorar las defensas reales de una organización (Spitzner, 2023).

2.2.24. Ip interno

Una IP interna es una dirección IP asignada a dispositivos dentro de una red local, que no es accesible desde fuera de la red sin el uso de tecnologías como NAT (Network Address Translation). Estas direcciones IP pertenecen a rangos específicos reservados para uso privado, como los bloques 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16. Las IPs internas permiten a los dispositivos dentro de una red local comunicarse entre sí, pero no están directamente expuestas a Internet. Esto ayuda a proteger la red interna de accesos no autorizados desde el exterior, lo cual es esencial en la configuración de sistemas de seguridad, como los honeypots (Cisco, 2025).

Los honeypots, a menudo utilizan IP internas para simular una red vulnerable dentro de una infraestructura de seguridad. Estas IPs internas permiten que los honeypots operen como señuelos, sin exponer directamente las direcciones IP reales de los sistemas de producción. A través de la interacción de los atacantes con estos honeypots, los administradores de seguridad pueden analizar los métodos de ataque y fortalecer las defensas de la red real. Además, el uso de IPs internas ayuda a evitar que los atacantes descubran y comprometan sistemas críticos, ya que las IPs de los honeypots están aisladas del entorno de producción (Imagina Formación, 2021).

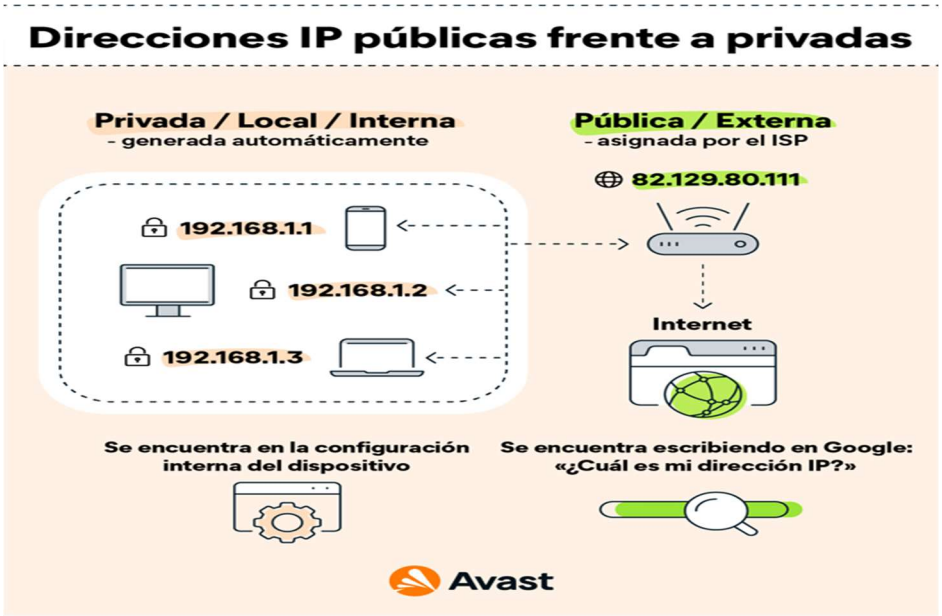


Figura 7. Diferencias IPS

2.2.25. Csirt cedia

El CSIRT CEDIA (Equipo de Respuesta a Incidentes de Seguridad Informática de la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia) es una unidad especializada que tiene como objetivo proteger el entorno tecnológico de sus instituciones miembros, principalmente universidades y centros de investigación en Ecuador (CSIRT CEDIA, s.f.). Su labor incluye la detección temprana de amenazas, gestión de incidentes de seguridad, asesoramiento en buenas prácticas de ciberseguridad, emisión de alertas sobre vulnerabilidades y la capacitación en temas de seguridad informática (CSIRT CEDIA, s.f.).

Además, promueven el desarrollo de políticas internas de seguridad y colaboran en la creación de una cultura de prevención dentro de las organizaciones académicas (CSIRT CEDIA, s.f.).

Un honeypot se relaciona estrechamente con las funciones del CSIRT CEDIA, ya que es una herramienta que simula ser un objetivo vulnerable para los atacantes, con el fin de atraerlos, detectar sus actividades, analizar sus métodos de ataque y mejorar las estrategias de defensa (CSIRT CEDIA, s.f.).

Es decir, un honeypot actúa como "trampa" controlada que permite al CSIRT obtener información valiosa sobre los vectores de ataque actual y futuro.

De esta manera, el CSIRT puede anticiparse a amenazas reales y fortalecer la seguridad de la red de sus afiliados (CSIRT CEDIA, s.f.).

2.2.26. Nmap

Nmap (Network Mapper) es una herramienta de código abierto utilizada para la exploración de redes y auditoría de seguridad. Permite identificar hosts activos, servicios disponibles, sistemas operativos y detectar posibles vulnerabilidades en una red. Su capacidad para realizar escaneos detallados la convierte en una herramienta esencial para profesionales de la ciberseguridad y administradores de sistemas.

En el contexto de los honeypots, Nmap desempeña un papel crucial. Los honeypots son sistemas diseñados para simular vulnerabilidades y atraer a posibles atacantes, con el objetivo de analizar sus comportamientos y técnicas. Al utilizar Nmap en conjunto con honeypots, es posible identificar patrones de ataque, escanear la red en busca de actividades sospechosas y fortalecer las defensas antes de que ocurran incidentes reales.

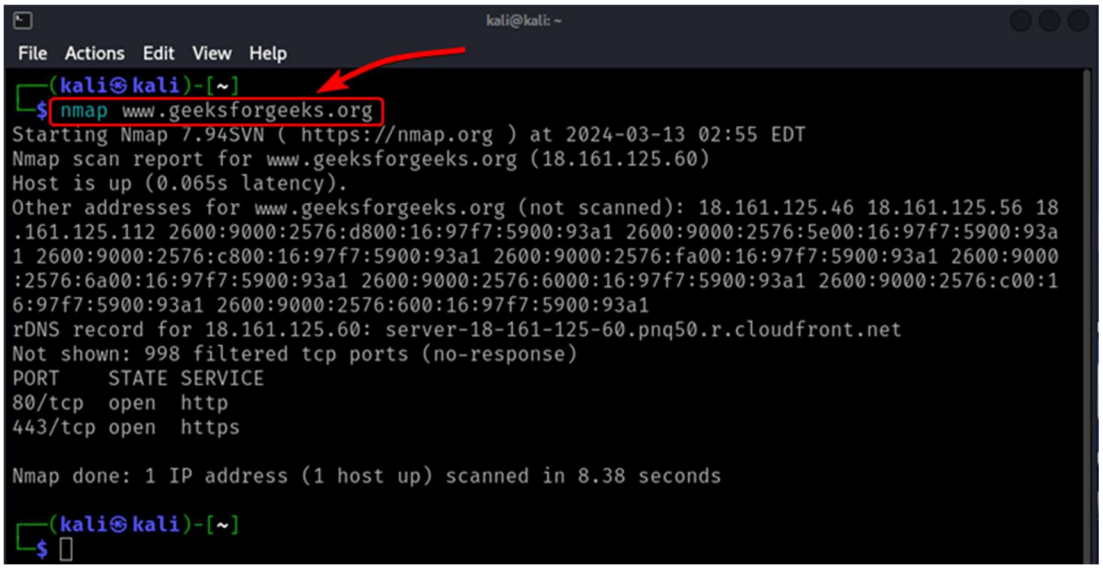


Figura 8. Nmap

2.2.27. Tcp

TCP (Transmission Control Protocol) es un protocolo de comunicación de la capa de transporte que garantiza una transmisión confiable de datos entre dispositivos a través de redes. TCP establece una conexión entre el emisor y el receptor antes de la transmisión de datos, asegurando que los paquetes lleguen de manera ordenada y sin errores, a través de un proceso llamado "handshake" o saludo. Además, se encarga de la retransmisión de los paquetes que no han sido correctamente entregados, lo que hace de TCP uno de los protocolos más utilizados para aplicaciones que requieren alta confiabilidad, como la navegación web o la transferencia de archivos (Tanenbaum & Wetherall, 2011).

En el contexto de un honeypot, el protocolo TCP juega un papel crucial, ya que la mayoría de los ataques cibernéticos se llevan a cabo sobre conexiones TCP. Los honeypots, al simular servicios reales en un entorno controlado, utilizan TCP para establecer conexiones y atraer a los atacantes, simulando servidores y aplicaciones vulnerables. Esta interacción permite a los administradores de seguridad estudiar los métodos y técnicas que los atacantes usan al intentar explotar vulnerabilidades en la red, proporcionando valiosa información para mejorar las defensas de los sistemas reales (Spitzner, 2003).

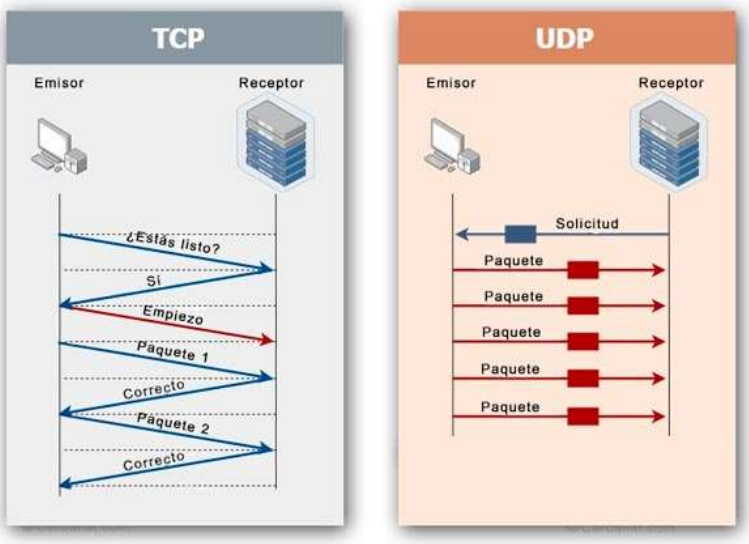


Figura 9. TCP (Transmission Control Protocol)

2.2.28. RAID

RAID (Redundant Array of Independent Disks) es una tecnología que combina varios discos duros en una sola unidad lógica para lograr mejor desempeño, mayor capacidad de almacenamiento o tolerancia a fallos (Red Hat, s.f.). Dependiendo del tipo de configuración (por ejemplo, RAID 0, 1, 5, 10), RAID puede hacer copias de seguridad automáticas de los datos o distribuir la información para optimizar la velocidad de lectura y escritura.:
En el caso de los honeypots, RAID puede ser muy útil porque:

Tabla 11. Funciones del RAID

Función	Descripción
Protección de registros y evidencias	Si el honeypot es atacado, RAID ayuda a que los registros (logs) y las pruebas de ataque se almacenen de manera segura y no se pierdan, incluso si un disco falla.

Mejora del rendimiento	Algunos honeypots recopilan mucha información (tráfico, intentos de conexión, payloads de malware) y necesitan un sistema de almacenamiento rápido y confiable.
Aseguramiento de la continuidad	En ambientes donde el honeypot es una herramienta crítica de monitoreo, RAID ayuda a que el sistema siga funcionando, aunque haya fallos de hardware.

En resumen: un honeypot puede recolectar grandes volúmenes de información sensible sobre ciberataques, y usar RAID garantiza que esos datos estén seguros, disponibles y respaldados.

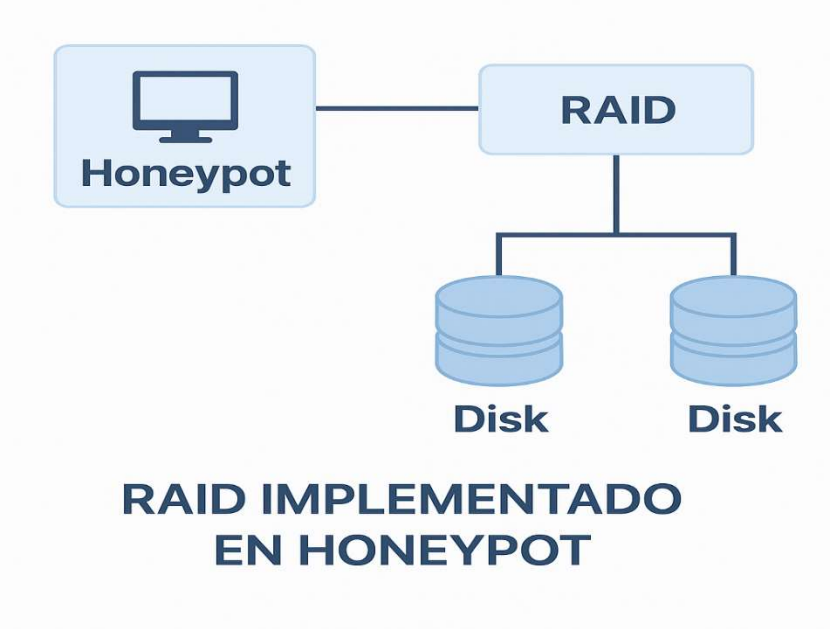


Figura 10. RAID

2.2.29. Protocolo HTTPS

El protocolo HTTPS (HyperText Transfer Protocol Secure) es una versión segura de HTTP que protege la comunicación entre el navegador del usuario y el servidor web mediante el cifrado de datos usando TLS (Transport Layer Security). Este protocolo garantiza que la información transmitida, como credenciales de acceso o datos personales, no pueda ser interceptada o modificada por terceros malintencionados. Además, brinda autenticidad al usuario al verificar que el sitio web es legítimo, lo cual es fundamental para la seguridad en línea (Mozilla Developer Network, s.f.).

Cuando se incorpora el protocolo HTTPS en un honeypot, se busca imitar sitios legítimos con medidas de seguridad actuales, haciendo que la trampa sea más creíble para los atacantes. Esta

combinación permite estudiar amenazas en entornos cifrados y entender mejor las técnicas utilizadas por ciberdelincuentes modernos (Spitzner, 2023).

2.2.30. Cvedetails.com

CVEDetails.com es una plataforma en línea que proporciona una base de datos detallada sobre vulnerabilidades de seguridad informática, conocidas como CVE (Common Vulnerabilities and Exposures), ampliamente usada para identificar, analizar y gestionar vulnerabilidades en diferentes sistemas (SecurityScorecard, s.f.).

La plataforma ofrece información como detalles de cada vulnerabilidad, productos afectados, versiones específicas, puntuaciones CVSS (Common Vulnerability Scoring System), exploits conocidos y alertas actualizadas (SecurityScorecard, s.f.). También permite buscar vulnerabilidades filtradas por proveedor, producto, tipo y fecha, facilitando el análisis de riesgos específicos.

Originalmente desarrollado como un proyecto personal por Serkan Özkan, CVEDetails.com actualmente es operado por SecurityScorecard, empresa que mantiene la base de datos actualizada y en sincronización con fuentes oficiales como el National Vulnerability Database (NVD) (SecurityScorecard, s.f.).

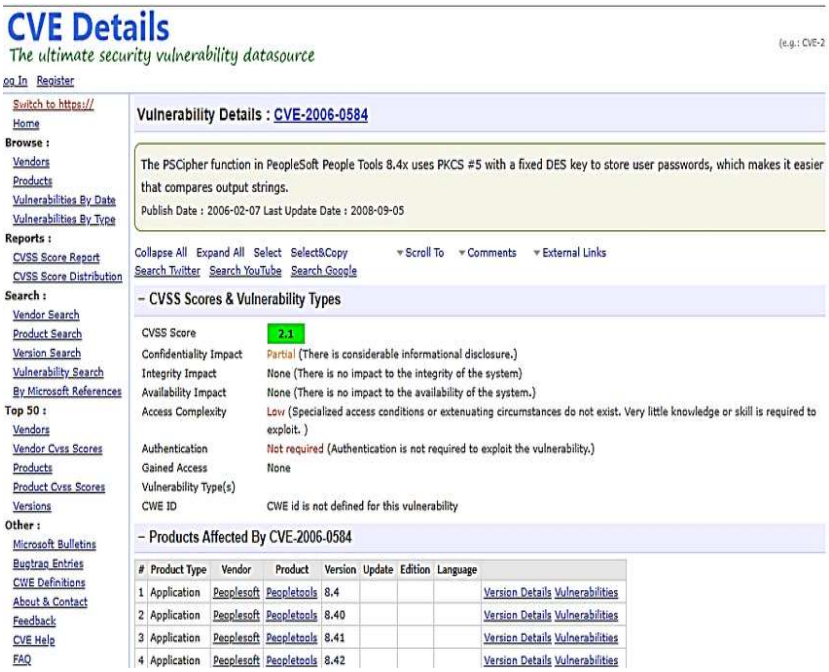


Figura 11. Cv Deteails

2.2.31. Cedia

Según el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA, s.f.), esta organización sin fines de lucro está conformada por universidades e instituciones de investigación de Ecuador, y su misión principal es fortalecer la educación superior, la innovación y la investigación científica en el país. Para ello, CEDIA promueve el uso de tecnologías de información avanzadas, redes académicas de alta velocidad y proyectos colaborativos entre sus miembros, contribuyendo así al desarrollo tecnológico y académico del Ecuador.

CEDIA proporciona servicios de conectividad avanzada y proyectos colaborativos que pueden apoyar técnicamente la implementación de una honeynet. A través de sus recursos en investigación e infraestructura, puede facilitar el acceso a redes académicas seguras, ancho de banda dedicado y soporte técnico especializado, fundamentales para desplegar una honeynet efectiva en una universidad como la UPEC.

2.2.32. Elasticsearch

Elasticsearch es un motor de búsqueda y análisis de datos distribuido que permite almacenar, indexar y buscar grandes volúmenes de datos en tiempo real. Es una herramienta diseñada para facilitar la búsqueda rápida y la gestión eficiente de grandes cantidades de información.

Utilizado ampliamente en aplicaciones de análisis de logs, monitoreo de sistemas y en la gestión de bases de datos no estructurados, Elasticsearch se destaca por su escalabilidad y flexibilidad. A través de su arquitectura distribuida, puede manejar desde pequeñas cantidades de datos hasta petabytes, lo que lo convierte en una opción ideal para sistemas que requieren rapidez y eficiencia en la búsqueda y análisis de datos (Imagina Formación, 2021).

La relación entre Elasticsearch y un honeypot radica en su capacidad para procesar los grandes volúmenes de datos generados por el honeypot. Los honeypots, diseñados para atraer y detectar atacantes, producen información clave sobre tácticas y técnicas de ataque.

Elasticsearch facilita el almacenamiento y la indexación de esta información, permitiendo a los analistas de seguridad buscar y analizar los datos rápidamente. Combinado con herramientas de visualización como Kibana, Elasticsearch proporciona dashboards interactivos que permiten una visualización clara y eficiente de los patrones de ataque, ayudando a los equipos de seguridad a tomar decisiones informadas y mejorar las defensas (Pohl, 2021).

Dentro de la honeynet, Elasticsearch es esencial para el procesamiento, almacenamiento y análisis de los grandes volúmenes de datos generados por los honeypots.

Su integración permite que los datos capturados por la honeynet (como logs de ataques o patrones de comportamiento malicioso) sean indexados y visualizados eficientemente, lo que mejora el análisis forense y la toma de decisiones en ciberseguridad dentro de la DMZ.

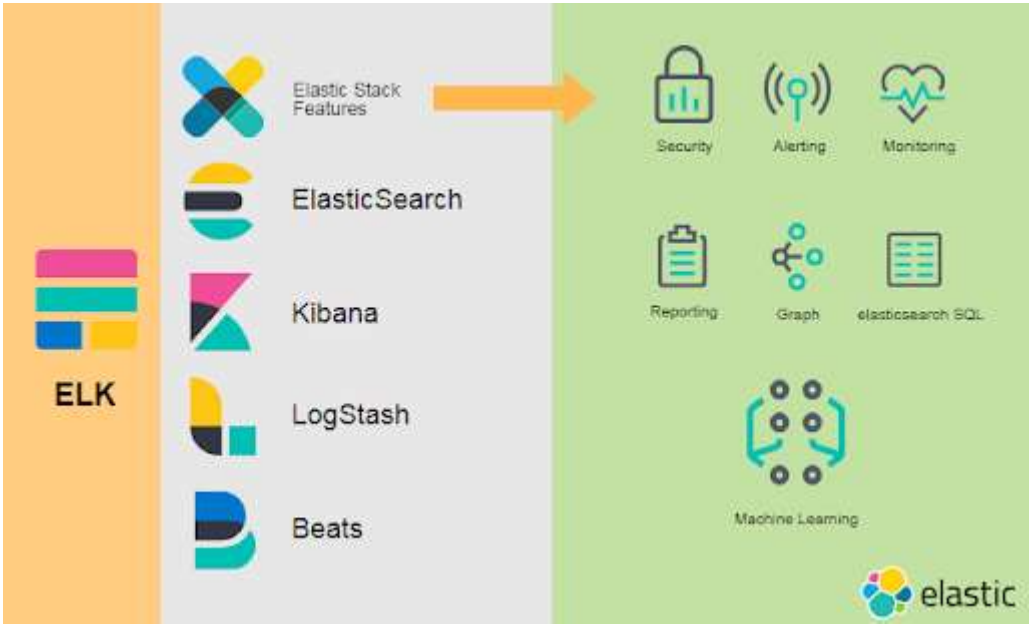


Figura 12. ElasticSerarch

2.2.33. Dashboard

"Los dashboards son herramientas que permiten compartir, agrupar, centralizar y proporcionar una visualización gráfica de la información relevante de una organización, facilitando la toma de decisiones" (Córdova Viera, Martínez Borrego & Córdova Viera, 2021, p. 56).

Esta definición proviene del artículo titulado Propuesta de metodología para el diseño de dashboard, publicado en la Revista Cubana de Transformación Digital, una publicación académica indexada en AmeliCA.

Un dashboard visualiza los datos recolectados por la honeynet en tiempo real. Esta herramienta es fundamental para que los analistas de la UPEC puedan interpretar rápidamente las amenazas detectadas, su frecuencia, tipo de ataque, origen, entre otros, facilitando la gestión de incidentes desde un entorno centralizado.

2.2.34. Centos 7

CentOS 7 es una distribución de Linux de código abierto y gratuito, basada en Red Hat Enterprise Linux (RHEL), diseñada para servidores y entornos empresariales. Es conocida por su estabilidad, seguridad y soporte a largo plazo, lo que la convierte en una opción popular para infraestructuras críticas. CentOS 7 incluye herramientas y servicios como SELinux, firewalld y systemd, que permiten una administración robusta y segura del sistema (Imagina Formación, 2021).

En el contexto de ciberseguridad, CentOS 7 es una plataforma adecuada para implementar honeypots, sistemas diseñados para atraer y estudiar a atacantes. Por ejemplo, se puede desplegar un honeypot SSH interactivo utilizando Cowrie, un software de código abierto que emula un servidor SSH vulnerable. Al instalar Cowrie en CentOS 7, se puede registrar información sobre intentos de acceso y comandos ejecutados por atacantes, proporcionando datos valiosos para el análisis de amenazas. Además, herramientas como T-Pot integran múltiples honeypots en una sola plataforma, facilitando la detección y análisis de ataques (Issa, 2024).

CentOS 7 sirve como sistema operativo base para desplegar honeypots o herramientas de análisis dentro de la honeynet. Su estabilidad y compatibilidad con software de ciberseguridad como Cowrie o T-Pot lo hacen ideal para entornos de producción y pruebas dentro de la DMZ universitaria.

Figura 13. CentOS 7

2.2.35. Cisco talos

Cisco Talos es el equipo de inteligencia de amenazas de Cisco, compuesto por expertos dedicados a identificar, analizar y mitigar amenazas cibernéticas a nivel global. Talos se enfoca en ofrecer protección avanzada mediante la recopilación y análisis de datos de amenazas en tiempo real, lo que fortalece las soluciones de seguridad de Cisco y contribuye a la comunidad de ciberseguridad. Su misión es mejorar la seguridad de los productos de Cisco y proporcionar inteligencia procesable que ayuda a prevenir y responder a incidentes de seguridad (Cisco, 2025).

La relación entre Cisco Talos y los honeypots radica en que Talos utiliza sistemas como honeypots para detectar, analizar y comprender los comportamientos de los atacantes. Los honeypots actúan como señuelos que atraen a los atacantes, permitiendo a Talos observar sus métodos y tácticas. Esta información es crucial para mejorar las defensas de seguridad y compartir inteligencia sobre nuevas amenazas. Además, Talos se encarga de la investigación de vulnerabilidades y el análisis de malware, muchas veces obteniendo datos a través de ataques simulados mediante honeypots, lo que les permite anticiparse a posibles riesgos y ataques en el mundo real (Cisco, 2025).

Cisco Talos proporciona inteligencia de amenazas que puede ser utilizada como referencia para configurar las reglas de detección en la honeynet. También emplea honeypots para mejorar sus análisis, por lo que representa un modelo de cómo una infraestructura de inteligencia puede complementarse con honeynets como la que se pretende implementar en la UPEC.

2.2.36. Login ssh

El *login SSH* (Secure Shell) es un protocolo de red que permite a los usuarios acceder de forma segura a un sistema remoto mediante una conexión cifrada. Se utiliza comúnmente para administrar servidores y sistemas de forma remota, garantizando la confidencialidad e integridad de la información transmitida (Stallings, 2017).

La mayoría de honeypots interactivos simulan servicios SSH, que son frecuentemente atacados. El monitoreo de intentos de acceso vía SSH permite recolectar datos sobre credenciales forzadas, comandos ejecutados y orígenes de ataques. Esto es clave para el estudio de amenazas reales dirigidas a los servidores de la universidad.

2.2.37. Putin

Putin es un término incorrecto o mal escrito, probablemente te refieres a *PuTTY*, que es un cliente de terminal gratuito y de código abierto para conexiones remotas a través de protocolos como SSH, Telnet, rlogin y otros. PuTTY facilita la conexión y gestión de sistemas remotos desde una interfaz gráfica (Williams, 2020).

PuTTY es útil para los administradores al momento de conectarse remotamente a los honeypots desplegados en la DMZ. Esta herramienta permite gestionar y revisar el comportamiento del honeypot desde una estación segura, facilitando la administración remota de los nodos.

2.2.38. Backups

Los *backups* o copias de seguridad son procesos de duplicación y almacenamiento de datos que permiten preservar información en caso de pérdida, daño o fallo del sistema original. Constituyen una práctica esencial para la protección y recuperación de datos en entornos informáticos (Kim & Solomon, 2016).

Las copias de seguridad son esenciales para mantener la integridad de la información recolectada por la honeynet. Dado que estos sistemas pueden ser atacados intencionalmente, realizar backups periódicos garantiza que los datos no se pierdan y se pueda continuar con el análisis de incidentes sin interrupciones.

2.2.39. Auto Logout

El auto logout o cierre automático de sesión es una medida de seguridad que finaliza la sesión de un usuario tras un periodo de inactividad para evitar accesos no autorizados. Esta práctica ayuda a proteger datos sensibles y minimizar los riesgos de intrusión en sistemas críticos (Microsoft, 2023).

La función de auto logout incrementa la seguridad de los sistemas de administración de la honeynet. Al implementar esta medida en las estaciones desde donde se monitorean los honeypots, se previene el acceso no autorizado en caso de inactividad del operador.

2.2.40. Shodan

Shodan es un motor de búsqueda especializado en encontrar dispositivos conectados a Internet, tales como cámaras de seguridad, servidores o routers, recopilando información técnica como puertos abiertos y servicios activos, en lugar de páginas web (Xataka, 2022). Esta herramienta

es fundamental en ciberseguridad para identificar vulnerabilidades expuestas y monitorear dispositivos públicos.

En relación con los honeypots, Shodan puede ser utilizado tanto para detectar sistemas señuelo desplegados en Internet como para verificar si un honeypot ha sido expuesto accidentalmente (Shodan, s.f.). A través de servicios como HoneyScore, los investigadores analizan si una IP corresponde a un posible honeypot, lo que permite ajustar su configuración para mantener la efectividad del engaño y la recolección de datos de ataques reales.

Shodan puede utilizarse para verificar si alguno de los honeypots está siendo detectado por herramientas públicas, lo cual podría comprometer su efectividad. También permite a los investigadores de la UPEC validar si su red DMZ presenta servicios expuestos accidentalmente, permitiendo ajustar la configuración de la honeynet.

2.2.41. Escala de privilegios

La escala de privilegios (o elevación de privilegios) es una técnica utilizada por atacantes para obtener niveles de acceso más altos dentro de un sistema que los que originalmente poseen. Esto puede implicar pasar de un usuario estándar a un administrador, o de un proceso de baja seguridad a uno con mayores permisos, permitiendo así ejecutar acciones más críticas o acceder a información sensible (MITRE, 2024).

Uno de los objetivos de los honeypots es observar intentos de escala de privilegios. Esta técnica es común en ataques avanzados, y su análisis dentro de la honeynet permite entender cómo los atacantes intentan comprometer sistemas de la red interna de la universidad, brindando información valiosa para prevenir ataques reales.

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

Enfoque Metodológico

La presente investigación adopta un enfoque mixto, integrando los métodos cualitativo **y** cuantitativo con el objetivo de analizar de manera integral la implementación de una Honeynet en la seguridad informática de la Universidad Politécnica Estatal del Carchi. Este enfoque permite recopilar, analizar y relacionar tanto datos numéricos como información descriptiva, asegurando una comprensión más profunda del fenómeno estudiado.

Enfoque Cuantitativo

El enfoque cuantitativo se fundamenta en la recolección y análisis de datos medibles a través de técnicas estructuradas, lo que facilita la evaluación de tendencias, patrones y correlaciones dentro del ámbito de la seguridad informática. Para ello, se empleará la aplicación de encuestas dirigidas a administradores de redes y expertos en ciberseguridad dentro de la universidad, con el propósito de obtener información cuantificable sobre la percepción y efectividad del uso de Honeynets en la detección de intrusos.

Además, se utilizarán métricas de seguridad, como la cantidad de intentos de acceso no autorizado detectados, los tipos de ataques registrados y el tiempo de respuesta ante incidentes. La recopilación de estos datos permitirá realizar un análisis estadístico para evaluar el impacto del sistema implementado y determinar su efectividad en la protección de los servidores de la institución.

Enfoque Cualitativo

Por otro lado, el enfoque cualitativo se aplicará en el análisis y exploración de información relevante sobre las técnicas de ataque utilizadas por los intrusos dentro de la Honeynet. Este análisis se llevará a cabo mediante un estudio de caso, permitiendo describir detalladamente el comportamiento de los atacantes, los métodos que emplean y las vulnerabilidades que intentan explotar dentro del sistema de la universidad.

Asimismo, el enfoque cualitativo facilitará la interpretación de los datos obtenidos, identificando patrones de ataque y proporcionando información clave para mejorar la seguridad de la red institucional. Se realizará una revisión documental de investigaciones previas relacionadas con Honeynets y ciberseguridad, con el fin de contextualizar los hallazgos dentro de un marco teórico sólido.

Importancia del Enfoque Mixto

La combinación de estos dos enfoques resulta fundamental para obtener un análisis más robusto y confiable. Mientras que el enfoque cuantitativo permite medir el impacto y la efectividad del sistema implementado, el enfoque cualitativo contribuye a comprender en profundidad las dinámicas de los ataques informáticos y su evolución.

En este sentido, la implementación de la Honeynet no solo permitirá mejorar la seguridad de la universidad, sino que también brindará información valiosa para el desarrollo de estrategias de defensa más efectivas. La complementariedad entre los datos numéricos y la interpretación cualitativa garantizará una evaluación más precisa y completa, asegurando la validez y pertinencia de los resultados obtenidos en la investigación.

3.1.2. Tipo de Investigación

Para esta tesis sobre la implementación de Honeynets en la seguridad informática de una universidad, se pueden aplicar varios tipos de investigación, dependiendo del enfoque, los métodos y los objetivos planteados. A continuación, se describen los más relevantes:

Investigación Exploratoria

Justificación: Este tipo de investigación permite obtener un panorama inicial sobre el uso de Honeypots y Honeynets en la seguridad informática. Dado que el tema puede no estar ampliamente estudiado en el contexto específico de la universidad, se requiere un análisis preliminar para identificar los desafíos y oportunidades de su implementación (Hernández Sampieri et al., 2022).

Investigación Descriptiva

Justificación: Se centra en detallar las características, funcionamiento y aplicación de las Honeynets. Es útil para definir cómo operan estos sistemas y cómo pueden mejorar la seguridad informática, proporcionando datos sobre patrones de ataques y vulnerabilidades comunes en entornos académicos (Biswas, 2020).

Investigación Explicativa

Justificación: Permite analizar la relación causa-efecto entre la implementación de una Honeynet y el incremento en la seguridad y monitoreo de servidores en producción. Ayuda a entender cómo este sistema contribuye a la identificación de amenazas y al fortalecimiento de estrategias de ciberseguridad (Provos & Holz, 2020).

Investigación Experimental

Justificación: En caso de implementar y probar una Honeynet en la universidad, este tipo de investigación sería clave para medir su impacto en la detección de ataques. Se pueden establecer pruebas controladas, variando configuraciones y escenarios para evaluar la efectividad de la herramienta (Spitzner, 2021).

Investigación Aplicada

Justificación: Dado que el objetivo es mejorar la seguridad informática mediante la implementación de una Honeynet, esta investigación busca generar soluciones prácticas y aplicables en un entorno real. Es decir, no solo se estudiará el concepto, sino que se llevará a cabo su puesta en marcha para solucionar un problema específico (Chirillo & Blaul, 2022).

Investigación Cuantitativa

Justificación: Se utilizarán datos estadísticos sobre intentos de ataque detectados, frecuencia de eventos de seguridad y métricas de rendimiento de la Honeynet. Este enfoque permitirá medir objetivamente la efectividad de la herramienta implementada (Zhuge et al., 2021).

Investigación Cualitativa

Justificación: Además del análisis de datos numéricos, es necesario evaluar las percepciones de los administradores de sistemas y expertos en seguridad informática sobre el impacto de la Honeynet en la protección de la red universitaria. Se pueden realizar entrevistas o encuestas para comprender su experiencia y opiniones (Mokube & Adams, 2022).

Investigación Documental

Justificación: Se revisarán antecedentes, estudios previos y literatura científica sobre Honeypots, Honeynets y seguridad informática para fundamentar teóricamente la investigación y contextualizar los hallazgos en el marco de trabajos previos (Hernández Sampieri et al., 2022).

En conclusión, esta tesis puede abordar múltiples enfoques metodológicos, combinando técnicas cualitativas y cuantitativas, así como exploraciones teóricas y experimentales. La selección de estos tipos de investigación garantizará un análisis integral de la implementación de *Honeynets* en la seguridad informática universitaria.

3.2. IDEA A DEFENDER

La implementación estratégica de una Honeynet en la zona desmilitarizada de la red de la Universidad Politécnica Estatal del Carchi es una solución viable y eficaz para fortalecer la ciberseguridad institucional, permitiendo identificar patrones de ataque, anticiparse a amenazas emergentes y optimizar la protección de los sistemas de información en un entorno académico vulnerable.

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES

Variables de la Investigación

Variable Dependiente: Nivel de seguridad de la red institucional

La variable dependiente en esta investigación es el nivel de seguridad de la red institucional de la Universidad Politécnica Estatal del Carchi. Esta variable está condicionada por la implementación de una red espejo virtual **(**Honeynet**)**, cuya configuración influye en la precisión y efectividad de la identificación de accesos no autorizados. La capacidad de la plataforma *T-Pot* para registrar, analizar y clasificar los intentos de ataque determinará el impacto de la *Honeynet* en la seguridad de la red universitaria. En este contexto, el grado de configuración y calibración de la herramienta afecta directamente la detección de amenazas y su posterior análisis para mejorar la seguridad informática.

Variable Independiente: Implementación y configuración de una honeynet en la zona desmilitarizada (DMZ)

La variable independiente en este estudio es la implementación y configuración de una Honeynet, la cual será gestionada y manipulada por los investigadores. Esta variable tiene existencia propia y se ajustará en función de los objetivos del estudio, ya que la estrategia utilizada en la simulación y monitoreo de ataques cibernéticos tendrá un impacto directo en la variable dependiente. A través del despliegue de Honeynets, se espera analizar el

comportamiento de los atacantes, identificar patrones de intrusión y proponer mejoras en la infraestructura de seguridad de la universidad.

Tabla 12. Operacionalización de la variable independiente

Variable	Definición	Dimensión	Indicador	Técnica	Instrumento
		Diseño de la infraestructura	- Cantidad y tipo de honeypots implementados- Segmentación de red aplicada- Herramientas de monitoreo configuradas	Revisión documental, Observación	Ficha técnica Esquema de red
Implementación y configuración de una honeynet en la zona desmilitarizada (DMZ)	Una honeynet es una red de sistemas deliberadamente vulnerables diseñada para atraer y analizar ataques informáticos sin comprometer la red interna.	Seguridad de la red	- Nivel de aislamiento de la DMZ- Capacidad de detección de amenazas- Número de eventos de intrusión capturados	Análisis de registros, Entrevistas	Bitácora de eventos Cuestionario
		Funcionamiento de los honeypots	- Actividad maliciosa registrada- Frecuencia de interacción con atacantes- Tipos de ataques detectados	Monitoreo, Análisis de logs	Reportes del sistema Dashboard de T-Pot
		Capacidad de respuesta	- Tiempo medio de detección- Tiempo de respuesta del sistema ante ataques- Aplicación de medidas correctivas	Entrevista, Revisión documental	Cuestionario Informe técnico

Tabla 13. Operacionalización de la variable dependiente

Variable	Definición	Dimensión	Indicador	Técnica	Instrumento
		Detección de amenazas	Número de eventos detectados- Precisión del sistema en identificar accesos sospechosos	Análisis de registros	Bitácora de eventos
Nivel de seguridad de la red institucional	Estado de protección de los activos, servicios y comunicaciones de la red universitaria frente a accesos no autorizados, ataques y fallos.	Integridad de los sistemas	Alteraciones en sistemas críticos- Frecuencia de intentos de modificación	Revisión documental, Monitoreo	Informe técnicoLogs de seguridad
		Continuidad operativa	Tiempo de disponibilidad de servicios- Interrupciones por amenazas externas	Entrevista a responsables de red	Cuestionario
		Tiempo de respuesta ante incidentes	Tiempo medio de respuesta- Protocolos de contención activados	Entrevista, Simulación de incidentes	Registro de incidentes Encuesta

Hasta el momento, no se ha establecido un método estandarizado para el diseño y simulación de una red Honeynet, por lo que se ha optado por desarrollar una metodología propia, adaptada a las necesidades y particularidades de la infraestructura de la Universidad Politécnica Estatal del Carchi (UPEC).

Dado que la implementación se realizará en un entorno virtual, no se efectuarán modificaciones en los servidores actuales, garantizando así la seguridad y estabilidad de la red en producción. En este sentido, el proceso metodológico se estructurará en cuatro fases:

Fase 1: Análisis y Diseño Lógico de la Red Actual

Se llevará a cabo un estudio detallado de las herramientas de seguridad virtualizadas utilizadas en la Oficina del Sistema de TIC de la UPEC, así como un análisis de los equipos disponibles y de los tipos de ataques más frecuentes a los que está expuesta la infraestructura. Toda esta información se documentará en un informe técnico, que servirá como base para el diseño lógico de la red existente.

Fase 2: Diseño Lógico de la Solución Propuesta

En esta fase, se definirán los servicios de red que ofrecerá la Honeynet, detallando los procesos de simulación del modelo y los mecanismos de análisis de vulnerabilidades en los servicios y aplicaciones utilizadas en la red universitaria. Se establecerán los protocolos de seguridad y las estrategias de respuesta ante posibles intentos de intrusión.

Fase 3: Simulación del Diseño Lógico

Se procederá a la implementación virtual de la red Honeynet, ejecutando pruebas generales para evaluar su funcionamiento y la capacidad del sistema para detectar y registrar actividades sospechosas. Se verificarán la efectividad de los sensores de monitoreo y los mecanismos de alerta, garantizando que el diseño propuesto cumpla con los objetivos de la investigación.

Fase 4: Elaboración del Diagrama de Procesos

En esta última fase, se realizará un análisis detallado de los procesos internos de la Honeynet, estableciendo la complejidad de los algoritmos utilizados en la detección y clasificación de amenazas. La representación gráfica de los procesos facilitará la interpretación del flujo de datos y permitirá optimizar el desempeño del sistema de monitoreo.

Con esta metodología estructurada, se busca proporcionar una solución efectiva para el análisis de ataques informáticos y la mejora continua de las estrategias de seguridad dentro de la universidad.

3.4. MÉTODOS UTILIZADOS

3.4.1.1. Método analítico

El método analítico se caracteriza por permitir descomponer el problema de investigación en todas sus partes, con el objetivo de estudiar y analizar por separado cada una de ellas (Neill y Cortez, 2018).

En la presente investigación se aplicó el método analítico al desglosar los distintos componentes relacionados con la implementación de honeypots y honeynets como herramientas de ciberseguridad. Se estudiaron individualmente los elementos técnicos como la arquitectura de red institucional, la configuración de entornos virtuales, los sistemas de monitoreo y análisis de tráfico, así como los protocolos de respuesta ante incidentes. Este enfoque permitió comprender con mayor profundidad las debilidades existentes en la red de la Universidad Politécnica Estatal del Carchi, así como las características y beneficios de las tecnologías honeynet para mitigar riesgos asociados a ciberataques.

3.4.1.2. Método sintético

El método sintético parte del analítico, ya que posterior al análisis de cada una de las partes permite relacionarlas para plantear una conclusión (Neill y Cortez, 2018).

Este método fue empleado para integrar los distintos conocimientos adquiridos durante el análisis teórico y práctico de los componentes estudiados. La información obtenida fue sintetizada para proponer una solución tecnológica integral, enfocada en el fortalecimiento de la seguridad perimetral de la universidad mediante la implementación de una honeynet en la zona desmilitarizada (DMZ). De esta manera, se estableció la relación entre las vulnerabilidades identificadas en la red y las capacidades de los honeypots para capturar y analizar comportamientos maliciosos, lo cual orientó el diseño final de la propuesta de seguridad y su validación a través de simulaciones de intrusión controladas.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

4.1.1 PROPUESTA

La presente propuesta consiste en diseñar e implementar una Honeynet dentro de la zona desmilitarizada (DMZ) de la infraestructura de red de la Universidad Politécnica Estatal del Carchi, con el propósito de fortalecer su sistema de ciberseguridad y permitir la detección temprana de ataques informáticos. Esta solución tecnológica simulará vulnerabilidades reales para atraer posibles amenazas y registrar su comportamiento, sin comprometer los sistemas operativos en producción.

La propuesta contempla la integración de herramientas especializadas como Nmap para el escaneo de puertos, CVE Details para la identificación de vulnerabilidades conocidas, y ELK Stack para el monitoreo, análisis y visualización de eventos en tiempo real. Estas herramientas permitirán automatizar la recolección de datos sobre accesos no autorizados y patrones de ataque, facilitando así la toma de decisiones informadas en materia de seguridad informática.

La implementación de esta Honeynet busca dotar a la universidad de una solución adaptable a su infraestructura actual, escalable para futuras ampliaciones, y capaz de actuar como un sistema de alerta temprana ante intentos de intrusión. Al mismo tiempo, pretende servir como una plataforma de análisis e investigación en el ámbito académico, fomentando la formación práctica en ciberseguridad para estudiantes y personal técnico.

Con esta propuesta se espera no solo reforzar la protección de la información institucional, sino también sentar las bases para una cultura organizacional orientada a la seguridad digital,

promoviendo el uso de tecnologías avanzadas como parte de las buenas prácticas de gestión de riesgos en entornos educativos.

4.1.1.2 Introducción

TÍTULO: Diseño e Implementación de una Honeynet en la Zona Desmilitarizada (DMZ) de la Universidad Politécnica Estatal del Carchi como Estrategia de Fortalecimiento de la Ciberseguridad Institucional

En un mundo donde las amenazas informáticas evolucionan constantemente, las instituciones educativas han dejado de ser simples entes académicos para convertirse en custodios de vastas cantidades de información crítica. Las universidades manejan datos sensibles sobre estudiantes, personal académico, administrativo, investigaciones y estrategias institucionales. Esta realidad las convierte en blancos atractivos para actores maliciosos.

La Universidad Politécnica Estatal del Carchi (UPEC), consciente de los desafíos de la era digital, ha desarrollado infraestructura tecnológica para apoyar sus procesos académicos y administrativos. Sin embargo, la sofisticación de los ataques actuales exige soluciones innovadoras que trasciendan las barreras perimetrales tradicionales. Por ello, esta propuesta plantea la implementación de una Honeynet en la zona desmilitarizada (DMZ) de su red, como parte integral de una estrategia de ciberseguridad avanzada.

Una Honeynet consiste en un conjunto de honeypots que simulan vulnerabilidades reales con el fin de atraer posibles atacantes, registrando sus acciones dentro de un entorno controlado. La información recolectada facilita la identificación de vectores de ataque, la elaboración de inteligencia de amenazas y la implementación de políticas de protección más efectivas.

Este documento presenta una propuesta detallada para el diseño e implementación de una Honeynet adaptada a la infraestructura de la UPEC. Se integran herramientas especializadas como Nmap, CVE Details y ELK Stack para la detección, análisis y visualización de eventos de seguridad.

METODOLOGÍA DE DESARROLLO: METODOLOGÍA EN CASCADA

Para la ejecución del presente proyecto se ha optado por utilizar la Metodología en Cascada, un enfoque de desarrollo secuencial y estructurado que permite una clara delimitación de fases y objetivos. Este modelo resulta especialmente adecuado para proyectos donde se puede establecer una planificación detallada desde un inicio y cada fase depende de la finalización de la anterior.

La metodología en cascada se compone de las siguientes fases:

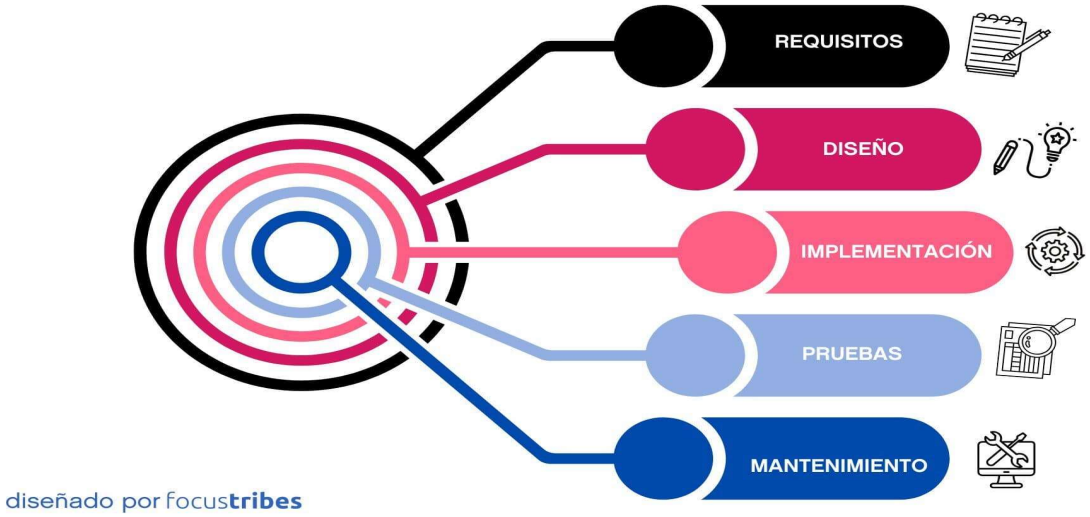


Figura 14.METODOLOGÍA DE DESARROLLO: METODOLOGÍA EN CASCADA

4.1. Fase I: Recolección y Análisis de Requisitos

La fase de recolección y análisis de requisitos constituye una etapa fundamental en el proceso de diseño e implementación de la Honeynet, ya que permite establecer una base sólida para su desarrollo, alineada con las necesidades específicas de la Universidad Politécnica Estatal del Carchi (UPEC). Para ello, se adoptó un enfoque metodológico mixto que combinó la investigación documental con el levantamiento de información directa a través de diversas técnicas cualitativas.

En primera instancia, se llevaron a cabo reuniones estructuradas con los responsables de la infraestructura tecnológica de la UPEC, lo cual permitió conocer de manera detallada la arquitectura actual de la red institucional, los niveles de segmentación implementados, y las políticas de seguridad existentes en la zona desmilitarizada (DMZ). Estos encuentros facilitaron la identificación de limitaciones técnicas, así como la disponibilidad de recursos físicos y virtuales para la implementación del sistema.

Paralelamente, se realizó un análisis exhaustivo de la documentación técnica institucional, incluyendo diagramas de red, manuales de configuración, informes de auditoría interna y registros de incidentes de seguridad. Esta información proporcionó un contexto operativo relevante para comprender el entorno en el que se desplegará la Honeynet, permitiendo anticipar posibles interferencias o incompatibilidades.

Adicionalmente, se llevaron a cabo entrevistas semiestructuradas con docentes del área de redes y seguridad informática, así como con expertos en ciberseguridad, cuyo aporte resultó clave para definir los requerimientos funcionales y no funcionales del sistema. Entre los aspectos abordados se destacan la selección de herramientas de monitoreo y análisis, los niveles de interacción deseados en los honeypots, las estrategias de contención de amenazas, y los mecanismos de recolección de datos para investigación académica.

Como resultado de este proceso, se determinaron las configuraciones técnicas necesarias, las capacidades mínimas del hardware y software involucrado, así como los criterios de escalabilidad y sostenibilidad del proyecto. Asimismo, se identificaron riesgos potenciales asociados a la exposición controlada de servicios simulados, entre los cuales destacan la posibilidad de evasión del sistema por parte de atacantes avanzados, la sobrecarga de recursos por ataques intensivos, y el mal uso de la infraestructura con fines no académicos.

En conclusión, esta fase permitió definir con claridad los requerimientos que guiarán la arquitectura, el diseño lógico y físico, y la posterior implementación de la Honeynet, asegurando su alineación con los objetivos institucionales de fortalecimiento de la ciberseguridad y generación de conocimiento aplicado.

Tabla 14. Recolección y Análisis de Requisitos

Categoría	**Descripción**
Enfoque metodológico	Enfoque mixto: investigación documental y técnicas cualitativas (reuniones, entrevistas).
Reuniones técnicas	Con responsables de infraestructura de la UPEC. Identificación de arquitectura de red, segmentación, políticas de seguridad y recursos disponibles en la DMZ.
Análisis documental	Revisión de diagramas de red, manuales de configuración, informes de auditoría e incidentes de seguridad.
Entrevistas con expertos	Docentes de redes y seguridad, especialistas en ciberseguridad. Definición de requerimientos funcionales y no funcionales.

Aspectos abordados	Selección de herramientas (Nmap, ELK Stack), niveles de interacción en honeypots, estrategias de contención, recolección de datos para investigación académica.
Configuraciones técnicas	Requisitos de hardware/software, topología de red, criterios de escalabilidad y sostenibilidad.
Riesgos identificados	Evasión por parte de atacantes avanzados, sobrecarga de recursos por ataques masivos, mal uso de infraestructura con fines no académicos.
Resultado general	Definición clara de los requerimientos que guían la arquitectura lógica y física de la Honeynet, alineada con los objetivos institucionales de ciberseguridad y docencia aplicada.

4.2. Fase II: Diseño del Sistema

Una vez completado el proceso de recolección y análisis de requisitos, se procedió al diseño integral de la Honeynet, abarcando tanto los aspectos lógicos como físicos del sistema. Esta fase resultó determinante para garantizar que la arquitectura propuesta cumpla con los objetivos de detección, monitoreo y análisis de actividades maliciosas, sin comprometer la seguridad ni la operatividad de la red institucional de la Universidad Politécnica Estatal del Carchi (UPEC).

En primer lugar, se definió la topología de red de la Honeynet, la cual se integró de manera controlada dentro de la zona desmilitarizada (DMZ) de la infraestructura tecnológica de la UPEC. Esta topología adoptó un enfoque de segmentación lógica y aislamiento, con el fin de evitar que cualquier interacción maliciosa dentro del entorno de honeypots afecte los sistemas productivos. Se establecieron VLANs dedicadas y reglas estrictas en los firewalls para controlar el tráfico entrante y saliente desde y hacia los nodos de la Honeynet.

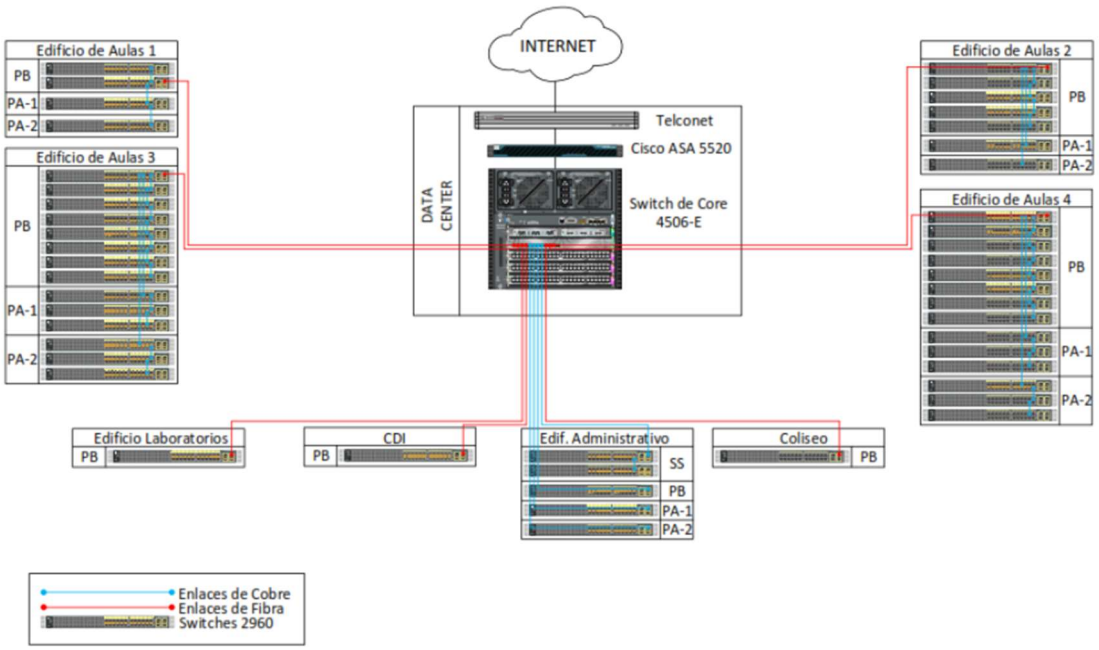


Figura 15. Topología de red

El diseño incluyó la selección e implementación de diversos honeypots de baja y media interacción, específicamente:

1. Cowrie: simula una shell SSH y Telnet para atraer atacantes que buscan explotar servicios remotos.
2. Honeyd: permite la emulación de múltiples servicios y sistemas operativos en una única máquina, ideal para simular una red heterogénea.

3. Dionaea: especializado en capturar malware, sobre todo aquellos diseñados para explotar vulnerabilidades en servicios como SMB, HTTP, FTP, entre otros.

Cada uno de estos honeypots fue configurado con objetivos específicos, emulando sistemas vulnerables de uso común en entornos reales, con el propósito de maximizar la probabilidad de interacción con atacantes.

A nivel de recolección de datos y análisis, se integró un nodo central basado en la pila de herramientas ELK Stack (Elasticsearch, Logstash y Kibana). Esta arquitectura permitió el almacenamiento eficiente, la correlación de eventos y la visualización de patrones de ataque en tiempo real. Logstash fue configurado para recibir los logs generados por los honeypots a través de protocolos seguros como Filebeat y syslog, mientras que Kibana proporcionó un entorno interactivo para la interpretación visual de los datos.

Además, se definieron los protocolos de comunicación internos para asegurar la integridad de la información recolectada, así como la autenticación entre nodos. Se establecieron políticas de control de acceso basadas en listas blancas, monitoreo activo del tráfico en los switches y alertas automáticas ante comportamientos anómalos.

Finalmente, como parte de las medidas de aislamiento y contención, se configuraron entornos virtualizados independientes para cada honeypot, empleando software de virtualización ligera (como VirtualBox y contenedores Docker), lo que permite un control granular y rápido restablecimiento ante cualquier evento de compromiso. Se aplicaron técnicas de enrutamiento y filtrado que impiden que el tráfico malicioso capturado pueda ser redirigido a otros segmentos de la red institucional.

En resumen, el diseño del sistema respondió a una planificación técnica rigurosa y fundamentada en criterios de seguridad, escalabilidad y eficacia en la recopilación de inteligencia de amenazas. Esta arquitectura sienta las bases para una implementación segura y funcional, capaz de contribuir tanto a la protección de los activos digitales de la UPEC como al desarrollo académico en ciberseguridad.

Tabla 15. Composición

Componente	**Descripción**
Topología de Red	Integrada en la DMZ con segmentación lógica y aislamiento mediante VLANs y reglas de firewall. Diseñada para contener interacciones maliciosas sin afectar sistemas productivos.
Honeypots	Cowrie (emulación SSH/Telnet), Honeyd (emulación de servicios/SO), Dionaea (captura de malware). Cada uno configurado para simular vulnerabilidades comunes.
Entornos Virtualizados	VirtualBox y contenedores Docker utilizados para crear entornos independientes por honeypot, permitiendo control granular y restauración rápida ante compromisos.
Recolección de Datos	Nodo central con ELK Stack. Logstash recibe logs mediante Filebeat y syslog. Elasticsearch almacena y Kibana visualiza datos en tiempo real.
Seguridad de Comunicación	Protocolos seguros, autenticación entre nodos, listas blancas, monitoreo de tráfico y alertas ante comportamientos anómalos.
Políticas de Contención	Filtrado de tráfico y técnicas de enrutamiento que impiden la redirección de amenazas hacia otros segmentos de red institucional.

Objetivo del Diseño	Planificación técnica rigurosa centrada en seguridad, escalabilidad y eficacia para la recopilación de inteligencia de amenazas.

4.3. Fase III: Implementación

Durante esta fase se llevó a cabo la implementación técnica de la Honeynet, ejecutando tanto el despliegue físico como lógico de los componentes previamente diseñados. El proceso se inició con la preparación del entorno virtualizado, mediante la instalación de los honeypots seleccionados (Cowrie, Honeyd y Dionaea) en máquinas virtuales independientes, aisladas y configuradas específicamente para simular sistemas reales vulnerables.

Posteriormente, se estableció la conexión de estos honeypots con un servidor centralizado de administración, el cual permite gestionar su comportamiento, supervisar la actividad del sistema y recolectar de manera segura los registros de interacción. Para garantizar un monitoreo proactivo y facilitar la identificación de amenazas conocidas, se integraron herramientas de escaneo y evaluación de vulnerabilidades como Nmap, para la detección de puertos abiertos, y CVE Details, para correlacionar servicios detectados con vulnerabilidades reportadas públicamente.

Una vez verificados los servicios activos en los honeypots, se configuraron filtros y reglas para permitir únicamente el tráfico deseado, restringiendo cualquier intento de salida que comprometa la red institucional. A continuación, se integraron los registros de los honeypots con la plataforma de análisis ELK Stack, estableciendo pipelines de envío de datos a través de Filebeat y Logstash. De esta forma, se habilitó la visualización de eventos de ataque en tiempo real mediante paneles personalizados en Kibana, facilitando el análisis forense y la toma de decisiones informadas.

Esta fase concluyó con la verificación de conectividad, consistencia de los datos recolectados, estabilidad del entorno de ejecución y comportamiento seguro de los honeypots frente a ataques simulados.

Tabla 16. Implementación

Actividad	**Descripción**
Preparación del entorno virtualizado	Instalación de honeypots Cowrie, Honeyd y Dionaea en máquinas virtuales independientes, configuradas y aisladas para simular sistemas vulnerables reales.

Conexión a servidor centralizado	Establecimiento de conexión con servidor para gestión, supervisión y recolección segura de registros de interacción de los honeypots.
Integración de herramientas de escaneo y vulnerabilidades	Uso de Nmap para detección de puertos abiertos y CVE Details para correlación con vulnerabilidades reportadas, facilitando monitoreo y detección proactiva de amenazas.
Configuración de filtros y reglas de tráfico	Establecimiento de reglas para permitir solo tráfico autorizado y restringir salidas que puedan comprometer la red institucional.
Integración con plataforma ELK Stack	Configuración de pipelines mediante Filebeat y Logstash para envío de datos, permitiendo visualización en tiempo real de eventos en Kibana a través de paneles personalizados para análisis forense y toma de decisiones.
Verificación final	Pruebas de conectividad, consistencia de datos, estabilidad del entorno y comportamiento seguro de los honeypots frente a ataques simulados para validar la correcta implementación.

4.4. Fase IV: Verificación y Validación

Una vez implementado el sistema, se procedió a realizar pruebas de funcionalidad, rendimiento y seguridad. Se llevaron a cabo simulaciones de intrusión para evaluar la capacidad de la Honeynet para detectar y registrar ataques. Además, se validó la integridad de los datos recolectados y la estabilidad del sistema ante diferentes vectores de ataque.

4.5. Fase V: Documentación y Capacitación

Con la Honeynet completamente desplegada, se dio inicio a la fase de verificación y validación, cuyo propósito fue asegurar que el sistema cumpliera con los requerimientos funcionales, operativos y de seguridad establecidos durante las fases de diseño e implementación. Esta etapa resultó esencial para garantizar que la solución implementada no solo fuera técnicamente viable, sino también efectiva en su propósito de identificar, registrar y analizar actividades maliciosas en un entorno controlado.

En primer lugar, se realizaron pruebas funcionales orientadas a verificar el correcto funcionamiento de los honeypots (Cowrie, Honeyd y Dionaea). Estas pruebas incluyeron la validación de la emulación de servicios, la disponibilidad de puertos simulados, y la correcta interacción con agentes externos que ejecutaban acciones propias de un atacante. Se comprobó que cada honeypot registrara eventos en los formatos esperados y que estos fueran enviados de forma continua y sin errores al nodo de análisis central.

Posteriormente, se ejecutaron pruebas de rendimiento, simulando múltiples vectores de ataque en diferentes momentos y desde distintas ubicaciones dentro de la red de pruebas. Estas simulaciones incluyeron escaneos con Nmap, intentos de explotación de vulnerabilidades conocidas, inyecciones de código y tráfico anómalo para evaluar la resiliencia del sistema. Se midió la capacidad de respuesta ante cargas elevadas de eventos, así como la eficiencia en el procesamiento y visualización de datos a través de la interfaz de Kibana, integrada en la pila ELK Stack.

En cuanto a la seguridad del entorno, se aplicaron simulaciones de intrusión controlada, ejecutando ataques de tipo “black-box” con el fin de determinar si los honeypots podían ser utilizados como punto de pivote hacia otros segmentos de red. Las pruebas confirmaron que las políticas de aislamiento y segmentación establecidas funcionaban correctamente, ya que el tráfico malicioso quedó contenido dentro del entorno de la Honeynet, sin posibilidad de propagación.

Adicionalmente, se llevó a cabo la validación de la integridad y fidelidad de los datos recolectados. Para ello, se compararon eventos registrados en los honeypots con los datos procesados y visualizados en ELK Stack, verificando que no existiera pérdida de información durante la transmisión ni errores en la correlación temporal de los registros. Esta revisión garantizó la trazabilidad completa de los eventos desde su origen hasta su análisis.

Finalmente, se evaluó la estabilidad del sistema a lo largo de varios días de operación continua. El sistema mantuvo un comportamiento estable, sin caídas críticas ni pérdida de servicios, lo que evidencia su madurez técnica y operativa para integrarse como herramienta de análisis e investigación dentro del ecosistema de ciberseguridad institucional.

En conclusión, la fase de verificación y validación permitió confirmar que la Honeynet implementada cumple con los criterios de funcionamiento esperados, siendo capaz de detectar y registrar intrusiones, garantizar la integridad de los datos, y operar de manera estable en un entorno realista. Estos resultados respaldan su utilidad como recurso tanto para fines

académicos como para el fortalecimiento de la seguridad perimetral de la Universidad Politécnica Estatal del Carchi.

Tabla 17. Pruebas

Actividad	**Descripción**
Pruebas funcionales	Verificación del correcto funcionamiento de honeypots Cowrie, Honeyd y Dionaea, validando emulación de servicios, disponibilidad de puertos y registro continuo y correcto de eventos hacia el nodo central.
Pruebas de rendimiento	Simulación de ataques múltiples y variados (escaneos Nmap, explotación de vulnerabilidades, inyecciones, tráfico anómalo) para evaluar resiliencia, capacidad de respuesta y eficiencia en el procesamiento y visualización en Kibana.
Simulaciones de intrusión controlada	Ejecución de ataques “black-box” para verificar políticas de aislamiento y segmentación, asegurando que el tráfico malicioso se mantenga contenido en la Honeynet sin propagación a la red institucional.
Validación de integridad de datos	Comparación entre eventos registrados en honeypots y datos visualizados en ELK Stack, garantizando ausencia de pérdidas o errores en transmisión y correlación temporal para asegurar la trazabilidad completa.
Evaluación de estabilidad	Monitorización del sistema durante días de operación continúa para confirmar estabilidad, sin caídas críticas ni pérdida de servicios, demostrando madurez técnica y operativa.
Conclusión de la fase	Confirmación de que la Honeynet cumple con los requerimientos funcionales, de seguridad y operativos, siendo efectiva para detección de intrusiones, integridad de datos y operación estable, útil para fines académicos y seguridad perimetral institucional.

4.6. Fase VI: Mantenimiento y Mejora Continua

Aunque el modelo en cascada es secuencial, esta última fase contempla la posibilidad de mejoras a futuro. Se estableció un plan de mantenimiento preventivo y correctivo, así como la recolección continua de datos para retroalimentar futuros ajustes en la configuración del sistema.

Este enfoque metodológico permitió un control riguroso del desarrollo, una planificación precisa de los recursos y una trazabilidad clara de las decisiones tomadas en cada etapa.

5. RESULTADOS ESPERADOS

- Funcionamiento estable de la Honeynet dentro de la DMZ institucional, sin afectar la infraestructura productiva.
- Detección y análisis de múltiples vectores de ataque, incluyendo escaneos, explotación de vulnerabilidades y fuerza bruta.
- Generación de reportes visuales en tiempo real que permitan la toma de decisiones informadas.
- Capacitación de personal técnico y estudiantes en el uso práctico de herramientas de ciberseguridad.
- Desarrollo de una cultura institucional de prevención, monitoreo y respuesta ante incidentes de seguridad informática.
- Establecimiento de un laboratorio académico de referencia para proyectos de investigación aplicada en seguridad digital.

La implementación de este proyecto contribuirá de manera directa al fortalecimiento de la postura de seguridad institucional y al posicionamiento de la UPEC como líder regional en innovación y defensa digital.

4.2. DISCUSIÓN

El objetivo principal de esta investigación fue implementar y configurar una Honeynet en la zona desmilitarizada de la infraestructura de red de la Universidad Politécnica Estatal del Carchi (UPEC), con el propósito de fortalecer la seguridad institucional frente a posibles ciberataques. Para ello, se partió del análisis teórico de los fundamentos de la ciberseguridad, con énfasis en las tecnologías de detección de intrusiones y en la utilidad de los Honeypots y Honeynets como herramientas clave para la recolección de datos sobre el comportamiento de los atacantes.

A través de una exhaustiva revisión bibliográfica, se identificaron diversas metodologías y enfoques que permitieron sustentar teóricamente el diseño e implementación de la Honeynet. Autores como Panchana (2020) y Altamirano & Ganan (2020) destacan la eficacia de estas herramientas en entornos educativos y empresariales como mecanismos de alerta temprana y análisis forense. Esta base teórica guió el diseño del entorno experimental simulado dentro de la red universitaria.

Desde un enfoque mixto, la investigación incluyó entrevistas a personal técnico de la universidad, observación estructurada del entorno tecnológico actual y la configuración de un entorno virtual para las pruebas de rendimiento de los Honeypots. Esto permitió identificar las principales falencias en la infraestructura tecnológica de la UPEC, especialmente en lo relativo a la detección de accesos no autorizados, así como en la ausencia de monitoreo constante de eventos maliciosos.

Durante el desarrollo de la solución, se seleccionaron tecnologías compatibles con entornos académicos, priorizando herramientas de código abierto como ELK Stack para la recolección, análisis y visualización de los registros generados por los Honeypots. La implementación se dividió en fases: en primer lugar, se diseñó la arquitectura lógica de la Honeynet; en segundo lugar, se desplegaron y configuraron múltiples Honeypots con vulnerabilidades simuladas en la DMZ; y finalmente, se llevaron a cabo pruebas de simulación de ataques para evaluar su desempeño y eficacia.

Como resultado, se obtuvo una infraestructura funcional capaz de registrar intentos de intrusión y analizar comportamientos sospechosos en tiempo real. Este sistema no solo permitió evaluar el nivel de exposición de la red institucional, sino que también ofreció una visión clara sobre las rutas y técnicas utilizadas por posibles atacantes. La información recolectada posibilitó la formulación de estrategias proactivas de defensa y la propuesta de recomendaciones específicas para el fortalecimiento de la ciberseguridad en la universidad.

Comparando esta experiencia con estudios previos, se evidencia una tendencia creciente en la adopción de tecnologías de detección y análisis de amenazas en entornos académicos. Por ejemplo, investigaciones similares en universidades latinoamericanas han demostrado que la integración de Honeynets permite mejorar el nivel de protección sin requerir grandes inversiones económicas, siempre que se cuente con personal capacitado y un plan de gestión de incidentes estructurado.

Además, al igual que en entornos corporativos como el caso de Google, citado por Panchana (2020), la implementación de Honeynets en universidades permite anticiparse a nuevas amenazas, detectar vulnerabilidades antes de que sean explotadas y generar conocimiento útil para la formación académica en áreas como la ciberseguridad, redes y administración de sistemas.

En conclusión, la experiencia obtenida a través de este proyecto demuestra que es viable y beneficioso integrar soluciones de seguridad como los Honeypots en la infraestructura tecnológica de instituciones de educación superior. Su implementación no solo eleva el nivel de protección de los datos institucionales, sino que también constituye una herramienta de aprendizaje aplicada para estudiantes y docentes en carreras afines a las tecnologías de la información.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- En la fundamentación teórica de técnicas y metodologías en Honeypots Se logró establecer una base teórica sólida sobre las técnicas y metodologías aplicadas en los honeypots, permitiendo comprender a profundidad su funcionamiento, beneficios y diversas aplicaciones en el ámbito de la ciberseguridad. Esta fundamentación resultó crucial para orientar el diseño e implementación de la Honeynet, asegurando que las prácticas adoptadas fueran técnicamente válidas y efectivas para la detección y análisis de amenazas.
- En el diseño de la Honeynet para simulación y atracción de atacantes se adaptó a la infraestructura tecnológica de la Universidad Politécnica Estatal del Carchi, esto permitió seleccionar y configurar adecuadamente los honeypots para simular vulnerabilidades reales dentro de la zona desmilitarizada (DMZ). Esta arquitectura segura y segmentada facilitó la atracción de atacantes sin comprometer los sistemas productivos, constituyendo una herramienta clave para el monitoreo activo y la generación de inteligencia sobre amenazas específicas del entorno institucional.
- Las pruebas realizadas evidenciaron que los honeypots desplegados en la Honeynet poseen la capacidad adecuada para detectar y registrar accesos no autorizados, además de responder eficientemente ante ataques simulados. La evaluación práctica confirmó la resiliencia y efectividad de los sistemas para captar patrones de comportamiento malicioso, aportando datos valiosos para fortalecer las defensas cibernéticas de la universidad.
- El análisis de los datos recolectados mediante la integración con herramientas como ELK Stack permitió corroborar la efectividad de la Honeynet como mecanismo de seguridad y monitoreo continuo. Los resultados sugieren que esta solución no solo es viable en contextos con recursos limitados, sino que también posee un alto valor académico y operativo. Se recomienda continuar con la mejora y adaptación constante

del sistema para enfrentar amenazas emergentes y optimizar su desempeño en la protección de la infraestructura institucional.

5.2. RECOMENDACIONES

- Ampliar el uso de Honeypots dentro de otras zonas de la red de la universidad, con el objetivo de cubrir diferentes vectores de ataque y fortalecer la seguridad en capas múltiples.
- Capacitar al personal técnico de la UPEC en administración, monitoreo y análisis de Honeynet, de manera que puedan gestionarlas eficazmente, responder ante incidentes y mantener la infraestructura actualizada frente a nuevas amenazas.
- Incorporar los resultados y experiencias del proyecto en los programas académicos relacionados con redes, seguridad informática y tecnologías emergentes, fomentando el aprendizaje práctico y la investigación aplicada entre los estudiantes.
- Buscar alianzas estratégicas con instituciones gubernamentales y privadas para obtener recursos técnicos y financieros, que permitan escalar el proyecto y mantener una infraestructura de ciberseguridad robusta y sostenible.
- Diseñar un protocolo institucional de gestión de incidentes cibernéticos, tomando como base la información recopilada por la Honeynet, que sirva como guía para actuar de manera coordinada y oportuna ante futuros ataques.

VI. REFERENCIAS BIBLIOGRÁFICAS

Altamirano, L., & Ganan, D. (2020). Ciberseguridad en redes educativas de América Latina: evaluación del uso de honeynets. Editorial Académica.

Bravo, M., & Revilla, J. (2021). Evaluación del uso de honeypots en zonas de alto riesgo de redes universitarias. Revista de Ciberseguridad y Educación, 5(2), 45–62.

Brown, J., Thompson, R., & Li, Y. (2022). Advanced honeynet architectures for cybersecurity research and threat intelligence. Cyber Defense Journal, 15(2), 45–61.

Cadenas, M., & Pérez, L. (2019). Rendimiento de procesadores en entornos de seguridad informática. Revista de Ingeniería Informática, 18(3), 42–55.

Chirillo, J., & Blaul, T. (2022). Network security deployment strategies using honeypots. Journal of Advanced Cyber Techniques, 11(3), 67–79.

Fernández, D., & Romero, J. (2020). Entornos virtuales seguros mediante Docker y VMware en sistemas educativos. Revista de Ciberseguridad Aplicada, 7(2), 77–89.

Gómez, P., & García, S. (2022). Impacto de los honeypots en la ciberseguridad de las redes universitarias. Revista de Seguridad Informática, 14(3), 101–119.

González, A., & Pérez, R. (2019). Monitorización de redes con herramientas open source: Un enfoque práctico. Revista de Seguridad Informática, 12(4), 30–44.

Heredia, D., & Ocampo, F. (2021). Implementación de una honeynet virtual con tecnologías de código abierto en redes académicas. Revista Tecnológica Universitaria, 12(1), 33–49.

IEEE. (2024). SDN-based honeynet deployments for adaptive threat detection. IEEE Transactions on Network and Service Management, 21(1), 50–68.

IEEE. (2025). Advances in intrusion detection and threat intelligence. IEEE Xplore Digital Library. https://ieeexplore.ieee.org/

IEEE Xplore. (2025). Honeypots and their role in modern cyber defense: An analytical report. IEEE Transactions on Information Forensics and Security. https://ieeexplore.ieee.org/

Jones, A., & Patel, S. (2023). Honeynets and their role in proactive cybersecurity. Cybersecurity Research Review, 10(1), 88–99.

Laudon, K. C., & Laudon, J. P. (2022). Management information systems: Managing the digital firm (17th ed.). Pearson.

Martínez, F., & Gómez, C. (2021). Análisis del rendimiento de memoria RAM en sistemas de detección de intrusos. Revista Ecuatoriana de Tecnología, 9(2), 17–28.

Maya, S., & Vinueza, J. (2022). Honeynet híbrida para el monitoreo de seguridad en redes universitarias. Revista Latinoamericana de Tecnología y Redes, 7(1), 65–80.

Mokube, I., & Adams, M. (2022). Honeypot classification and deployment strategies in cybersecurity. Journal of Information Security Research, 10(1), 23–35.

Panchana, J. (2020). Ciberseguridad en el entorno académico: Uso de honeypots y honeynets para la protección de datos [Tesis de pregrado, Universidad de Guayaquil].

Provos, N., & Holz, T. (2007). Virtual honeypots: From botnet tracking to intrusion detection. Addison-Wesley.

Provos, N., & Holz, T. (2020). Virtual honeypots: From botnet tracking to intrusion detection. Addison-Wesley.

Rodríguez, M., & Pérez, A. (2021). Análisis de ataques informáticos mediante honeypots en instituciones de educación superior. Revista de Ingeniería en Seguridad, 9(2), 75–91.

Rodríguez, S., & Sánchez, P. (2020). El papel de la GPU en la simulación de entornos honeypot gráficos. Revista Andina de Computación, 5(1), 55–63.

Sánchez, A., & Ramírez, L. (2023). Detección temprana de vulnerabilidades con honeypots en redes educativas. Revista de Seguridad Digital, 11(1), 50–67.

Sánchez, E., & López, M. (2021). Linux en la ciberseguridad moderna: Razones para su elección como sistema operativo de defensa. Boletín Tecnológico, 14(3), 33–47.

Smith, T., Liu, H., & Rodríguez, J. (2024). Artificial intelligence in intrusion detection systems: Accuracy, scalability, and real-time response. Journal of Cyber Defense Systems, 16(2), 110–125.

Spafford, E. H., & Zamboni, D. (2022). Network infrastructure security and trunking in distributed environments. Communications in Cybersecurity, 8(4), 93–105.

Spitzner, L. (2003). Honeypots: Tracking hackers. Addison-Wesley.

Spitzner, L. (2021). Honeypots: Tracking hackers. Addison-Wesley.

Stallings, W. (2018). Computer security: Principles and practice (4th ed.). Pearson.

Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.

Stallings, W., & Brown, L. (2021). Computer security: Principles and practice (5th ed.). Pearson.

Vera, J., & Paredes, M. (2021). Uso de honeypots en redes de universidades para el análisis de ciberamenazas. Revista Andina de Seguridad Informática, 6(2), 89–105.

Zhuge, J., Han, X., & Wang, Y. (2021). Virtualized honeypots for cloud and academic network security. International Journal of Cyber Research, 9(4), 112–128.

VII. ANEXOS

Anexo 1. Acta de la sustentación de Predefensa del TIC

Anexo 2. Certificado del abstract por parte de idiomas

Anexo 3 Manual

Anexo 4 Fichas técnicas.

Anexo 5 carta de conformidad.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERÍA EN INFORMATICA

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL INFORME DE INVESTIGACIÓN DE:

NOMBRE: VILLARREAL GARCÍA BYRON ADAIR **CÉDULA DE IDENTIDAD:** 0401576905
NIVEL/PARALELO: 0 **PERIODO ACADÉMICO:** 2025A

TEMA DE INVESTIGACIÓN: "Implementación y configuración de una honeynet en la zona desmilitarizada de la infraestructura de red de la Universidad Politécnica Estatal del Carchi"

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. ARCOS PONCE GEORGINA GUADALUPE
LECTOR: MSC. NARANJO CEDEÑO JEFFERY ALEX
ASESOR: MSC. DEL HIERRO MOSQUERA MILTON GABRIEL

De acuerdo al artículo 21: Una vez entregados los requisitos para la realización de la pre-defensa el Director de Carrera Integrará el Tribunal de Pre-defensa del informe de Investigación, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 4 **AULA:** 111
FECHA: Jueves, 17 de Julio de 2025
HORA: 9H30
Obteniendo las siguientes notas:
1) Sustentación de la predefensa: 5,95
2) Trabajo escrito 2,55
Nota final de PRE DEFENSA **8,50**
Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 24.- De los estudiantes que aprueban el Plan de Investigación con observaciones. - El estudiante tendrá el plazo de 10 días laborables para proceder a corregir su informe de Investigación de conformidad a las observaciones y recomendaciones realizadas por los miembros Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el jueves, 17 de julio de 2025

MSC. ARCOS PONCE GEORGINA GUADALUPE
PRESIDENTE

MSC. DEL HIERRO MOSQUERA MILTON GABRIEL
TUTOR

MSC. NARANJO CEDEÑO JEFFERY ALEX
LECTOR

Adj.: Observaciones y recomendaciones

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGES CENTER

ABSTRACT- EVALUATION SHEET

NAME: Byron Adair Villarreal García
DATE: Viernes, 22 de agosto de 2025
Topic: Implementación y configuración de una honeynet en la zona desmilitarizada de la infraestructura de red de la Universidad Politécnica Estatal del Carchi
MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events ■	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐

TOTAL/AVERAGE	9 - 10: EXCELLENT 7 - 8,9: GOOD 5 - 6,9: AVERAGE 0 - 4,9: LIMITED	TOTAL 9

1

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI- FOREIGN AND NATIVE LANGUAGES CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Byron Adair Villarreal García
Fecha de recepción del abstract: Miércoles, 20 de agosto de 2025
Fecha de entrega del informe: Viernes, 22 de agosto de 2025

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:

Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según la rúbrica de evaluación de la traducción en Inglés, ésta alcanza un valor de 9; por lo cual se valida dicho trabajo.

Atentamente

Firmado electrónicamente por: MARTHA ARACELLY VIVEROS ALMEIDA
Validar únicamente con FirmaEC

MA. Martha Viveros
Docente responsable del
CIDEN

2

Manual de Usuario
Implementación e instalación de honeynet en la infraestructura de red de la Universidad Politécnica Estatal Del Carchi.

Titulación de tesis
Adair Villarreal.

Tabla de contenido

Introducción

El presente documento corresponde al manual de usuario desarrollado como parte del proyecto de titulación llamado “Instalación y configuración de una Honeynet en la Universidad Politécnica Estatal del Carchi”. Este manual tiene como finalidad orientar a los usuarios en el uso, administración y mantenimiento básico del sistema implementado, basado en la plataforma T-Pot, una solución de código abierto que integra diversos honeypots para la detección y análisis de amenazas cibernéticas.

El proyecto busca fortalecer las capacidades de monitoreo y estudio del comportamiento de posibles atacantes en redes informáticas, mediante la creación de un entorno controlado conocido como Honeynet. Esta infraestructura permite recopilar información valiosa sobre vectores de ataque, técnicas utilizadas y patrones de comportamiento de actores maliciosos, todo ello sin poner en riesgo los sistemas reales de la universidad.

Este manual está dirigido a personal técnico, estudiantes e investigadores que requieran operar o continuar desarrollando la Honeynet. A lo largo del documento se detallan los procedimientos necesarios para el uso básico del sistema, incluyendo el acceso a la interfaz gráfica, interpretación de registros, revisión de alertas y pautas para la administración responsable del entorno.

Con esta guía se busca asegurar la continuidad y el aprovechamiento académico y técnico del proyecto, contribuyendo a la formación en ciberseguridad dentro de la institución.

Documentos relacionados

Nombre	Descripción
Clasificación de las CVE según su vulnerabilidad más explotada con datos obtenidos de T-pot honeypot.	La clasificación de las CVE es un componente fundamental de la estrategia de seguridad cibernética de una organización, que contribuye significativamente a su postura de seguridad general.

Análisis de los patrones y tácticas de los atacantes mediante una T-pot honeypot.	Este trabajo analiza los patrones y tácticas de ataques y se hablará sobre los procesos para obtener resultados precisos y útiles. La selección de herramientas adecuadas, la captura y el análisis de los datos, la interpretación de los resultados y la documentación de los hallazgos son pasos críticos para realizar un análisis efectivo de los patrones y tácticas de los ataques.

Descripción

Objetivo general:

Brindar una guía clara y práctica sobre el uso y administración del sistema Honeynet implementado en la Universidad Politécnica Estatal del Carchi, con base en la plataforma T-Pot.

Objetivos específicos:

Explicar los componentes y funcionalidades del entorno Honeynet.
Guiar en el acceso, monitoreo y análisis de datos recolectados.
Establecer buenas prácticas para el mantenimiento seguro del sistema.
Facilitar la continuidad del proyecto para fines académicos y de investigación.

Contenido

Este manual está dirigido a usuarios con conocimientos básicos o intermedios en redes y seguridad informática.

- El acceso al entorno gráfico de T-Pot.
- La visualización e interpretación de datos.
- La gestión básica del sistema operativo y servicios.
- Consideraciones de seguridad y mantenimiento.

No contempla tareas de desarrollo avanzado ni modificaciones profundas al código fuente de los servicios.

Recursos Utilizados

Recursos de Hardware

- Procesador: Intel Core i7 Octava Generación
- Memoria RAM: 24GB
- Almacenamiento: 512 GB Nvme m.2
- Tarjeta Gráfica: NVIDIA GTX 1660 Ti o superior

Recursos de Software

- Sistema operativo base: Debian GNU/Linux 11 (bullseye)
- Imágen ISO de T-Pot (última versión disponible)

Descarga de T-Pot

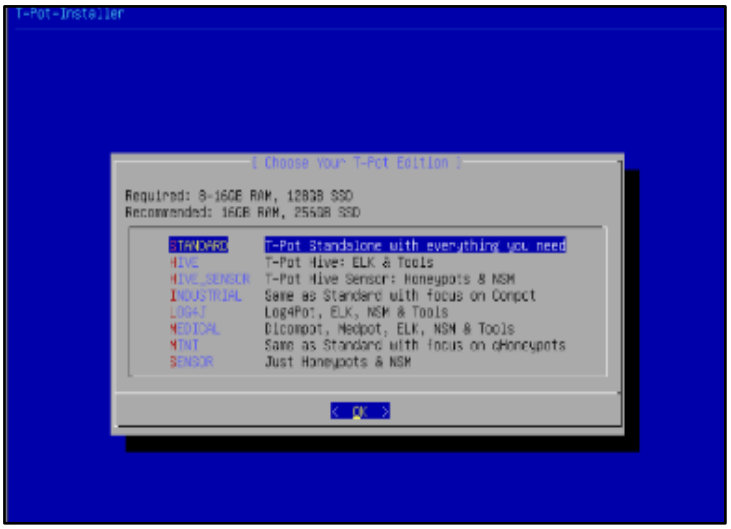
1. Acceder al repositorio oficial: https://github.com/telekom-security/tpotce
2. Descargar la imagen ISO más reciente o clonar el repositorio.

Creación del Medio de Instalación

Utilizamos balenaEtcher para crear un USB booteable con la imagen ISO.

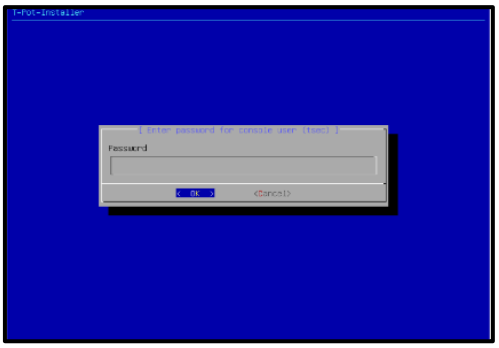
Proceso de Instalación

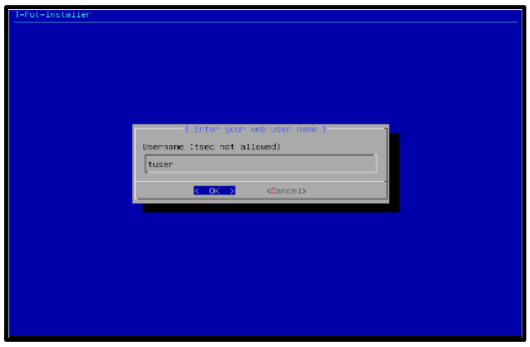
Iniciar desde el USB con T-Pot.



Seleccionar el modo de instalación (Standard Installation recomendado).

Configurar el hostname, zona horaria, usuario y contraseña.





4. Finalizar la instalación y reiniciar el sistema.

Componentes del Sistema

El sistema T-Pot se distingue por integrar múltiples honeypots especializados que operan simultáneamente dentro de contenedores Docker. Cada uno está diseñado para emular servicios y protocolos específicos, permitiendo capturar y analizar distintas formas de comportamiento malicioso. A continuación se describen los principales honeypots incluidos en la implementación:

Dionaea:

Diseñado para capturar malware a través de protocolos como SMB, HTTP, FTP, TFTP y más. Este honeypot es particularmente útil para recolectar muestras de código malicioso y estudiar su comportamiento, ya que simula vulnerabilidades comunes en sistemas Windows y Linux. Dionaea permite construir una base de datos de amenazas que puede alimentar motores antivirus o ser usada en investigación académica.

Cowrie:

Emula un entorno de línea de comandos vulnerable mediante los servicios SSH y Telnet. Es altamente interactivo, lo que permite registrar comandos ejecutados por atacantes, archivos descargados e intentos de escalamiento de privilegios. Cowrie resulta clave para estudiar técnicas de intrusión manuales y automatizadas, incluyendo ataques por fuerza bruta o scripts maliciosos.

Conpot:

Honeypot enfocado en la simulación de sistemas industriales SCADA (Supervisory Control And Data Acquisition). Es ideal para entornos donde se desea investigar amenazas dirigidas a infraestructuras críticas como plantas de energía, sistemas de agua o control de tráfico. Conpot emula dispositivos como PLCs (Controladores Lógicos Programables), facilitando el estudio de vectores específicos del mundo OT

(Operational Technology).

ElasticPot:

Reproduce el comportamiento de instancias de **Elasticsearch** mal configuradas, las cuales suelen ser blanco de atacantes que buscan explotar bases de datos expuestas. ElasticPot permite detectar actividades como escaneo automatizado, inyecciones maliciosas y explotación de APIs, ofreciendo datos valiosos sobre ataques a infraestructuras de big data.

Snort / Suricata:

Aunque no son honeypots per se, funcionan como **motores IDS/IPS** (Sistemas de Detección/Prevención de Intrusiones) que inspeccionan el tráfico entrante en tiempo real. Detectan patrones de ataque conocidos y anomalías mediante firmas predefinidas y análisis de comportamiento. Su integración en T-Pot fortalece la detección proactiva y proporciona una capa de seguridad adicional que complementa a los honeypots emulados.

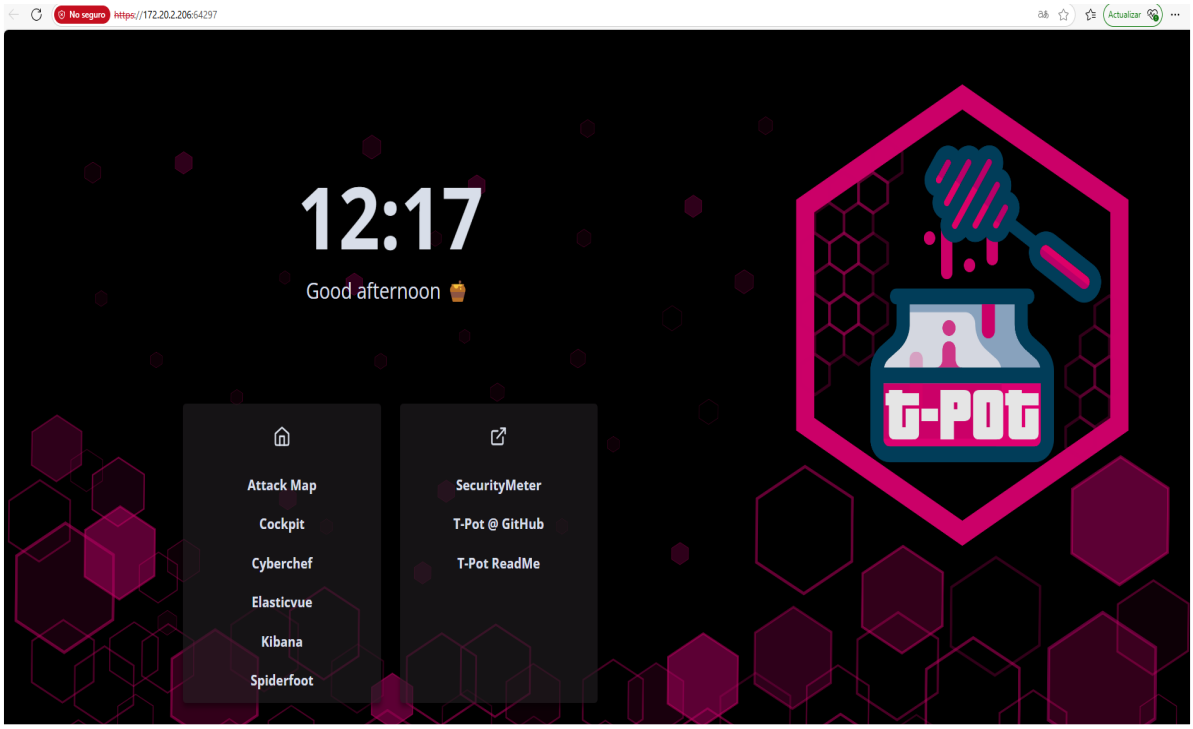
Acceso al Sistema

1. *Desde un navegador web en la misma red, ingresar a:*

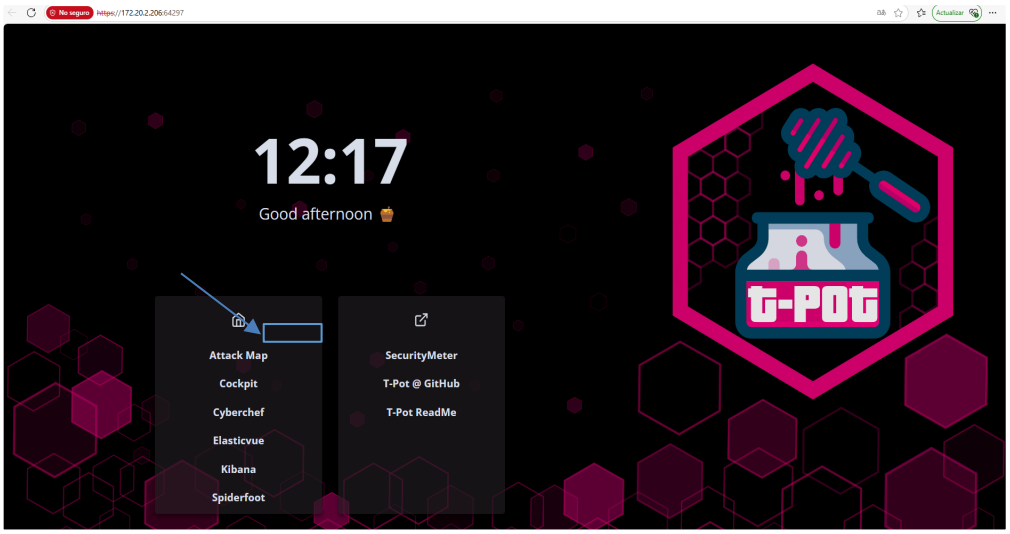
https://172.20.2.206:64297/

Nuestro usuario es tsec

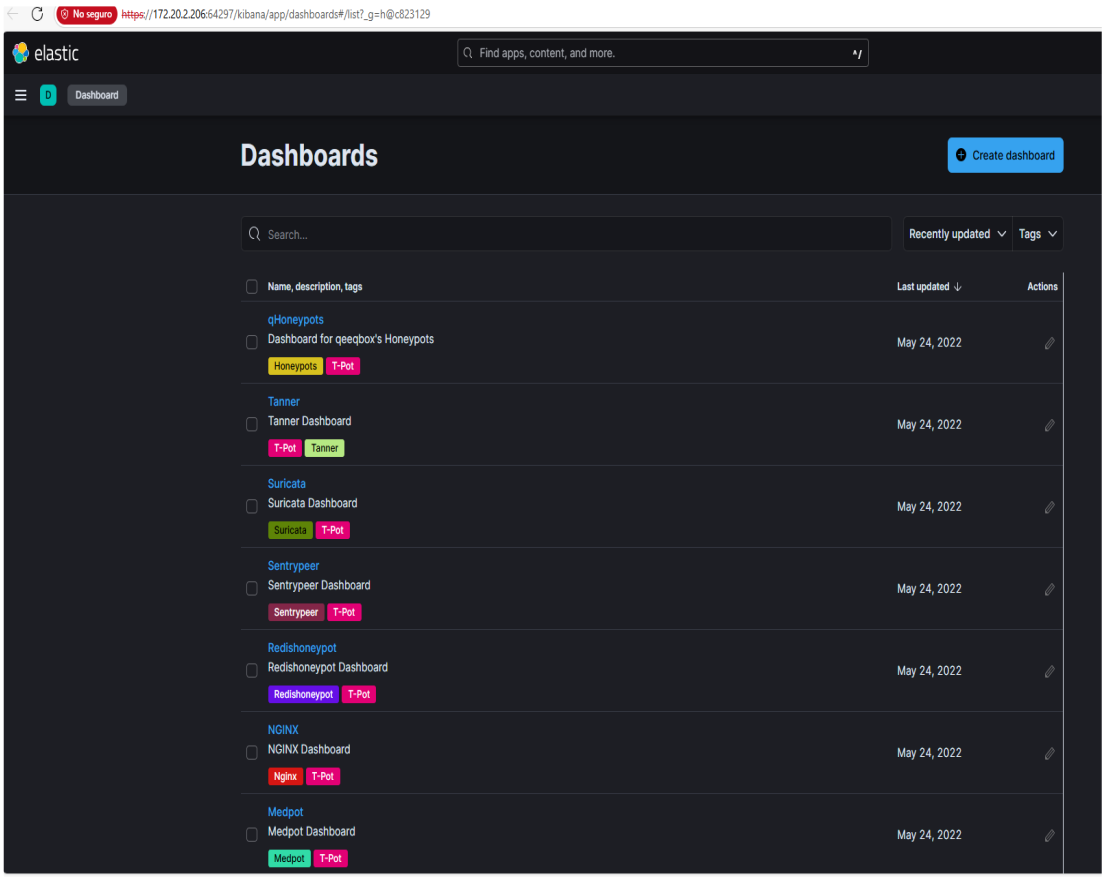
Y la clave es: Up3c



Acceso a Kibana



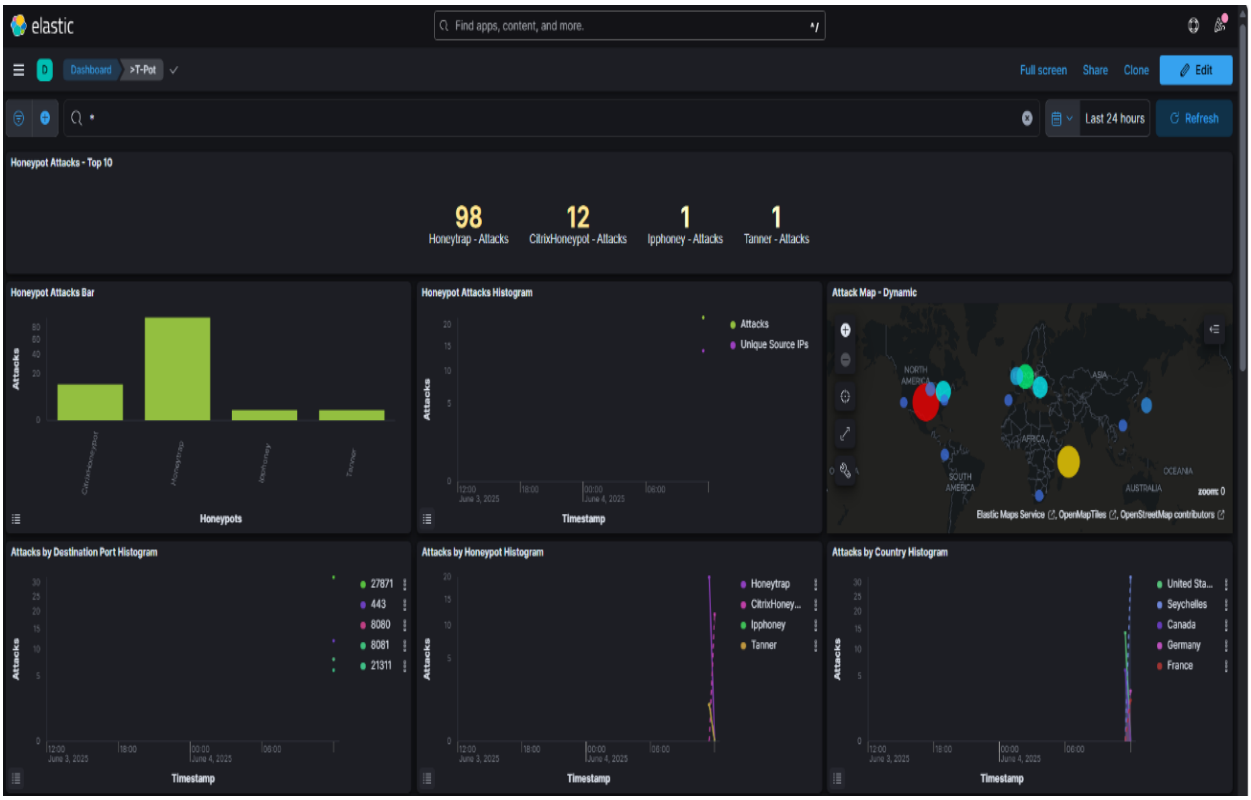
Una vez ingresados a nuestro gestor web entramos donde dice Kibana.



El panel principal de T-Pot, accesible desde la interfaz web a través de Kibana, proporciona una visión unificada y centralizada de toda la actividad observada por los honeypots. Este dashboard está diseñado para ofrecer una visualización inmediata y dinámica de los intentos de ataque, las fuentes de amenazas, los tipos de servicios comprometidos y el volumen de tráfico sospechoso.

T-Pot combina múltiples fuentes de datos (como Cowrie, Dionaea, Conpot, etc.) y los agrupa en paneles visuales mediante gráficos, mapas y tablas interactivas. Esto permite a los operadores:

- Identificar patrones de comportamiento malicioso.
- Reconocer direcciones IP que generan más tráfico sospechoso.
- Analizar tendencias en ataques durante distintos períodos.
- Ver la distribución geográfica de las amenazas.
- Evaluar en tiempo real la intensidad y frecuencia de los ataques.

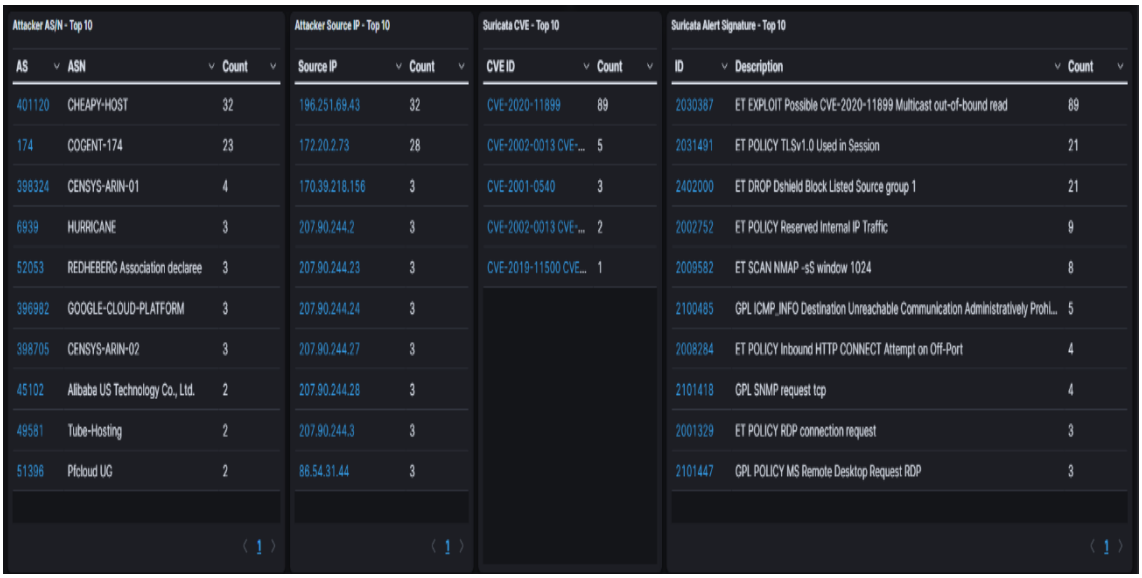


Componentes del Dashboard

Módulo	*Función*
Resumen de Eventos	*Muestra el número total de conexiones y alertas en tiempo real.*
Mapa de Ataques	*Localiza geográficamente las IPs atacantes con datos de geolocalización.*
Servicios Atacados	*Enumera los servicios (puertos) más comprometidos (SSH, HTTP, etc.).*
IPs Más Activas	*Lista los principales atacantes por cantidad de eventos registrados.*
Línea de Tiempo	*Permite observar los picos de actividad en intervalos de tiempo.*
Clasificación por Honeypot	*Separa los eventos por tipo de honeypot que los capturó.*

Este dashboard representa una herramienta clave no solo para la defensa activa, sino también como un entorno de aprendizaje. Los estudiantes y analistas pueden explorar diferentes técnicas

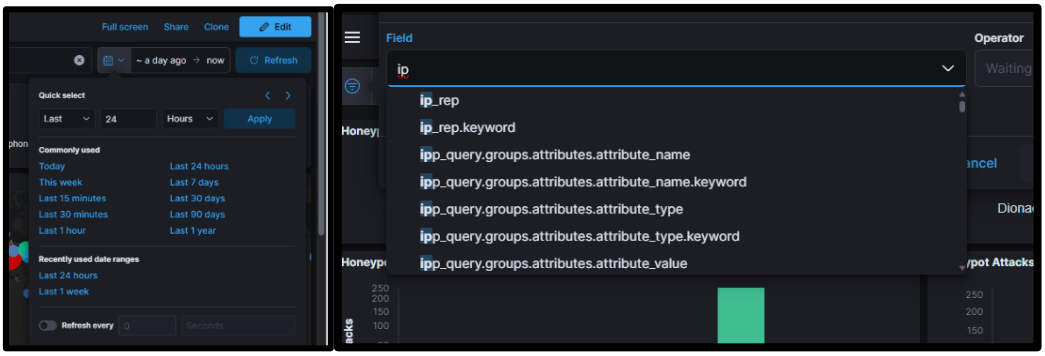
de ataque en un entorno seguro, evaluando sus firmas y *comportamientos sin poner en riesgo la red institucional.*



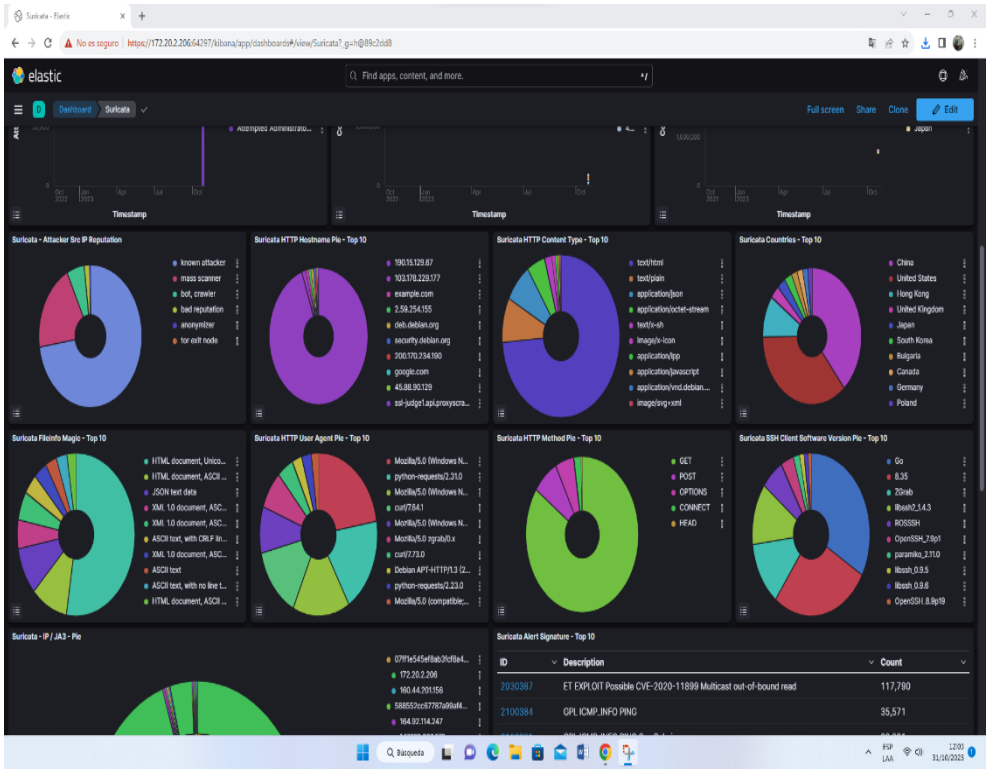
8. Uso Básico del Sistema

8.1 Uso de Kibana

- Filtrar eventos por IP, protocolo o fechas.



- Analizar patrones de ataque y generar informes.



Seguridad y Buenas Prácticas

Implementar una Honeynet dentro de una red universitaria implica riesgos inherentes si no se siguen medidas de seguridad adecuadas. Las buenas prácticas aseguran que el entorno de análisis no se convierta en un punto de entrada para atacantes, ni comprometa otros sistemas conectados a la red.

- **No exponer la Honeynet directamente a la red productiva:** Aislar la Honeynet en una zona desmilitarizada (DMZ) o en una subred separada minimiza la posibilidad de propagación accidental de amenazas hacia sistemas reales.
- **Cambiar contraseñas por defecto de acceso:** Las credenciales predeterminadas son el blanco más común de ataques automatizados. Se recomienda el uso de contraseñas seguras y únicas por cada servicio.
- **Configurar reglas de firewall (UFW) para limitar accesos:** Es esencial restringir el acceso a los servicios expuestos sólo a direcciones IP específicas o rangos internos de administración, evitando accesos no autorizados.
- **Realizar respaldos regulares del sistema y datos:** Tener copias de seguridad programadas permite restaurar el entorno ante incidentes, corrupciones o

actualizaciones fallidas.

- **Registrar y documentar cualquier cambio en el entorno:** Mantener una bitácora o changelog de modificaciones ayuda a auditar el sistema, facilita la resolución de problemas y permite replicar configuraciones en futuras instalaciones.

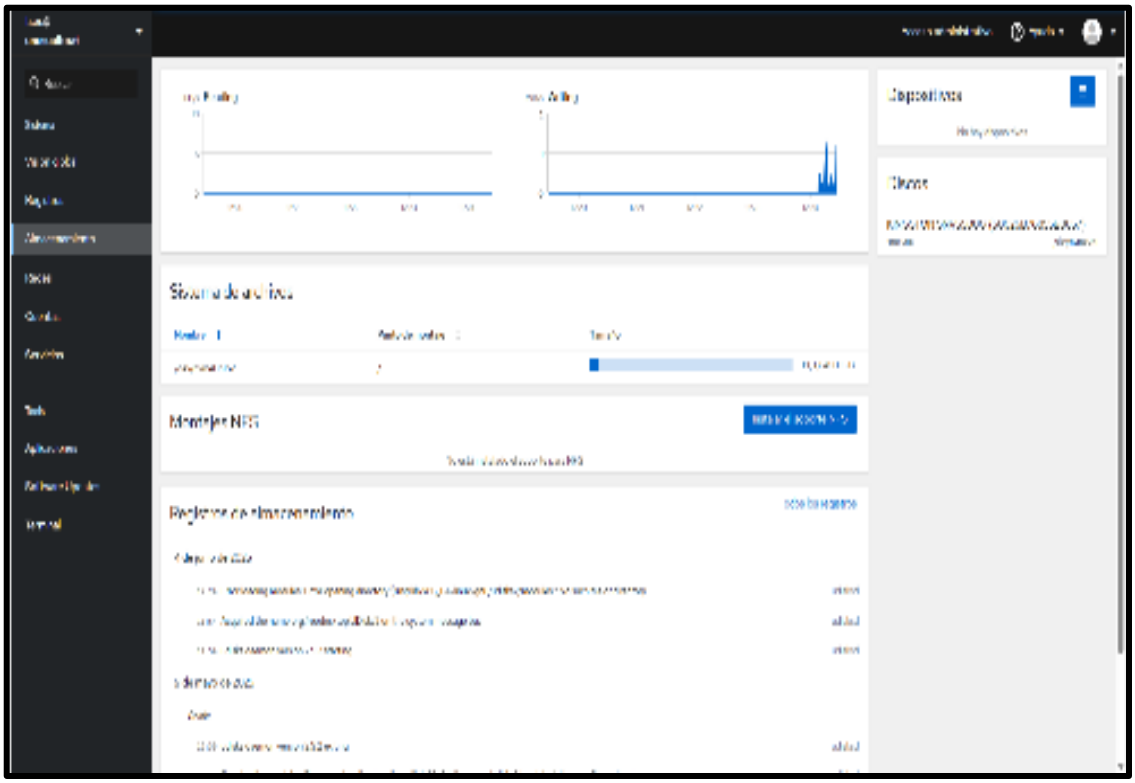
Estas medidas refuerzan la estabilidad, integridad y continuidad operativa del entorno Honeynet, permitiendo que cumpla su función investigativa sin generar vulnerabilidades colaterales.

Mantenimiento del Sistema

El mantenimiento periódico del entorno Honeynet es fundamental para garantizar su correcto funcionamiento y longevidad. Dado que se trata de un sistema que simula vulnerabilidades de forma controlada, cualquier descuido podría comprometer su operatividad o incluso convertirse en un riesgo si no se detectan fallos a tiempo.

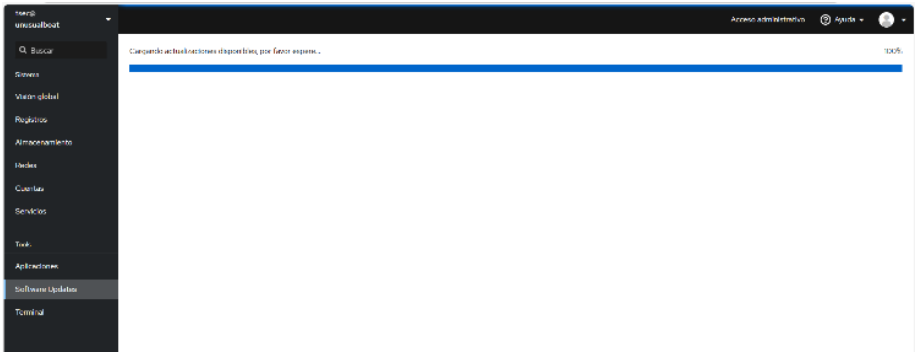
- Verificar espacio en disco y uso de CPU/RAM.

La recopilación constante de registros y tráfico puede llenar el disco rápidamente. Además, el uso excesivo de CPU o RAM puede indicar procesos anómalos o mal configurados.



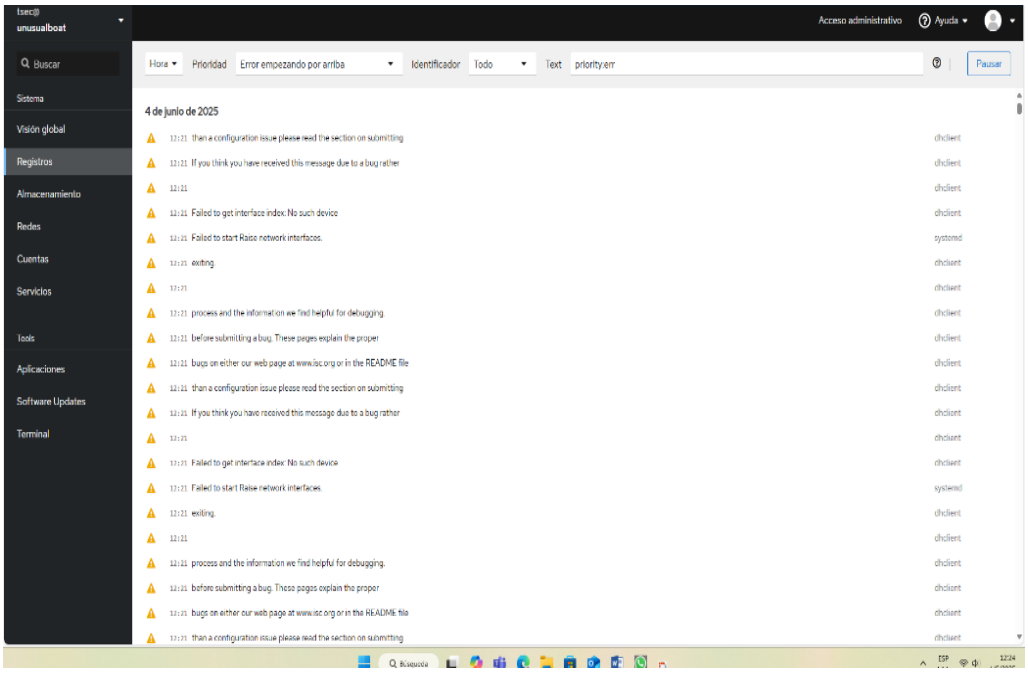
- Actualizar contenedores Docker con precaución.

Las actualizaciones son importantes para aplicar parches de seguridad y mejoras, pero deben realizarse de forma controlada y con respaldo previo, para evitar la pérdida de configuraciones personalizadas.



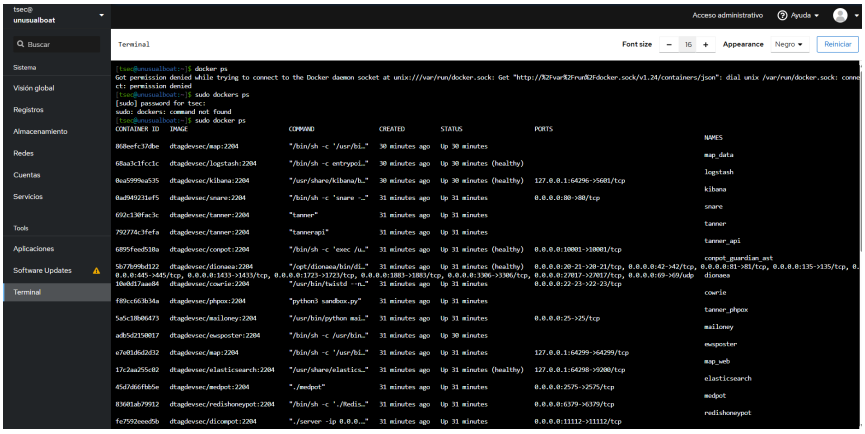
- Revisar logs y alertas semanalmente.

Es indispensable analizar los registros con frecuencia para detectar patrones nuevos, errores del sistema, o intentos de evasión por parte de atacantes más sofisticados.



- Comprobar estado y funcionamiento de dockers.

Verificar que todos los servicios en contenedores Docker estén activos y estables garantizando la disponibilidad del sistema. Herramientas como Cockpit facilitan esta tarea.



Estas tareas deben ser calendarizadas y asignadas claramente, especialmente si el entorno es utilizado con fines académicos o investigativos, asegurando así una base estable para el análisis continuo de amenazas.

Conclusión

Este manual proporciona una guía clara, estructurada y accesible para la correcta operación y mantenimiento del sistema Honeynet basado en la plataforma T-Pot, implementado en la Universidad Politécnica Estatal del Carchi. Su elaboración responde a la necesidad de establecer procedimientos estandarizados que garanticen la estabilidad, seguridad y continuidad operativa del entorno.

La implementación de esta Honeynet representa un aporte significativo al fortalecimiento de las capacidades institucionales en materia de ciberseguridad. Permite a estudiantes, docentes e investigadores interactuar con un sistema real de recolección y análisis de amenazas, en un entorno seguro y controlado. A través de la visualización de eventos, el análisis de patrones de ataque y la detección de comportamientos anómalos, se promueve un aprendizaje activo basado en la experiencia.

Además, esta infraestructura se constituye como una herramienta valiosa para fomentar la investigación aplicada en seguridad informática, brindando datos reales y contextualizados que pueden ser utilizados en tesis, proyectos académicos y publicaciones científicas. Al observar directamente las técnicas utilizadas por atacantes, los usuarios pueden desarrollar una comprensión más profunda del funcionamiento de las amenazas y proponer estrategias efectivas de defensa.

Anexos - Manual de Usuario

Anexo 1: Paneles de Acceso por Puerto (T-Pot)

Servicio	Puerto		Descripción
Admin Web T-Pot	64297		Interfaz principal
Kibana	5601		Análisis de datos
Portainer	9000		Gestión de contenedores
Cockpit	9090		Administración del sistema
CyberChef	8000		Análisis y decodificación de datos

Anexo 2: Comandos Útiles para la Administración

A. Comandos del Sistema (Ubuntu)

```
df -h                    #  Ver uso de disco
htop                     # Uso de CPU y RAM
ip a                     # Ver IP del servidor
sudo shutdown now        # Apagar sistema
sudo reboot              # Reiniciar sistema
journalctl -xe           # Ver logs del sistema
```

B. Comandos Docker (T-Pot)

```
docker ps          # Ver contenedores activos
```

docker logs <nombre> # Ver logs de contenedor
docker exec -it <nombre> /bin/bash # Acceder al contenedor
docker restart <nombre> # Reiniciar servicio
docker stats # Ver uso de recursos

C. Red y Seguridad

netstat -tunap # Conexiones activas
lsof -i -P -n # Puertos abiertos
sudo ufw status # Ver estado del firewall
sudo ufw allow ssh # Permitir acceso SSH

D. Mantenimiento

sudo apt update # Actualizar paquetes
sudo apt upgrade # Instalar actualizaciones
docker container prune # Eliminar contenedores inactivos
docker image prune -a # Limpiar imágenes no usadas

Anexo 4. Fichas técnicas

	UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	Ficha técnica de requisitos de Implementación e instalación de honeynet en la infraestructura de red de la Universidad Politécnica Estatal Del Carchi.

Informe Técnico 1: Arquitectura y Configuración de Red de la Honeynet con T-Pot.

Objetivo

Este informe técnico describe la arquitectura lógica y la configuración de red empleada para desplegar la honeynet utilizando T-Pot sobre un entorno Debian 7. El objetivo es documentar cómo se segmenta la red, los puertos utilizados y las medidas de seguridad para aislar el tráfico malicioso del resto del entorno de red.

Diseño Lógico de la Red

La honeynet fue desplegada en la zona desmilitarizada (DMZ) de la red institucional, conectada a través de un switch administrable configurado con una VLAN dedicada. La topología consta de:

- Nodo T-Pot (host único con múltiples contenedores)
- Router/firewall con reglas restrictivas
- Cliente externo para pruebas de penetración

Todos los puertos están direccionados hacia la máquina honeypot ubicada en la DMZ, permitiendo la captación de tráfico entrante malicioso sin comprometer la red interna, y asegurando así un entorno controlado para su análisis.

Puertos y Servicios Configurados

Los siguientes puertos fueron habilitados para monitorear los servicios comúnmente atacados:

- Puerto 22 (SSH - Cowrie)
- Puerto 23 (Telnet - Cowrie)
- Puerto 80/443 (HTTP/HTTPS - Web Honeypots)
- Puerto 161 (SNMP - Honeytrap)
- Puerto 445 (SMB - conpot)
- Otros puertos según configuración predeterminada de T-Pot

Se configuraron redirecciones NAT para permitir acceso desde redes externas, manteniendo el sistema segmentado con firewall de marca Mikrotik

Seguridad y Aislamiento de Red

Para evitar comprometer la red institucional, se implementaron las siguientes medidas:

- Uso de VLAN para separar el tráfico de honeypot del tráfico administrativo.

- Reglas de iptables para bloquear conexiones salientes desde el honeypot.

- Recolección de tráfico solo entrante para evitar fugas de información.

- Monitoreo constante con Wireshark y Snort en un nodo espejo de red.

Conclusión.

La arquitectura de red desplegada permite una operación segura de la honeynet, captando tráfico malicioso sin poner en riesgo la infraestructura de red principal. La correcta segmentación y control del entorno facilita el análisis detallado de patrones de ataque.

Firmas.

Adair Villarreal G.
Ejecutor de la investigación

Msc.Javier Torres.
Analista de redes y telecomunicaciones UPEC.

POLITECNICA DEL CARCHI

Ing.Milton Del Hierro Msc.
Tutor de Investigación.

Informe Técnico 2: Configuración de Sensores Honeypot Activos en T-Pot.

Objetivo

Este informe técnico documenta los sensores honeypot configurados en la plataforma TPot instalada sobre Debian 7 en una infraestructura local. Se detallan los servicios emulados, sus funcionalidades, y los tipos de ataques que permiten monitorear.

Sensores Honeypot Activos.

La plataforma T-Pot integra múltiples sensores honeypot que funcionan como contenedores independientes dentro del entorno Docker. Para esta implementación, se activaron los siguientes sensores:

- Cowrie: Emula servicios SSH y Telnet para capturar ataques de fuerza bruta y comandos ejecutados por los atacantes.

- Citrix Honeypot: Detecta intentos de explotación relacionados con la vulnerabilidad CVE-2019-19781 en servidores Citrix ADC.

- Conpot: Simula sistemas de control industrial (ICS/SCADA).

- ElasticPot: Emula instancias de Elasticsearch vulnerables.

- Heralding: Captura intentos de conexión a múltiples protocolos como FTP, SMTP y MSSQL.

- Honeytrap: Escucha múltiples puertos para capturar escaneos de red y conexión inicial.

- Dionaea: Diseñado para capturar malware que ataca servicios SMB, HTTP, FTP y otros.
- Suricata: IDS/IPS que realiza inspección profunda de paquetes.

Configuración General

Los sensores se ejecutan automáticamente al iniciar T-Pot y son gestionados por Docker Compose. La configuración por defecto fue adaptada para permitir el almacenamiento persistente de logs y visualización centralizada mediante Kibana. Cada contenedor expone puertos específicos según el tipo de servicio emulado.

Los archivos de configuración de cada sensor están ubicados dentro del contenedor correspondiente, accesibles mediante:

sudo docker exec -it <nombre_contenedor> /bin/bash

Los logs generados por cada sensor se almacenan en la ruta:

/data/<sensor_name>/log

Funcionalidades Específicas

Cowrie permite observar intentos de autenticación y registrar sesiones completas de los atacantes.

- Dionaea permite capturar muestras de malware para análisis posterior.

- Conpot facilita la detección de exploraciones hacia infraestructura crítica.

- Heralding ofrece información valiosa de reconocimiento temprano.

- Suricata actúa como sistema de alerta ante patrones de tráfico sospechoso.

Conclusión.

La diversidad de sensores incluidos en T-Pot permite una cobertura amplia de vectores de ataque, facilitando el análisis del comportamiento de los atacantes. Su configuración modular en contenedores permite un mantenimiento sencillo y escalable.

Firmas.

Adair Villarreal G.
Ejecutor de la investigación

Msc.Javier Torres.
Analista de redes y telecomunicaciones UPEC.

POLITÉCNICA DEL CARCHI

Ing.Milton Del Hierro Msc.
Tutor de Investigación.

Informe Técnico 3: Visualización y Análisis de Logs con Kibana y Elasticsearch.

Objetivo

Este informe describe la configuración y uso de las herramientas Kibana y Elasticsearch en el entorno T-Pot, para la visualización y análisis de los datos recolectados por los sensores honeypot. Estas herramientas son clave para interpretar el comportamiento de los atacantes y extraer patrones útiles en ciberseguridad.

Configuración de Elasticsearch

Elasticsearch actúa como motor de búsqueda distribuido para almacenar, indexar y consultar los logs generados por los honeypots. En la implementación con T-Pot, viene preconfigurado y ejecutándose en un contenedor Docker. Los datos se almacenan en índices específicos, por ejemplo:

- cowrie- (para sesiones SSH/Telnet)

- dionaea- (para muestras de malware)

- suricata- (para alertas IDS)

El contenedor se puede verificar con: sudo docker ps | grep elasticsearch

Configuración de Kibana

Kibana proporciona la interfaz gráfica para visualizar los datos indexados en Elasticsearch. Está accesible mediante navegador web a través del puerto 64297 (por defecto en T-Pot):

http://172.168.2.216:64297

Desde la interfaz, se pueden crear dashboards, realizar búsquedas avanzadas y visualizar gráficos como:

- Número de intentos de acceso por hora
- Países de origen
- Usuarios más intentados
- Contraseñas más usadas
- Comandos ejecutados por los atacantes

Se recomienda crear filtros personalizados para cada tipo de sensor y exportar reportes en formato CSV o PDF.

Análisis de Logs de Seguridad

Durante el monitoreo se identificaron varios patrones de comportamiento malicioso:

- Repetición de IPs provenientes de Vietnam y China

- Uso masivo de credenciales por defecto como 'root', 'admin', 'ubnt'

- Actividad elevada en fines de semana

- Peticiones sospechosas HTTP/SIP detectadas por Cowrie y Citrix Honeypot

Estos datos fueron fundamentales para detectar patrones automatizados, posibles botnets, y ataques dirigidos.

Conclusión.

El uso de Elasticsearch y Kibana dentro del entorno T-Pot es esencial para transformar grandes volúmenes de datos de seguridad en información comprensible y accionable. Su correcta utilización permite optimizar la respuesta ante incidentes y enriquecer la inteligencia de amenazas.

Firmas.

Adair Villarreal G.
Ejecutor de la investigación

Msc.Javier Torres.
Analista de redes y telecomunicaciones UPEC.

Ing.Milton Del Hierro Msc.
Tutor de Investigación.

Informe Técnico 4: Buenas Prácticas y Lecciones Aprendidas en la Implementación de T-Pot

Objetivo

Este informe resume las buenas prácticas observadas y las lecciones aprendidas durante la implementación y operación de la plataforma de honeypots T-Pot sobre Debian 7. La experiencia adquirida permite mejorar futuras implementaciones y reforzar la seguridad en entornos controlados para análisis de amenazas.

Buenas Prácticas Aplicadas

- Aislamiento de la honeynet en una red separada mediante VLAN o switch dedicado.

- Uso de Docker para contenerizar los honeypots, permitiendo modularidad y fácil reinicio.

- Registro detallado de logs por sensor y almacenamiento persistente.

- Acceso restringido a los puertos de gestión de T-Pot para evitar interferencias externas.

- Programación de backups automáticos de logs y configuraciones.

- Monitoreo visual de eventos en tiempo real con Kibana.

Lecciones Aprendidas

- Debian 7 presenta limitaciones de compatibilidad con versiones recientes de Docker y herramientas de red, por lo que se recomienda considerar versiones más actuales o distribuciones basadas en Ubuntu.
- Algunos contenedores pueden fallar si no se les asigna suficiente RAM. Es recomendable tener al menos 16 GB de RAM.

- Durante las pruebas, se observó que ciertos ataques automatizados se intensificaban los fines de semana, lo cual requiere configurar alertas para detectar picos de actividad.

- Es importante excluir la IP del administrador de las métricas de Kibana para evitar falsos positivos.

- Se identificaron intentos de evasión que no generaron alertas inmediatas, lo cual resalta la necesidad de complementar los honeypots con sistemas IDS adicionales como Snort o Suricata bien configurados.

Recomendaciones futuras.

- Considerar el uso de T-Pot sobre Ubuntu Server LTS o Debian 10+.

- Implementar autenticación multifactor para acceder a la interfaz de administración.

- Desplegar nodos honeypot adicionales en otras ubicaciones geográficas para mejorar cobertura.

- Automatizar el análisis de logs con herramientas como Logstash y alertas por correo electrónico.

- Establecer una política de actualización de contenedores para mitigar vulnerabilidades en los servicios honeypot.

Conclusión.

La implementación de T-Pot ha sido una experiencia enriquecedora que proporciona visibilidad sobre técnicas y patrones de ataque reales. Las prácticas adoptadas y las lecciones

aprendidas constituyen una base sólida para desarrollar entornos de ciberseguridad avanzados y mejorar las capacidades de análisis de amenazas en la institución.

Firmas.

Adair Villarreal G.
Ejecutor de la investigación

Msc.Javier Torres.
Analista de redes y telecomunicaciones UPEC.

Ing.Milton Del Hierro Msc.
Tutor de Investigación.

Informe Técnico 5: Buenas Prácticas y Lecciones Aprendidas en la Implementación de T-Pot

Objetivo

Este informe resume las buenas prácticas observadas y las lecciones aprendidas durante la implementación y operación de la plataforma de honeypots T-Pot sobre Debian 7. La experiencia adquirida permite mejorar futuras implementaciones y reforzar la seguridad en entornos controlados para análisis de amenazas.

Buenas Prácticas Aplicadas

- Aislamiento de la honeynet en una red separada mediante VLAN o switch dedicado.

- Uso de Docker para contenerizar los honeypots, permitiendo modularidad y fácil reinicio.

- Registro detallado de logs por sensor y almacenamiento persistente.

- Acceso restringido a los puertos de gestión de T-Pot para evitar interferencias externas.

- Programación de backups automáticos de logs y configuraciones.

- Monitoreo visual de eventos en tiempo real con Kibana.

Lecciones Aprendidas

- Debian 7 presenta limitaciones de compatibilidad con versiones recientes de Docker y herramientas de red, por lo que se recomienda considerar versiones más actuales o distribuciones basadas en Ubuntu.
- Algunos contenedores pueden fallar si no se les asigna suficiente RAM. Es recomendable tener al menos 16 GB de RAM.

- Durante las pruebas, se observó que ciertos ataques automatizados se intensificaban los fines de semana, lo cual requiere configurar alertas para detectar picos de actividad.

- Es importante excluir la IP del administrador de las métricas de Kibana para evitar falsos positivos.

- Se identificaron intentos de evasión que no generaron alertas inmediatas, lo cual resalta la necesidad de complementar los honeypots con sistemas IDS adicionales como Snort o Suricata bien configurados.

Recomendaciones futuras.

- Considerar el uso de T-Pot sobre Ubuntu Server LTS o Debian 10+.

- Implementar autenticación multifactor para acceder a la interfaz de administración.

- Desplegar nodos honeypot adicionales en otras ubicaciones geográficas para mejorar cobertura.

- Automatizar el análisis de logs con herramientas como Logstash y alertas por correo electrónico.

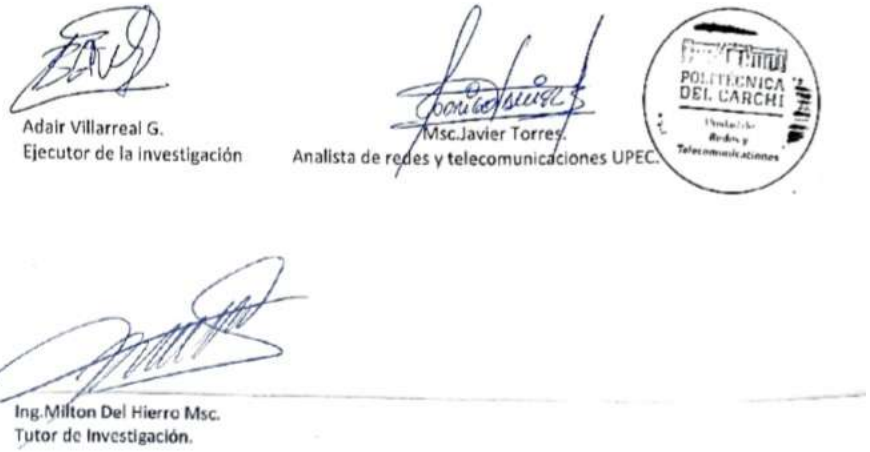
- Establecer una política de actualización de contenedores para mitigar vulnerabilidades en los servicios honeypot.

Conclusión.

La implementación de T-Pot ha sido una experiencia enriquecedora que proporciona visibilidad sobre técnicas y patrones de ataque reales. Las prácticas adoptadas y las lecciones

aprendidas constituyen una base sólida para desarrollar entornos de ciberseguridad avanzados y mejorar las capacidades de análisis de amenazas en la institución.

Firmas.



Anexo 5. Carta de Conformidad

	UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	requisitos de Implementación e instalación de honeynet en la infraestructura de red de la Universidad Politécnica Estatal Del Carchi.

Carta de Conformidad del Departamento de TICs

Tulcán, Ecuador

07 de junio de 2025

Por medio de la presente, el Departamento de Tecnologías de la Información y Comunicaciones (TICs) de la Universidad Politécnica Estatal del Carchi (UPEC) certifica que se ha llevado a cabo de manera satisfactoria la implementación de una plataforma honeynet utilizando la herramienta T-Pot en un entorno controlado dentro de nuestras instalaciones.

Dicha implementación, ejecutada con base en una infraestructura local bajo sistema Debian 7 y contenedores Docker, ha permitido simular servicios vulnerables y registrar intentos reales de acceso por parte de actores maliciosos, generando información valiosa para el análisis de amenazas y fortalecimiento de nuestras defensas en ciberseguridad.

El sistema honeynet ha sido evaluado y cumple con los objetivos propuestos, por lo que este departamento manifiesta su conformidad y aprobación. En consecuencia, se procederá con la recepción formal del entorno honeypot para su uso y continuidad operativa dentro del área de seguridad informática de la institución.

Sin más por el momento, extiendo mis felicitaciones al equipo implementador por su compromiso con la innovación y la mejora continua en temas de seguridad tecnológica.

POLITÉCNICA DEL CARCHI
DIRECCIÓN DE TIC

Atentamente,

Msc. Javier Torres.
Director Departamento de TICs
Universidad Politécnica Estatal del Carchi

Guía de Ataque Simulado a Honeypot Cowrie en T-Pot.

Objetivo

Esta guía documenta cómo simular un ataque realista de fuerza bruta SSH contra Cowrie, uno de los honeypots incluidos en la plataforma T-Pot. La demostración está diseñada para usarse en entornos de laboratorio o académicos.

Requisitos.

- T-Pot corriendo en una máquina (IP ejemplo: 192.168.2.206).

- Cowrie habilitado (activo por defecto en T-Pot).

- Una máquina atacante en la misma red (ej: Kali Linux).

- Hydra instalado: sudo apt install hydra

- Diccionarios: users.txt, passwords.txt, combo.txt, rockyou.txt

Pasos para ejecutar el ataque

1. Verificar conectividad al honeypot con Nmap: nmap
   -p 22 192.168.2.206 nmap -sV 192.168.2.206 nmap
   -A 192.168.2.206

2. Ejecutar ataque básico con diccionarios comunes:

hydra -L users.txt -P passwords.txt ssh://192.168.2.206 -t 4 -V
- Es importante excluir la IP del administrador de las métricas de Kibana para evitar falsos positivos.

3. Ejecutar ataque con combinaciones usuario:contraseña: hydra -C
combo.txt ssh://192.168.1.100 -t 4 -V

4. Ataque realista con diccionario rockyou.txt:

hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.2.206 -t 4 -V

Revisión de logs en T-Pot

- Interfaz Kibana: https://192.168.2.206:64297

- Buscar en dashboards: cowrie.login.failed, cowrie.session.connect

- Archivos de log locales:

sudo cat /data/cowrie/log/cowrie.json | grep login

Conclusión.

El ataque de fuerza bruta SSH realizado contra el honeypot Cowrie, implementado en la plataforma T-Pot, permitió verificar que el sistema responde de forma eficiente ante intentos de intrusión simulados. Durante la ejecución de los ataques desde una máquina en la misma red, T-Pot logró:

Detectar múltiples intentos de autenticación fallida (fuerza bruta).

Registrar las credenciales utilizadas, direcciones IP de origen y comandos enviados.

Visualizar estos eventos en tiempo real a través del panel de Kibana.

Almacenar los registros detallados en el archivo cowrie.json dentro del sistema de archivos (/data/cowrie/log/).

Además, se confirmó que Cowrie simula un entorno SSH realista, permitiendo el acceso con credenciales ficticias y capturando la actividad del atacante en sesiones falsas, lo cual es ideal para análisis forense y evaluación de tácticas de ataque.

En resumen, T-Pot respondió de manera efectiva y confiable, capturando con precisión todos los eventos asociados al ataque, lo cual demuestra su utilidad como herramienta de detección, recolección y análisis de amenazas en un entorno controlado.

Firmas.