INVESTIGACIÓN

Despliegue de Honeypots para la detección proactiva de amenazas cibernéticas

Deployment of honeypots for proactive detection of cyber threats

Ing. Heidy Rodríguez Malvarez*, Ing. Elizabeth Molina Mena[2], Dra.C. Mónica Peña Casanova[3]

Recibido: 11/2025 | Aceptado: 11/2025 | Publicado: 11/2025

Resumen

En un entorno digital cada vez más amenazado por actores maliciosos, la necesidad de implementar mecanismos proactivos de seguridad se ha vuelto crítica. Este artículo presenta el diseño, la configuración y la validación de un sistema de honeypots, con especial énfasis en la herramienta T-Pot, orientado a la detección proactiva de amenazas cibernéticas. T-Pot, reconocido por su arquitectura modular y versatilidad, se despliega como el núcleo de una solución capaz de capturar, analizar y monitorear actividades malintencionadas en tiempo real. En primer lugar, se aborda el estado de la cuestión de los honeypots y sus aplicaciones en la ciberseguridad, destacando su relevancia como técnica de engaño para observar y analizar el comportamiento de los atacantes. En segundo lugar, se define una arquitectura flexible y escalable implementada en un entorno de laboratorio controlado, donde se simulan ataques

* Departamento de Infraestructuras Tecnológicas, Facultad Ciberseguridad, Universidad de las Ciencias Informáticas. heidyrm@uci.com

[2] Dirección de Seguridad Informática, Universidad de las Ciencias Informáticas. angelagv@uci.cu

[3] Departamento de Infraestructuras Tecnológicas, Decana Facultad de Ciberseguridad, Universidad de las Ciencias Informáticas. monica@uci.cu

diversos para evaluar la eficacia del sistema. Los resultados obtenidos permiten validar la capacidad del honeypot para identificar intentos de intrusión y comportamientos sospechosos lo que demuestra la efectividad de T-Pot como herramienta para la detección proactiva de amenazas.

Palabras clave: amenazas cibernéticas, ciberseguridad, detección proactiva, honeypot, T-Pot

Abstract

In an increasingly threatened digital environment, the need to implement proactive security mechanisms has become critical. This article presents the design, configuration and validation of a honeypot system, focusing on the T-Pot tool, aimed at proactive cyber threat detection. T-Pot, recognized for its modular architecture and versatility, is deployed as the core of a solution capable of capturing, analyzing, and monitoring malicious activities in real time. The work begins with an overview of honeypots and their applications in cybersecurity, emphasizing their relevance as a deception technique to observe and analyze attacker behavior. A flexible and scalable architecture is defined and implemented in a controlled laboratory environment where various attacks are simulated to evaluate system effectiveness. The results validate the honeypot's ability to identify intrusion attempts and suspicious behavior, demonstrating T-Pot's effectiveness as a tool for proactive threat detection.

Keywords: *Cyber Threats, Cybersecurity, Proactive Detection, Honeypot, T-Pot*

Introducción

En el panorama contemporáneo de la ciberseguridad, las organizaciones enfrentan una creciente sofisticación y diversificación de las amenazas cibernéticas (Fadziso et al., 2023). Los actores maliciosos, que abarcan desde individuos aislados hasta grupos organizados, emplean tácticas cada vez más avanzadas con el objetivo de comprometer sistemas informáticos, sustraer información confidencial o interrumpir servicios esenciales (Cherqi et al., 2023). Esta

situación ha impulsado la necesidad de adoptar mecanismos proactivos que permitan anticipar los ataques y responder de manera eficaz antes de que estos causen daños irreversibles.

De forma tradicional, las estrategias de defensa de los centros de operaciones de seguridad (SOC) se han basado en el uso de herramientas como los sistemas de detección y prevención de intrusiones (IDS/IPS) y los programas antivirus. Sin embargo, estos métodos presentan limitaciones ante la evolución de las técnicas de evasión utilizadas por los atacantes, quienes logran eludir las soluciones que dependen de firmas o patrones antes conocidos (Skopik et al., 2016). De ahí que resulte imperativo implementar soluciones que trasciendan la detección reactiva y que permitan observar y analizar el comportamiento real de los atacantes en un entorno controlado.

En este contexto, los honeypots emergen como una tecnología eficaz para la localización y el estudio de actividades maliciosas. Estos sistemas, diseñados para parecer vulnerables y atractivos a los atacantes, actúan como señuelos y permiten registrar sus tácticas, técnicas y procedimientos sin poner en riesgo los activos reales de la organización (Lorusso Montiel & Uc Ríos, 2022). La información obtenida mediante honeypots resulta invaluable para fortalecer las defensas de la infraestructura tecnológica y para anticiparse a futuras amenazas.

El presente trabajo tiene como objetivo evaluar el despliegue de honeypots como medida proactiva para la detección temprana de amenazas cibernéticas en entornos organizacionales, con especial énfasis en el uso de la herramienta T-Pot reconocida por su arquitectura modular, capacidad de integración y soporte para múltiples servicios de emulación.

Para alcanzar este propósito, se implementó una solución basada en un entorno de laboratorio controlado que simula diferentes tipos de ataques y analizar la efectividad de la herramienta en la captura, el monitoreo y la correlación de datos relacionados con incidentes de seguridad. Este enfoque contribuye no solo a la validación experimental del honeypot, sino también al fortalecimiento de las estrategias de defensa cibernética de las organizaciones.

Materiales y métodos

El desarrollo de esta investigación se sustentó en un enfoque metodológico mixto. Se combinaron métodos teóricos y empíricos para diseñar, implementar y validar una arquitectura de honeypots orientada a la detección proactiva de amenazas cibernéticas en entornos organizacionales.

Diseño general de la investigación

La investigación se estructuró en tres fases fundamentales: diseño, implementación y validación del honeypot T-Pot.

En la primera fase se realizó una revisión bibliográfica sobre los mecanismos de detección proactiva de amenazas y los diferentes tipos de honeypots, esto posibilitó la selección de la herramienta más adecuada para los requerimientos de la Empresa de Tecnologías de la Información (ETI) de BioCubaFarma.

En la segunda fase se diseñó una arquitectura experimental basada en el despliegue de T-Pot en un entorno controlado de laboratorio, donde se simularon ataques de red y web, para reproducir condiciones similares a las que enfrenta un centro de operaciones de seguridad (COS).

En la tercera fase se realizó la validación empírica del sistema, a través el uso de las métricas de detección, correlación de eventos y análisis de alertas. Esta estructura metodológica demostró la eficacia de T-Pot como mecanismo complementario a las soluciones tradicionales de seguridad (IDS/IPS y antivirus) utilizadas por la ETI (Empresa de Tecnologías de la Información, 2024).

Entorno y herramientas tecnológicas utilizadas

El entorno experimental se desplegó en una infraestructura virtual compuesta por:

- Servidor principal (Ubuntu Server 22.04 LTS): se implementó la plataforma T-Pot, una solución de honeypot de código abierto desarrollada por Deutsche Telekom.
- Máquinas virtuales de ataque: se utilizaron para simular amenazas con herramientas como Nmap y OWASP ZAP, desde un sistema operativo Kali Linux.

- Red virtual controlada (VirtualBox): se configura para aislar los experimentos del entorno productivo y garantizar la seguridad del laboratorio.

En la Figura 1 se muestra el entorno explicado anteriormente:

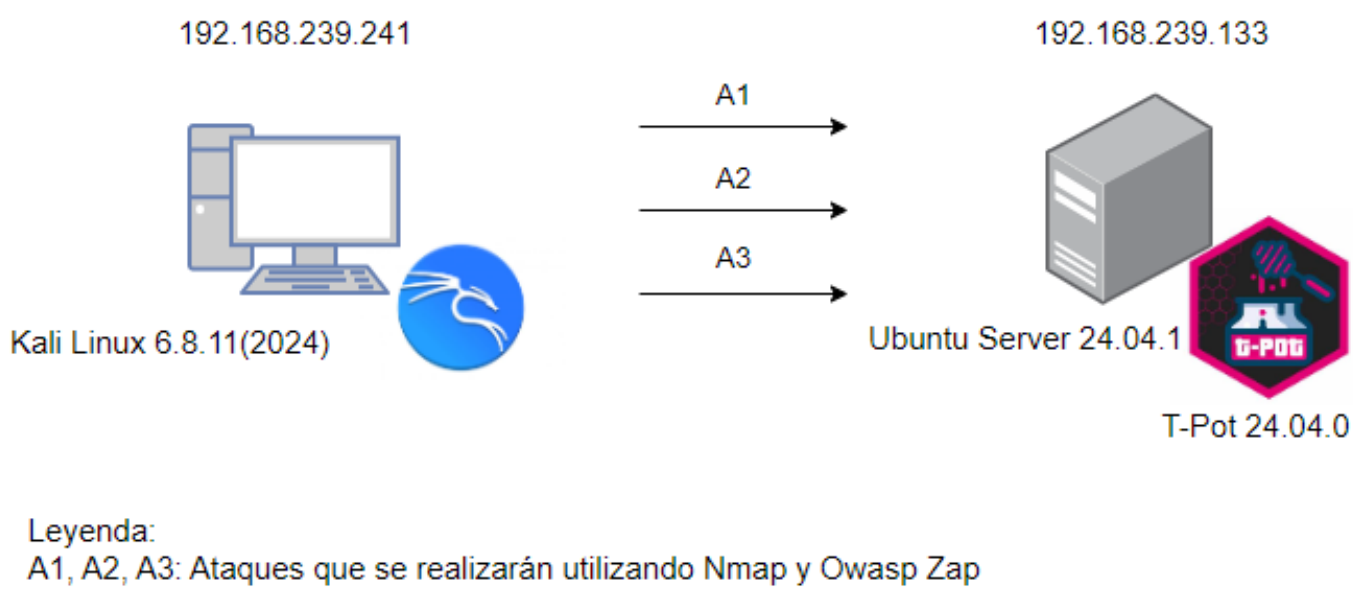

Figura 1. Entorno de laboratorio controlado

El honeypot T-Pot integra diversos módulos de emulación de servicios, entre que destacan Cowrie (SSH/Telnet), Dionaea *(malware catcher)*, *E*lasticpot *(Elasticsearch* honeypot), Heralding (servidor de autenticación) y Mailoney (SMTP falso). Esta arquitectura modular facilita la recolección y clasificación de eventos de acuerdo con el vector de ataque y el servicio objetivo (Telekom Security, 2024).

Para el monitoreo y análisis de datos se emplearon herramientas complementarias como:

- Kibana: permite la visualización de métricas e indicadores de ataque.
- Elasticsearch: funciona como motor central de almacenamiento y análisis.
- Suricata: se emplea para la detección y correlación de tráfico malicioso.
- Spiderfoot y Elasticvue: se utiliza para el reconocimiento automatizado de *hosts* y consultas a los índices de datos capturados.

Métodos científicos

Se aplicaron los siguientes métodos teóricos y empíricos:

- Histórico-lógico: aplicado para analizar la evolución de las amenazas cibernéticas y la progresión de las estrategias de defensa digital.

- Analítico-sintético: para estudiar las tecnologías de honeypots existentes, identificar sus ventajas y desventajas, y fundamentar la elección de T-Pot como solución experimental.
- Modelación: para diseñar el entorno de red simulado que replicó la infraestructura tecnológica de la ETI, con el fin de evaluar la efectividad de la herramienta bajo condiciones reales de ataque.
- Medición: utilizada para valorar el desempeño del honeypot en función de la cantidad y tipo de eventos detectados, frecuencia de alertas generadas y efectividad en la correlación de datos.

Estas herramientas y métodos permitieron establecer un marco experimental sólido, caracterizado por una configuración controlada del honeypot que garantizó la reproducibilidad del estudio y la validez de los resultados obtenidos.

Resultados y discusión

Durante la fase de validación, el honeypot T-Pot demostró su capacidad para capturar y analizar una amplia gama de actividades maliciosas en tiempo real. El sistema registró eventos relacionados con escaneos de red, intentos de autenticación no autorizada, ataques de denegación de servicio y explotación de vulnerabilidades en servicios simulados.

En la Figura 2 muestra un entorno muy activo en términos de ciberamenazas, con un total de 34,818 ataques hacia múltiples honeypots. De este total de ataques se puede establecer que el *Honeytrap* fue el honeypots que más ataques detectó con un total de 32,507 ataques, lo que indica la prevalencia de escaneos automatizados y conexiones no solicitadas dirigidas a servicios frecuentes.

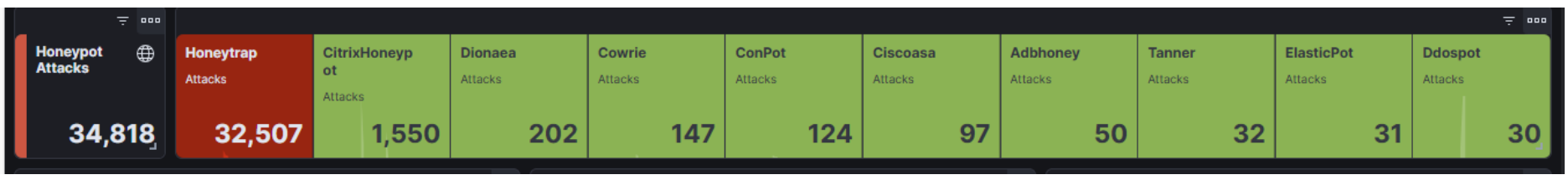

Figura 2. Ataques detectados por el T-Pot

En las pruebas realizadas, se observó que los servicios más atacados fueron SSH (puerto 22), HTTP (puerto 80) y SMB (puerto 445), lo que evidencia la prevalencia de tácticas automatizadas de

reconocimiento y explotación. Estas actividades fueron visualizadas mediante paneles de Kibana, donde se generaron histogramas, gráficos de densidad y mapas geográficos que representaron la procedencia y volumen de los ataques.

El motor Suricata generó múltiples alertas clasificadas según la severidad y tipo de incidente como se presenta en la Figura 3. La categoría predominante es *Generic Protocol Command Decode*, representada en color rojo, que muestra un volumen muy alto de actividad sospechosa relacionada con comandos genéricos de protocolos, asociados a intentos de reconocimiento o escaneo masivo. En menor proporción, se registran otras categorías como *Potentially Bad Traffic* (color verde), que incluye tráfico con características anómalas; *Web Application Attack* (color azul), que representa intentos de ataques dirigidos a aplicaciones web; y *A Network Trojan was Detected* (color morado), relacionada con patrones de troyanos. Además, se identificó tráfico marcado como *Not Suspicious Traffic* (color rosado claro), el cual, aunque no presentó de forma clara comportamientos maliciosos, fue registrado para análisis.

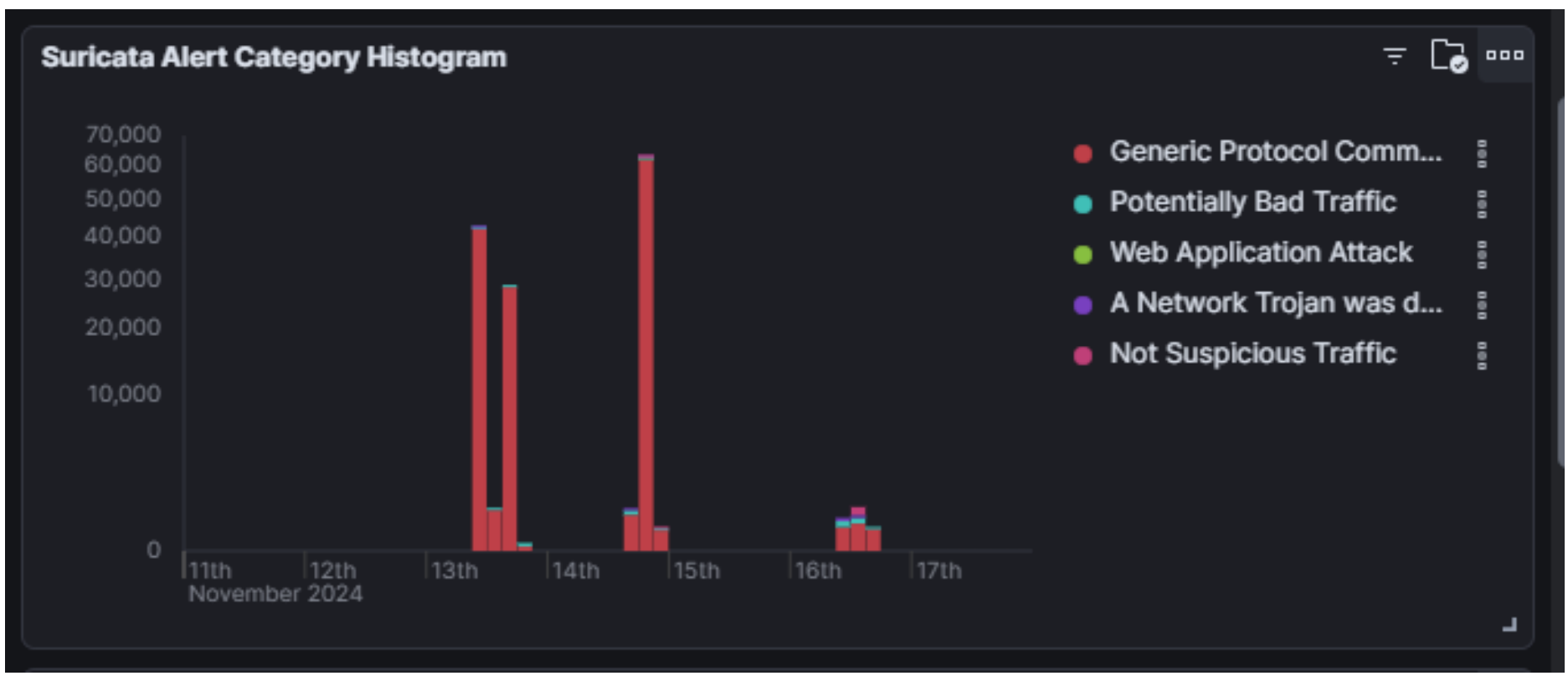

Figura 3. Alertas generadas por Suricata

Uno de los hallazgos más relevantes fue la identificación de patrones repetitivos en las tácticas de ataque. La Figura 4 presenta nubes de palabras (*tag clouds*) que visualizan información relacionada con los intentos de autenticación en el tráfico capturado por el honeypot. En la nube de nombres de usuario se observan varias

entradas de texto relacionadas con los nombres de usuario utilizados en las solicitudes. La palabra «anonymous» es la más destacada, lo que indica que muchos intentos de acceso se realizaron con un nombre de usuario anónimo o no identificado. Otras entradas, como «sip» o «From: sip:nm@nm», podrían sugerir intentos de acceso a servicios relacionados con el protocolo SIP (*Session Initiation Protocol*), es muy común su utilización en comunicaciones VoIP. Otros términos como «Max-Forwards: 70» y «Call-ID: 50000» refuerzan la hipótesis de un ataque o escaneo dirigido a servicios VoIP. Por su parte, la nube de contraseñas resalta los intentos de contraseñas observados durante los ataques. Algunas de las contraseñas más comunes fueron «anonymous», «(empty)», «IEUser@», y «lolo», lo que indica que los atacantes intentaron acceder utilizando credenciales débiles o fácilmente adivinables. El término «(empty)» implica que se intentaron iniciar sesiones sin contraseña, mientras que «anonymous» refuerza el uso de accesos no autenticados.

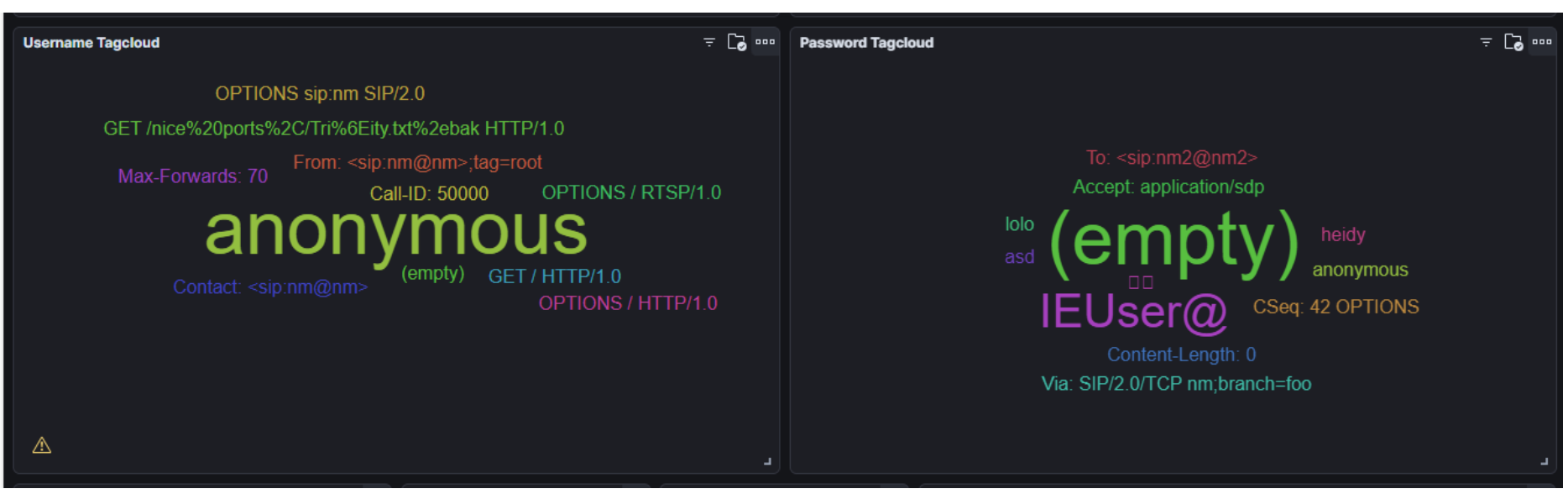

Figura 4. Nube de palabras

Los resultados obtenidos demuestran que el despliegue de T-Pot no solo es útil para la detección temprana de amenazas, sino que también contribuye a la inteligencia de amenazas cibernéticas (CTI), lo que permite a las organizaciones observar el ciclo completo de ataque, desde la fase de exploración hasta la ejecución.

Además, el uso de herramientas integradas como *Elasticvue* facilitó las consultas precisas sobre los datos recolectados, esto optimizó el análisis forense y la clasificación de incidentes. Esta integración pone de manifiesto la fortaleza de T-Pot como plataforma escalable y adaptable, capaz de incorporarse en infraestructuras corporativas o académicas para fines de monitoreo, formación y análisis de amenazas.

Conclusiones

El despliegue del sistema T-Pot como honeypot avanzado en un entorno de laboratorio controlado validó su efectividad como mecanismo proactivo de detección de amenazas cibernéticas. Los resultados confirman que esta herramienta es capaz de identificar intentos de intrusión, escaneos de red y patrones de comportamiento malicioso, ofreciendo una visión integral del panorama de amenazas.

La arquitectura modular de T-Pot, junto con su integración nativa con herramientas de análisis como Kibana, Elasticsearch y Suricata, proporciona un entorno eficiente para la recopilación, la visualización y la correlación de eventos en tiempo real. Esta capacidad constituye una ventaja significativa frente a los mecanismos tradicionales, al permitir una respuesta anticipada ante amenazas emergentes.

Además, el estudio evidencia que la adopción de honeypots puede contribuir a fortalecer las estrategias defensivas del centro de operaciones de seguridad de la ETI, al servir como fuente de información para la inteligencia de amenazas, la capacitación del personal técnico y la investigación de nuevas tendencias de ataque. Como líneas futuras, se propone integrar T-Pot con sistemas SIEM (como OSSIM o ELK), para mejorar la correlación automática de eventos y explorar el despliegue de honeypots distribuidos que posibiliten ampliar el espectro de detección y aumentar la cobertura de la red.

En síntesis, el trabajo realizado demuestra que la implementación de honeypots constituye una alternativa viable, escalable y de bajo costo para el fortalecimiento de la ciberseguridad en infraestructuras críticas y entornos empresariales cubanos.

Referencias bibliográficas

Cherqi, O., El Omri, A., & Achahbar, A. (2023). *Cyber Threat Intelligence approaches for proactive security*. *Journal of Cyber Defense Studies*, 9(2), 45–59.

Empresa de Tecnologías de la Información. (2024). *Centro de Operaciones de Seguridad de BioCubaFarma*. La Habana, Cuba.

Fadziso, F., Moyo, T., & Zhou, M. (2023). *The evolution of cyber threats and defense mechanisms. International Journal of Information Security*, 22(3), 214–229.

Lorusso Montiel, J., & Uc Ríos, A. (2022). *Honeypots como estrategia de defensa cibernética. Revista de Seguridad Informática*, 18(2), 45–53.

Skopik, F., Settanni, G., & Fiedler, R. (2016). *A survey on threat intelligence sharing platforms. Computers & Security*, 61, 1–16.

Telekom Security. (2024). *T-Pot Documentation: Multi-Honeypot Platform*. Deutsche Telekom AG. Recuperado de https://github.com/telekom-security/tpotce