TẠP CHÍ KHOA HỌC ĐẠI HỌC CỬU LONG
https://tapchikhdhcl.edu.vn
https://vjol.info.vn/index.php/dhcl
P-ISSN 3093-3196
E-ISSN 3093-3226

NGHIÊN CỨU VÀ ĐÁNH GIÁ HỆ THỐNG HONEYPOT TÍCH HỢP T-POT TRONG GIÁM SÁT TẤN CÔNG MẠNG

RESEARCH AND EVALUATION OF A T-POT-INTEGRATED HONEYPOT SYSTEM FOR CYBER ATTACK MONITORING

Huỳnh Tấn Khoa, Phạm Phú Thạnh, Nguyễn Tuấn Kiệt, Phan Hồ Duy Phương, Trần Thị Thúy*
Trường Đại học Cửu Long
Email: tranthithuy@mku.edu.vn

DOI: https://doi.org/10.65934/mkusj.2026.43.830
Ngày nhận bài: 15/12/2025 *Ngày phản biện: 05/01/2026* *Ngày duyệt bài: 01/06/2026*

TÓM TẮT

Trong bối cảnh các mối đe dọa an ninh mạng ngày càng gia tăng về số lượng và mức độ tinh vi, việc triển khai các cơ chế giám sát chủ động trở thành yêu cầu cấp thiết đối với các hệ thống thông tin. Nghiên cứu này tập trung thiết kế, triển khai và đánh giá hệ thống Honeypot tích hợp T-Pot trên nền tảng Linux, kết hợp với Elastic Stack và Kibana nhằm thu thập, phân tích và trực quan hóa dữ liệu tấn công mạng trong môi trường thực tế. Hệ thống cho phép ghi nhận và phân loại nhiều hình thức tấn công phổ biến như brute-force SSH/Telnet, khai thác dịch vụ mạng và dò quét ứng dụng Web; đồng thời xác định địa chỉ IP nguồn và phân tích hành vi tương tác sau xâm nhập. Kiến trúc tích hợp giúp chuẩn hóa, lưu trữ và trực quan hóa log theo thời gian thực, hỗ trợ phát hiện bất thường và kích hoạt cơ chế cảnh báo tự động khi vượt ngưỡng cấu hình. Kết quả thực nghiệm cho thấy T-Pot không chỉ đóng vai trò là công cụ thu thập dữ liệu thụ động mà còn nâng cao hiệu quả giám sát an ninh thông qua khả năng phân tích tập trung, trực quan hóa xu hướng tấn công và hỗ trợ phản ứng kịp thời. Mô hình triển khai tiệm cận các chức năng cơ bản của hệ thống SIEM, chứng minh tính khả thi và hiệu quả của giải pháp trong nghiên cứu, đào tạo và thử nghiệm an ninh mạng.

***Từ khóa**: Honeypot, T-Pot, An ninh mạng, Phân tích tấn công, SIEM, Elastic Stack*

ABSTRACT

In the context of increasingly sophisticated cyber threats, proactive monitoring mechanisms are essential for protecting information systems. This study presents the design, deployment, and evaluation of an integrated honeypot system based on T-Pot, deployed on a Linux platform and integrated with the Elastic Stack and Kibana for centralized data collection, analysis, and visualization of network attack events. The system records and categorizes common attack types, including SSH/Telnet brute-force attempts, network service exploitation, and web-based reconnaissance activities. It also enables source IP identification and behavioral analysis of attacker interactions within the simulated environment. The integrated architecture facilitates log normalization, indexing, and real-time visualization, supporting anomaly detection and automated alert mechanisms based on predefined thresholds. Experimental results indicate that T-Pot not only functions as a passive data collection tool but also significantly enhances security monitoring capabilities through centralized analytics and trend visualization. The proposed model approaches the core functionalities of a basic SIEM solution, demonstrating its practicality and effectiveness for cybersecurity research, training, and experimental deployments.

***Keywords**: Honeypot, T-Pot, Cybersecurity, Attack Analysis, SIEM, Elastic Stack*

GIỚI THIỆU

Trong bối cảnh số lượng và mức độ phức tạp của các cuộc tấn công mạng ngày càng gia tăng, đặc biệt là các cuộc tấn công tự động như quét lỗ hổng (*scanning*) hay tấn công dò mật khẩu (*brute-force*), việc đảm bảo an ninh mạng trở nên cấp thiết hơn bao giờ hết. Việc thu thập dữ liệu tấn công thực tế đóng vai trò then chốt trong việc cải thiện các cơ chế phòng thủ, giúp các tổ chức nhận diện kịp thời các mối đe dọa, dự đoán xu hướng

tấn công và tăng cường khả năng phản ứng trước các sự cố bảo mật.

Honeypot là một công cụ phòng thủ chủ động, được thiết kế để giả lập các hệ thống hoặc dịch vụ dễ bị tấn công nhằm thu thập thông tin về hành vi của kẻ tấn công, thay vì chỉ phòng thủ thụ động. Trong nghiên cứu này, mục tiêu chính là: (1) Thiết lập một hệ thống Honeypot tích hợp T-Pot hoạt động ổn định trên nền tảng Linux; (2) Kết hợp hệ thống phân tích và trực quan hóa dữ liệu Elastic Stack để giám sát và đánh giá các cuộc tấn công mạng; và (3) Đánh giá hiệu quả của hệ thống trong việc mô phỏng hành vi hệ thống thật, phát hiện tấn công và cảnh báo kịp thời các mối đe dọa.

Bài báo được trình bày gồm các phần sau: phần Tổng quan cung cấp các nghiên cứu liên quan và khung lý thuyết; phần Phương pháp mô tả chi tiết cách triển khai hệ thống T-Pot và tích hợp Elastic Stack; phần Kết quả trình bày dữ liệu thu được từ thực nghiệm và phân tích hiệu quả hệ thống; cuối cùng, phần Kết luận tổng hợp kết quả nghiên cứu và đề xuất hướng phát triển tương lai.

1. Tổng quan nghiên cứu về Honeypot và giám sát tấn công mạng

Honeypot là một hệ thống bảo mật được thiết kế để mô phỏng các dịch vụ hoặc hệ thống thật nhằm thu hút và ghi nhận các hành vi tấn công mạng. Mục tiêu chính của Honeypot là thu thập thông tin về kỹ thuật, chiến lược và nguồn gốc tấn công, hỗ trợ nghiên cứu và cải thiện các cơ chế phòng thủ. Về cơ bản, Honeypot được phân thành hai loại: Honeypot tương tác thấp (Low-interaction), mô phỏng các dịch vụ cơ bản và hạn chế rủi ro với hệ thống thật; và Honeypot tương tác cao (High-interaction), cung cấp môi trường gần giống hệ thống thật, cho phép quan sát toàn bộ hành vi của kẻ tấn công nhưng đi kèm nguy cơ cao hơn.

Trong những năm gần đây, Honeypot đã được nghiên cứu rộng rãi như một phương pháp phòng thủ chủ động, đóng vai trò quan trọng trong việc thu thập dữ liệu tấn công thực tế và hỗ trợ xây dựng các chiến lược an ninh mạng hiệu quả. Khác với các hệ thống phòng thủ truyền thống như Firewall hay IDS/IPS vốn chỉ phản ứng với lưu lượng đáng ngờ, Honeypot chủ động "thu hút" kẻ tấn công, từ đó ghi nhận chi tiết các hành vi xâm nhập, kỹ thuật khai thác và công cụ được sử dụng.

Nhiều nghiên cứu chỉ ra rằng Honeypot đặc biệt hiệu quả trong việc phát hiện các cuộc tấn công tự động quy mô lớn như scanning, brute-force và malware propagation, vốn chiếm tỷ lệ cao trong lưu lượng tấn công Internet hiện nay (Kumar et al., 2023; Fuzi et al., 2024). Ngoài ra, dữ liệu từ Honeypot còn được sử dụng để xây dựng tập dữ liệu huấn luyện cho các hệ thống phát hiện xâm nhập dựa trên học máy, góp phần nâng cao khả năng phát hiện các mối đe dọa chưa từng biết trước (zero-day).

Xu hướng nghiên cứu gần đây tập trung vào việc tích hợp Honeypot với các nền tảng phân tích log và SIEM, nhằm nâng cao khả năng giám sát tập trung và phản ứng sự cố. Các mô hình này cho phép không chỉ ghi nhận dữ liệu thô mà còn phân tích mối tương quan giữa các sự kiện, xác định xu hướng tấn công theo thời gian và hỗ trợ cảnh báo sớm. Tuy nhiên, việc triển khai SIEM thương mại thường đòi hỏi chi phí cao và hạ tầng phức tạp.

Trong bối cảnh đó, T-Pot nổi lên như một giải pháp mã nguồn mở tích hợp sẵn nhiều Honeypot và Elastic Stack, cho phép triển khai nhanh chóng một hệ thống giám sát tấn công tiệm cận SIEM với chi phí thấp. Mặc dù đã có nhiều nghiên cứu đề cập đến T-Pot, vẫn còn thiếu các đánh giá thực nghiệm chi tiết trong môi trường triển khai thực tế, đặc biệt là phân tích hiệu quả giám sát, khả năng cảnh báo và giá trị ứng dụng trong đào tạo và nghiên cứu an ninh mạng. Nghiên cứu này được thực hiện nhằm bổ sung góc nhìn đó thông qua triển khai và đánh giá trực tiếp hệ thống T-Pot tích hợp Elastic Stack.

T-Pot là một giải pháp Honeypot tích hợp, kết hợp nhiều loại Honeypot như Cowrie, Dionaea, ElasticPOT cùng các công cụ phân tích dữ liệu và trực quan hóa như Elastic Stack. So với việc triển khai từng Honeypot riêng lẻ, T-Pot mang lại nhiều lợi ích, bao gồm khả năng quản lý tập trung, tối ưu hóa thu thập dữ liệu, đồng thời cung cấp môi trường đa dạng mô phỏng nhiều loại dịch vụ và giao thức, từ đó nâng cao chất lượng thông tin thu thập được.

Elastic Stack bao gồm Elasticsearch, Logstash và Kibana, được sử dụng để xử lý, lưu trữ và trực quan hóa dữ liệu log từ các Honeypot. Hệ thống

này cho phép tổng hợp lượng lớn dữ liệu tấn công, phân loại các sự kiện, và cung cấp các biểu đồ, dashboard trực quan, hỗ trợ việc giám sát liên tục và cảnh báo kịp thời. Khi được triển khai kết hợp với T-Pot, Elastic Stack tiệm cận mô hình SIEM (Security Information and Event Management) chuẩn, cung cấp khả năng phát hiện, phản ứng và ghi nhận các mối đe dọa một cách hiệu quả.

2. Phương pháp triển khai và nghiên cứu

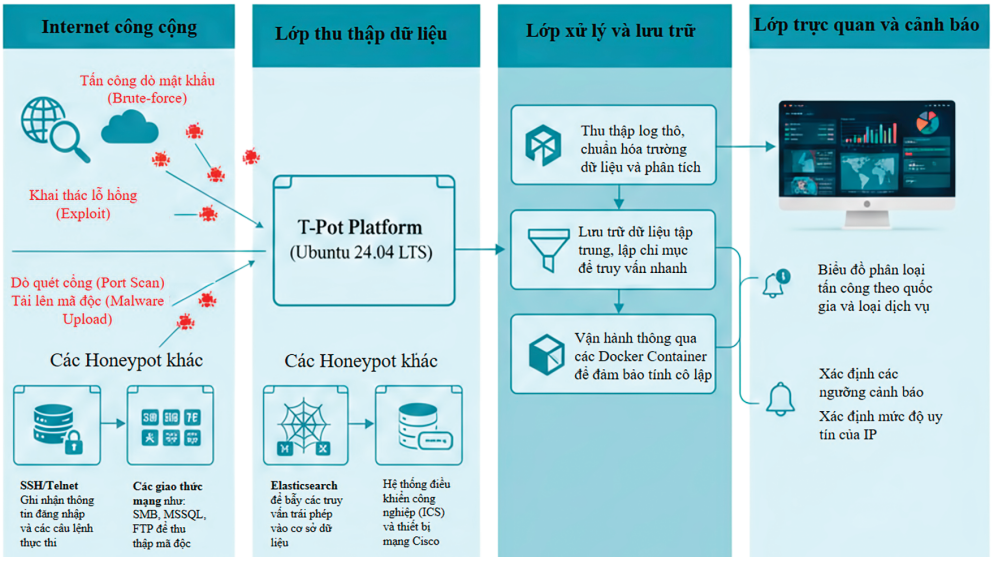
Thiết kế mô hình hệ thống

Hệ thống nghiên cứu được thiết kế theo kiến trúc tích hợp tập trung, trong đó T-Pot đóng vai trò nền tảng lõi để triển khai và quản lý nhiều Honeypot thành phần trong cùng một môi trường (Hình 1). Kiến trúc này cho phép xây dựng một chu trình khép kín từ thu thập dữ liệu, xử lý, lưu trữ đến trực quan hóa và cảnh báo, đảm bảo khả năng giám sát liên tục trước các mối đe dọa trên Internet. Các Honeypot được vận hành dưới dạng container nhằm đảm bảo tính cô lập, hạn chế rủi ro lan truyền nếu xảy ra khai thác thành công trong môi trường giả lập.

Ở lớp thu thập dữ liệu, nhiều Honeypot hoạt động song song để mô phỏng các dịch vụ mạng phổ biến. Cụ thể, Cowrie giả lập dịch vụ SSH và Telnet nhằm ghi nhận các cuộc tấn công brute-force và tương tác dòng lệnh sau khi đăng nhập thành công; Dionaea tập trung thu thập các khai thác nhắm vào dịch vụ mạng như SMB, FTP hoặc MSSQL; trong khi ElasticPOT mô phỏng dịch vụ Elasticsearch để phát hiện các truy vấn trái phép và hành vi dò quét dữ liệu. Các Honeypot này tiếp xúc trực tiếp với Internet công cộng, qua đó ghi nhận lưu lượng tấn công thực tế từ nhiều nguồn khác nhau.

Luồng dữ liệu trong hệ thống được thiết kế theo trình tự tự động hóa. Khi một sự kiện tấn công xảy ra, Honeypot tương ứng sẽ ghi nhận thông tin chi tiết như địa chỉ IP nguồn, cổng truy cập, thời gian, chuỗi lệnh thực thi hoặc tệp được tải xuống. Các log này sau đó được chuyển đến Logstash để chuẩn hóa, phân tích trường dữ liệu và chuyển đổi sang định dạng thống nhất. Dữ liệu đã xử lý tiếp tục được lưu trữ và lập chỉ mục trong Elasticsearch, cho phép tìm kiếm và truy vấn nhanh theo nhiều tiêu chí khác nhau. Trên cơ sở đó, Kibana cung cấp các dashboard trực quan hiển thị số lượng sự kiện, loại hình tấn công, phân bố địa lý và xu hướng theo thời gian thực.

Bên cạnh chức năng giám sát, hệ thống còn được cấu hình cơ chế cảnh báo tự động. Khi phát hiện các điều kiện vượt ngưỡng, chẳng hạn số lượng lớn đăng nhập thất bại trong thời gian ngắn hoặc lưu lượng truy cập tăng đột biến, hệ thống sẽ kích hoạt thông báo nhằm hỗ trợ người quản trị phản ứng kịp thời. Nhờ thiết kế theo mô hình nhiều lớp với khả năng mở rộng linh hoạt, kiến trúc này không chỉ phục vụ mục tiêu nghiên cứu và thực nghiệm mà còn có thể phát triển thành một hệ thống giám sát an ninh mạng tiệm cận mô hình SIEM cơ bản trong môi trường thực tế.



Hình 1. Kiến trúc hệ thống T-Pot Tích hợp Elastic Stack

Cấu hình và triển khai

Hệ thống được triển khai trên nền tảng Ubuntu 24.04 LTS nhằm đảm bảo tính ổn định lâu dài, khả năng cập nhật bảo mật và mở rộng linh hoạt. Giải pháp Honeypot được sử dụng là T-Pot, một nền tảng mã nguồn mở tích hợp nhiều loại Honeypot và công cụ phân tích tập trung. Quá trình triển khai bao gồm việc thiết lập môi trường hệ thống trên hạ tầng ảo hóa (Cloud/VPS) để máy chủ có thể tiếp xúc trực tiếp với môi trường Internet thực tế, sau đó tiến hành cài đặt và cấu hình T-Pot ở chế độ Standard, cho phép kích hoạt đồng thời hơn 10 loại Honeypot khác nhau. Các thành phần Honeypot được vận hành dưới dạng container nhằm đảm bảo tính cô lập và an toàn hệ thống. Đồng thời, hệ thống được tích hợp với Elastic Stack để thu thập, lưu trữ và trực quan hóa dữ liệu tấn công theo thời gian thực.

Trong số các Honeypot được triển khai, Cowrie đóng vai trò quan trọng khi giả lập các dịch vụ SSH và Telnet, cho phép ghi nhận các cuộc tấn công brute-force, thu thập thông tin đăng nhập do kẻ tấn công sử dụng và lưu lại toàn bộ phiên tương tác phục vụ phân tích hành vi. Các tham số cấu hình của hệ thống được tinh chỉnh nhằm cân bằng giữa khả năng ghi nhận dữ liệu đầy đủ, hiệu năng vận hành và đảm bảo an toàn cho hạ tầng thật, tránh nguy cơ bị lợi dụng làm bàn đạp cho các hoạt động tấn công khác.

Để đảm bảo tính khách quan và khả năng tái lặp của thực nghiệm, môi trường triển khai được thiết lập với cấu hình phần cứng gồm CPU 4 nhân, RAM 8GB và ổ cứng SSD 100GB, đáp ứng yêu cầu vận hành đồng thời nhiều container Honeypot và hệ thống phân tích log. Dữ liệu được thu thập liên tục trong vòng 24 giờ, từ 00:00 ngày 06/09/2025 đến 00:00 ngày 07/09/2025. Cách tiếp cận này giúp đảm bảo môi trường quan sát đủ thực tế để ghi nhận các hành vi tấn công phổ biến trên Internet, đồng thời duy trì được sự kiểm soát và an toàn cho hệ thống nghiên cứu.

Cơ chế thu thập và cảnh báo

Dữ liệu tấn công từ các Honeypot được thu thập liên tục và gửi đến Elastic Stack thông qua Logstash, nơi dữ liệu được xử lý, phân loại và lưu trữ. Kibana cung cấp trực quan hóa dạng biểu đồ, bảng thống kê và dashboard tổng quan. Ngoài ra, cơ chế cảnh báo tự động được triển khai bằng các script tùy chỉnh, kết hợp với công cụ như msmtp, để gửi thông báo khi phát hiện các hành vi đáng ngờ, đảm bảo người quản trị có thể phản ứng nhanh chóng trước các sự cố bảo mật.

3. Phân tích kết quả nghiên cứu

Trong quá trình triển khai hệ thống T-Pot, dữ liệu về các cuộc tấn công mạng được thu thập liên tục trong một khoảng thời gian xác định. Thống kê định lượng cho thấy nhiều loại tấn công phổ biến như SSH brute-force, Telnet, và các yêu cầu Web (HTTP/HTTPS) đã được ghi nhận. Phân tích nguồn tấn công chỉ ra các địa chỉ IP hàng đầu cùng với quốc gia xuất xứ, giúp xác định các mối đe dọa chủ yếu. Dữ liệu này được trực quan hóa bằng Kibana dưới dạng biểu đồ và bảng thống kê, cho phép dễ dàng quan sát số lượng, loại hình và nguồn gốc tấn công.

Phân tích định lượng các cuộc tấn công ghi nhận

Dữ liệu thống kê cho thấy tổng số sự kiện tấn công tập trung chủ yếu vào các Honeypot giả lập dịch vụ truy cập từ xa (Hình 2). Cụ thể, Cowrie ghi nhận hơn 11.000 sự kiện (chiếm khoảng 64,7%), chủ yếu là các phiên brute-force nhắm vào SSH và Telnet. Điều này cho thấy các chiến dịch dò quét tự động sử dụng danh sách tài khoản và mật khẩu phổ biến vẫn là phương thức tấn công chủ đạo.

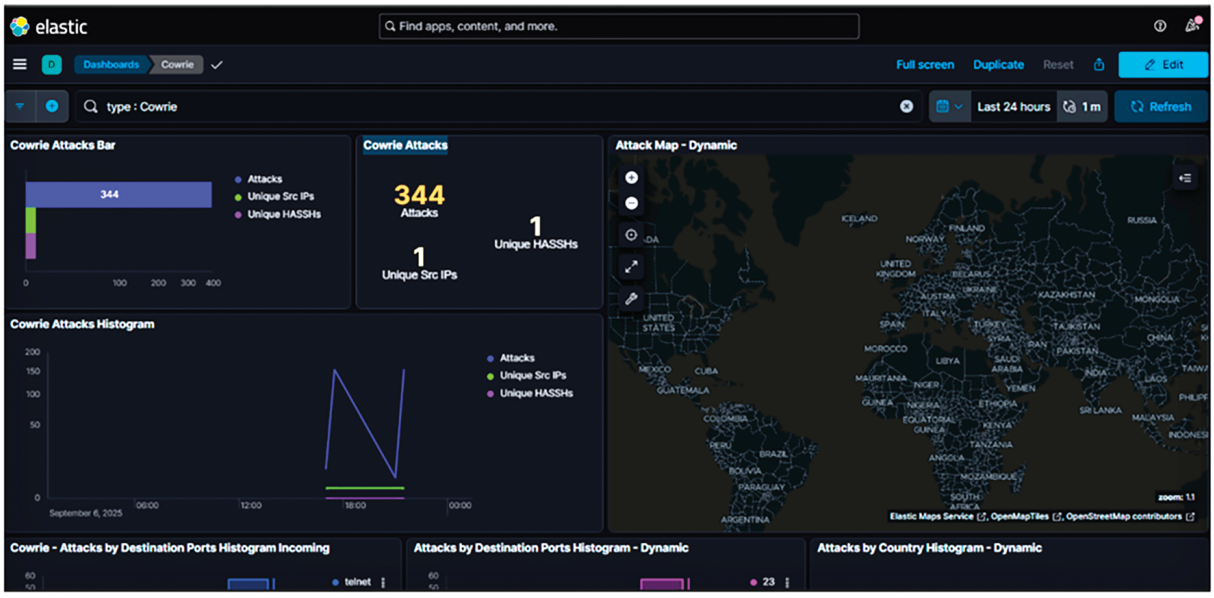
Honeypot Dionaea ghi nhận khoảng 5.000 sự kiện (29,4%), tập trung vào các giao thức như SMB và MSSQL, phản ánh xu hướng khai thác lỗ hổng dịch vụ mạng. Trong khi đó, ConPot ghi nhận 611 sự kiện (3,6%), cho thấy các hệ thống điều khiển công nghiệp (ICS) vẫn là mục tiêu bị dò quét dù với tần suất thấp hơn. Các Honeypot khác như ElasticPOT, ADB hoặc Mail chiếm khoảng 2,3% tổng số sự kiện.

Phân tích theo trục thời gian cho thấy tần suất tấn công đạt đỉnh vào khoảng 18:00, với sự gia tăng đột biến của các phiên brute-force SSH. Hiện tượng này có thể liên quan đến chu kỳ hoạt động của botnet toàn cầu hoặc thời điểm kích hoạt chiến dịch quét tự động.

Phân tích địa chỉ IP nguồn và dữ liệu địa lý cho thấy phần lớn các cuộc tấn công xuất phát từ nhiều khu vực khác nhau, tập trung tại các quốc

gia có hạ tầng Internet phát triển ở Bắc Mỹ và châu Âu. Tuy nhiên, cần lưu ý rằng đây thường là các máy chủ trung gian hoặc thiết bị thuộc botnet phân tán, không phản ánh chính xác vị trí thực của kẻ tấn công.

Đáng chú ý, khi kẻ tấn công đăng nhập thành công vào môi trường giả lập của Cowrie, hệ thống ghi nhận nhiều lệnh kiểm tra thông tin hệ thống, tải xuống tệp thực thi, hoặc cố gắng thiết lập kết nối điều khiển từ xa. Những hành vi này tương ứng với các chiến thuật và kỹ thuật phổ biến trong chuỗi xâm nhập, cung cấp dữ liệu giá trị cho việc phân tích TTPs (Tactics, Techniques, and Procedures).



Hình 2. Kết quả ghi nhận cuộc tấn công SSH/Telnet trên Cowrie Honeypot

Phân tích nguồn gốc và hành vi tấn công

Phân tích địa chỉ IP nguồn và thông tin địa lý cho thấy các cuộc tấn công đến từ nhiều quốc gia và khu vực khác nhau, trong đó tập trung chủ yếu tại các khu vực có hạ tầng Internet phát triển. Kết quả này phù hợp với xu hướng toàn cầu được ghi nhận trong các báo cáo an ninh mạng, nơi phần lớn các cuộc tấn công xuất phát từ các mạng trung gian, máy chủ bị chiếm quyền hoặc botnet phân tán trên nhiều quốc gia.

Một điểm đáng chú ý là hệ thống T-Pot cho phép ghi nhận chi tiết các hành vi sau khi kẻ tấn công đăng nhập thành công vào Honeypot Cowrie. Các lệnh được thực thi thường nhằm kiểm tra môi trường hệ thống, tải mã độc, thiết lập backdoor hoặc mở rộng quyền truy cập. Những hành vi này phản ánh các kịch bản xâm nhập phổ biến trong thực tế và cung cấp nguồn dữ liệu có giá trị cao cho việc phân tích chiến thuật, kỹ thuật và quy trình tấn công (Tactics, Techniques, and Procedures - TTPs).

Đánh giá hiệu quả giám sát và cảnh báo

Việc tích hợp T-Pot với Elastic Stack đã nâng cao đáng kể khả năng giám sát tập trung và phân tích dữ liệu tấn công. Các dashboard trên Kibana cung cấp cái nhìn tổng quan theo thời gian thực về số lượng, loại hình và nguồn gốc các cuộc tấn công, giúp người quản trị nhanh chóng nhận diện các xu hướng bất thường và đánh giá mức độ nghiêm trọng của từng sự kiện (Hình 3).

Cơ chế cảnh báo tự động được triển khai hoạt động ổn định và kịp thời, đặc biệt hiệu quả trong việc phát hiện các hành vi đáng ngờ như số lượng lớn lần đăng nhập thất bại trong thời gian ngắn hoặc sự gia tăng đột biến của lưu lượng tấn công. Mặc dù hệ thống chưa tích hợp cơ chế phản ứng tự động ở mức độ cao như các nền tảng SOAR thương mại, kết quả thực nghiệm cho thấy T-Pot kết hợp Elastic Stack đã tiệm cận mô hình SIEM cơ bản, đủ khả năng đáp ứng nhu cầu giám sát và phân tích trong môi trường nghiên cứu, đào tạo và triển khai thử nghiệm.

Hình 3. Tổng quan các cuộc tấn công ghi nhận bởi Honeypot trên T-Pot

4. Đánh giá kết quả nghiên cứu

Từ các kết quả thu được, có thể khẳng định rằng Honeypot T-Pot không chỉ là công cụ thu thập dữ liệu tấn công mà còn là một nền tảng hiệu quả cho việc nghiên cứu và nâng cao năng lực phân tích an ninh mạng. So với các cơ chế phòng thủ truyền thống vốn chỉ phản ứng với lưu lượng đáng ngờ, Honeypot cung cấp góc nhìn chủ động và chi tiết hơn về hành vi của kẻ tấn công, đặc biệt hữu ích trong việc nghiên cứu các mối đe dọa mới và xu hướng tấn công đang nổi lên.

Kết quả nghiên cứu có sự tương đồng với các công trình trước đây khi khẳng định hiệu quả của T-Pot trong việc phát hiện và ghi nhận các cuộc tấn công tự động quy mô lớn. So với nghiên cứu của Fuzi et al. (2024), công trình này không chỉ xác nhận khả năng phát hiện tấn công brute-force mà còn mở rộng bằng việc cấu hình cơ chế cảnh báo tự động thông qua dịch vụ gửi email (MSMTP), nâng cao tính kịp thời trong phản ứng sự kiện. So với nghiên cứu của Biswa et al. (2025), vốn tập trung vào so sánh giữa Honeytrap và T-Pot, nghiên cứu này đi sâu vào khả năng tích hợp T-Pot với Elastic Stack nhằm tiệm cận mô hình SIEM. Việc thu thập, phân tích và trực quan hóa tập trung giúp hệ thống không chỉ dừng lại ở mức ghi nhận thụ động mà còn hỗ trợ đánh giá xu hướng, phát hiện bất thường và xây dựng quy trình giám sát an ninh có hệ thống.

Tuy nhiên, hệ thống vẫn tồn tại một số hạn chế. Phần lớn các Honeypot trong T-Pot thuộc loại tương tác thấp đến trung bình, do đó chưa phản ánh đầy đủ hành vi của hệ thống thật trong các kịch bản tấn công phức tạp. Ngoài ra, hệ thống hiện mới dừng lại ở mức phát hiện và cảnh báo, chưa tích hợp các cơ chế phản ứng tự động nhằm giảm thiểu hoặc ngăn chặn tác động của tấn công trong thời gian thực. Những hạn chế này mở ra tiềm năng phát triển trong tương lai, đặc biệt khi kết hợp Honeypot với các kỹ thuật học máy, phân tích hành vi nâng cao và mô hình phòng thủ chủ động.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Bài báo đã trình bày việc thiết lập thành công hệ thống Honeypot tích hợp T-Pot trên nền tảng Linux, kết hợp với Elastic Stack để thu thập, phân tích và trực quan hóa các dữ liệu tấn công mạng. Hệ thống cho thấy khả năng ghi nhận chi tiết các hành vi xâm nhập, phân loại các loại tấn công và cung cấp cảnh báo kịp thời, từ đó nâng cao hiệu quả giám sát và hỗ trợ việc quản lý rủi ro. Kết quả nghiên cứu khẳng định rằng Honeypot là một công cụ phòng thủ hữu hiệu, đặc biệt khi được tích hợp với các công cụ phân tích dữ liệu, góp phần nâng cao năng lực phát hiện và phòng ngừa các mối đe dọa mạng.

Trên cơ sở kết quả hiện tại, các hướng nghiên cứu tiếp theo có thể bao gồm: (1) Nâng cấp hệ thống lên các Honeypot tương tác cao hơn nhằm mô phỏng hành vi hệ thống thật một cách toàn diện hơn; (2) Tích hợp các công cụ phân tích nâng cao,

như học máy (machine learning), để tự động phân loại và dự đoán các kiểu tấn công mới; và (3) Xây dựng mô hình phản ứng tự động (Active Defense) kết hợp với Honeypot để vừa phát hiện vừa chủ động ngăn chặn các cuộc tấn công, hướng tới một hệ thống phòng thủ mạng thông minh và tự động.

TÀI LIỆU THAM KHẢO

Mohd Faris Mohd Fuzi, Mazlan, M. F., Jamaluddin, M. N. F., & Abd Halim, I. H. (2024). Performance analysis of network intrusion detection using T-Pot honeypots. *Journal of Computing Research and Innovation*, *9*(2), 348-360.

Biswa, S., Wangmo, P., Rangdel, T., Wangchuk, T., Tshering, Y., & Yangchen, T. (2025). Securing network using honeypots: A comparative study on Honeytrap and T-Pot. *JNEC Thruel Rig Sar Toed*, *7*(1), 12-20.

Kumar, V., Bhardwaj, S., Chouksey, P., Sadotra, P., & Chopra, M. (2023). Emerging trends in honeypot research: A review of applications and techniques. *International Journal of Human Computations & Intelligence*.

Sihombing, R. A., & Dewi, N. M. J. P. (2024). A literature review: Honeypot-based security solutions for safeguarding critical data at BMKG. *Journal of Computation Physics and Earth Science (JoCPES)*.

Adnyana, I. G., Dirgayusari, A. M., & Atmaja, K. J. (2023). Data visualization for building a cyber-attack monitoring dashboard based on honeypot. *Sinkron: Jurnal dan Penelitian Teknik Informatika*, *8*(4).

Kosheliuk, V., & Tulashvili, Y. (2023). Implementing honeypots for detecting cyber threats with AWS using the ELK. *International Journal of Computing*.

Hafiz, M., & Soewito, B. (2022). Information security systems design using SIEM, SOAR and honeypot. *Jurnal Pendidikan Tambusai*, *6*(2), 15527-15541.

Lu, K. C., Liu, I. H., Liao, J. W., Wu, S. C., Liu, Z. C., & Li, J. S. (2019). Evaluation and build to honeypot system about SCADA security for large-scale IoT devices. *Journal of Robotics, Networking and Artificial Life*.

Alatawi, E., & Albalawi, U. (2025). Harnessing AI for cyber defense: Honeypot-driven intrusion detection systems. *Symmetry*, *17*(5), Article 628.

Martínez, C. J. S., Moreno, H. O. A., & Hernández, M. B. A. (2023). Analysis of intrusions into computer systems using honeypots. *International Journal of Intelligent Systems and Applications in Engineering*.

Spitzner, L. (2003). *Honeypots: Tracking Hackers*. Addison-Wesley Professional.

Provos, N., & Holz, T. (2008). *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison-Wesley Professional.

Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., & Schönfelder, J. (2016). A survey on honeypot software and data analysis. *ACM Computing Surveys*, 49(2), Article 25.

Grudziecki, P., Hamann, R., & Schmitz, C. (2012). The Honeynet Project: Detecting and analysing cyber attacks. In *Proceedings of the International Conference on Cyber Conflict (CyCon)*.

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology (NIST).

Behl, A., & Behl, K. (2017). Cybersecurity and cyberwar: What everyone needs to know about honeypots and intrusion detection. *International Journal of Information Security Science*, 6(4), 67-75.

Almeshekah, M. H., & Spafford, E. H. (2014). Planning and integrating deception into computer security defenses. In *Proceedings of the 2014 New Security Paradigms Workshop (NSPW)*.