Máy tính & Bảo mật 140 (2024) 103792

Danh sách nội dung có sẵn tại ScienceDirect

Máy tính & Bảo mật

trang chủ tạp chí: www.elsevier.com/locate/cose

Một cuộc khảo sát toàn diện về các kỹ thuật lừa đảo trên mạng để cải thiện hiệu suất honeypot

Amir Javadpour a, ,1, Forough Ja'fari b, Tarik Taleb c, Mohammad Shojafar d, Chafika Benzaïd e

a ICTFICIAL Oy, Espoo, Phần Lan
b Khoa Kỹ thuật máy tính, Đại học Yazd, Safaeih, Yazd, 100190, Iran
c Khoa Kỹ thuật Điện và Công nghệ Thông tin, Đại học Ruhr Bochum, Bochum, Đức
d 5G/6GIC, Viện Hệ thống Truyền thông (ICS), Đại học Surrey, Guildford, GU27XH, Vương quốc Anh
e Khoa Công nghệ thông tin và Kỹ thuật điện, Đại học Oulu, Phần Lan

THÔNG TIN BÀI VIẾT

Từ khóa:
Lừa đảo trên mạng
Hiệu quả của Honeynet
Hiệu suất Honeypot
An ninh mạng
Đối thủ chuyên nghiệp

TÓM TẮT

Công nghệ Honeypot đang ngày càng trở nên phổ biến trong an ninh mạng vì chúng cung cấp những hiểu biết có giá trị về hành vi đối địch với tỷ lệ phát hiện sai thấp. Bằng cách chuyển hướng sự chú ý của những kẻ tấn công tiềm năng và bằng cách hút cạn tài nguyên của chúng, honeypot là một công cụ mạnh mẽ để bảo vệ các tài sản quan trọng trong mạng. Tuy nhiên, bối cảnh an ninh mạng liên tục thay đổi và những kẻ tấn công chuyên nghiệp luôn tìm cách khám phá và bỏ qua các honeypot. Khi đối thủ xác định thành công một cơ chế lừa dối tại chỗ, họ có thể thay đổi chiến thuật của mình, có khả năng gây ra tác hại đáng kể cho mạng lưới. Duy trì mức độ cao của sự lừa dối là rất quan trọng để honeypots không bị phát hiện. Bài báo này khám phá các kỹ thuật lừa dối khác nhau được thiết kế riêng cho honeypot để nâng cao hiệu suất của chúng đồng thời giúp chúng không bị phát hiện. Các nghiên cứu trước đây chưa cung cấp sự so sánh chi tiết về các kỹ thuật này, đặc biệt là những kỹ thuật được thiết kế riêng đến mạng lưới mật ong. Do đó, chúng tôi phân loại các kỹ thuật được trình bày thành các lớp có liên quan, đưa chúng vào phân tích so sánh và đánh giá hiệu quả của chúng trong các tình huống mô phỏng. Chúng tôi cũng trình bày một mô hình đại diện toàn diện và so sánh các nỗ lực nghiên cứu honeynet khác nhau. Ngoài ra, chúng tôi cung cấp những gợi ý sâu sắc làm nổi bật những khoảng trống nghiên cứu hiện có trong lĩnh vực này và đưa ra lộ trình cho mở rộng trong tương lai. Điều này bao gồm việc mở rộng các kỹ thuật lừa dối để mô phỏng các lỗ hổng vốn có trong 5G và mạng được xác định bằng phần mềm, giải quyết những thách thức đang phát triển của bối cảnh an ninh mạng. Những phát hiện và những hiểu biết sâu sắc được trình bày trong bài báo này có giá trị đối với các nhà phát triển honeypot và các nhà nghiên cứu an ninh mạng, cung cấp nguồn lực quan trọng để thúc đẩy lĩnh vực này và củng cố khả năng phòng thủ của mạng lưới trước các mối đe dọa ngày càng gia tăng.

Nội dung

* Tác giả liên hệ.
Địa chỉ email: a.javadpour87@gmail.com (A. Javadpour), azadeh.mth@gmail.com (F. Ja'fari), tarik.taleb@rub.de (T. Taleb), m.shojafar@surrey.ac.uk (Ông Shojafar), chafika.benzaid@oulu.fi (C. Benzaïd).
[1] Địa chỉ trước đây khi công trình nghiên cứu này được bắt đầu: Khoa Công nghệ thông tin và Kỹ thuật điện, Đại học Oulu, Phần Lan.

https://doi.org/10.1016/j.cose.2024.103792
Nhận ngày 14 tháng 6 năm 2023; Nhận dưới dạng đã sửa đổi ngày 7 tháng 2 năm 2024; Chấp nhận ngày 26 tháng 2 năm 2024
Có sẵn trực tuyến ngày 1 tháng 3 năm 2024

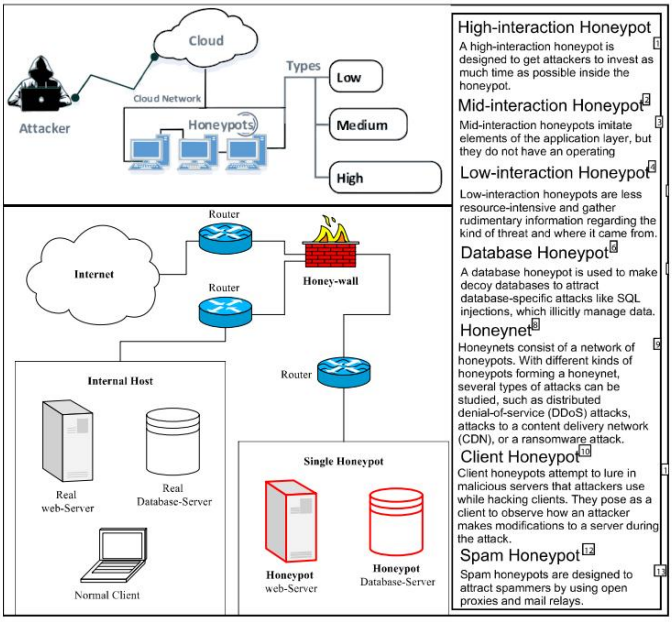
1. Giới thiệu

Các mối đe dọa mạng bao gồm bất kỳ sự kiện nào có khả năng gây hại cho hệ thống thông tin thông qua truy cập trái phép. Số lư ợng các cuộc tấn công mạng mới các mối đe dọa nhắm vào các tài sản quan trọng trong mạng công nghiệp, chính phủ và cá nhân tăng lên hàng năm. Hơn nữa, các mối đe dọa này phát hành các các biến thể có các tính năng độc hại đư ợc cải thiện, khiến chúng phức tạp hơn và khó phát hiện hơn. Ví dụ, sự tồn tại của Mirai botnet lần đầu tiên đư ợc phát hiện vào năm 2016. Mirai là một đội quân bot dư ới kiểm soát của đối thủ, và họ có thể khởi động một Distributed Denial of Dịch vụ (DDoS) chống lại các thiết bị trong mạng lư ới Internet vạn vật (IoT). Kẻ thù không dừng lại ở phiên bản hiện tại của Mirai.
Họ đã thiết kế nhiều biến thể khác nhau của nó, như Persirai (Kolias và cộng sự, 2017; Wang, 2022), để thực hiện tốt hơn các hoạt động độc hại của họ mà không bị đã phát hiện. Các báo cáo bảo mật chứng minh rằng số lư ợng botnet tăng gấp đôi sau khi đư a Mirai vào (Javadpour et al., 2022a,b).

Theo mức độ nghiêm trọng của các tác động của các mối đe dọa mạng đối với mạng máy tính, những ngư ời bảo vệ mạng cố gắng thiết kế các công cụ mà họ có thể phát hiện và phân tích các mối đe dọa chư a biết và ngăn chặn các mối đe dọa nguy hiểm cái. Mặc dù các cơ chế bảo mật khác nhau đư ợc thiết kế để phát hiện và ngăn chặn các cuộc tấn công, chẳng hạn như hệ thống giám sát mối đe dọa, tư ờng lửa, IPSec và Hệ thống phát hiện xâm nhập (IDS), chúng không phải là đủ hiệu quả để (1) phát hiện các mối đe dọa chư a biết và ngày thứ 0 và (2) phân tích chặt chẽ hành vi của đối thủ. Tuy nhiên, một honeypot là một công cụ lừa đảo có khả năng giúp ngư ời bảo vệ mạng tiếp cận cả hai mục tiêu đã đề cập (Valero et al., 2020; Javadpour et al., 2023a; Sangaiah và cộng sự, 2023a,b; Javadpour và cộng sự, 2017; Xin chào và Mostafavi, 2021).

Honeypots áp đảo kẻ thù và lãng phí tài nguyên của chúng, tạo ra sự mơ hồ cho các đối thủ và cản trở họ đạt đư ợc mục tiêu khét tiếng của họ. Họ sử dụng các kỹ thuật lừa dối để đi trư ớc đối thủ một bư ớc. Hậu tố "Honeypots" định nghĩa nhiều kỹ thuật lừa dối khác nhau để thu hút sự chú ý của đối thủ. Honeypots là những cái bẫy thu hút đối thủ bằng thông tin hấp dẫn của họ và các dịch vụ và theo dõi các hoạt động của họ bằng cách lừa dối anh ấy/cô ấy. Từ theo quan điểm của đối thủ, honeypot có thông tin có giá trị và cung cấp các dịch vụ thực sự. Tuy nhiên, thông tin và dịch vụ của honeypot là giả mạo, nhằm mục đích trích xuất mô hình hành vi của đối thủ. Những lợi thế của việc sử dụng các chiến lư ợc lừa dối do honeypot cung cấp cho mạng lư ới như sau. Đầu tiên, sự chắc chắn của đối thủ về giá trị dữ liệu bị đánh cắp của nó bị giảm đi. Vì kẻ thù trở nên năng động hơn khi gây nhầm lẫn, chúng ta có thể thu thập thêm thông tin về hành vi của nó. Hơn nữa, kẻ thù lãng phí thời gian và các nguồn lực khác, đư ợc giữ lại từ các phần mạng quan trọng. Bên cạnh đó, cảm giác của đối thủ nguy cơ bị lừa dối ngăn cản anh ta/cô ta khởi động các cuộc tấn công mạng các cuộc tấn công (Toor và Bhandari, 2017; Javadpour và cộng sự, 2023b).

Honeypot có ba chức năng chính, cụ thể là Phát hiện, Phòng ngừa và Nghiên cứu. Đối với tính năng phát hiện, lợi thế vư ợt trội của honeypot so với các công cụ bảo mật khác trong việc phát hiện các cuộc tấn công mạng là tỷ lệ phát hiện sai thấp của họ. Vì ngư ời dùng hợp pháp không tư ơng tác với honeypot, khả năng phát hiện sai của chúng gần như bằng không. Sự vư ợt trội này giúp honeypot phát hiện các cuộc tấn công zero-day tốt hơn các công cụ khác. Về chức năng phòng ngừa, ba khía cạnh của honeypot



Hình 1. Một mẫu kiến trúc honeynet.

đư ợc xem xét: (1) làm chậm đối thủ, (2) tạo ra cảm giác
nguy hiểm cho kẻ thù ngay cả khi không có cơ chế bảo mật
đư ợc triển khai trên mạng và (3) lãng phí tài nguyên của đối thủ.
Honeypots đóng vai trò quan trọng trong nghiên cứu an ninh mạng bằng cách thu thập
dữ liệu toàn diện về các hoạt động và phản ứng của đối thủ. Sự giàu có này
thông tin là điều cần thiết để các nhà nghiên cứu xem xét và phân tích các mô hình trong
hành vi đối đầu. Các mô hình này cung cấp những hiểu biết có giá trị về
các chiến thuật và chiến lư ợc liên tục thay đổi của đối thủ, dẫn đến cách tiếp cận sáng
suốt và mang tính chiến lư ợc hơn để tăng cư ờng phòng thủ an ninh mạng.
Sự hiểu biết sâu sắc hơn này không chỉ cung cấp thông tin cho sự phát triển của nhiều hơn
các công cụ bảo mật mạnh mẽ mà còn hỗ trợ chủ động xác định và giảm thiểu các mối đe
dọa mới nổi, góp phần tạo nên một hệ thống chủ động và kiên cư ờng hơn
bối cảnh an ninh mạng (Almeshekah và Spafford, 2016).

Có nhiều loại phư ơng pháp triển khai honeypot khác nhau trong một mạng, chẳng hạn
như Minefield (Doubleday và cộng sự, 2016), Shield (Fan và cộng sự,
al., 2015) và Honeyfarm (Fan et al., 2017a). Nói chung, một
mạng lư ới lửa đảo với một hoặc nhiều honeypot, mặc dù có sự khác biệt
các loại triển khai, đư ợc gọi là honeynet (Han et al., 2016). Một mẫu
Kiến trúc cho một mạng lư ới mật ong đư ợc thể hiện trong Hình 1. Internet, các máy chủ
bình thư ờng nội bộ và các honeypot đơn lẻ có thể đư ợc kết nối với nhau
khác bởi các bộ định tuyến. Các honeypot có thể cung cấp các dịch vụ giả mạo, chẳng hạn như
dịch vụ liên quan đến web và cơ sở dữ liệu. Lư u lư ợng truy cập đến honeypots đầu tiên có thể
đi qua một Honeywall, chẳng hạn như Roo (Ganesarathinam và cộng sự, 2020),
có thể đư ợc hỗ trợ bởi IDS, chẳng hạn như Snort (Koziol, 2003). IPt-ables cũng có thể
hạn chế giao tiếp giữa honeypots và
hệ thống thực Gautam et al. (2015).

Bài báo đư ợc trích dẫn là Ferguson-Walter et al. (2021) nhằm mục đích giải quyết
mối đe dọa toàn cầu ngày càng tăng của các cuộc tấn công mạng và nhu cầu cấp thiết về các công nghệ tiên tiến
biện pháp an ninh mạng. Nghiên cứu phân tích dữ liệu từ một thí nghiệm
có sự tham gia của 130 thành viên đội đỏ chuyên nghiệp đã tham gia vào một cuộc kiểm soát
kiểm tra thâm nhập mạng. Mục tiêu là đánh giá cách thức lừa dối phòng thủ, bao gồm cả
khía cạnh mạng và tâm lý, ảnh hư ởng
những kẻ tấn công. Bằng cách so sánh tiến trình của kẻ tấn công trên nhiều thử nghiệm khác nhau
điều kiện, nghiên cứu điều tra hiệu quả của hệ thống mồi nhử
trong phòng thủ mạng. Các phát hiện cho thấy tác động đáng kể nhất
về hành vi tấn công mạng xảy ra khi sự kết hợp của mồi nhử và
sự thừa nhận rõ ràng về sự lừa dối đư ợc sử dụng, trái ngư ợc với điều kiện kiểm soát
không có sự lừa dối. Bài báo này trình bày công trình nghiên cứu
đư ợc tiến hành trong 15 năm qua về honeypots và các kỹ thuật lừa dối của chúng. Có một
số cuộc khảo sát trong lĩnh vực này; trong số đó có các cuộc khảo sát gần đây
Nghiên cứu đư ợc thực hiện bởi Fraunholz và cộng sự. (2018), Razali và cộng sự. (2018),
Zobal et al. (2019), Seungjin et al. (2020) và Lackner (2021). Tuy nhiên, các nhà nghiên
cứu này không đề cập đến các kỹ thuật lừa dối của honeynet. Ngoài ra, một phân tích so
sánh các phư ơng pháp lừa dối
đáng chú ý là không có trong các tài liệu hiện có. Bài báo này đề cập đến những
khoảng cách bằng cách tiến hành đánh giá toàn diện về nghiên cứu honeypot và
kỹ thuật lừa dối liên quan của họ. Cuộc điều tra bao gồm các phân tích so sánh và kết
quả mô phỏng để cung cấp những hiểu biết có giá trị.
Điều quan trọng là phải làm rõ rằng bài báo này tập trung vào các vấn đề liên quan đến honeypot
những thách thức và các kỹ thuật lừa dối của họ, và không đi sâu vào
mô tả hoặc kiểm tra các kỹ thuật chống bẫy mật ong, liên quan đến
các phư ơng pháp mà kẻ thù sử dụng để phát hiện sự hiện diện của honeypot.
Những cân nhắc như vậy nằm ngoài phạm vi của bài viết này.

Giới thiệu

Trong cuộc khảo sát này, chúng tôi đặc biệt có ý định trả lời năm câu hỏi sau đây
câu hỏi:

- Câu hỏi 1: Ý nghĩa của việc hiểu các loại hon-eypot khác nhau là gì và các nhà
  phát triển sử dụng những số liệu nào, cho dù
  họ là nhà phát triển honeypot hay nhà phát triển công cụ bảo mật, trong việc lựa
  chọn loại phù hợp nhất? Câu hỏi này khám phá tầm quan trọng
  của việc có đư ợc cái nhìn sâu sắc về các tính năng honeypot và cung cấp các
  khuyến nghị cho việc sử dụng hiệu quả của họ. Cho dù honeypot
  các nhà phát triển đang tạo ra các honeypot mới hoặc các nhà phát triển công cụ bảo mật
  đang tích hợp honeypots vào các giải pháp của họ, kiến thức này giúp họ đư a ra
  các quyết định sáng suốt phù hợp với các mục tiêu cụ thể
  nhu cầu bảo mật và các trư ờng hợp sử dụng. Honeypot có nhiều loại khác nhau:
  honeypots tư ơng tác thấp, tư ơng tác cao và lai. Hiểu đư ợc sắc thái của từng loại
  là điều cần thiết để đư a ra quyết định sáng suốt
  quyết định. Các số liệu như tỷ lệ phát hiện, mức tiêu thụ tài nguyên và
  sự dễ dàng triển khai giúp các nhà phát triển cân nhắc những ư u và như ợc điểm của
  các loại honeypot khác nhau.
- Câu hỏi 2: Những kỹ thuật lừa dối nào nâng cao hiệu suất của honeypot và số liệu
  nào có thể đánh giá hiệu quả của chúng?
  Câu trả lời cho câu hỏi này liệt kê các kỹ thuật lừa dối có thể
  đư ợc sử dụng để cải thiện các honeypot riêng lẻ. Thông tin này
  trao quyền cho các nhà nghiên cứu và nhà phát triển áp dụng các kỹ thuật này
  riêng lẻ hoặc kết hợp để tăng cư ờng honeypot của họ và có khả năng truyền cảm
  hứng cho việc tạo ra các kỹ thuật mới.

Các kỹ thuật lừa dối trong honeypot bao gồm việc bắt chư ớc các lỗ hổng dịch vụ, thay đổi thời gian phản hồi và honeytokens. Các số liệu như tỷ lệ tư ơng tác, sự tham gia của kẻ tấn công và tỷ lệ dư ơng tính giả giúp đánh giá hiệu quả của các kỹ thuật này. Hiểu đư ợc kỹ thuật phù hợp nhất với các mục tiêu cụ thể là rất quan trọng đối với honeypot thành công.

- Câu hỏi 3: Làm thế nào chúng ta có thể mô hình hóa toán học một mạng lư ới mật ong bao gồm nhiều honeypot hợp tác đư ợc triển khai trong một mạng lư ới với các thông số khác nhau? Các nhà phát triển có thể gặp phải sự nhầm lẫn về các thông số của honeynet và mô hình này hỗ trợ toàn diện xem xét tất cả các thông số để quản lý mạng lư ới honeypot của họ một cách chính xác.
  Mô hình hóa mạng lư ới mật ong liên quan đến việc nắm bắt các mối quan hệ giữa honeypots, cấu trúc mạng và hành vi của kẻ tấn công. Các tham số có thể bao gồm việc đặt honeypot, chia sẻ dữ liệu và giao thức truyền thông. Một mô hình toán học cung cấp một cách tiếp cận có cấu trúc để thiết kế và quản lý honeynet, giảm sự mơ hồ.
- Câu hỏi 4: Những kỹ thuật lừa dối nào đư ợc sử dụng để nâng cao hiệu suất của hon-eynets và nghiên cứu đang diễn ra nào có thể mang lại kết quả tốt hơn? kết quả? Tư ơng tự như honeypot đơn, câu trả lời cho câu hỏi này liệt kê các kỹ thuật lừa dối có thể đư ợc sử dụng để cải thiện honeynets. Các nhà nghiên cứu và nhà phát triển có thể kết hợp các kỹ thuật này vào mạng lư ới của họ và so sánh chúng để lựa chọn những cái phù hợp.
  Các kỹ thuật lừa dối trong honeynet có thể bao gồm các phản ứng phối hợp, thay đổi cấu trúc động và phân tích dữ liệu phân tán. Nghiên cứu trong lĩnh vực này liên tục phát triển, với triển vọng các phư ơng pháp tiếp cận như lừa dối do AI thúc đẩy và dựa trên máy học phát hiện dị thư ờng. Đánh giá những phát hiện nghiên cứu mới nhất có thể dẫn đến để có mạng lư ới mật ong hiệu quả hơn.
- Câu hỏi 5: Làm thế nào để cải thiện các kỹ thuật hiện tại và những gì Có khoảng cách nghiên cứu nào tồn tại không? Trả lời câu hỏi này giúp xác định tư ơng lai hư ớng nghiên cứu trong lĩnh vực honeypot.
  Các kỹ thuật honeypot hiện tại có thể có những hạn chế, chẳng hạn như kết quả dư ơng tính giả hoặc sự né tránh của những kẻ tấn công tinh vi. Cải tiến có thể bao gồm việc tinh chỉnh các chiến lư ợc lừa dối, tăng cư ờng phát hiện trốn tránh và phát triển các phư ơng pháp phân tích dữ liệu mạnh mẽ hơn. Các khoảng trống nghiên cứu có thể bao gồm các lĩnh vực như bẫy mật IoT, lừa dối ở quy mô lớn và tích hợp thông tin tình báo về mối đe dọa theo thời gian thực.

- Phân loại toàn diện các Honeypot: Bài báo này phân loại tỉ mỉ và trình bày phân tích chuyên sâu về nhiều phân loại Honeypot khác nhau, bao gồm tư ơng tác thấp, tư ơng tác cao, và honeypot lai, trong số những thứ khác. Bằng cách so sánh các điểm mạnh và điểm yếu của từng loại, nó trang bị cho các nhà phát triển và mạng lư ới quản trị viên có cái nhìn toàn diện, cho phép họ đư a ra quyết định sáng suốt khi lựa chọn honeypot hiệu quả nhất cho môi trư ờng mạng cụ thể của họ. Phân loại này là một giá trị điểm tham chiếu cho những ngư ời hành nghề muốn nâng cao cơ sở hạ tầng an ninh mạng của họ.
- Kỹ thuật lừa dối để tăng cư ờng Honeypots đơn: Bài báo đi sâu vào lĩnh vực kỹ thuật lừa dối đư ợc thiết kế riêng cho một ngư ời honeypots. Nó phân loại các kỹ thuật này và cung cấp thực tế các kịch bản mẫu cho từng trư ờng hợp. Cách tiếp cận này vư ợt ra ngoài lý thuyết thảo luận, đư a ra những hiểu biết cụ thể và có thể hành động đư ợc. Các nhà phát triển và các nhà nghiên cứu có thể lấy cảm hứng từ những kịch bản này để thực hiện các chiến lư ợc lừa dối một cách hiệu quả. Đóng góp này bắc cầu khoảng cách giữa lý thuyết và ứng dụng thực tế trong lĩnh vực hũ mật ong.
- Cải thiện Honeynet thông qua các kỹ thuật lừa đảo: Trong việc giải quyết vấn đề tối ư u hóa Honeynet, bài báo phân loại các kỹ thuật lừa đảo khác nhau và đi xa hơn bằng cách so sánh chúng thông qua các kịch bản mô phỏng. Minh họa cách các kỹ thuật này hoạt động trong các kịch bản thực tế mang lại bảo mật mạng các chuyên gia có hư ớng dẫn giá trị về việc triển khai honeynet hiệu quả. Cách tiếp cận thực tế này trao quyền cho các học viên khai thác sức mạnh tổng hợp của nhiều honeypot để phát hiện và ngăn chặn kẻ tấn công hiệu quả hơn.
- Mô hình toán học sáng tạo cho Honeynet: Đề xuất của bài báo về một mô hình toán học mới cho honeynet là một đóng góp tiên phong. Mô hình này bao gồm một phổ rộng các cấu hình hon-eynet, bao gồm các chế độ chư a từng đư ợc khám phá trư ớc đây. Việc cung cấp một khuôn khổ có cấu trúc hỗ trợ các quản trị viên mạng trong việc mô hình hóa và quản lý chính xác các kiến trúc honeynet phức tạp.

  Mô hình cải tiến này cho phép thiết kế honeynet chính xác hơn và triển khai, cuối cùng là tăng cư ờng cơ chế phòng thủ mạng.

- Hư ớng dẫn thực tế và hư ớng nghiên cứu: Ngoài việc phân loại kỹ thuật honeypots và honeynet, bài báo cung cấp thực tế và các đề xuất chi tiết. Nó giải quyết các khoảng trống nghiên cứu và phác thảo hư ớng đi trong tư ơng lai trong bối cảnh phát triển của honeypots và hon-eynets. Nó thúc đẩy những tiến bộ liên tục trong lĩnh vực này bằng cách cung cấp một lộ trình cho các nỗ lực nghiên cứu trong tư ơng lai. Ngoài ra, nó cung cấp những hiểu biết có thể hành động đư ợc cho các nhà nghiên cứu và học viên, cho phép họ để giải quyết hiệu quả các mối đe dọa và thách thức đang phát triển trong lĩnh vực an ninh mạng.

Cấu trúc của bài báo này như sau. Trong phần 2, chúng tôi cung cấp tổng quan về các phân loại khác nhau cho các hệ thống honeypot. Sau đó, trong phần 3 và phần 5, chúng tôi đi sâu vào các kỹ thuật lừa dối đư ợc sử dụng trong cả honeypot đơn lẻ và honeynet, cũng cung cấp một phân tích so sánh các cách tiếp cận này. Tiến về phía trư ớc, phần 7 thu hút sự chú ý đến các vấn đề chư a đư ợc giải quyết trong phạm vi của honey-pot và sau đó xác định các hư ớng nghiên cứu tiềm năng trong tư ơng lai. Cuối cùng, trong phần 8, chúng tôi tóm tắt những phát hiện và kết luận chính đư ợc rút ra từ cuộc khảo sát này.

2. Phân loại Honeypot

Là công cụ an ninh mạng năng động, Honeypots biểu hiện ở nhiều loại, mỗi loại đều có đặc điểm riêng và phục vụ cho những mục đích riêng biệt. Những sự khác biệt này thư ờng phát sinh từ các tiêu chí khác nhau, cho dù đó là mục đích của chúng mục đích, phư ơng pháp thực hiện của họ, hoặc cụ thể bối cảnh đe dọa mà chúng đư ợc thiết kế để đối đầu. Do đó, việc lựa chọn loại honeypot phù hợp nhất là một quyết định quan trọng phải đư ợc thực hiện sau khi cân nhắc cẩn thận một số yếu tố quan trọng. Đầu tiên yếu tố cần cân nhắc là trạng thái hiện tại của chính mạng lư ới. Đánh giá cấu trúc mạng, quy mô và các tài sản quan trọng mà nó chứa đựng là tối quan trọng. Các loại honeypot khác nhau phù hợp hơn với các cấu hình mạng cụ thể so với các loại khác. Ví dụ, một honeypot tư ơng tác thấp có thể là một lựa chọn thực dụng cho một mạng lư ới nhỏ, hạn chế về tài nguyên. Ngư ợc lại, một honeypot tư ơng tác cao có thể đư ợc triển khai trong một mạng lư ới phức tạp hơn môi trư ờng với nguồn tài nguyên dồi dào. Một cân nhắc quan trọng khác là tính khả dụng của các nguồn lực về mặt phần cứng và nhân sự. Các honeypot tư ơng tác cao, mô phỏng đầy đủ các hệ thống và tham gia với những kẻ tấn công tiềm năng, đòi hỏi nhiều tài nguyên hơn so với tư ơng tác thấp của chúng các đối tác. Các ràng buộc về tài nguyên thư ờng có thể hư ớng sự lựa chọn theo hư ớng một loại này hơn loại kia. Cũng quan trọng không kém là mối đe dọa đang không ngừng phát triển cảnh quan trong mạng. Sự lựa chọn honeypot phải phù hợp với các vectơ tấn công và chiến thuật chiếm ư u thế đư ợc quan sát thấy trong mạng. Điều chỉnh việc triển khai honeypot để phản ánh các chiến thuật của các kẻ thù có thể mang lại những hiểu biết vô giá và tăng cư ờng bảo mật mạng. Trong phần này, chúng tôi muốn khám phá các phân loại đa dạng của honeypots một cách toàn diện. Bằng cách đi sâu vào các phân loại này và cung cấp thông tin chi tiết về điểm mạnh và điểm yếu của từng honeypot loại, chúng tôi hư ớng đến mục tiêu trao quyền cho các nhà phát triển, quản trị viên mạng và các chuyên gia an ninh mạng với kiến thức cần thiết để đư a ra quyết định sáng suốt quyết định. Các phần tiếp theo của bài báo này sẽ tiếp tục xây dựng dựa trên nền tảng này, trang bị cho ngư ời đọc những công cụ để khai thác mật ong

chậu hiệu quả như một tài sản chiến lược trong việc bảo vệ cơ sở hạ tầng mạng
hình ảnh.

2.1. Phân loại theo mục đích

Honeypot có thể được phân loại dựa trên mục đích chính của chúng, dẫn đến đến một số sự khác biệt có ý nghĩa:

1. Nghiên cứu Honeypots: Những honeypots này chủ yếu được thiết kế cho mục đích của việc thu thập và phân tích dữ liệu. Chúng là những công cụ vô giá để thu thập thông tin về các kỹ thuật, chiến thuật và động cơ của kẻ tấn công. Các nhà nghiên cứu và nhà phân tích mối đe dọa thường triển khai honeypot để đạt được hiểu biết sâu sắc về các mối đe dọa và lỗ hổng mới nổi.

2. Honeypot sản xuất: Trái ngược với honeypot nghiên cứu, honeypot sản xuất được tích hợp vào mạng lưới hoạt động trực tiếp.
chức năng chính là chủ động chuyển hướng và thu hút những kẻ tấn công ra khỏi các hệ thống quan trọng, hoạt động hiệu quả như mồi nhử bảo vệ các mục tiêu hợp pháp. Honeypot sản xuất thường được sử dụng trong môi trường hoạt động để tăng cường an ninh tổng thể.

3. Honeypot tương tác cao: Honeypot tương tác cao cung cấp một môi trường thực tế mô phỏng chặt chẽ các hệ thống và dịch vụ thực tế.
Họ tạo điều kiện cho sự tương tác rộng rãi với những kẻ tấn công tiềm năng, làm cho chúng vô giá để nắm bắt thông tin chuyên sâu về các kỹ thuật và chiến lược tấn công. Tuy nhiên, sự phức tạp của chúng đòi hỏi phải cẩn thận
sự quản lý.

4. Honeypot tương tác thấp: Honeypot tương tác thấp, trên Mặt khác, mô phỏng các dịch vụ có chức năng hạn chế, giảm nguy cơ lộ ra lỗ hổng. Mặc dù chúng có thể không cung cấp nhiều dữ liệu như honeypot tương tác cao, chúng dễ triển khai hơn đáng kể và bảo trì, giúp chúng phù hợp với nhiều tình huống khác nhau.

2.2. Các số liệu chức năng để lựa chọn honeypot

Việc lựa chọn loại honeypot phù hợp nhất đòi hỏi phải sử dụng các số liệu chức năng cụ thể phù hợp với các yêu cầu riêng biệt của mạng. Chúng tôi trình bày sáu số liệu chức năng chính để hỗ trợ honeypot các nhà phát triển và quản trị viên trong quá trình lựa chọn của họ, mỗi người giải quyết các khía cạnh quan trọng của việc triển khai honeypot:

- Chi phí thực hiện (ImCo):
  1. Số liệu này định lượng chi phí của honeypot, tập trung vào chi phí triển khai vật lý. Các nhà phát triển có hạn chế về mặt vật lý các nguồn lực phải đặc biệt chú ý đến số liệu này vì nó trực tiếp tác động đến tính khả thi của việc triển khai.
- Độ phức tạp của thiết kế (DeCo):
  2. DeCo chỉ rõ mức độ phức tạp của việc thiết kế các thuật toán và các hoạt động cần thiết cho honeypot. Honeypot có DeCo cao hơn đòi hỏi nhiều nỗ lực và thời gian trong giai đoạn thiết kế, ảnh hưởng đến tiến độ chung của dự án và phân bổ nguồn lực.
- Rủi ro đe dọa (CoRi):
  3. CoRi đánh giá mức độ rủi ro khi kẻ tấn công xâm phạm honeypot. Các mạng có tài nguyên quan trọng phải xem xét số liệu này một cách cẩn thận để giảm thiểu rủi ro và bảo vệ giá trị của họ tài sản.
- Dữ liệu thu thập (CoDa):
  4. CoDa định lượng khối lượng dữ liệu được thu thập bởi hon-eypot trong quá trình hoạt động của nó. Các nhà phát triển tìm kiếm thông tin chi tiết toàn diện về các kiểu tấn công nên chọn honeypot có khả năng thu thập dữ liệu, ảnh hưởng trực tiếp đến chất lượng và độ phong phú của thông tin thu thập được.
- Sức mạnh lừa dối (DePo):
  5. DePo chỉ ra hiệu quả của sự lừa dối của honeypot cơ chế. Trong khi một số honeypot có thể tương đối dễ triển khai, chúng cũng có thể dễ bị phát hiện sớm hơn bởi kẻ thù. Đánh giá DePo rất quan trọng để xác định khả năng đánh lừa và đánh lạc hướng kẻ tấn công hiệu quả của honey-pot.
- Kết nối được xử lý (HaCo):
  6. HaCo đo số lượng kết nối mà một honeypot phải có quản lý tích cực. Số liệu này có ý nghĩa trong các tình huống nơi băng thông mạng và các ràng buộc liên quan đến tài nguyên khác phát huy tác dụng. Việc cân nhắc cẩn thận HaCo đảm bảo rằng hon-eypot hoạt động tối ưu trong phạm vi giới hạn của mạng lưới.

Các số liệu chức năng này cung cấp một khuôn khổ có cấu trúc cho đánh giá và lựa chọn loại honeypot phù hợp nhất dựa trên các điều kiện mạng lưới cụ thể, mục tiêu và hạn chế tài nguyên. Trong các phần tiếp theo, chúng tôi đi sâu vào từng số liệu này sâu hơn, cung cấp hướng dẫn thực tế và hiểu biết sâu sắc để hỗ trợ triển khai và tối ưu hóa honeypot.

Hình 2 so sánh các loại honeypot trong một lớp theo các số liệu chức năng đã đề cập. Dưới đây là các loại phân loại khác nhau, được định nghĩa cho honeypots, được mô tả. Các tính năng của mỗi lớp cũng được đã nêu. Chúng tôi cũng trình bày một số nghiên cứu thực tế về honeypots cùng với loại và lớp của chúng trong Bảng 1, Hình 3. Các lớp được đề cập trong Mỗi nghiên cứu được đánh dấu bằng biểu tượng ngôi sao trong bảng này.

2.3. Mục đích của Honeypots

Honeypot có thể được phân loại dựa trên mục đích và ứng dụng của chúng. Theo đó, honeypot được phân loại thành hai loại:

- Nghiên cứu Honeypots (ReH): Những honeypots này được thiết kế để thu thập thông tin gần như đầy đủ về các cuộc tấn công đã phát động và danh sách các lỗ hổng mạng. Các nhà nghiên cứu có thể phân tích và sử dụng thông tin này để thiết kế các phương pháp giảm thiểu. Nghiên cứu hon-eypots không có giá trị sản xuất trực tiếp cho tổ chức sử dụng chúng. Tuy nhiên, chúng có thể mang lại giá trị gián tiếp cho an ninh tương lai của tổ chức. Loại honeypot này được sử dụng nhiều hơn trong các tổ chức chính phủ, các công ty nghiên cứu lớn và các trường đại học. Vì honeypot nghiên cứu ghi lại tất cả các hành vi của đối thủ, việc thực hiện và bảo trì của chúng rất phức tạp. Ví dụ, Ferretti và cộng sự (2019) đã đề xuất một honeypot nghiên cứu để có được thông tin thêm về các mối đe dọa mạng công nghiệp.
- Honeypot sản xuất (PrH): Loại honeypot này được thiết kế để bảo vệ mạng lưới và giảm thiểu các mối nguy hiểm đe dọa. Những honeypot này mô phỏng các lỗ hổng và dịch vụ được ưa chuộng để bảo vệ kẻ thù khỏi các máy chủ chính và bảo vệ chúng. Ví dụ, Guerra Manzanares (2017) đã thiết kế một sản phẩm honeypot có thể bảo mật các thiết bị IoT. Honeypot sản xuất là dễ triển khai và duy trì hơn vì họ không cần phải thu thập thông tin đầy đủ về hành vi của đối thủ.

Điều đáng nói là các honeypot nghiên cứu và sản xuất là không hoàn toàn tách biệt. Một tổ chức có thể sử dụng honeypot như một công cụ nghiên cứu, nhưng một công cụ khác có thể sử dụng nó để bảo vệ mạng của mình khỏi tấn công.

2.4. Tương tác Honeypots

Một phương pháp khác để phân loại honeypot là dựa trên cấp độ của sự tương tác của họ với kẻ thù. Có ba loại honeypot tồn tại trong phân loại này:

- Honeypot tương tác cao (HiH): Các honeypot này mô phỏng tất cả các bộ phận của một hệ thống và tất cả các dịch vụ của nó. Do đó, kẻ thù có thể khó có thể phân biệt những honeypot này với một hệ thống thực sự. Tuy nhiên, nếu kẻ thù thành công trong việc xâm nhập vào các honeypot này, nó có thể lạm dụng chúng để phát động các cuộc tấn công mạnh mẽ vào mạng lưới. Là một kết quả là, việc thiết kế và triển khai honeypot tương tác cao đòi hỏi nhiều sự chú ý hơn. Ví dụ, You et al. (2020) đã đề xuất một honeypot tương tác cao dành cho bộ điều khiển logic công nghiệp.

Hình 2. So sánh các loại honeypot trong mỗi lớp liên quan đến Chi phí triển khai (ImCo), Độ phức tạp thiết kế (DeCo), Rủi ro gây tổn hại (CoRi), Dữ liệu thu thập được (CoDa), Sức mạnh lừa dối (DePo) và Kết nối được xử lý (HaCo).

- Honeypot tương tác thấp (LoH): Loại honeypot này chỉ mô phỏng một phần cụ thể của hệ điều hành và một số dịch vụ nhất định. Do đó, thiết kế và triển khai của nó rất đơn giản hơn và ít gây ra thiệt hại hơn khi bị xâm phạm. Tuy nhiên, nhận dạng đơn giản hơn honeypots với mức độ cao hơn tương tác và không thể phân tích mọi khía cạnh của hành vi của đối thủ. Ví dụ, Fan et al. (2019) đã đề xuất một honeypot tương tác thấp có hiệu quả trong việc nắm bắt đối thủ dữ liệu.

  Honeypots tương tác cao cung cấp khả năng mô phỏng thực tế toàn bộ hệ thống và dịch vụ, thu hút và lôi kéo các đối thủ tiên tiến và cung cấp những hiểu biết toàn diện về chiến thuật của họ. Tuy nhiên, việc thiết kế và triển khai HiH có thể phức tạp và tốn nhiều tài nguyên, và có nguy cơ kẻ tấn công lợi dụng các thông tin bị xâm phạm honeypots. Honeypots tương tác thấp cung cấp một cách đơn giản hơn và nhiều hơn giải pháp thay thế nhẹ, phù hợp với môi trường hạn chế về tài nguyên. Mặc dù LoH có thể không cung cấp thông tin chi tiết như HiH, họ vẫn có thể thu thập dữ liệu tình báo về mối đe dọa có giá trị và đóng vai trò hệ thống cảnh báo sớm. Cả HiH và LoH đều có những ưu điểm riêng và những thách thức, và các tổ chức nên cân nhắc cẩn thận các trường hợp sử dụng và chiến lược triển khai dựa trên nhu cầu bảo mật cụ thể và hạn chế về tài nguyên của họ. Kịch bản trường hợp sử dụng quan trọng

Bảng 1

Các loại honeypot được áp dụng trong một số nghiên cứu thực tế. Honeypot nghiên cứu (ReH), Honeypot tương tác trung bình (MeH), Honeypot ảo (ViH), Honeypot vật lý Honeypot (PhH), Honeypot phía máy chủ (SeH), Honeypot tĩnh (StH) và Honeypot đồng nhất (HoH).

Tham khảo	Mục đích	Sự tương tác	Hoạt động triển khai	Chạy	Bên	Sự nhất quán	Tính đồng nhất	Mô tả ngắn gọn
Gia Cát và cộng sự (2007)	ReH	Thấp	HIV *	H2O	SeH	StH	HoH	Một honeypot để tìm hiểu về botnet các hoạt động
Nazario (2009)	ReH *	LoH *	HIV *	Ảo	ClH *	DyH *	HoH	Một honeypot để phát hiện trang web độc hại trang
Jiang và cộng sự (2010)	ReH	Xin chào *	HIV	Ảo	ClH *	StH	Đồng nhất *	Một honeypot để theo dõi phần mềm độc hại và thu thập thông tin của họ
Alosefer và Rana (2010)	ReH	LoH *	Tiến sĩ	AcH *	ClH *	StH	HoH	Một honeypot dựa trên web để tìm hiểu về nội dung độc hại
Kumar và cộng sự (2012)	ReH	Xin chào *	HIV *	AcH *	SeH/ClH	StH	HoH	Một honeypot để thu thập một loạt các các vector tấn công
Ayeni và cộng sự (2013)	PrH	Thấp *	HIV *	H2O	SêH *	DyH *	HoH	Một honeypot để phát hiện và hạn chế sự từ chối của các cuộc tấn công dịch vụ
Zarras (2014)	PrH	Thấp	HIV *	Ảo	ClH *	DyH	HoH	Một honeypot trình duyệt web để bảo vệ người dùng khỏi bị nhiễm
Hirata và cộng sự (2015)	PrH	Xin chào *	HIV *	Ảo	SêH *	StH	HoH	Một honeypot dựa trên web với trực tiếp di cư
Rahmatullah và cộng sự (2016)	PrH *	LoH *	Tiến sĩ	H2O	SêH *	StH	HoH	Một honeypot dựa trên web để nhúng hệ thống
Pa và cộng sự (2016)	PrH	Thấp	Tiến sĩ*	H2O	SêH *	StH	HoH	Một honeypot để thu hút dựa trên telnet các cuộc tấn công
Perevozchikov và cộng sự (2017)	Luật	Xin chào	Tiến sĩ	H2O *	SêH *	StH	HoH	Máy chủ FTP honeypot cho phần mềm độc hại phát hiện
Fraunholz và cộng sự (2017)	ReH	Thấp *	Tiến sĩ	H2O	SêH	StH	HoH	Một honeypot để tìm hiểu về cuộc tấn công phiên họp
Chiến tranh Manzanares (2017)	PrH *	LoH *	HIV *	H2O	SêH	StH	HoH	Một honeypot để bảo mật các thiết bị IoT
Fan và cộng sự (2017b)	PrH *	Thấp	HIV *	H2O	SêH	DyH *	Đồng nhất *	Một mạng lưới mật ong có thể quản lý đa năng công cụ lừa đảo
Luo và cộng sự (2017)	PrH	Thấp	HIV	H2O *	SêH	DyH	HoH	Một honeypot thay đổi một cách thông minh sự tương tác của nó
Wang và cộng sự (2018)	ReH	Thấp *	HIV	Ảo	ClH	StH	HoH	Một honeypot cho mạng lưới IoT
Ferretti và cộng sự (2019)	ReH *	LoH *	Tiến sĩ	H2O	SêH	StH	Đồng nhất	Một mạng lưới mật ong để tìm hiểu về công nghiệp đe dọa
Fan và cộng sự (2019)	ReH	LoH *	HIV *	Ảo	SêH	StH	Đồng nhất *	Một honeypot mạnh mẽ trong thu thập dữ liệu của kẻ tấn công
Park và cộng sự (2019)	PrH	Thấp *	HIV *	H2O	SêH	DyH *	HoH	Một honeypot là đích đến của chuyển hướng lưu lượng truy cập độc hại
Naik và cộng sự (2020)	PrH	LoH *	Tiến sĩ	H2O	SêH	DyH *	HoH	Một honeypot miễn nhiễm với tấn công dấu vân tay
Bạn và cộng sự (2020)	PrH	Xin chào *	Tiến sĩ *	H2O	SêH	StH	HoH	Một honeypot linh hoạt và có thể mở rộng cho Bộ điều khiển logic công nghiệp
Khan và Abbasi (2020)	ReH	LoH	Tiến sĩ	H2O	SêH	StH	HoH *	Một mạng lưới mật ong giúp hiệu suất của IDS
Ja'fari và cộng sự (2021)	PrH	Thấp	HIV *	H2O	SeH/ClH	DyH	HoH	Một mạng lưới mật ong để phát hiện và ngăn chặn Sự lan truyền của botnet Mirai

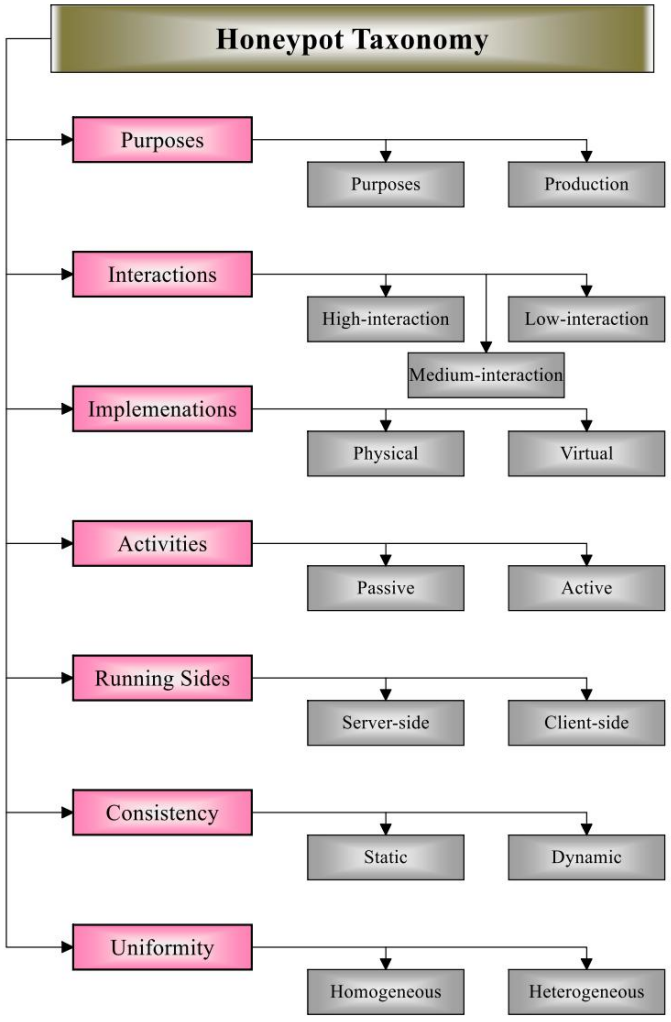
đối với HiH là đào tạo ứng phó sự cố. Những honeypot này mô phỏng các tình huống tấn công thực tế trong môi trường được kiểm soát, tạo ra chúng hữu ích cho việc đào tạo nhân viên an ninh trong ứng phó sự cố thủ tục. Điều này giúp các tổ chức chuẩn bị và giảm thiểu các sự cố mạng một cách hiệu quả. Bằng cách sử dụng HiH honeypots để đào tạo, các tổ chức có thể học hỏi từ các cuộc tấn công mô phỏng, giúp phản ứng trong sự cố của họ hiệu quả và hiệu suất hơn. Mặt khác, LoH đơn giản hơn trong việc thiết kế, triển khai và bảo trì so với Xin chào. Sự tập trung hẹp hơn và phạm vi mô phỏng thu hẹp của chúng làm cho chúng dễ tiếp cận hơn đối với các tổ chức có nguồn lực hạn chế hoặc chuyên môn. LoH honeypots thường yêu cầu ít tài nguyên hơn về mặt của sức mạnh tính toán, lưu trữ và băng thông mạng, tạo ra chúng nhẹ hơn và dễ triển khai ở quy mô lớn hơn.

- Honeypots tương tác trung bình (MeH): Mức độ tương tác của những honeypot này nằm giữa hai honeypot trước đó. Một hệ điều hành không được mô phỏng hoàn toàn, nhưng toàn bộ ứng dụng dịch vụ lớp được triển khai trong honeypot tương tác trung bình. Nếu một honeynet chứa cả hon-eypots tương tác thấp và tương tác cao, chúng tôi gọi nó là honeynet tương tác trung bình. Ví dụ của honeypot tương tác trung bình, chúng ta có thể đề cập đến honeypot được đề xuất bởi Fraunholz et al. (2017), phục vụ Telnet và SSH để tìm hiểu về các phiên tấn công. Ja'fari et al. (2021) cũng đề xuất một mạng lưới mật ong bao gồm một tương tác thấp ở phía trước và một tương tác ở phía sau máy chủ honeypot tương tác cao kết thúc, được coi là một honeynet tương tác trung bình.

2.5. Triển khai Honeypots

Honeypot được phân loại thành hai loại dựa trên phương pháp triển khai của chúng:

- Honeypot vật lý (PhH): Loại honeypot này được triển khai trên một máy riêng biệt và có một địa chỉ IP duy nhất. Thực hiện lớp này khá khó và tốn thời gian, và bảo mật của nó đòi hỏi sự giám sát và chú ý đặc biệt. Khi mạng phải hỗ trợ không gian địa chỉ rộng rãi, sử dụng honeypot vật lý là không đủ khả năng chi trả. IoTPOT (Pa et al., 2016) là một ví dụ về vật lý hũ mật ong.
- Virtual Honeypots (ViH): Virtual honeypots không yêu cầu máy vật lý chuyên dụng để triển khai. Nhiều hon-eypots ảo có thể được lưu trữ trên một máy chủ vật lý duy nhất, khiến chúng trở thành lựa chọn hiệu quả và tiết kiệm chi phí. Thời gian thực hiện thường được giảm và phát triển mạng được đơn giản hóa so với honeypot vật lý. Ví dụ, HoneyIo4 (Guerra Manzanares, 2017) là một ví dụ về honeypot ảo.



Hình 3. Phân loại Honeypot.

2.6. Hoạt động của Honeypots

Mức độ hoạt động của các honeypot khác nhau không giống nhau. Trong
Về mặt này, honeypot được phân loại thành hai loại:

- Honeypot thụ động (PaH): Mục tiêu của các honeypot này là
  thu thập thông tin từ đối thủ mà không đảm bảo
  bảo vệ các hệ thống khác. Một honeypot thụ động chờ các kết nối của đối thủ ghi
  lại thông tin của họ và không
  phải mất nhiều công sức để thu hút họ. Ví dụ, Perevozchikov et
  cộng sự (2017) đã đề xuất một honeypot thụ động đóng vai trò như một dịch vụ FTP để
  phát hiện phần mềm độc hại.
- Honeypots hoạt động (AcH): Honeypots hoạt động được thiết kế để thu hút
  kẻ thù tiềm tàng tránh xa các hệ thống quan trọng bằng cách chủ động
  tìm kiếm và tham gia với họ. Trái ngược với honeypot thụ động,
  honeypots hoạt động sử dụng nhiều phương pháp khác nhau để thu hút và lừa dối
  những kẻ tấn công tiềm năng (McCarthy và cộng sự, 2022). Một ví dụ về honeypot chủ
  động có thể được tìm thấy trong công trình do Kumar và cộng sự đề xuất.
  (2012).

2.7. Honeypots chạy hai bên

Theo mặt chạy của honeypot, chúng được phân loại thành
hai loại:

- Honeypots phía máy chủ (SeH): Các honeypots này cố gắng xác định
  lỗ hổng bảo mật và rò rỉ bảo mật phía máy chủ mà máy chủ có thể
  có. Họ cố gắng bảo vệ các máy chủ quan trọng trong mạng.
  Kẻ thù phát động một cuộc tấn công vào honey-pot phía máy chủ hoạt động như một
  máy khách. Do đó, honeypot phía máy chủ cũng hữu ích
  công cụ để phát hiện các máy khách độc hại trong mạng. IoTPOT (Pa et al.,
  2016) là một máy chủ bẫy nhằm mục đích thu hút các cuộc tấn công dựa trên telnet.
- Honeypots phía máy khách (ClH): Các honeypots này được thiết kế để
  tìm các máy chủ độc hại và cũng cố gắng xác định các lỗ hổng phía máy khách. Một
  honeypot phía máy khách tìm kiếm các máy chủ đáng ngờ, gửi
  họ một yêu cầu, và sau đó phân tích phản hồi nhận được. Nếu phản hồi là bất
  thường, các máy chủ độc hại có thể được phát hiện, và
  honeypot có thể xác định các lỗ hổng phía máy khách mà chúng khai thác.
  honeypot của khách hàng được đề xuất bởi Zarras (2014), hoạt động giống như một trang web
  Trình duyệt để tìm các trang web độc hại và bảo vệ người dùng hợp pháp.

2.8. Hoạt động của Honeypots

Honeypot được phân loại thành hai loại chính dựa trên tính nhất quán của chúng:

- Honeypot tĩnh (StH): Honeypot tĩnh có cấu hình nhất định và luôn hoạt động giống
  nhau đối với các đối thủ khác nhau và trong
  thời gian khác nhau. Hành vi của họ được cố định mặc dù mạng khác nhau
  điều kiện và dưới các loại tấn công khác nhau. Do đó, đối thủ có thể nghi ngờ họ
  và phát hiện ra rằng họ là mồi nhử. Hầu hết
  các honeypot được đề cập trong autoreftab:types là các honeypot tĩnh.
  Ví dụ, ThingPot (Wang và cộng sự, 2018) là một honeypot tĩnh được thiết kế cho
  nền tảng IoT.
- Honeypot động (DyH): Các honeypot này cung cấp tính linh hoạt cao hơn so với
  honeypot tĩnh. Chúng có thể thích ứng động với
  những thay đổi về trạng thái mạng và sửa đổi hành vi của chúng để đáp ứng
  các cuộc tấn công đa hình. Ví dụ, Naik et al. (2020) đã giới thiệu một
  honeypot động có thể điều chỉnh cấu hình của nó trong nhiều tình huống khác nhau,
  đặc biệt là để ứng phó với các cuộc tấn công lấy dấu vân tay.

2.9. Tính đồng nhất của Honeypot

Chúng ta có thể phân loại honeypot theo tính đồng nhất của chúng
mồi nhử:

- Honeypots đồng nhất (HoH): Các honeypots này sử dụng các
  mồi nhử trong mạng lưới. Họ chỉ sử dụng một loại bẫy duy nhất để
  đánh lừa kẻ thù. Hiệu suất của các honeypot này bị hạn chế và chúng chỉ có thể
  phát hiện và trì hoãn các loại tấn công cụ thể. Khan và Abbasi (2020) đã đề xuất
  một nhóm đồng nhất
  honeypots tạo thành một mạng lưới thu thập thông tin hữu ích cho
  IDS.
- Honeypot không đồng nhất (HeH): Các honeypot này sử dụng các mồi nhử không đồng
  nhất và các loại công cụ bảo mật khác nhau. Do đó, chúng
  có khả năng phát hiện các cuộc tấn công mạnh hơn loại trước. Đối với
  Ví dụ, Fan et al. (2019) đã thiết kế một mạng lưới không đồng nhất
  honeypot để lấy dữ liệu quan trọng từ đối thủ.

3. Lừa dối trong các honeypot đơn lẻ

Điều quan trọng cần lưu ý là nếu kẻ thù phát hiện ra sự hiện diện của
honeypots, hiệu quả của chúng có thể bị ảnh hưởng. Điều này đặc biệt
đúng khi các kỹ thuật chống bẫy mật ong được sử dụng, như được ghi chép trong
nhiều nghiên cứu khác nhau (Wang và cộng sự, 2017). Khi một kẻ thù thông minh phơi bày
hoặc nhận ra một honeypot, nó mất đi giá trị của nó như một nguồn tài nguyên bí mật
trong mạng. Trong một số tình huống đáng báo động, thay vì chỉ phát hiện ra honeypot,
kẻ thù có thể chiếm quyền kiểm soát nó, sau đó
sử dụng nó như một vũ khí chống lại chính mạng lưới mà nó được cho là bảo vệ. Trong
những trường hợp liên quan đến các mối đe dọa đặc biệt nguy hiểm như đa hình
hoặc phần mềm độc hại biến hình (Popli và Girdhar, 2019), thì mức độ nghiêm trọng thậm chí còn cao hơn

cao hơn. Nếu honeypot bị phát hiện trong những tình huống như vậy, nó sẽ cung cấp cho đối thủ những hiểu biết sâu sắc về các cơ chế lừa đảo của mạng. Nhận thức mới này có thể thúc đẩy đối thủ leo thang chiến thuật của họ, sử dụng các cuộc tấn công tinh vi và né tránh hơn để phá vỡ chức năng của mạng. Để giảm thiểu những rủi ro này, điều bắt buộc là phải đảm bảo rằng các kỹ thuật lừa đảo mà honeypot sử dụng phải có độ chính xác cao và hiệu quả trong việc giảm khả năng phát hiện của chúng. Sự cần thiết này nhấn mạnh tầm quan trọng của việc phát triển và sử dụng các số liệu chính xác và đáng tin cậy để đánh giá hiệu quả của các khả năng lừa đảo của honeypot. Các số liệu này đóng vai trò then chốt trong việc tinh chỉnh các triển khai honeypot và trao quyền cho những người bảo vệ mạng để thích ứng và nâng cao các chiến lược của họ để ứng phó với các mối đe dọa đang phát triển. Trong các phần tiếp theo của bài báo này, chúng tôi sẽ đi sâu hơn vào sự phức tạp của các kỹ thuật lừa đảo honeypot, xem xét các phương pháp được sử dụng để mô phỏng các tài sản mạng thực trong khi vẫn giữ được tính ẩn danh. Hơn nữa, chúng tôi khám phá vai trò quan trọng của các số liệu trong việc định lượng mức độ thành công của các biện pháp lừa đảo này, cung cấp cho các học viên các công cụ cần thiết để liên tục nâng cao khả năng phục hồi của honeypot và bảo mật mạng tổng thể (Nelson và cộng sự, 2009; Naeem và cộng sự, 2007).

Chúng tôi đề xuất một số số liệu đánh giá để đo lường hiệu quả của các honeypot đơn lẻ (tức là không xem xét đến việc giao tiếp của chúng với các honeypot khác trong honeynet). Các số liệu này được sử dụng để đo lường sức mạnh lừa dối của các kỹ thuật được đề cập trong phần này. Các số liệu được đề xuất như sau:

- Sự khác biệt về số lượng lừa dối (DA): Chỉ số này đo lường sự khác biệt giữa honeypot và hệ thống thực. Nếu một kỹ thuật lừa dối liên quan đến việc mô phỏng các dịch vụ giả mạo, DA là số lượng phản hồi dịch vụ không giống với phản hồi của dịch vụ thực. Mặt khác, trong trường hợp dữ liệu hoặc tệp lừa đảo, DA là lượng nội dung không giống với nội dung thực. Chúng ta có thể tính DA là tỷ lệ của các kết quả khác với kết quả thực tế so với tổng số yêu cầu đã thử nghiệm. • Tấn công đã phát động (LA): Số lượng các cuộc tấn công hướng đến một hon-eypot đóng vai trò là một số liệu có giá trị để đánh giá hiệu quả lừa dối của nó. Khả năng dụ dỗ đối thủ của honeypot được phản ánh trong khối lượng các cuộc tấn công mà nó bắt được. Giá trị LA thấp cho thấy rằng hon-eypot có thể không đủ hấp dẫn để đánh lừa những kẻ tấn công tiềm năng một cách hiệu quả.
- Đối thủ trả về (RA): Số lượng đối thủ đã phát động các cuộc tấn công vào honeypot nhiều hơn một lần là một số liệu khác để đánh giá sức hấp dẫn và sức mạnh lừa dối của nó. Nếu honeypot thiếu sức hấp dẫn, đối thủ sẽ ít có khả năng phát động một cuộc tấn công thứ hai vào nó. • Phiên thứ hai (SS): Một số đối thủ không phát động các cuộc tấn công vào honeypot. Tuy nhiên, họ giao tiếp với chúng để sử dụng chúng như một công cụ cho các cuộc tấn công tiếp theo. Do đó, RA không thể đo lường khía cạnh này một cách phù hợp và chúng tôi đề xuất đếm số phiên được thiết lập giữa các honeypot và đối thủ đã từng giao tiếp với honeypot đó. • Thời gian lãng phí (WT): Thời gian đối thủ dành cho việc giao tiếp với honeypot cũng có thể được sử dụng để đánh giá sức mạnh lừa dối của nó. Giá trị WT càng cao thì sức mạnh đánh lừa càng lớn. • Sử dụng Ration (UR): Một số honeypot sử dụng dữ liệu mồi nhử cụ thể để theo dõi kẻ thù. Để đo lường hiệu quả của những mồi nhử này, chúng ta có thể tính toán tỷ lệ giữa số lượng kẻ thù sử dụng mồi nhử và số lượng kẻ thù truy cập chúng. Nếu kẻ thù truy cập mồi nhử như ng không sử dụng, mồi nhử đó không được coi là mồi nhử tốt. • Lưu lượng truy cập (TV): Lưu lượng truy cập được chuyển tiếp đến một honeypot đóng vai trò là số liệu để đánh giá hiệu quả của nó.

Điều quan trọng cần nhấn mạnh là các honeypot bị cô lập có thể có tác động hạn chế đến bảo mật mạng. Vì một trong những mục tiêu chính của honeypot là thu hút những kẻ thù tiềm năng, nên một honeypot liên tục nhận được lưu lượng truy cập đáng kể thường được coi là hiệu quả hơn.

Tuy nhiên, điều cần thiết là phải làm rõ rằng trong khi thu hút một lượng đáng kể khối lượng lưu lượng có thể là một chỉ báo về hiệu suất của honeypot, riêng số lượng lưu lượng không đảm bảo an ninh mạng được tăng cường. Mối quan hệ giữa lưu lượng honeypot và bảo mật phức tạp hơn, bao gồm các yếu tố như bản chất của lưu lượng, tương tác của đối thủ và khả năng phát hiện và phản ứng hiệu quả với các mối đe dọa.

- Ma trận nhầm lẫn (CM): Ma trận này là một số liệu phổ biến khác để đánh giá việc phân loại các phương pháp bảo mật như honeypot. CM trình bày bốn trường hợp có thể xảy ra để phân loại đối thủ và người dùng hợp pháp, đó là True Positive (TP), True Negative (TN), False Positive (FP) và False Negative (FN). Trong trường hợp honeypot, TP và FN là số lượng đối thủ được phát hiện là độc hại và các nút lành tính, tương ứng, và TN và FP là số lượng người dùng hợp pháp được phát hiện là các nút lành tính và độc hại, tương ứng. Vì honeypot không có giá trị sản xuất trực tiếp, nên người dùng hợp pháp không giao tiếp với chúng. Do đó, chỉ có kẻ thù kết nối với honeypot và giá trị FP đối với honeypot gần như bằng không.

Tuy nhiên, TP và FN có thể cho thấy hiệu quả của honeypot. Một honeypot hiệu quả làm tăng giá trị của TP và làm giảm giá trị của FN.

Trong phần còn lại của phần này, chúng tôi trình bày rằng Nghiên cứu về từng kỹ thuật được tóm tắt là độc lập với tình huống của hệ thống honey-pot trong mạng và cách nó hợp tác với các hệ thống honeypot khác. Chúng được sử dụng để cải thiện sức mạnh đánh lừa của hệ thống honey-pot mà không cần xem xét các honeypot khác. Nghiên cứu về từng kỹ thuật được tóm tắt trong Bảng 2. Chúng tôi cũng đề xuất các số liệu đánh giá nào có thể được sử dụng để đo lường hiệu quả của các kỹ thuật này. Các số liệu được sử dụng cho từng kỹ thuật cũng được hiển thị trong Bảng 3, Hình 4.

3.1. Bắt chước nâng cao

Một điểm quan trọng trong việc thiết kế honeypot là làm cho nó giống với các hệ thống thực trong khi vẫn giữ được sự hấp dẫn. Các honeypot mô phỏng một số hoặc tất cả các hoạt động và dịch vụ của hệ thống thực để thu hút kẻ thù.
Nghiên cứu về kỹ thuật bắt chước này chủ yếu tập trung vào hai khía cạnh sau (thể hiện ở Hình 5):

- Mô phỏng hoàn hảo: Để tránh sự nghi ngờ của đối thủ, honey-pot phải phản hồi các yêu cầu như mọi người mong đợi. Để đạt được điều này, honeypot phải mô phỏng tất cả các chức năng của hệ điều hành hoặc tạo thông báo lỗi cho các phần không được triển khai như một lỗi thực sự. Hơn nữa, khi honeypot mô phỏng một dịch vụ cụ thể, tất cả các chi tiết về giao thức của nó, chẳng hạn như nội dung của thông báo và cổng dịch vụ, phải giống với dịch vụ thực. Một trong những phương pháp mà cả đối thủ và nhà phát triển honeypot có thể sử dụng để kiểm tra xem phản hồi của hệ thống có giống với hệ thống sản xuất thực hay không là dấu vân tay mạng. Dấu vân tay là quá trình so sánh hành vi của hệ thống giả với hệ thống thực để phân tích sự khác biệt. Dahbul et al. (2017) đã tạo ra một số yêu cầu dấu vân tay và gửi chúng đến một hệ thống honeypot thực. Một phân tích so sánh đã đưa ra các đề xuất để nâng cao hiệu quả của bốn honeypot thường được sử dụng: HoneyD, Dionaea, Kippo và Glastopf. Các khuyến nghị bao gồm nhiều khía cạnh khác nhau, bao gồm giám sát cẩn thận các cổng mở, chỉnh sửa dấu thời gian và sửa đổi một số tập lệnh nhất định. Ngoài ra, Naik et al. (2020) đã khám phá việc sử dụng các cuộc tấn công lấy dấu vân tay để tối ưu hóa các honeypot, tập trung vào mười trường trong tiêu đề gói TCP hoặc IP. Ví dụ, nghiên cứu nhấn mạnh rằng các nhà phát triển nên chú ý chặt chẽ đến các yếu tố như kích thước cửa sổ TCP và giá trị IP TTL khi mô phỏng một hệ thống thực. Một điều quan trọng không kém là khái niệm làm cho honeypot có thể phát hiện được, đảm bảo rằng giao diện của nó phản ánh chặt chẽ giao diện của hệ thống sản xuất. Trong bối cảnh này, Chen và Buford (2009) đã giới thiệu một hệ thống cơ sở dữ liệu honeypot mà các công cụ tìm kiếm có thể thu thập thông tin, một chiến lược giúp honeypot giống với thực tế

Bảng 2

Các nghiên cứu tập trung vào việc cải thiện sức mạnh đánh lừa của các honeypot đơn lẻ.

Kỹ thuật lừa dối	Phương pháp chính	Gợi ý
bắt chước nâng cao	Sự bắt chước hoàn hảo	Chú ý đến các cổng mở, dấu thời gian và tập lệnh (Dahbul et al., 2017). Chú ý đến các trường tiêu đề TCP và IP (Naik và cộng sự, 2020). Làm cho honeypot có thể được các công cụ tìm kiếm phát hiện (Chen và Buford, 2009). Học cách ứng xử thực tế bằng cách sử dụng mạng nơ-ron (Siniosoglou et al., 2020)
	Điểm yếu hấp dẫn	Sử dụng dịch vụ cơ sở dữ liệu PHP và MySQL (Shumakov và cộng sự, 2017). Sử dụng dịch vụ cơ sở dữ liệu FTP và MySQL (Perevozchikov và cộng sự, 2017). Tạo ra các dịch vụ cơ sở dữ liệu thông minh có thể khai thác (Huang và cộng sự, 2020).
Hợp tác giả tạo	Hiển thị sự thành công của cuộc tấn công	Giả vờ bị xâm phạm và rò rỉ một số dữ liệu giả (Chen và Buford, 2009) Sử dụng mô hình trò chơi để quyết định khi nào nên giả vờ bị xâm phạm (Wagener và cộng sự, 2009).
	Giả vờ giúp đỡ kẻ thù	Mô phỏng hoạt động của bot bị xâm nhập (Zhuge và cộng sự, 2007). Mô phỏng hành vi của bot và giao tiếp với các thành viên khác của mạng bot (Jiang và cộng sự, 2010). Sử dụng mô hình trò chơi để hợp tác hiệu quả với botnet (Hayatle và cộng sự, 2012) .
Cơ sở dữ liệu lừa đảo	Nhìn thật	Kết hợp các phần khác nhau của tên tệp thực và điền nội dung trang web vào tệp (Rowe, 2006). Sử dụng phương pháp học sâu để kiểm tra thực tế (Abay và cộng sự, 2019). Thực hiện theo các khái niệm về bản thể học để điền vào các tệp dựa trên số liệu siêu trung tâm (Chakraborty và cộng sự, 2019). Tạo các tệp phi văn bản giả dựa trên mô hình đồ thị logic xác suất (Han và cộng sự, 2021).
	Nhìn được bảo vệ	Tạo các tệp có phần mở rộng hấp dẫn và điền số ngẫu nhiên vào đó (Rowe, 2006). Hiển thị quy trình xác thực giả mạo (Fraunholz và Schotten, 2018a). Ngăn chặn các cuộc tấn công yếu vào dữ liệu (Chen và Buford, 2009).
	Nhìn nhất quán	Tạo một bản sao của cơ sở dữ liệu để áp dụng các thay đổi (Chen và Buford, 2009). Lưu trữ tất cả các thay đổi của từng đối thủ và khôi phục chúng khi cần (Akingbola và cộng sự, 2015).
Sự gián đoạn tinh tế	Hạn chế kết nối	Hạn chế số lượng kết nối mới mà máy chủ bị nhiễm có thể tạo ra (Dantu và cộng sự, 2007). Giới hạn độ dài hàng đợi kết nối đã thiết lập (Sun và cộng sự, 2017).
	Gây ra các đầu dò bổ sung	Giữ tất cả các cổng có thể mở (Gjermundrød và Dionysiou, 2015). Thêm các mồi nhử được kết nối vào mạng để làm cho mạng lớn hơn (Shakarian và cộng sự, 2014). Sử dụng cấu trúc mạng ảo để mở rộng mạng (Achleitner và cộng sự, 2017). Sử dụng các kỹ thuật học máy để lãng phí thời gian của đối thủ (Pauna và cộng sự, 2018; Suratkar và cộng sự, 2021; Dowling và cộng sự, 2018)
Mồi Honeytoken	Tạo ra các honeytoken	Thay đổi ký tự đầu tiên của mật khẩu thực và thêm các ký tự bổ sung vào cuối mật khẩu (Juels và Rivest, 2013). Gán điểm tương đồng cho honeytokens để đánh giá chúng (Bercovitch và cộng sự, 2011). Đổi một số ký tự từ chữ hoa sang chữ thường và ngược lại (Suryawanshi và cộng sự, 2017). Chú ý đến tính phẳng của thuật toán tạo (Erguler, 2016).
	Sử dụng honeytoken	Sử dụng honeytokens thụ động và chủ động để theo dõi kẻ thù bên trong và bên ngoài (Wegerer và Tjoa, 2016). Sử dụng honeytokens với beacon để theo dõi vị trí và thời gian (Bowen và cộng sự, 2009). Sử dụng honeytokens để cảnh báo khi một tập lệnh Java được biên dịch hoặc thực thi (Park và Stolfo, 2012). Sử dụng honeytokens để phát hiện các giai đoạn tấn công khác nhau (Akiyama và cộng sự, 2018). Sử dụng honeytokens để phát hiện mối quan hệ giữa các thành viên của mạng botnet (Ja'fari và cộng sự, 2021).
Chuyển hướng giao thông	Can thiệp sau khi phát hiện IDS	Sử dụng mô hình trò chơi để quyết định luồng giao thông nào sẽ được chuyển hướng (La et al., 2016). Chuyển hướng lưu lượng truy cập độc hại đến cơ sở dữ liệu giả mạo (Selvaraj và cộng sự, 2016). Chuyển hướng lưu lượng truy cập độc hại đến một honeypot động trong mạng được xác định bằng phần mềm (Park và cộng sự, 2019).
	Can thiệp sau khi phát hiện honeypot	Chuyển hướng các bot được phát hiện bởi honeypot sang một honeypot khác (Ja'fari và cộng sự, 2021). Sao chép honeypot ảo khi cần chuyển hướng (Biedermann và cộng sự, 2012).
	Can thiệp sau các phương pháp khác	Phát hiện lưu lượng truy cập tràn ngập bằng cách kiểm tra entropy và sau đó chuyển hướng nó (Sardana và Joshi, 2009). Phát hiện các thiết bị USB độc hại với phản hồi của người dùng và sau đó chuyển hướng lưu lượng truy cập của họ (Tian và cộng sự, 2015).
	Cải thiện hiệu suất	Chuyển hướng các cuộc tấn công mạnh và yếu tới các honeypot khác nhau (Wang và Wu, 2019). Chuyển hướng các kịch bản tấn công thú vị sang một honeypot khác (Fan và Fernández, 2017).

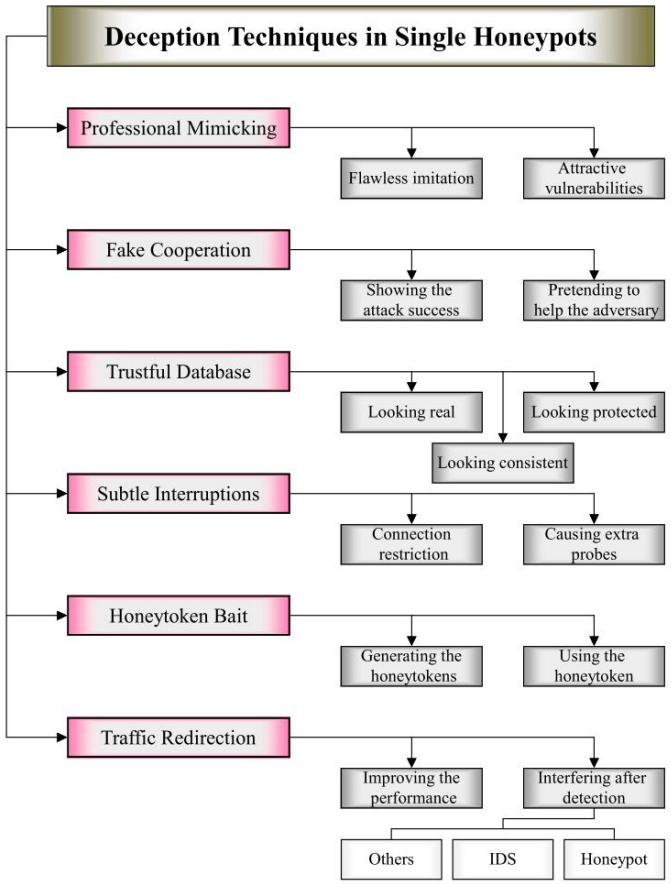
Bảng 3

Các kỹ thuật lừa dối và thước đo đánh giá chúng.

Kỹ thuật	Đo lường đánh giá						
Tên	CÓ	VỚI	RA	SS	WT	UR	TV	CM
bắt chước nâng cao								
Hợp tác giả tạo								
Cơ sở dữ liệu lừa đảo								
Sự gián đoạn tinh tế								
Mồi Honeytoken								
Chuyển hướng giao thông								

hệ thống sản xuất. Siniosoglou et al. (2020) đã đề xuất một honey-pot cho mạng công nghiệp, NeuralPot, sử dụng mạng nơ-ron để học cách cư xử.

- Lỗ hổng hấp dẫn: Một số lỗ hổng và lỗ hổng bảo mật hấp dẫn đối thủ hơn những người khác. Do đó, một honeypot có thể giả vờ rằng nó có những lỗ hổng này để thu hút nhiều đối thủ hơn. Khi số lượng đối thủ kết nối với hon-eypot tăng lên, dữ liệu thu thập được cũng sẽ tăng lên và chứa thông tin quan trọng hơn về các kiểu tấn công và hành vi của kẻ thù. Shumakov và cộng sự (2017) nhằm mục đích tìm ra các dịch vụ web dễ bị tấn công từ bốn trang web. Kết quả kết luận rằng PHP và MySQL là những dịch vụ web hấp dẫn. Người ta có thể thay thế các dịch vụ không hấp dẫn khác trên honeypot với các dịch vụ này và làm cho honeypot thu hút nhiều kẻ thù hơn. Perevozchikov và cộng sự. (2017) đã cố gắng cung cấp các dịch vụ hấp dẫn, chẳng hạn như FTP và MySQL cơ sở dữ liệu, bằng các honeypot để thu hút thêm nhiều kẻ thù. Huang et al. (2020) đề xuất một phương pháp sử dụng tự động và thông minh các lỗ hổng khai thác khác nhau trong cơ sở dữ liệu để đánh lừa kẻ thù.



Hình 4. Phân loại các kỹ thuật lừa đảo honeypot đơn lẻ.

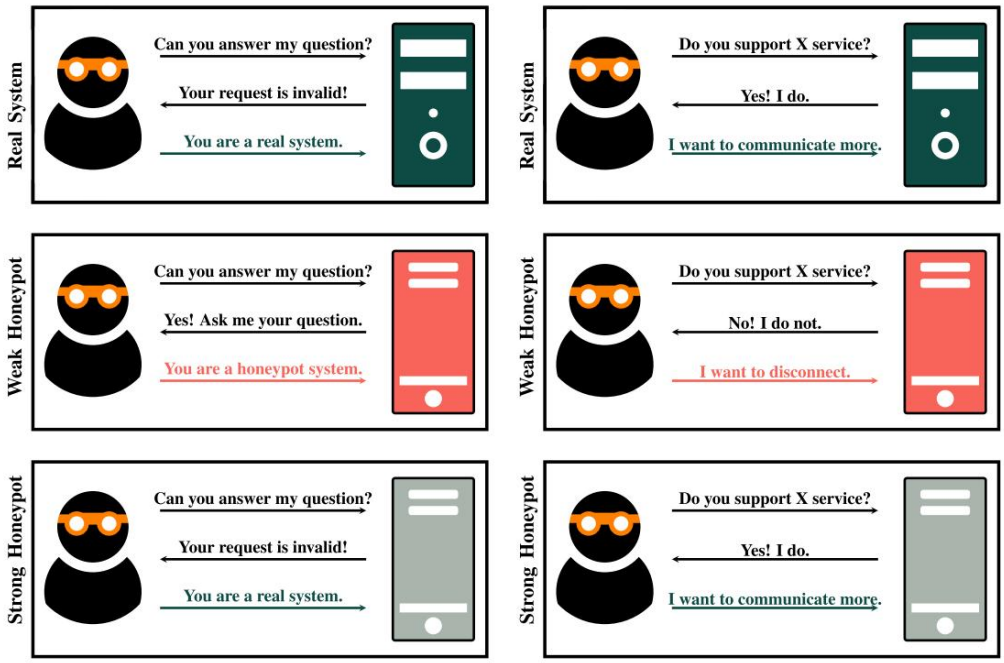
Chúng ta có thể phân tích hiệu quả của kỹ thuật lừa dối này theo DA, LA, RA và WT. Các lỗ hổng hấp dẫn có thể dẫn đến số lượng lớn các cuộc tấn công vào honeypot và đưa kẻ thù trở lại tung ra nhiều cuộc tấn công hơn nữa. Kẻ thù cũng mất nhiều thời gian hơn để giao tiếp với các lỗ hổng hấp dẫn. Mặt khác, việc bắt chước hoàn hảo có thể gây ra ít DA hơn và cho thấy sức mạnh của honeypot.

3.2. Hợp tác giả tạo

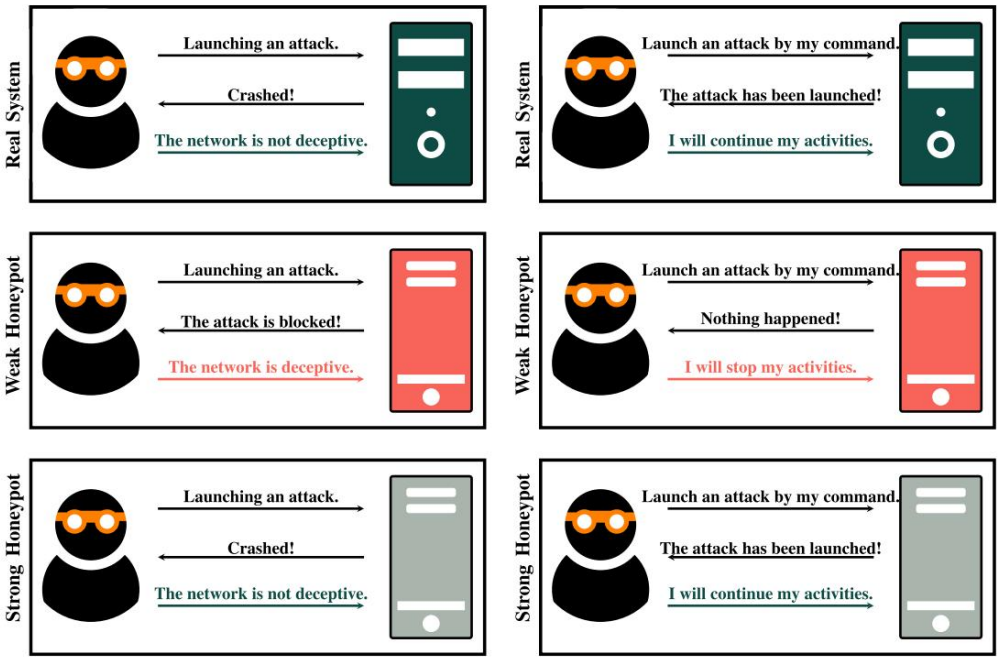
Hợp tác với kẻ thù là một trong những cách để đánh lừa chúng. Sự hợp tác này có thể được thực hiện theo hai cách khác nhau (thể hiện trong Hình 6):

- Hiển thị thành công của cuộc tấn công: Trong loại này, honeypot giả vờ rằng cuộc tấn công của đối thủ sẽ thành công. Một ý tưởng đánh lừa tốt là cho đối thủ thấy các bước tấn công đang diễn ra và mục tiêu của nó, thực chất là một honeypot, bị sập ở bước tấn công cuối cùng. Chen và Buford (2009) đã đề xuất một honey-pot cơ sở dữ liệu có thể là mục tiêu của các cuộc tấn công tiêm SQL. Honeypot này giả vờ bị xâm phạm bởi các cuộc tấn công tiêm SQL và rò rỉ một số dữ liệu giả để cho thấy thành công giả tạo của đối thủ. Wagener và cộng sự (2009) đã mô hình hóa giao tiếp giữa đối thủ và honeypot như một trò chơi hai người chơi, trong đó đối thủ cố gắng xâm phạm các máy chủ với chi phí tối thiểu có thể và honeypot nhằm mục đích học hỏi càng nhiều càng tốt từ đối thủ.

  Trò chơi này nhằm mục đích tìm ra những tình huống mà honeypot có thể giả vờ bị đối thủ xâm phạm mà không phải đối mặt với các mối đe dọa nguy hiểm. •
- Giả vờ giúp đối thủ: Trong loại này, honeypot đi cùng đối thủ để giả vờ giúp họ phát động cuộc tấn công. Loại này được sử dụng khi mạng bị tấn công bởi botnet hoặc các mối đe dọa mạng tương tự, trong đó đối thủ xâm phạm một số máy chủ mạng để tập hợp một đội quân. Nếu một thành viên trong đội quân này không tuân theo lệnh của đối thủ, nó sẽ cố gắng tập hợp một đội quân khác. Do đó, honeypot giả vờ bị xâm phạm và tuân theo lệnh của đối thủ. Kỹ thuật lừa dối này rất khó thiết kế. Nhiều tình huống phức tạp phải được xem xét để honeypot không bị phát hiện. Mặt khác, việc giả vờ theo dõi đối thủ trong khi không gây ra thiệt hại thực sự cho mạng là một thách thức. Zhuge và cộng sự (2007) đã đề xuất Honeyd, một honeypot mô phỏng các hoạt động của một



Hình 5. Các tình huống của kỹ thuật bắt chước tiên tiến.



(a) Showing the attack success (b) Pretending to help the adversary

Hình 6. Các kịch bản của kỹ thuật Hợp tác giả.

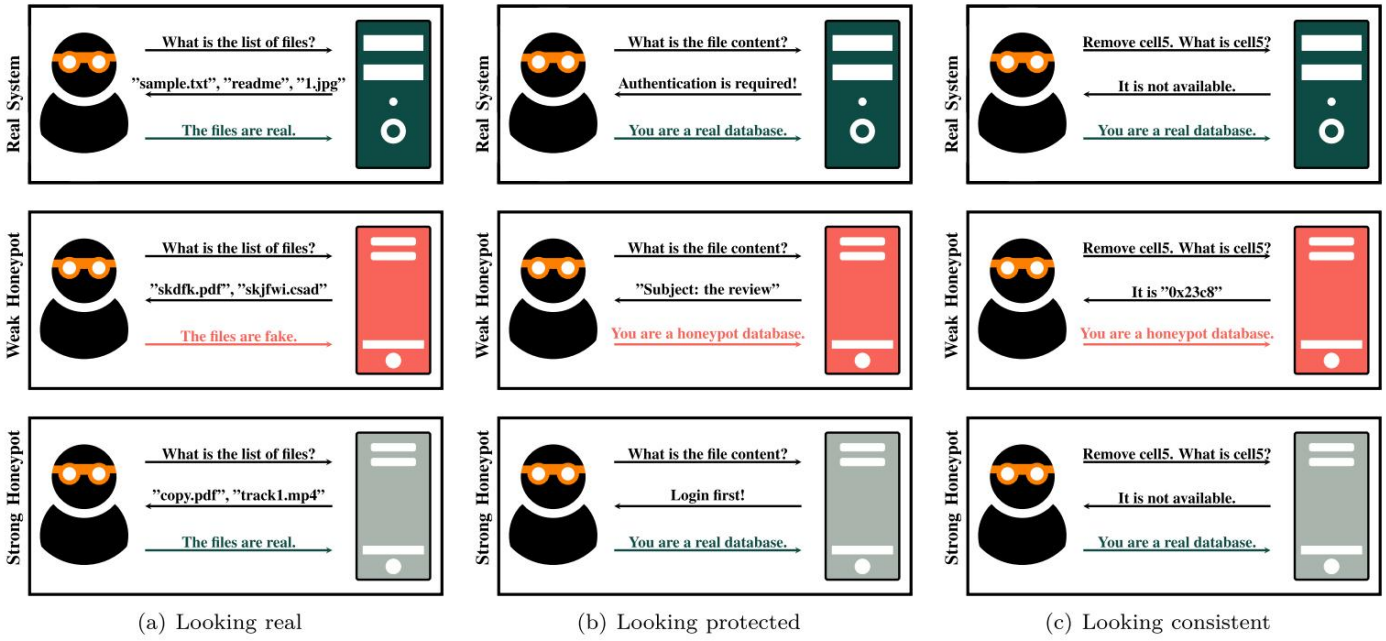
chủ nhà bằng cách giả vờ là một bot. Jiang et al. (2010) cũng đề xuất một công cụ theo dõi các botnet trong đó hệ thống mô phỏng bot hành vi và giao tiếp với các thành viên botnet khác. Hơn nữa, Hayatle et al. (2012) đã mô hình hóa botmaster và honeypot tương tác như một trò chơi Bayesian. Trong mỗi bước, honeypot quyết định tuân theo lệnh của botmaster hoặc bỏ qua nó, và botmaster lựa chọn giữa các hành động sau: kiểm tra bot, tránh các thông tin liên lạc tiếp theo hoặc gửi lệnh tấn công. Sử dụng mô hình này, nhà phát triển có thể tìm ra chiến lược tốt nhất có thể tăng cường sự tin tưởng của đối thủ vào các honeypot hợp tác với kẻ thù.

Hiệu quả của kỹ thuật lừa dối này có thể được đo lường bằng thời gian mà đối thủ lãng phí trên mạng (tức là WT). Nếu đối thủ cảm thấy rằng honeypot đang hợp tác với anh ta/cô ta để thành công trong mục tiêu tấn công, anh ta/cô ta sẽ dành nhiều thời gian hơn để giao tiếp với nó. Chúng ta cũng có thể sử dụng SS để đo lường sức mạnh của sự hợp tác lừa dối.

3.3. Cơ sở dữ liệu lừa đảo

Nhiều đối thủ quan tâm đến việc tiếp cận thông tin bí mật thông tin. Do đó, một honeypot phải có khả năng tạo ra thông tin không hợp lệ dữ liệu hấp dẫn đánh lừa đối thủ trong khi vẫn giữ cho mình không thể nhận ra. Nhưng quá trình này là thách thức theo sau các khía cạnh (hiển thị trong Hình 7):

- Trông giống thật: Nội dung dữ liệu giả phải giống với dữ liệu thật càng tốt. Tên vô nghĩa, cấu trúc dữ liệu bất thường và nội dung tệp tri-fling là những mẫu dữ liệu giả vô dụng tiết lộ danh tính của honeypot. Rowe (2006) đã đề xuất một phương pháp để tạo ra dữ liệu có ý nghĩa nhưng không hợp lệ để sử dụng trong honeypot. Trong phương pháp này, tên tệp được tạo ra bằng cách kết hợp các phần khác nhau của tên tệp thực và nội dung tệp được tạo ra bằng cách trích xuất dữ liệu từ các trang web khác nhau. Abay et al. (2019) đã kiểm tra tính xác thực của dữ liệu giả bằng các phương pháp học sâu. Chakraborty và cộng sự (2019) đề xuất FORGE; một trình tạo dữ liệu giả. FORGE tạo ra các các tập tin giả nhưng đáng tin cậy cho mỗi tập tin thực để giảm khả năng rò rỉ dữ liệu thực. Nội dung của một tập tin giả được xây dựng dựa trên một phép đo siêu trung tâm liên quan đến các khái niệm bản thể học để trông có vẻ thật. Vì FORGE chỉ có thể tạo dữ liệu dạng văn bản, Han et al. (2021) đã đề xuất một phương pháp khác để tạo ra dữ liệu đáng tin cậy, cũng có thể tạo ra nội dung không phải văn bản, chẳng hạn như sơ đồ, phương trình, và bảng. Phương pháp này đầu tiên mô hình hóa một tài liệu với một đồ thị logic xác suất có thể thể hiện đầy đủ các phần khác nhau của nó. Sau đó một thuật toán tham lam được thực hiện để tạo ra các đồ thị giả liên quan đến những cái thật, và cuối cùng, những đồ thị giả được chuyển thành đồ thị giả tài liệu.
- Có vẻ được bảo vệ: Dữ liệu giả không được dễ dàng truy cập kẻ thù. Vì dữ liệu quan trọng khó truy cập, nếu kẻ thù thu thập nó mà không cần nỗ lực, nó trở nên nghi ngờ và phát hiện ra rằng dữ liệu thu thập được là vô giá trị. Ví dụ, mã hóa làm cho dữ liệu giả được lưu trữ trong cơ sở dữ liệu honeypot có giá trị và thực tế hơn. Bởi vì khi đối thủ đối mặt với dữ liệu đơn giản, nó sẽ không có động lực để tiếp tục tấn công vào hệ thống hiện tại. Rowe (2006) gợi ý rằng chúng ta có thể tạo các tập tin có phần mở rộng hấp dẫn chẳng hạn như ".enc" và ".cyc" và điền chúng bằng các số ngẫu nhiên cho hấp dẫn hơn. Một ví dụ khác là quá trình xác thực để cấp quyền truy cập. Dữ liệu cần xác thực để truy cập có thể khuyến khích kẻ thù tấn công chúng. Tuy nhiên, quá trình xác thực không được khó khăn xâm nhập. Fraunholz và Schotten (2018a) đã sử dụng một trang xác thực giả cho máy chủ web lừa đảo được đề xuất để dụ dỗ và thu hút nhiều kẻ thù hơn. Chen và Buford (2009) đã sử dụng một phương pháp khác để dụ kẻ thù về dữ liệu được bảo vệ. Nghiên cứu này sử dụng một honeypot cơ sở dữ liệu để giảm thiểu một số cuộc tấn công tiêm SQL yếu. Do đó, kẻ thù trở nên không nghi ngờ gì về sự tồn tại của cơ sở dữ liệu honeypot.
- Có vẻ nhất quán: Những thay đổi do đối thủ thực hiện phải áp dụng cho dữ liệu giả để nó có thể quan sát dữ liệu được cập nhật không chỉ trong phiên hiện tại mà còn trong các phiên tiếp theo. Nếu đối thủ tìm thấy bất kỳ xung đột nào trong giao tiếp với honeypot, nó sẽ nghi ngờ một cơ chế lừa đảo trong mạng. Chen và Buford (2009) đã thiết kế một honeypot để phát hiện và giảm thiểu SQL tấn công tiêm. Khi kẻ thù sửa đổi cơ sở dữ liệu giả trong honeypot cơ sở dữ liệu này, những thay đổi được áp dụng cho phiên bản sao chép của cơ sở dữ liệu đó. Do đó, kẻ thù sẽ chắc chắn về tính nhất quán



Hình 7. Các tình huống của kỹ thuật Cơ sở dữ liệu lừa đảo.

của cơ sở dữ liệu. Akingbola và cộng sự (2015) cũng đề xuất một phương pháp mạnh hơn, trong đó một bảng được xem xét cho mỗi đối thủ để lưu trữ các thay đổi của họ trong cơ sở dữ liệu. Do đó, khi đối thủ đó quay lại, anh ta/cô ta sẽ thấy các thay đổi trước đó. Địa chỉ IP và MAC của họ xác định đối thủ trong phương pháp này.

Các số liệu đo lường hiệu quả của kỹ thuật này giống với kỹ thuật lỗ hổng hấp dẫn . LA, RA và WT có thể đo lường độ tin cậy của dữ liệu giả honeypot theo quan điểm của đối thủ.

3.4. Sự gián đoạn tinh tế

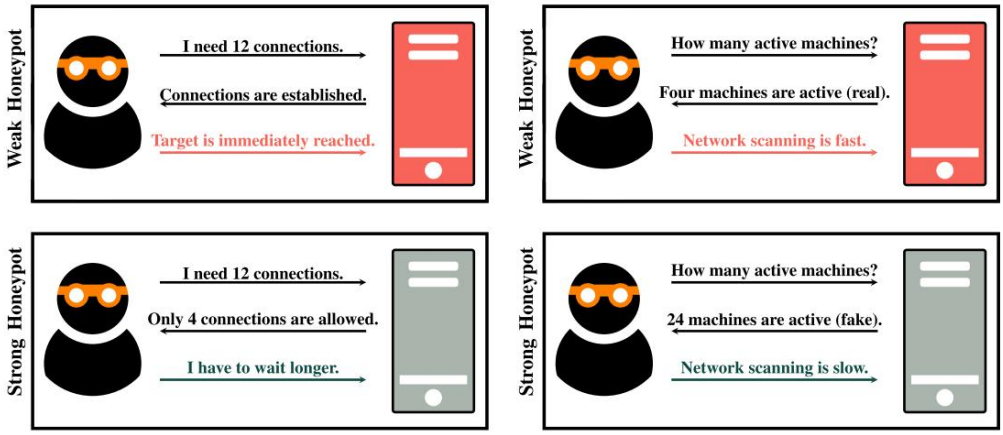
Các cuộc tấn công mạng tiếp tục phát triển về mặt tinh vi, đặt ra thách thức ngày càng lớn đối với việc phát hiện trong bối cảnh đe dọa động. Honeypot nổi lên như một công cụ đáng gờm trong phương pháp phòng thủ chiến lược này. Hoạt động như các hệ thống mồi nhử chuyên dụng được thiết kế tỉ mỉ để mô phỏng các môi trường thực, honeypot dụ dỗ và đánh lừa những kẻ tấn công tiềm năng. Các hệ thống mồi nhử này sử dụng nhiều kỹ thuật khác nhau để tạo ra sự chậm trễ và chướng ngại vật có chủ đích, cản trở đáng kể tiến trình của đối thủ. Trong kỹ thuật đánh lừa "Sự gián đoạn tinh vi", một chiến lược đáng chú ý là sử dụng tarpits. Tarpits là một cơ chế khéo léo để bẫy đối thủ bằng cách cố ý làm chậm tiến trình của họ. Những đầm lầy kỹ thuật số này được thiết kế để lãng phí thời gian và tài nguyên của đối thủ, buộc họ phải điều hướng các mê cung ảo cản trở sự tiến bộ của họ. Các chiến thuật trì hoãn này bao gồm một loạt các động thái đánh lừa, chẳng hạn như mô phỏng các phản ứng phức tạp của hệ thống, đưa vào các phức tạp giả hoặc thay đổi cấu hình mạng một cách linh hoạt. Ví dụ, một honeypot có thể bắt chước một cách thuyết phục kết nối mạng chậm chạp hoặc cố tình gây ra sự chậm trễ trong thời gian phản hồi của các ứng dụng cụ thể. Những chiến lược tinh tế này, bao gồm cả tarpit, tiêu tốn thời gian và tài nguyên của đối thủ một cách hiệu quả, làm giảm tác động tổng thể của cuộc tấn công sắp xảy ra. Tuy nhiên, việc thực hiện thành công các phương pháp trì hoãn này phụ thuộc vào độ chính xác tỉ mỉ. Bất kỳ sai lầm nào trong quá trình triển khai đều có nguy cơ vô tình tiết lộ bản chất thực sự của honeypot, do đó làm giảm hiệu quả của nó như một công cụ lừa đảo. Việc đạt được sự cân bằng tinh tế giữa việc cản trở sự tiến triển của đối thủ và duy trì trạng thái bí mật của honeypot vẫn là một thách thức tinh tế trong phòng thủ an ninh mạng (Rowe và cộng sự, 2007; Dalamagkas và cộng sự, 2019; Bringer và cộng sự, 2012). Một số cuộc tấn công mạng giảm dần theo thời gian. Do đó, lãng phí thời gian của đối thủ hoặc làm chậm họ có thể làm giảm đáng kể hiệu ứng tấn công. Honeypot có thể sử dụng các phương pháp khác nhau để trì hoãn đối thủ. Tuy nhiên, các phương pháp này phải được thực hiện cẩn thận để tránh tiết lộ sự tồn tại của honeypot. Kỹ thuật gián đoạn tinh vi có thể được thực hiện bằng hai phương pháp chính (hiển thị trong Hình 8):

- Hạn chế kết nối: Hạn chế kết nối của đối thủ là một cách để làm chậm họ lại. Dantu và cộng sự (2007) đã đề xuất một phương pháp để ngăn chặn sự lan truyền phần mềm độc hại bằng cách giới hạn số lượng kết nối mới mà máy chủ bị nhiễm có thể tạo ra. Sun và cộng sự (2017) đã đề xuất một khuôn khổ để triển khai honeypot, trong đó độ dài hàng đợi lưu trữ các kết nối đã thiết lập bị giới hạn. Điều này có thể gây trở ngại cho đối thủ và gây ra gián đoạn.
- Gây ra nhiều cuộc thăm dò hơn: Một cách khác để làm gián đoạn đối thủ là mở rộng không gian mục tiêu của họ, dẫn đến nhiều nỗ lực thăm dò hơn. Gjermundrød và Dionysiou (2015) đã đề xuất một honeypot, được gọi là CloudHoneyCY, trong đó tất cả các cổng có thể đều mở và nếu đối thủ giao tiếp qua các cổng này, honeypot sẽ phản hồi bằng các thông điệp bị bóp méo. Kỹ thuật này có thể tốn thời gian vì đối thủ thăm dò tất cả các cổng đang hoạt động. Shakarian và cộng sự (2014) đã thêm các cụm gây mất tập trung, là các mồi nhử được kết nối, tại các điểm mạng cụ thể để làm đối thủ kinh ngạc và khiến mạng có vẻ lớn hơn. Achleitner và cộng sự (2017) cũng đã sử dụng một kỹ thuật tương tự và đề xuất một hệ thống dựa trên honeypot có tác dụng làm chậm đối thủ bằng cách xây dựng các cấu trúc mạng ảo mất nhiều thời gian để quét và thăm dò. Pauna và cộng sự (2018), Suratkar và cộng sự (2021) và Dowling và cộng sự (2018) đã đề xuất các cơ chế học Q và học tăng cường, là một loại kỹ thuật học máy mà qua đó honeypot học cách tương tác với đối thủ để lãng phí thời gian của mình.

Hiệu quả của kỹ thuật lừa dối này có thể được đo bằng số lượng đối thủ giao tiếp với honeypot trong hơn một phiên (SS). Nếu sự gián đoạn không thường xuyên, đối thủ sẽ không quay lại honeypot đó.

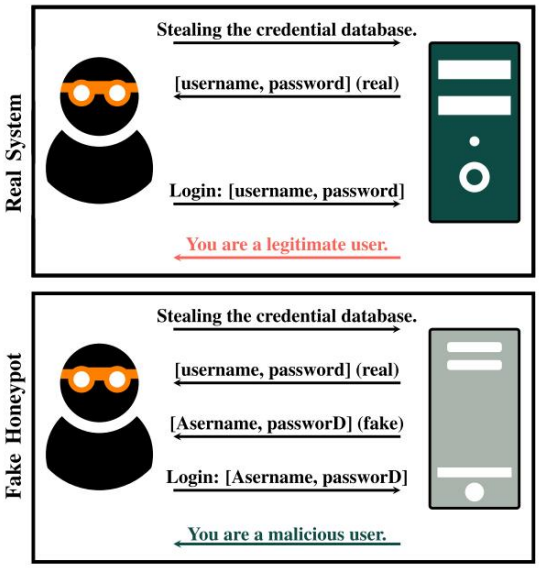
3.5. Mồi Honeytoken

Honeytoken là một thông tin hoặc tài nguyên giả mạo giúp honeypot theo dõi kẻ thù. Vì honeytoken không chứa



(a) Connection restriction (b) Causing extra probes

Hình 8. Các tình huống của kỹ thuật Gián đoạn tinh tế.



Hình 9. Kịch bản của kỹ thuật Honeytoken Bait.

thông tin hợp lệ, bất kỳ ai sử dụng chúng đều được coi là kẻ thù hoặc người dùng bất hợp pháp. Ví dụ, hệ thống xác thực honeypot có thể lưu trữ một số cặp thông tin xác thực giả trong cơ sở dữ liệu của nó. Nếu một đối thủ xâm nhập vào cơ sở dữ liệu và có được quyền truy cập vào các thông tin xác thực này, nó sẽ sớm sử dụng chúng để đăng nhập vào hệ thống. Sử dụng các thông tin xác thực cụ thể này tuyên bố rằng chủ sở hữu của họ là một người dùng có ác ý. Những thông tin đăng nhập giả mạo này là mẫu honeytokens (Shabtai và cộng sự, 2016; Msaad và cộng sự, 2022). A tình huống mẫu trong việc sử dụng honeytoken được thể hiện trong Hình 9. Một honeytoken, một hiện vật kỹ thuật số lừa đảo, là một công cụ mạnh mẽ trong an ninh mạng. Được chế tạo một cách có chủ đích để ngụy trang thành dữ liệu hoặc tài nguyên hợp pháp, chức năng chính là trao quyền cho honeypot trong việc xác định và theo dõi những kẻ thù tiềm tàng. Đặc biệt, honeytoken khác biệt với dữ liệu thông thường về bản chất; không có giá trị thực sự, chúng thiếu tính xác thực liên quan đến thông tin hợp lệ. Đặc điểm nội tại này mang lại cho honeytoken một mục đích riêng biệt: bất kỳ ai tham gia với họ được đánh dấu ngay lập tức là một đối thủ hoặc một người dùng bất hợp pháp trong hệ thống. Hãy xem xét kịch bản của một hệ thống xác thực honeypot: khéo léo, nó nhúng một kho lưu trữ các cặp thông tin xác thực giả mạo trong cơ sở dữ liệu của nó. Những kẻ xâm nhập xâm nhập vào hệ thống và có được quyền truy cập vào các thông tin xác thực lừa đảo này sau đó triển khai chúng để đạt được mục nhập. Phản ứng của hệ thống đối với các hành động như vậy là một dấu hiệu rõ ràng rằng ý định của người dùng là xấu. Những thông tin xác thực cố ý làm giả này tiêu biểu cho bản chất của honeytoken, thể hiện sự kết hợp của sự lừa dối và hiểu biết chiến lược. Minh họa ứng dụng của chúng, hãy hình dung một trường hợp sử dụng thực tế được mô tả trong Hình 9. Ở đây, quỹ đạo của đối thủ hành động diễn ra, đan xen với việc triển khai các honeytokens. Điều này hình ảnh trực quan cung cấp cái nhìn hữu hình về điệu nhảy phức tạp giữa mồi nhử kỹ thuật số và tác nhân độc hại. Với mỗi tương tác, honeytoken cho thấy sức mạnh của chúng không chỉ là một công cụ lừa dối nhưng như một cơ chế trao quyền cho những người bảo vệ để xác định và phản ứng để đe dọa với độ chính xác cao hơn. Kết hợp honeytoken vào bối cảnh an ninh mạng minh họa cho một chiến lược năng động vượt qua sự chuyển hướng đơn thuần. Nó là minh chứng cho sự tiến hóa của quốc phòng cơ chế, thể hiện cách thức đổi mới và hiểu biết kết hợp để đánh bại đối thủ trong một chiến trường kỹ thuật số luôn thay đổi (Mokube và Adams, 2007; Srinivasa và cộng sự, 2020).

- Tạo ra các honeytoken: Bối cảnh tạo ra honeytoken đã chứng kiến sự phát triển mạnh mẽ của các phương pháp luận, mỗi phương pháp đều đóng góp cách tiếp cận độc đáo của mình để củng cố hiệu quả của phương pháp này. kỹ thuật an ninh mạng lừa đảo. Như được nêu bật bởi Juels và Rivest (2013), một trong những chiến lược này liên quan đến việc thao túng mật khẩu người dùng để tạo thành honeytoken. Honeytoken là một cách khéo léo được tạo ra bằng cách thay đổi ký tự đầu tiên và thêm vào các ký tự bổ sung ký tự ở cuối mật khẩu hợp lệ. Biến thể này của hon-eytokens, thường được gọi là "honeywords", viết hoa chữ cái đầu tiên để của việc chuyển hướng người dùng trái phép sang những thứ bịa đặt này điểm vào. Mở rộng câu chuyện, Bercovitch và cộng sự (2011) đã giới thiệu một bước nhảy vọt mang tính đột phá có tên là "HoneyGen". Tự động này honeytoken generator đã cách mạng hóa cách honeytoken được hình thành và sử dụng. Điều khiển HoneyGen trở nên khác biệt là khả năng xây dựng các mã thông báo mật ong phản ánh liền mạch dữ liệu xác thực. Hoạt động theo nguyên tắc rằng các yếu tố lừa dối có hiệu quả nhất khi gần giống với thực tế, HoneyGen sẽ chỉ định một điểm cho mỗi honeytoken được tạo ra. Cơ chế chấm điểm này định lượng sự giống nhau giữa honeytoken và dữ liệu thực tế, đảm bảo mồi nhử đủ hấp dẫn để bẫy những mối đe dọa tiềm tàng. tầm quan trọng của những phương pháp này vượt ra ngoài phạm vi kỹ thuật của chúng sự phức tạp. Chúng nhấn mạnh tính năng động trong an ninh mạng, trong đó sự đổi mới và khéo léo được khai thác để lừa dối và qua mặt kẻ thù. Các kỹ thuật tạo ra honeytoken này thể hiện sự tiến hóa liên tục của các cơ chế phòng thủ, thích ứng với bối cảnh luôn thay đổi của các mối đe dọa mạng. Bằng cách tỉ mỉ điều chỉnh honeytoken thông qua các phương pháp như những phương pháp được đề xuất bởi Juels và Rivest (2013) và Bercovitch et al. (2011), lĩnh vực an ninh mạng tăng cường khả năng ngăn chặn, phát hiện và ứng phó để phát hiện các vi phạm tiềm ẩn với độ chính xác và sự nhanh nhẹn cao hơn. bối cảnh của thế hệ honeytoken là một đấu trường năng động nơi sự đổi mới phát triển mạnh mẽ, thể hiện rõ trong các phương pháp đa dạng nhằm tìm kiếm

nâng cao độ chính xác và hiệu quả của các công cụ an ninh mạng tinh vi này. Đi sâu hơn vào lĩnh vực này, Suryawanshi et al. (2017) đã giới thiệu một cách tiếp cận mới xoay quanh thay đổi chiến lược trong mật khẩu xác thực của người dùng. Kỹ thuật phức tạp này bao gồm việc chuyển đổi các ký tự ở các chỉ số cụ thể, và chuyển đổi chúng giữa chữ hoa và chữ thường. Đáng chú ý, phương pháp này mang lại hiệu quả cao hơn so với phương pháp trước và vẫn giữ được một thuộc tính quan trọng—ý nghĩa. Nếu bản gốc mật khẩu có ý nghĩa quan trọng, các từ ngữ mật ong kết quả lặp lại điều này ý nghĩa. Sự khéo léo này làm giảm đáng kể khả năng gây nghi ngờ giữa những kẻ thù tiềm năng, khiến Honeytokens thậm chí còn giỏi hơn trong việc lừa dối. Chạy song song với đổi mới này, Erguler (2016) đã bắt đầu một quỹ đạo tương tự, ủng hộ một phương pháp chỉ lưu trữ mật khẩu chính hãng và chỉ mục của ký tự đã thay đổi trong cơ sở dữ liệu. Bên dưới bề mặt kỹ thuật, sự đóng góp đặc biệt của tác phẩm này nằm ở trong khái niệm "phẳng". Nguyên tắc này khẳng định rằng mật khẩu được tạo ra phải phản ánh chặt chẽ các mật khẩu do người dùng con người tạo ra, xóa bỏ ranh giới giữa xác thực và giả mạo. Việc theo đuổi sự phẳng lặng nổi lên như một mệnh lệnh chiến lược, tăng cường ảo tưởng và tạo ra sự khác biệt giữa các mã thông báo mật ong thật và giả hầu như không thể nhận ra. Chuyển từ lĩnh vực lý thuyết sang lĩnh vực thực tế, các nhà nghiên cứu cam kết tối đa hóa hiệu quả của honeytokens trong bối cảnh thực tế.

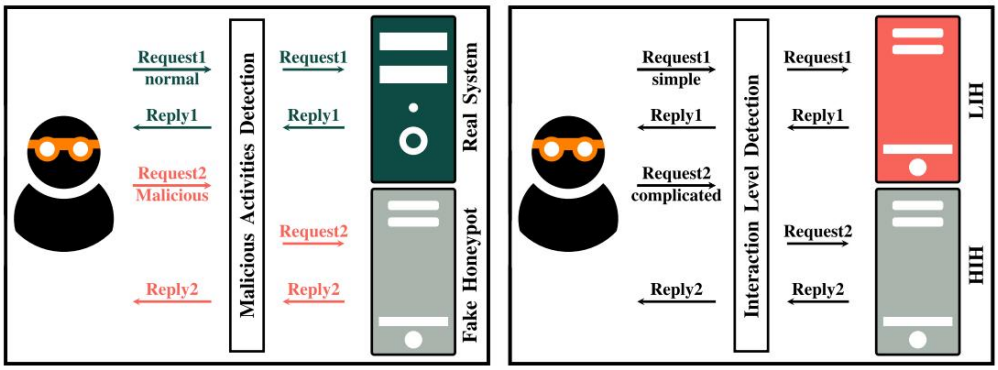
- Sử dụng honeytokens: Wegerer và Tjoa (2016) đáng kể thúc đẩy mục tiêu này bằng cách phác thảo tỉ mỉ các bước triển khai cho máy chủ cơ sở dữ liệu MySQL honeypot. Công nghệ tiên tiến này máy chủ tích hợp honeytokens thụ động và chủ động, phục vụ cho nhu cầu riêng biệt của việc truy tìm kẻ thù bên trong và bên ngoài. Điều này cách tiếp cận đa diện nhấn mạnh tính linh hoạt của honeytoken như một chiến lược an ninh mạng, bao gồm nhiều kịch bản khác nhau và những kẻ thù. Những phương pháp này thể hiện sự theo đuổi không ngừng nghỉ của đổi mới trong bối cảnh lừa dối. Vì an ninh mạng địa hình tiếp tục phát triển, các kỹ thuật này thể hiện mối quan hệ cộng sinh giữa sự khéo léo và phòng thủ chủ động chống lại các đối thủ kỹ thuật số. Bằng cách tinh chỉnh thêm các kỹ thuật tạo mã thông báo mật ong, như được đề xuất bởi Suryawanshi và cộng sự (2017) và Erguler (2016), và tích hợp chúng một cách liền mạch vào các ứng dụng thực tế như Wegerer và Tjoa (2016), các nhà nghiên cứu cung cấp một ngọn hải đăng cho sự tiến triển liên tục của các chiến lược an ninh mạng. Trong trong lĩnh vực triển khai honeytoken, các nhà nghiên cứu đã thúc đẩy sự phát triển của kỹ thuật an ninh mạng này bằng cách giới thiệu hệ thống và phương pháp cải tiến giúp tăng cường hiệu quả và tính linh hoạt của nó. Một đóng góp tiên phong của Bowen và cộng sự. (2009) được hiện thực hóa dưới dạng hệ thống 3. Trung tâm của hệ thống này Đổi mới là sự tích hợp một đèn hiệu vào mỗi honeytoken. Bộ truyền tín hiệu ẩn này đóng vai trò là một thành phần mang tính cách mạng, cho phép honeytokens thiết lập một đường dây liên lạc bí mật với hệ thống 3. Bằng cách truyền tải thông tin hiệu quả liên quan đến thời điểm và địa điểm các mã thông báo mật ong được kích hệ thống. hoạt, 3 tem cải thiện đáng kể độ chính xác của việc xác định mối đe dọa và mở rộng phạm vi hiểu biết có được từ các tương tác honeytoken. Mức độ báo cáo thời gian thực này về cơ bản chuyển đổi honeytokens từ những mồi nhử đơn thuần thành công cụ tình báo có thể hành động. Mở rộng chân trời của các ứng dụng dựa trên đèn hiệu, Park và Stolfo (2012) đi sâu vào việc triển khai chúng như các tác nhân cảnh báo trong quá trình biên dịch hoặc thực thi mã nguồn Java giả mạo mã, bao gồm cả honeytokens. Việc sử dụng khéo léo này khai thác vào môi trường thực thi động của Java, sử dụng nó để tạo ra các cảnh báo thời gian thực bất cứ khi nào có mã lừa đảo hoặc giả mạo, như honeytokens, được thực hiện. Cách tiếp cận này tăng cường thời gian thực khả năng phản ứng của các biện pháp an ninh mạng và minh họa tiềm năng đa dạng của mã thông báo mật ong vượt ra ngoài sự lừa dối thụ động. Hơn nữa làm phong phú thêm danh mục các ứng dụng honeytoken, Akiyama et al. (2018) đã khai thác sức mạnh của honeytokens để thu thập thông tin chi tiết vào các giai đoạn phức tạp của các cuộc tấn công dựa trên web. Bằng cách phân tán chiến lược các honeytoken qua các giai đoạn khác nhau của một cuộc tấn công, họ đã thu thập thành công dữ liệu vô giá, cung cấp một cách toàn diện hiểu biết về hành vi, chiến thuật và động cơ tiềm ẩn của kẻ tấn công. Cách tiếp cận sáng tạo này nhấn mạnh tính linh hoạt của Honeytokens như một công cụ thu thập thông tin tình báo về mối đe dọa chủ động. Mạo hiểm vào lãnh thổ mang tính đột phá, Ja'fari et al. (2021) đã giới thiệu khái niệm honeytokens "kích hoạt". Sự thay đổi mô hình mới lạ này mở rộng khái niệm lừa dối bằng cách giới thiệu một cơ chế để khám phá mối quan hệ giữa các thực thể khác nhau trong hệ sinh thái mạng. Cụ thể, honeytoken kích hoạt hoạt động như một kênh dẫn để tiết lộ các kết nối phức tạp giữa trình tải Mirai và các bot khác (Om Kumar và Sathia Bhama, 2019), làm sáng tỏ động lực phức tạp của các tương tác botnet. Để đánh giá toàn diện hiệu quả của những cách tiếp cận tiến bộ này, Tỷ lệ sử dụng (UR) nổi lên như là số liệu liên quan nhất. Không giống như quyền truy cập đơn thuần đến các mã thông báo mật ong, có thể không phản ánh chính xác đối thủ ý định thực sự, sử dụng honeytoken cung cấp một thước đo xác thực hơn về hiệu quả của chúng. Sử dụng honeytoken biểu thị một mức độ lừa dối, nhấn mạnh tầm quan trọng của UR như một chỉ số tác động của honeytoken trong việc chủ động ngăn chặn tiềm năng mối đe dọa.

- Tiết lộ tấm thảm đa chiều của Honeytokens: Với thiết kế sáng tạo và các ứng dụng đang phát triển, Honey-tokens đã nổi lên như một chiến lược an ninh mạng đa diện vượt ra ngoài các kỹ thuật lừa dối truyền thống. Cuộc thảo luận này mạo hiểm đi vào các chiều không gian chưa được khám phá của việc sử dụng honeytoken, làm sáng tỏ các phương pháp tiếp cận mới giúp tăng cường hiệu lực của chúng trong bảo vệ cảnh quan kỹ thuật số. Một khái niệm mang tính đột phá được giới thiệu bởi Bowen và cộng sự (2009) liên quan đến việc tích hợp các đèn hiệu trong honeytokens, tạo ra hệ thống khéo léo. Điều này 3 bước nhảy vọt mang tính chuyển đổi đưa Honeytokens vào một vai trò tích cực trong phòng thủ an ninh mạng. Đèn hiệu, nằm trong mỗi honeyto-ken, thiết lập một kênh truyền thông được mã hóa với 3 hệ thống. Việc trao đổi thông tin thời gian thực này trao quyền cho những người bảo vệ với những hiểu biết sâu sắc về cốt lõi của các hoạt động của đối thủ—nơi và khi honeytokens được kích hoạt. Cơ chế phản hồi động này định nghĩa lại honeytokens từ mồi nhử thụ động thành thực thể sống, cung cấp thông tin tình báo về mối đe dọa thời gian thực chưa từng có. Bằng cách kịp thời xác định các mối đe dọa và lỗ hổng, hệ thống 3 nâng cao việc triển khai honeytoken lên một chiến lược phòng thủ chủ động, năng động. Vượt ra ngoài ranh giới thông thường của sự lừa dối, Park và Stolfo (2012) đã khám phá ứng dụng sáng tạo của đèn hiệu cho mã thông báo mật ong trong một bối cảnh riêng biệt. Cách tiếp cận của họ tận dụng đèn hiệu để kích hoạt cảnh báo khi biên dịch hoặc thực thi Java lừa đảo mã nguồn, bao gồm honeytokens. Phản hồi chủ động này cơ chế giới thiệu một yếu tố tích cực cho các chiến thuật lừa dối. Tạo cảnh báo khi thực thi mã lừa đảo hợp nhất các honeytokens vào mô hình phòng thủ tích cực. Sự kết hợp này thể hiện sự hài hòa phức tạp giữa honeytoken và mối đe dọa thời gian thực nhận dạng, nơi mà honeytokens lừa dối và kích hoạt phản ứng hành động để ngăn chặn các mối đe dọa tiềm tàng. Mở rộng tầm nhìn thậm chí hơn nữa, Akiyama et al. (2018) đã đi sâu vào tiềm năng chưa được khai thác của honeytokens như nguồn thông tin chi tiết trong các giai đoạn khác nhau của các cuộc tấn công dựa trên web. Honeytokens được triển khai chiến lược trên nhiều các giai đoạn tấn công cung cấp dữ liệu vô giá giúp phát hiện ra kẻ tấn công chiến thuật, hành vi và động cơ tiềm ẩn. Áp dụng honeyto-kens như các dấu hiệu chiến lược trong suốt cuộc tấn công tăng cường mối đe dọa trí thông minh và biến chúng thành công cụ chủ động phân tích tấn công. Cách tiếp cận chiến lược này định vị honeytoken như các tác nhân làm sáng tỏ các câu chuyện tấn công, tăng cường phản ứng sự cố chiến lược với sự hiểu biết toàn diện về chiến thuật của đối phương. Một bước tiến đột phá của Ja'fari và cộng sự (2021) đã giới thiệu honeytokens "activa-tor", một khái niệm mang tính cách mạng vượt qua sự lừa dối

ranh giới. Những mã thông báo này đánh lừa và đóng vai trò là phương tiện để khám phá mối quan hệ trong hệ sinh thái mạng phức tạp. Trình kích hoạt hon-eytoken khám phá rõ ràng các kết nối giữa trình tải Mirai và các bot khác, làm sáng tỏ động lực của botnet. Tiên phong này ứng dụng thể hiện tiềm năng chuyển đổi của honeytokens, từ chỉ là những công cụ lừa dối cho đến những công cụ chiến lược giúp làm sáng tỏ mạng lưới tương tác mạng phức tạp. Kết hợp những cuộc thảo luận này trong bài báo làm phong phú thêm câu chuyện của mình bằng cách giới thiệu vai trò đang phát triển của honeytokens. Những hiểu biết sâu sắc này nhấn mạnh cách đổi mới có thể định hình lại các kỹ thuật truyền thống, làm nổi bật sự hiệp lực giữa các chiến lược tiên tiến và phòng thủ chủ động chống lại các cuộc tấn công mạng năng động mối đe dọa.

- Honeytokens: Khai thác ứng dụng web phong phú: Tài liệu phong phú xung quanh các ứng dụng web cung cấp một bức tranh phong phú của nghiên cứu tập trung vào việc triển khai honeytokens. Những điều lừa dối này các yếu tố, dưới dạng các giá trị khác nhau, được đan xen khéo léo vào cấu trúc phức tạp của các ứng dụng web, đóng vai trò là thành phần quan trọng trong kho vũ khí của các chiến lược an ninh mạng. Cuộc thảo luận này đào sâu hơn vào các chiều hướng đa diện của việc triển khai honeytoken trong các ứng dụng web, thể hiện vai trò quan trọng của chúng trong ngăn chặn các mối đe dọa mạng. Khi được tích hợp chiến lược vào các ứng dụng web, Honeytokens có nhiều hình thức khác nhau được thiết kế để làm rối và đánh lừa những kẻ thù tiềm năng (Qin và cộng sự, 2023). Những nhân tạo này các thành phần biểu hiện như các giá trị mồi nhử bao gồm các tham số HTTP, URL, biểu mẫu, cookie, phần tử HTML, quyền và thậm chí cả tài khoản người dùng được tạo sẵn. Bằng cách nhúng liền mạch các phần tử lừa đảo này các yếu tố trong kiến trúc của ứng dụng web, người bảo vệ tạo ra một mê cung những con đường mòn giả mà kẻ tấn công vô tình đi theo, cuối cùng là vạch trần các chiến thuật, mục tiêu và phương pháp của chúng. Các tham số HTTP lừa đảo, được tích hợp liền mạch vào các yêu cầu và phản hồi của các ứng dụng web, hoạt động như một mồi nhử hấp dẫn mà kẻ thù chắc chắn sẽ tham gia. Những yếu tố ảo tưởng này hướng dẫn một cách tinh tế những kẻ tấn công theo một con đường được xác định trước, cho phép những người phòng thủ hiểu được hành vi của kẻ thù, các kỹ thuật thăm dò và thậm chí các điểm dễ bị tổn thương tiềm ẩn. Tương tự như vậy, các URL lừa đảo, thường được ngụy trang thành các thành phần hợp pháp của cấu trúc ứng dụng, dụ dỗ kẻ tấn công vào các tương tác mang lại thông tin chi tiết có giá trị vào các mẫu điều hướng và chiến lược khám phá của họ. Việc kết hợp các honeytokens được xếp hạng là các biểu mẫu lừa đảo, cookie và các thành phần HTML sẽ thêm một lớp phức tạp vào mặt tiền của ứng dụng web (White và cộng sự, 2014). Những kẻ tấn công, bị thu hút bởi những thực thể bịa đặt này, vô tình để lại dấu vết tương tác cung cấp cho những người chống đối những manh mối vô giá về ý định và mục tiêu của họ. Bằng cách khi tham gia vào các yếu tố mồi nhử này, kẻ thù vô tình tiết lộ những khía cạnh quan trọng trong cách thức hoạt động của chúng, cho phép những người bảo vệ để điều chỉnh các biện pháp an ninh mạng của họ một cách chủ động. Tuy nhiên, ứng dụng của honeytokens mở rộng ra ngoài các mô hình tương tác đơn thuần. Các nhà nghiên cứu cũng đã khám phá tiện ích của chúng trong các quyền và tài khoản người dùng. Người bảo vệ hướng dẫn kẻ thù tham gia với các mục tiêu có vẻ có giá trị bằng cách đưa ra các quyền hoặc tài khoản người dùng giả mạo. Tương tác này phơi bày ý định của kẻ tấn công và hỗ trợ những người bảo vệ trong việc lập bản đồ các con đường và mục tiêu tiềm năng mà kẻ thù có thể theo đuổi. Việc triển khai toàn diện honeyto-kens trong các ứng dụng web thể hiện một bản giao hưởng của sự lừa dối được sắp xếp chính xác để trích xuất thông tin chi tiết từ hành vi của kẻ tấn công. Mỗi giá trị mồi nhử, được đan xen tỉ mỉ trong cấu trúc của ứng dụng web, góp phần tạo nên một câu chuyện lớn hơn tiết lộ chiến thuật và động cơ của đối thủ. Sự tương tác năng động giữa sự đổi mới, hiểu biết chiến lược và bối cảnh kỹ thuật số tạo ra một cơ chế phòng thủ mạnh mẽ giúp củng cố an ninh mạng trong khuôn mặt của các mối đe dọa kỹ thuật số đang phát triển (Papaspirou và cộng sự, 2021; Jon-sson và Marteni, 2022). Sau đây là mô tả mở rộng về từng mối đe dọa loại honeytoken, cùng với nhiều thông tin hơn:

  - Tham số HTTP giả mạo: Tham số HTTP giả mạo là dữ liệu giả mạo các thành phần được chèn một cách chiến lược vào HTTP của ứng dụng web các nhiệm vụ và phản hồi. Các tham số sai này bắt chước dữ liệu chính hãng và được thiết kế để thu hút sự chú ý của những kẻ tấn công tiềm năng. Như những kẻ tấn công tương tác với các tham số mồi nhử này, những người bảo vệ thu thập thông tin có giá trị về bản chất tương tác của họ. Điều này bao gồm thông tin chi tiết về các điểm cuối mục tiêu, dữ liệu họ tìm kiếm và các phương pháp họ sử dụng để thao túng ứng dụng. Việc phân tích các tương tác này giúp những người bảo vệ khám phá ra các chiến thuật và mục tiêu của kẻ thù, cho phép họ điều chỉnh phòng thủ cơ chế (Izagirre, 2017).
  - URL lừa đảo: URL lừa đảo là địa chỉ web giả mạo phản ánh các đường dẫn hợp lệ trong một ứng dụng web. Các URL này được chế tạo tỉ mỉ để xuất hiện như một phần không thể thiếu của ứng dụng cấu trúc. Những kẻ tấn công điều hướng các URL lừa đảo này cung cấp những người bảo vệ có hiểu biết sâu sắc về các mô hình khám phá của họ. Điều này giúp người bảo vệ hiểu được ứng dụng nào mà kẻ tấn công thấy hấp dẫn hoặc các bộ phận có khả năng dễ bị tổn thương. Bằng cách phân tích tần suất và trình tự tương tác với các URL lừa đảo, người bảo vệ đạt được hiểu sâu hơn về động cơ của kẻ tấn công và khả năng tấn công vectơ (Sahin và cộng sự, 2022).
  - Biểu mẫu mồi nhử: Biểu mẫu mồi nhử bao gồm các trường nhập liệu tổng hợp được nhúng một cách chiến lược vào các biểu mẫu web hợp pháp. Các trường này có vẻ chân thực, hấp dẫn những kẻ tấn công tham gia với họ. Thông tin do những kẻ tấn công gửi trong các biểu mẫu này cung cấp cho những người bảo vệ những hiểu biết có giá trị về ý định và mục tiêu của họ. Người bảo vệ có thể tìm hiểu về các điểm dữ liệu cụ thể mà kẻ tấn công tìm kiếm, các loại tấn công mà chúng đang cố gắng thực hiện và các chiến thuật mà chúng sử dụng để khai thác lỗ hổng. Thông tin này cho phép những người bảo vệ tăng cường an ninh các biện pháp an toàn, củng cố ứng dụng chống lại các mối đe dọa tiềm ẩn (Bowen và cộng sự, 2009).
  - Cookie lừa đảo: Cookie lừa đảo là mã thông báo dữ liệu giả mạo được đưa vào trình duyệt của người dùng khi tương tác với ứng dụng. Khi những kẻ tấn công vô tình tương tác với các cookie này, những người bảo vệ sẽ hiểu rõ hơn về hành vi của chúng. Điều này bao gồm các chi tiết như các trang họ truy cập, hành động của họ và các mẫu của họ. Bằng cách phân tích thông tin thu thập được từ các cookie lừa đảo, những người bảo vệ có thể phân biệt được động cơ của kẻ tấn công, chẳng hạn như nỗ lực trinh sát hoặc cố gắng thao túng dữ liệu phiên. Sự hiểu biết này thông báo các biện pháp phòng thủ chủ động (Sun và cộng sự, 2020).
  - Mồi phần tử HTML: Mồi phần tử HTML liên quan đến chiến lược chèn các thành phần HTML tổng hợp vào trong ứng dụng web mã nguồn. Những thành phần này thường bị ẩn khỏi người dùng thông thường nhưng lại hấp dẫn những kẻ tấn công tiềm năng. Khi những kẻ tấn công tương tác với những yếu tố ẩn này, những người bảo vệ có được cái nhìn sâu sắc về chiến thuật của họ và kỹ thuật. Điều này bao gồm các chi tiết về phương pháp của kẻ tấn công để khám phá cấu trúc của ứng dụng, có khả năng xác định các khu vực quan tâm hoặc lỗ hổng. Phân tích các tương tác với HTML mồi như nguyên tố thông báo cho người bảo vệ về các vectơ tấn công tiềm ẩn và hướng dẫn các chiến lược phòng thủ của họ (Voris và cộng sự, 2013).
  - Quyền được chế tạo: Quyền được chế tạo liên quan đến việc tạo mức độ truy cập tổng hợp được cấp cho các vai trò hoặc người dùng cụ thể trong ứng dụng. Những kẻ tấn công cố gắng khai thác những thứ bịa đặt này quyền vô tình tiết lộ mục tiêu của họ khi họ tham gia với các mức truy cập giả định này. Người bảo vệ có thể có được thông tin chi tiết về các con đường dự định của kẻ tấn công, các mục tiêu tiềm năng và mức độ về kiến thức của họ về cấu trúc quyền của ứng dụng. Thông tin này cho phép người bảo vệ áp dụng các biện pháp an ninh để chống lại các chiến lược tấn công cụ thể và hạn chế các vi phạm tiềm ẩn (Domingue và cộng sự, 2014).
  - Tài khoản người dùng giả mạo: Tài khoản người dùng giả mạo là tài khoản nhân tạo hồ sơ được đưa vào cơ sở người dùng của ứng dụng. Những tài khoản được chế tạo này xuất hiện như mục tiêu tiềm năng cho những kẻ tấn công đang cố gắng truy cập trái phép. Khi những kẻ tấn công tương tác với các tài khoản lừa đảo này, những người bảo vệ sẽ thu thập thông tin chi tiết về phương pháp xâm nhập của chúng, các con đường họ đi và ý định của họ. Bằng cách phân tích các tương tác với các tài khoản người dùng giả định, những người bảo vệ có thể điều chỉnh bảo mật



(a) Interfering after detection (b) Improving the performance

Hình 10. Các tình huống của kỹ thuật chuyển hư ớng lư u lư ợng.

các biện pháp nhằm giải quyết các vectơ tấn công cụ thể đư ợc quan sát thấy và tăng cư ờng bảo mật toàn bộ hệ thống (Jones, 2016).

Trong các ứng dụng web, điều cần thiết là phải lư u ý rằng phần hiện tại của chúng tôi, phư ơng pháp, không đề cập đến các chiến lư ợc nâng cao hơn, đặc biệt là những chiến lư ợc liên quan đến trí tuệ nhân tạo (AI). Cụ thể, các kỹ thuật như sử dụng thuật toán học sâu để tạo ra honeydata quan hệ vẫn chư a đư ợc khám phá trong nội dung. Việc kết hợp các phư ơng pháp tiếp cận dựa trên AI sẽ giới thiệu một lớp sự phức tạp và khả năng thích ứng với việc tạo ra honeytoken. Ví dụ, các mô hình học sâu có khả năng tăng cư ờng khả năng bắt chư ớc hành vi ngư ời dùng thực sự, dẫn đến các honeytokens thuyết phục hơn và phù hợp hơn về mặt ngữ cảnh. Phư ơng pháp này củng cố honeypot khả năng đánh lừa và phù hợp với bối cảnh đang phát triển của các mối đe dọa mạng thư ờng sử dụng các kỹ thuật tinh vi. Sâu học tập là một công cụ mạnh mẽ để tạo ra honeydata quan hệ, bao gồm việc tạo ra các tư ơng tác ngư ời dùng giả trong một ứng dụng web để đánh lừa những kẻ tấn công tiềm năng. Để đạt đư ợc điều này, học sâu các thuật toán như mạng nơ-ron hồi quy (RNN) hoặc mạng bộ nhớ dài hạn ngắn (LSTM) có thể đư ợc sử dụng để nắm bắt tuần tự phụ thuộc trong dữ liệu, làm cho chúng phù hợp để mô hình hóa các khía cạnh quan hệ. Bằng cách đào tạo về tư ơng tác ngư ời dùng hợp pháp, sâu các mô hình học tập có thể học các mẫu vốn có trong hành vi của ngư ời dùng, cho phép chúng tạo ra các mã thông báo mật ong rất giống hành động ngư ời dùng xác thực. Hơn nữa, các mô hình học sâu xuất sắc trong việc nắm bắt các sắc thái ngữ cảnh, cho phép tạo ra các honeytoken duy trì sự mạch lạc trong một trình tự hoặc mối quan hệ, làm cho chúng thuyết phục hơn đối với những kẻ tấn công tiềm năng. Thuật ngữ "quan hệ honeydata" ngụ ý rằng các honeytoken đư ợc tạo ra đã đư ợc chế tạo riêng lẻ để giống với các hành động xác thực và thể hiện mối quan hệ hoặc sự phụ thuộc giữa chúng. Một honeydata quan hệ trình tự có thể bao gồm ngư ời dùng đăng nhập, điều hư ớng qua nhiều trang khác nhau và hoàn tất giao dịch—tất cả đều đư ợc liên kết chặt chẽ với tạo nên một hành trình ngư ời dùng mạch lạc và đáng tin cậy. Một trong những điểm mạnh của việc học sâu là khả năng thích ứng của nó với các mô hình mới và phát triển bối cảnh. Khi kẻ tấn công thay đổi chiến lư ợc của chúng, các mô hình học sâu có thể đư ợc đào tạo lại để hiểu và tạo ra các mã thông báo mật ong thích nghi với những thay đổi này. Khả năng thích nghi này đặc biệt có giá trị trong cảnh quan năng động của bảo mật ứng dụng web, nơi tấn công các kỹ thuật liên tục phát triển (Mohan và cộng sự, 2022).

3.6. Chuyển hư ớng lư u lư ợng truy cập

Chuyển hư ớng lư u lư ợng trong mạng có chứa một hoặc nhiều honeypot thư ờng diễn ra trong hai tình huống (thể hiện ở Hình 10):

- Can thiệp sau khi phát hiện: Trong một số tình huống, đối thủ là đư ợc phát hiện trong mạng. Tuy nhiên, chúng tôi không chặn anh ấy/cô ấy khỏi quan sát nhiều hoạt động hơn từ anh ấy/cô ấy hoặc lãng phí thời gian của anh ấy/cô ấy. Do đó, chúng ta phải ngăn chặn đối thủ giao tiếp với những thông tin quan trọng tài nguyên trong mạng. Một số honeypot sử dụng kỹ thuật chuyển hư ớng lư u lư ợng để thay đổi đích đến của lư u lư ợng của đối thủ và gửi nó về phía họ. Kỹ thuật này phải thực hiện các quy trình thích hợp để ẩn sự chuyển hư ớng khỏi đối thủ.

  yêu cầu chính của kỹ thuật này là phát hiện mối đe dọa. Một cơ chế phát hiện trư ớc tiên phải đư ợc thực hiện để xác định phần mềm độc hại giao thông, có thể đư ợc thực hiện bằng một trong những phư ơng pháp sau:

  - Hệ thống phát hiện xâm nhập: Một số nhà nghiên cứu sử dụng IDS cho quá trình phát hiện. Ví dụ, La et al. (2016) đã đề xuất một mô hình trò chơi báo hiệu cho một mạng chuyển hư ớng lư u lư ợng độc hại đến một honeypot. Lư u lư ợng truy cập độc hại đư ợc xác định bằng cách triển khai một IDS. Chiến lư ợc giúp ngư ời bảo vệ mạng quyết định lư u lư ợng nào phải đư ợc chuyển hư ớng đư ợc lấy bằng cách sử dụng Bayesian cân bằng trong trò chơi này. Selvaraj và cộng sự (2016) đã sử dụng cơ sở dữ liệu honey-pot trong mạng và khi IDS phát hiện ra phần mềm độc hại giao thông, nó sẽ đư ợc chuyển hư ớng đến cơ sở dữ liệu giả mạo đó để bảo mật dữ liệu đư ợc lư u trữ. Hơn nữa, Park et al. (2019) đã sử dụng một honeypot, đư ợc gọi là DVNH, trong Mạng đư ợc xác định bằng phần mềm (SDN) là đích đến chuyển hư ớng của lư u lư ợng truy cập độc hại, đư ợc phát hiện bởi IDS.
  - Các loại honeypot khác: Một số nhà nghiên cứu khác cố gắng phát hiện lư u lư ợng truy cập độc hại bằng một loại honeypot khác và sau đó chuyển hư ớng nó. Trong số đó, chúng ta có thể đề cập đến công trình do Ja'-fari et al. (2021). Họ đã sử dụng kỹ thuật chuyển hư ớng để phát hiện những ngư ời tải botnet Mirai. Đầu tiên họ xác định những kẻ bị xâm phạm máy chủ bằng cách đặt mồi bẫy mật ong trong mạng, sau đó theo dõi họ tìm ra những ngư ời nạp và cuối cùng chuyển hư ớng lư u lư ợng nạp vào hệ thống bẫy mật để lãng phí thời gian của đối thủ. Công việc của Biedermann et al. (2012) cũng trong lĩnh vực này. Họ đã sử dụng một đám mây honeypot để phát hiện các cuộc tấn công quét từ điển và tấn công bằng vũ lực và sau đó sao chép một honeypot ảo trên máy mục tiêu tấn công để chuyển hư ớng.
  - Các phư ơng pháp phát hiện khác: Cuối cùng, chúng ta có thể thấy một số nghiên cứu cố gắng phát hiện lư u lư ợng truy cập độc hại bằng các phư ơng pháp khác. Đối với Ví dụ, Sardana và Joshi (2009) đã đề xuất một kiến trúc mạng để giảm thiểu các cuộc tấn công DoS bằng cách chuyển hư ớng luồng tràn ngập đến honeypots. Luồng lũ đư ợc phát hiện bằng cách kiểm tra lư u lư ợng truy cập entropy. Việc chuyển hư ớng duy trì chất lư ợng dịch vụ mạng cho ngư ời dùng hợp pháp. Tian et al. (2015) đã đề xuất một honeypot USB có thể chuyển hư ớng dữ liệu đư ợc gửi từ một thiết bị USB độc hại đến một honeypot. Phát hiện thiết bị USB bất thư ờng đư ợc thực hiện bởi ngư ời dùng cuối cùng trong nghiên cứu này.

- Cải thiện hiệu suất: Quá trình chuyển hư ớng cũng có thể đư ợc đư ợc sử dụng để tăng hiệu suất của honeypot. Ví dụ, Wang và Wu (2019) đã thiết kế một hệ thống, trong đó sức mạnh và các cuộc tấn công yếu đư ợc chuyển hư ớng đến tư ơng tác cao và tư ơng tác thấp honeypots, tư ơng ứng. Kỹ thuật này có thể giúp các nhà phát triển tạo ra các mạng lư ới mật ong có thể mở rộng và giảm chi phí của chúng. Fan và Fernán-dez (2017) đã thực hiện một kỹ thuật tư ơng tự để lọc các thông tin thú vị hơn

các kịch bản tấn công và gửi chúng đến honeypot. Trong tác phẩm này,
cơ chế phát hiện được thực hiện bởi Snort IDS.

WT là số liệu thích hợp nhất để đo lường kỹ thuật này
sức mạnh lừa dối. Khi kẻ thù dành quá nhiều thời gian của mình
giao tiếp với các honeypot này, chúng ta có thể nói rằng honeypot
đang thực hiện đúng nhiệm vụ của nó. Hơn nữa, Bedi et al. (2011) đã đề xuất
một mô hình trò chơi hai người chơi, trong đó người bảo vệ mạng cố gắng giảm thiểu các
cuộc tấn công DDoS bằng cách chuyển hướng lưu lượng truy cập của đối thủ đến một honeypot
hệ thống. Mô hình này giúp người bảo vệ tìm ra các thông số thích hợp để
được xem xét để chuyển hướng.

4. Lừa dối trong lưới mật

Các kỹ thuật lừa đảo trên mạng để cải thiện hiệu suất của honeypot bao gồm các chiến
lược sáng tạo được áp dụng trong an ninh mạng để tăng cường
hiệu quả và khả năng của honeypot. Honeypot, mô phỏng
các hệ thống hoặc dịch vụ dễ bị tổn thương, được thiết kế tỉ mỉ để thu hút và
đánh lừa những kẻ tấn công tiềm năng, chuyển hướng sự tập trung của chúng khỏi các hệ
thống sản xuất thực sự. Các kỹ thuật lừa dối này liên quan đến việc phát triển
môi trường honeypot phức tạp và hấp dẫn hơn. Mục đích là
không chỉ dụ kẻ tấn công mà còn nghiên cứu hành vi, phương pháp của chúng,
và động cơ một cách toàn diện. Sự hiểu biết sâu sắc hơn này trao quyền
các chuyên gia an ninh mạng với những hiểu biết có giá trị để tinh chỉnh khả năng phòng thủ
chiến lược và tăng cường giảm thiểu mối đe dọa. Tích hợp các chiến thuật tiên tiến
thúc đẩy sự tham gia, kéo dài tương tác và thu thập thông tin tình báo có ý nghĩa là
trọng tâm của khái niệm. Các kỹ thuật như vậy có thể bao gồm
bắt chước hành vi, trong đó honeypot bắt chước hành động của người thật
người dùng hoặc hệ thống, đánh lừa kẻ tấn công và tạo ra dữ liệu vô giá
về cách tiếp cận của họ. Một kỹ thuật khác liên quan đến việc mô phỏng dịch vụ động, theo
đó honeypot mô phỏng động nhiều dịch vụ khác nhau, làm cho môi trường trở nên thực tế và
phức tạp hơn. Sự phức tạp này
thách thức những kẻ tấn công phân biệt honeypots với các hệ thống thực tế. Những đóng góp
nghiên cứu trong lừa đảo mạng đã làm phong phú đáng kể
cảnh quan của các phương pháp honeypot (Srinivasa và cộng sự, 2022). Nhiều
các nghiên cứu đã đề xuất nhiều chiến lược khác nhau, từ việc kết hợp các biện pháp lừa dối
các yếu tố vào kiến trúc mạng để phát triển tương tác tiên tiến
mô hình. Hơn nữa, điều tra các khía cạnh tâm lý của kẻ tấn công
sự tham gia, chẳng hạn như thành kiến nhận thức, đã truyền cảm hứng cho những cách tiếp cận mới lạ
để thiết kế honeypot. Sử dụng các nguyên tắc lý thuyết trò chơi để tối ưu hóa sự lừa dối
và sự tham gia cũng nổi lên như một hướng nghiên cứu đầy hứa hẹn.
Những đóng góp này nhấn mạnh tính linh hoạt của các kỹ thuật lừa đảo trên mạng
và bản chất tiến hóa và vai trò then chốt của chúng trong việc tinh chỉnh hiệu suất
honeypot. Bằng cách khai thác các phương pháp sáng tạo này, các chuyên gia an ninh mạng
hướng đến mục tiêu tăng cường độ chính xác của việc phát hiện mối đe dọa, nâng cao hồ sơ
kẻ tấn công và tối ưu hóa các chiến lược ứng phó sự cố. Cuối cùng,
sự tương tác giữa nghiên cứu về sự lừa dối và việc thực hiện
các kỹ thuật tiên tiến thúc đẩy hiệu quả của honeypot, bảo vệ
tài sản kỹ thuật số và củng cố các tổ chức chống lại bối cảnh đang thay đổi
của các mối đe dọa mạng (de Nobrega, 2023).

- Chiến lược sáng tạo để nâng cao hiệu suất Honeypot
- Chuyển hướng kẻ tấn công bằng hệ thống Honeypot mô phỏng
- Tạo ra môi trường Honeypot thuyết phục và hấp dẫn
- Phương pháp lừa dối: Thông tin chi tiết về hành vi của kẻ tấn công
- Mô phỏng hành vi: Tiết lộ cách tiếp cận của kẻ tấn công
- Tính xác thực và thách thức: Mô phỏng dịch vụ động
- Làm giàu phương pháp Honeypot thông qua đóng góp nghiên cứu
các hành động
- Thiết kế theo tâm lý: Mô hình tương tác nâng cao
- Chiến lược tham gia: Áp dụng lý thuyết trò chơi vào Honeypots
- Phòng thủ chính xác: Những cải tiến nâng cao khả năng phát hiện mối đe dọa
- Từ Nghiên cứu đến Hành động: Tăng cường Hiệu quả của Honeypot

nội dung tiếp theo trình bày mô tả chi tiết cho từng điểm chính
đã đề cập trước đó. Những mô tả này cung cấp thông tin chi tiết về các chiến lược khác
nhau góp phần nâng cao hiệu suất của honeypot và
hiệu quả an ninh mạng. Các cuộc thảo luận bao gồm một loạt các
các kỹ thuật sáng tạo, bao gồm các phương pháp đánh lạc hướng kẻ tấn công bằng cách sử
dụng hệ thống bẫy mật giả, nghệ thuật chế tạo các phương pháp thuyết phục và hấp dẫn
môi trường bẫy mật, sử dụng sự lừa dối để hiểu rõ hơn về hành vi của kẻ tấn công và khái
niệm bắt chước hành vi để tiết lộ kẻ tấn công
cách tiếp cận. Ngoài ra, nội dung khám phá các chiến lược như mô phỏng dịch vụ năng
động, mang đến tính xác thực và thách thức,
làm giàu phương pháp honeypot thông qua đóng góp nghiên cứu, sử dụng thiết kế theo hướng
tâm lý, áp dụng lý thuyết trò chơi cho chiến lược
sự tham gia và tận dụng các sáng kiến để phòng thủ chính xác. Những hiểu biết sâu sắc
được chia sẻ trong mỗi mô tả cùng nhau góp phần vào sự hiểu biết toàn diện về cách các
phương pháp tiếp cận này tăng cường an ninh mạng và củng cố các tổ chức chống lại các
mối đe dọa đang phát triển (Shin và Lowry,
2020).

- Các kỹ thuật lừa đảo mạng để cải thiện hiệu suất của honeypot liên quan đến các
chiến lược sáng tạo trong an ninh mạng để nâng cao honeypot
hiệu quả: Phát triển các kỹ thuật lừa đảo trên mạng đã nổi lên như
một cách tiếp cận quan trọng để tăng cường hiệu suất honeypot trong bối cảnh an ninh mạng
luôn thay đổi. Bằng cách tận dụng sự kết hợp giữa thao túng tâm lý, đổi mới kỹ thuật và
thiết kế chiến lược, các kỹ thuật này nhằm mục đích đánh bại các tác nhân độc hại bằng
cách cung cấp cho chúng
mục tiêu có vẻ xác thực. Mục tiêu cốt lõi là tạo ra honeypot
thu hút kẻ tấn công và chủ động lừa dối và lôi kéo họ. Điều này liên quan đến việc tạo ra
các môi trường phản ánh các hệ thống thực trong khi nhúng
những mâu thuẫn tinh vi khiến kẻ tấn công càng lún sâu vào sự lừa dối.
Khi an ninh mạng liên tục phải đối mặt với những thách thức mới, việc triển khai an ninh mạng
kỹ thuật lừa dối cung cấp một cách tiếp cận năng động và nhạy bén để nâng cao hiệu quả
của honeypot (Almeshekah và cộng sự, 2013; Zhang và Thing,
2021).

- Honeypots là hệ thống mô phỏng chuyển hướng kẻ tấn công khỏi thực tế
hệ thống sản xuất bằng cách thu hút và đánh lừa chúng: Honeypots là
một trong những sáng tạo khéo léo trong an ninh mạng, hoạt động như một chiến thuật
chuyển hướng để chuyển hướng kẻ tấn công khỏi các hệ thống sản xuất thực tế. Với một
mặt tiền giả tạo, honeypot dụ dỗ kẻ tấn công tương tác, cung cấp cho người bảo vệ một
môi trường được kiểm soát để theo dõi chặt chẽ và
phân tích hành vi của kẻ tấn công. Cách tiếp cận đánh lạc hướng này là một cách có giá trị
hệ thống cảnh báo sớm, cho phép các chuyên gia an ninh phát hiện ra các nguy cơ tiềm ẩn
các mối đe dọa trước khi chúng có thể xâm phạm các tài sản quan trọng. Bằng cách khai thác
sự tò mò và ham muốn đối với các mục tiêu dễ bị tổn thương, honeypot đóng vai trò then chốt trong
thu thập thông tin tình báo giúp xây dựng các chiến lược an ninh mạng hiệu quả hơn.

Những kỹ thuật này tạo ra honeypot thuyết phục và hấp dẫn hơn
môi trường, nhằm mục đích thu hút những kẻ tấn công và thu thập thông tin chi tiết về chúng
chiến thuật: Việc tạo ra môi trường honeypot thuyết phục và hấp dẫn đòi hỏi sự cân bằng
tinh tế giữa tính xác thực và sự thao túng. Các chuyên gia an ninh mạng cố gắng tạo ra
môi trường thu hút kẻ tấn công
và thúc đẩy sự tham gia bền vững bằng cách bắt chước một cách tỉ mỉ các hành vi hợp pháp
sự xuất hiện, lỗ hổng và tương tác của hệ thống. Sự tham gia này
không chỉ là lừa dối kẻ tấn công; mà còn là tạo ra một môi trường
khuyến khích họ tiết lộ chiến thuật, sở thích và chiến lược của mình.
Cách tiếp cận này mang lại cho những người bảo vệ một cơ hội chưa từng có để nghiên cứu
quá trình ra quyết định của kẻ tấn công, sở thích về bộ công cụ và sự phát triển
kỹ thuật. Khi những kẻ tấn công tương tác với honeypot, những người bảo vệ sẽ có được
thông tin chi tiết thúc đẩy sự phát triển của an ninh mạng mạnh mẽ và linh hoạt hơn
biện pháp (Ackerman, 2020).

- Các phương pháp lừa dối không chỉ đánh lạc hướng kẻ tấn công mà còn cho phép
nghiên cứu sâu hơn về hành vi, phương pháp và động cơ của chúng: Lừa dối
phương pháp này đóng vai trò như con dao hai lưỡi trong lĩnh vực an ninh mạng.
Trong khi họ có hiệu quả chuyển hướng những kẻ xấu ra khỏi những mục đích có giá trị
tài sản, giá trị thực sự của chúng nằm ở những hiểu biết toàn diện mà chúng cung cấp về
thế giới của những kẻ thù mạng. Thông tin được thu thập
từ các tương tác honeypot cung cấp một cửa sổ độc đáo vào hành vi, phương pháp và động
cơ của kẻ tấn công. Sự hiểu biết sâu sắc hơn này cho phép
các nhà nghiên cứu an ninh mạng dự đoán những động thái tiếp theo của kẻ tấn công, củng cố
cơ chế phòng thủ và tinh chỉnh các chiến lược ứng phó sự cố (Mar-ble và cộng sự, 2015).
Bằng cách phân tích cẩn thận các cuộc giao tranh của kẻ tấn công trong
môi trường honeypot, các chuyên gia bảo mật có được bức tranh rõ ràng hơn về

bối cảnh đe dọa đang phát triển và các chiến thuật được sử dụng bởi những kẻ xấu các thực thể.

• Mô phỏng hành vi là một kỹ thuật mà trong đó honeypot bắt chước hành động của người dùng hoặc hệ thống thực, tạo ra dữ liệu có giá trị về kẻ tấn công cách tiếp cận (Shi et al., 2012): Kỹ thuật bắt chước hành vi đưa yếu tố tinh tế vào lĩnh vực bẫy mật. An ninh mạng các chuyên gia tận dụng các giả định và thói quen của kẻ tấn công bằng cách tỉ mỉ tạo ra các tương tác phản ánh hành động của người dùng hoặc hệ thống đích thực. Kẻ tấn công, bị thu hút bởi ảo tưởng tương tác với người dùng đích thực tài sản, tham gia vào honeypots theo những cách song song với các chiến lược thông thường của họ. Cách tiếp cận này mang đến cơ hội vô song để thu thập dữ liệu về cách tiếp cận, chiến thuật và mô hình ra quyết định của kẻ tấn công. Khi những kẻ tấn công vô tình điều hướng môi trường mô phỏng, những người bảo vệ có được những hiểu biết quan trọng về hoạt động bên trong của tội phạm mạng, giúp xây dựng chiến lược an ninh mạng chủ động.

• Mô phỏng dịch vụ động liên quan đến việc mô phỏng động nhiều dịch vụ khác nhau để tạo ra một môi trường chân thực và đầy thử thách hơn đối với những kẻ tấn công (Badr và cộng sự, 2015): Mô phỏng dịch vụ động thực hiện khái niệm về honeypots hơn nữa bằng cách kết hợp khả năng thích ứng theo thời gian thực. Honeypot truyền thống có thể cung cấp môi trường tĩnh, nhưng mô phỏng dịch vụ động mô phỏng tính lưu động của hệ thống thực tế. Bằng cách thay đổi động các dịch vụ được cung cấp, các chuyên gia an ninh mạng thách thức những kẻ tấn công phân biệt giữa các dịch vụ thực tế và mô phỏng, khiến các tương tác của chúng xác thực và đầy thử thách hơn. Cách tiếp cận này làm tăng tính phức tạp của môi trường honeypot, thu hút những kẻ tấn công tinh vi hơn bị thu hút bởi các cơ hội tham gia tinh tế được trình bày. Như những kẻ tấn công vật lộn với tính xác thực của môi trường, những người bảo vệ hiểu rõ hơn về khả năng và ý định của kẻ tấn công.

• Những đóng góp nghiên cứu về lừa đảo trên mạng đã làm giàu thêm honeypot phương pháp luận, đề xuất các chiến lược như tích hợp các yếu tố lừa dối vào kiến trúc mạng (Steingartner và cộng sự, 2021): Lừa đảo trên mạng đã chứng kiến sự gia tăng các đóng góp nghiên cứu sáng tạo làm phong phú thêm phương pháp luận xung quanh honeypots. Các nhà nghiên cứu đã khám phá nhiều con đường khác nhau, từ việc nhúng các yếu tố lừa đảo trực tiếp vào kiến trúc của mạng lưới để thiết kế các mô hình tương tác phức tạp phản ánh chặt chẽ các tình huống thực tế. Những đóng góp này đại diện cho một nỗ lực phối hợp để nâng cao hiệu quả của honeypot vượt ra ngoài các chiến thuật đánh lạc hướng đơn giản. Bằng cách đưa sự lừa dối vào chính cấu trúc của thiết kế mạng, các nhà nghiên cứu đã mở đường cho một cách tiếp cận toàn diện và chiến lược hơn đối với an ninh mạng. Những tiến bộ này đảm bảo rằng sự lừa dối các kỹ thuật phù hợp với chiến thuật tấn công đang phát triển, củng cố các tổ chức trước bối cảnh đe dọa ngày càng phức tạp.

• Các mô hình tương tác tiên tiến và các khía cạnh tâm lý như thành kiến nhận thức đã truyền cảm hứng cho các phương pháp tiếp cận mới đối với thiết kế bẫy mật: Các nhà nghiên cứu an ninh mạng đã đi sâu vào lĩnh vực tương tác tiên tiến các mô hình, khai thác hiểu biết từ tâm lý học nhận thức để tinh chỉnh thiết kế honey-pot. Các mô hình này tận dụng các hiện tượng tâm lý, chẳng hạn như như những thành kiến nhận thức, để tạo ra những cam kết cộng hưởng với quá trình ra quyết định của kẻ tấn công. Bằng cách khai thác những thành kiến này, an ninh mạng các chuyên gia thiết kế các tương tác honeypot phản ánh các tình huống thực tế, kéo dài thời gian giao tranh của kẻ tấn công và tăng khả năng trích xuất dữ liệu có giá trị. Cách tiếp cận này phù hợp với xu hướng rộng hơn của an ninh mạng lấy con người làm trung tâm, nhận ra rằng việc hiểu được tâm lý của kẻ tấn công đóng vai trò quan trọng trong việc định hình các chiến lược phòng thủ hiệu quả (Faveri, 2022).

• Áp dụng các nguyên tắc của lý thuyết trò chơi vào honeypots sẽ tối ưu hóa sự lừa dối và tương tác, phản ánh bản chất đang phát triển của sự lừa dối trên mạng kỹ thuật: Các nguyên tắc của lý thuyết trò chơi, nổi tiếng vì ứng dụng của chúng trong ra quyết định chiến lược, tìm sự phù hợp tự nhiên trong honeypot. Bằng cách áp dụng những nguyên tắc này, các chuyên gia an ninh mạng cân bằng chiến lược các yếu tố lừa dối và tương tác trong các tương tác honeypot. Điều này sự cân bằng tinh tế đảm bảo rằng honeypot có khả năng thích ứng và phản ứng để phát triển các chiến lược tấn công. Khi những kẻ tấn công thay đổi cách tiếp cận của họ, các nguyên tắc lý thuyết trò chơi hướng dẫn việc điều chỉnh các chiến thuật bẫy mật, tối ưu hóa sự lừa dối và động lực tương tác. Cách tiếp cận năng động này phản ánh bản chất đang phát triển của các kỹ thuật lừa đảo trên mạng, nơi thích ứng khả năng là chìa khóa để luôn đi trước kẻ tấn công (Zhu et al., 2021; Pawlick et al. và cộng sự, 2021).

• Các phương pháp cải tiến này nâng cao độ chính xác phát hiện mối đe dọa, cải thiện hồ sơ kẻ tấn công và tối ưu hóa các chiến lược ứng phó sự cố trong an ninh mạng: Việc tích hợp các kỹ thuật sáng tạo này sẽ làm thay đổi toàn bộ bối cảnh an ninh mạng, mang lại nhiều lợi ích đa dạng. Đầu tiên, sự tham gia cao hơn từ các kỹ thuật tiên tiến chuyển thành nhiều hơn phát hiện mối đe dọa chính xác. Các tương tác mở rộng cho phép bảo vệ để thu thập một tập dữ liệu toàn diện hơn để phân tích, dẫn đến cải thiện hồ sơ kẻ tấn công. Hồ sơ này, đến lượt nó, tinh chỉnh sự cố chiến lược ứng phó bằng cách cung cấp hiểu biết sâu sắc hơn về kẻ tấn công động lực, chiến lược và mục tiêu tiềm năng. Cách tiếp cận tích hợp này đảm bảo các biện pháp an ninh mạng được dựa trên kẻ tấn công trong thế giới thực hành vi, dẫn đến các chiến lược phòng thủ hiệu quả và có mục tiêu hơn (Althonayan và Andronache, 2019).

• Sự phối hợp giữa nghiên cứu lừa dối và thực hiện các kỹ thuật tiên tiến tăng cường hiệu quả của honeypot, củng cố các tổ chức chống lại các mối đe dọa mạng đang phát triển: Sự phối hợp giữa Nghiên cứu học thuật về sự lừa dối và ứng dụng thực tế của các kỹ thuật tiên tiến cung cấp một cơ chế phòng thủ toàn diện và năng động. Sự hợp tác này trang bị cho các tổ chức các honeypot có thể thích ứng với các mối đe dọa mới nổi và được thiết kế chiến lược để đánh lừa và ngăn chặn kẻ thù. Khi bối cảnh mối đe dọa liên tục phát triển, điều này được củng cố cách tiếp cận đảm bảo khả năng phòng thủ kiên cường, bảo vệ các tổ chức chống lại các chiến thuật thay đổi liên tục của các đối thủ mạng. Sự hợp tác này đại diện cho tuyến đầu phòng thủ, khai thác những hiểu biết nghiên cứu tốt nhất và đổi mới thực tế để tạo ra thế trận an ninh thông minh và có tính dự đoán.

5. Một mô hình toán học chung để phân tích honeynet

Một mạng lưới mật ong là một mạng lưới lừa đảo của mồi nhử đặt một số honeypots ở các vị trí mạng khác nhau để tận dụng lợi thế của sự hợp tác giữa những honeypot này. Cộng đồng honeypot này là hiệu quả hơn so với việc sử dụng một mồi nhử duy nhất trong một mạng lưới. Điều đáng chú ý là rằng các honeypot trong honeynet không phải lúc nào cũng ở trạng thái vật lý khác nhau máy móc. Honeypot ảo trên cùng một máy cũng có thể xây dựng mạng lưới mật ong. Vấn đề là kẻ thù nghĩ rằng chúng là những hệ thống khác nhau.

Ngoài việc làm cho các honeypot đơn lẻ trở nên mạnh mẽ trong việc đánh lừa kẻ thù, mạng lưới honeypot (tức là honeynet) cũng phải có hiệu quả. để đạt được mục tiêu lừa dối. Ví dụ, số lượng các hon-eypot đơn lẻ trong một mạng lưới mật ong và vị trí của chúng ảnh hưởng đáng kể đến tổng số sức mạnh lừa dối.

Hầu hết các nghiên cứu trong lĩnh vực này sử dụng các mô hình trò chơi để trình bày một honeynet trong đó người bảo vệ mạng và kẻ thù là chính người chơi. Trước khi trình bày các kỹ thuật lừa dối trong phần này, chúng tôi đề xuất một đại diện chung của honeynets, có thể phù hợp với các tác phẩm hiện tại trong lĩnh vực này. Tất cả các mô hình trò chơi được đề cập trong phần này có thể so sánh với cách biểu diễn mới này. Các ký hiệu được sử dụng trong biểu diễn này được tóm tắt trong Bảng 4. Một honeynet, , có thể là được viết là = { , , , }, trong đó là đặc điểm mạng, là chi tiết về chiến lược của người chơi, là tập hợp các chi phí mà người chơi có thể trả và là tập hợp các lợi ích mà người chơi có thể nhận được.

có thể được viết là = {*h*, , , }, trong đó *h*, , của là số honeypot, số lượng máy chủ thực sự dễ bị tấn công mạng các cuộc tấn công và số lượng máy chủ an toàn khác trong mạng. là danh sách các bằng cấp của máy chủ, trong đó *h* bằng cấp chủ nhà và là giá trị mức độ tối đa trong số tất cả các máy chủ. Số lượng liên kết kết nối với máy chủ được coi là cấp độ của máy chủ đó. , ,

Chúng ta có = { , *h*, ,*h*}, trong đó *h*, là , số lượng tối đa các nỗ lực tấn công mà đối thủ có thể thực hiện và *h* là số lượng kết nối được chấp nhận của đối thủ tới máy chủ chính và là tỷ lệ eypots. *h* là dịch vụ của honeypot và máy chủ thực.

tỷ lệ tấn công của đối thủ và các ký hiệu có dấu ngoặc kép là hệ số giảm của biểu tượng đó sau khi áp dụng chiến lược tối ưu. Đối với

Bảng 4

Danh sách các ký hiệu được sử dụng để biểu diễn mạng honeynet.

Ký hiệu	Sự miêu tả
	Mạng lưới mật ong
	Đặc điểm mạng
h	Số lượng honeypot
	Số lượng máy chủ thực tế dễ bị tấn công
	Số lượng máy chủ thực sự an toàn
	Danh sách các bằng cấp của máy chủ
	Mức độ của các máy chủ h
	Mức độ máy chủ tối đa
	Chiến lược của người chơi
	Số lượng tối đa các nỗ lực tấn công của đối thủ
h	Số lượng kết nối có thể chấp nhận được của đối thủ tới honeypot
h	Tỷ lệ dịch vụ honeypots
	tỷ lệ dịch vụ lưu trữ thực tế
	Tỷ lệ tấn công của đối thủ
$'$	Yếu tố giảm của tỷ lệ dịch vụ honeypots
h $'$	Yếu tố giảm của tỷ lệ dịch vụ máy chủ thực tế
$'$	Yếu tố giảm tốc độ tấn công của đối thủ
h	Số lượng honeypot tối ưu trong chiến lược tốt nhất của người phòng thủ
	Bộ chi phí của người chơi
h	Chi phí của đối thủ khi thăm dò một honeypot
	Chi phí của đối thủ khi thăm dò một máy chủ thực sự
h	Chi phí của đối thủ khi tấn công honeypot
	Chi phí của đối thủ khi tấn công một máy chủ thực sự
h	Chi phí của bên phòng thủ khi đối thủ thăm dò một honeypot
$'$	Chi phí của bên phòng thủ khi đối thủ thăm dò một máy chủ thực sự
h $'$	Chi phí của bên phòng thủ khi đối thủ tấn công honeypot
	Chi phí của bên phòng thủ khi đối thủ tấn công một máy chủ thực sự
	Chi phí của đối thủ khi bị bẫy mật ong bắt được
	Chi phí triển khai honeypot của bên bảo vệ
	chi phí của bên phòng thủ khi phải đáp trả những nỗ lực của đối thủ
	Chi phí tối đa có thể chấp nhận được của đối thủ
	Bộ lợi ích của người chơi
h	Lợi ích của kẻ thù khi tấn công thành công vào honeypot
	Lợi ích của kẻ thù khi tấn công thành công một máy chủ thực sự

Ví dụ, giả sử rằng tỷ lệ dịch vụ của honeypot là 100% và trong chiến lược tối ưu mà honeypot phải có tỷ lệ dịch vụ là 50%, re-là 0,5 (tức là giá trị yếu tố giảm của của là 0,5). h là tối ưu h số lượng honeypot cần thiết trong chiến lược tốt nhất của bên phòng thủ.

Tập hợp chi phí cho mỗi hoạt động có thể được viết là $= \{ h$, và lần lượt là $,$ $h, , h, , h, , , , , \}$, Ở đâu h chi phí của đối thủ khi thăm dò một honeypot và một máy chủ thực. h và chi phí của đối thủ khi tấn công một honeypot và một thực tế máy chủ, tương ứng. Các biểu tượng có dấu ngoặc kép có cùng chi phí cho người bảo vệ. là chi phí của đối thủ khi bị bắt bởi honeypot, là chi phí của bên phòng thủ khi triển khai một honeypot trong mạng và là chi phí của bên phòng thủ khi phản ứng lại các nỗ lực của đối thủ. Cuối cùng, là chi phí tấn công tối đa có thể chấp nhận được đối với kẻ thù.

Đối với tập hợp lợi ích, chúng ta có $= \{ \}$, trong đó và là lợi ích của đối h thủ khi tấn công thành công vào honeypot và một máy chủ thực sự, tương ứng. Điều đáng chú ý là một số đối thủ có thể thỏa hiệp các honeypot để kiểm soát chúng, và điều này được coi là tấn công thành công vào honeypot.

Sau đây, chúng tôi trình bày các kỹ thuật lừa dối được sử dụng để cải thiện hiệu suất của honeynet. Chúng tôi cũng đề cập đến các chiến lược được đề xuất trong mỗi nghiên cứu được thể hiện bằng mô hình của chúng tôi, . Chúng tôi cũng đã mô phỏng các tác phẩm có thể so sánh được để phân tích hiệu suất của chúng. Tóm tắt các nghiên cứu liên quan trong lĩnh vực này được trình bày trong Bảng 5 (lưu ý rằng một số tên cho các mô hình nghiên cứu được chỉ định bởi chính chúng ta).

5.1. Tối ưu hóa honeypot

Một trong những thông số mạng quan trọng nhất trong honeynet là số lượng honeypot đã triển khai. Đặt một vài honeypot trong mạng không đủ để thu hút kẻ thù và bảo vệ toàn bộ mạng lưới. Mặt khác, sử dụng quá nhiều honeypot trong mạng sẽ tốn kém, và trong một số trường hợp, nó có thể cảnh báo đối thủ về sự lừa dối cơ chế mà nó đang phải đối mặt. Do đó, việc tìm ra số lượng tối ưu honeypot cho mạng lưới là cần thiết.

Một trong những nghiên cứu đầu tiên trong việc tối ưu hóa số lượng honeypot được thực hiện bởi Rowe et al. (2007). Nghiên cứu này đề xuất một mô hình toán học để tính toán chi phí và lợi ích của đối thủ trong việc tấn công một mạng lưới mật ong. Nếu đối thủ chi nhiều hơn ngưỡng chi phí cho một hệ thống, nó sẽ bỏ qua hệ thống đó và cố gắng tấn công hệ thống khác. Vì mô hình này xem xét khả năng chịu đựng của đối thủ, chúng tôi gọi nó là TBM (viết tắt của Mô hình dựa trên dung sai). Sử dụng mô hình này, người bảo vệ mạng có thể thiết lập số lượng honeypot thích hợp để tăng chi phí tấn công hơn chi phí dự kiến của đối thủ. Giới hạn trên của chi phí tấn công được chấp nhận của một hệ thống duy nhất đối với đối thủ ( ) có thể được tính toán theo Phương trình (1).

$$= \frac{(+)((h + +) \quad h(+ h))}{(h + + + hh)} \tag{1}$$

Theo Phương trình (1), chúng ta có thể kết luận rằng số lượng tối ưu của honeypots (h) có thể được tính bằng Phương trình (2).

$$h = \frac{(+)(\quad + \quad)}{(h + 1) + h(+)} \tag{2}$$

Mặc dù mô hình trước đó có thể được sử dụng để tìm ra số lượng honeypot, người bảo vệ mạng phải có thông tin về chi phí và lợi ích được đối thủ nhận thức. Do đó, một mô hình khác được đề xuất bởi Crouse (2012) để tìm số lượng honeypot tối ưu không có các thông số nhận thức của đối thủ. Một mạng lưới mật ong được mô hình hóa như một URN chứa ba loại hạt có màu sắc khác nhau. Chúng tôi gọi mô hình này là URN. Các honeypot h , các máy chủ dễ bị tấn công và các thành phần mạng khác được hiển thị lần lượt là màu đỏ, xanh lá cây và xanh lam. Một hạt được lấy ra khỏi URN khi đối thủ tấn công một máy chủ. Trong mô hình này, kẻ thù cố gắng tấn công máy chủ, dẫn đến việc loại bỏ các hạt. Mô hình này giả định rằng đối thủ thành công nếu nó có thể khởi động một cuộc tấn công vào ít nhất một trong những máy chủ dễ bị tổn thương. Do đó, trong mô hình URN, kẻ thù đạt được mục tiêu nếu ít nhất một trong những hạt từ các hạt bị loại bỏ có màu xanh lá cây. Chúng tôi có thể tính toán xác suất của một cuộc tấn công thành công bằng giả định này Phương trình (3).

$$(\text{tấn công thành công}) = \sum_{=1}^{1} \frac{( )(\quad)}{(h + +)} \tag{3}$$

Người bảo vệ mạng có thể tính toán số lượng honeypot cần thiết Phương trình (3), xem xét các tình huống mạng để định lượng ngưỡng cho tỷ lệ tấn công thành công của đối thủ. Một ngưỡng đơn giản là thiết lập xác suất thành công tối đa là 0,5. Trong tình huống này, số của các cuộc tấn công thất bại vượt quá các cuộc tấn công thành công. Do đó, kẻ thù có thể tránh tấn công mạng.

Một số đối thủ sử dụng các chiến lược tấn công thông minh trong đó việc kết nối với một vài honeypot không thể tiết lộ danh tính của chúng. Do đó, chúng chấp nhận giao tiếp với một số lượng cụ thể các honeypot hướng tới đạt được mục tiêu của họ. Do đó, Crouse et al. (2015) đã đề xuất một mô hình URN tương tự cũng xem xét số lượng kết nối có thể chấp nhận được đến honeypots (h). Chúng tôi gọi mô hình này là URNt (viết tắt của URN với ngưỡng). Trong những điều kiện như vậy, khả năng tấn công thành công có thể được tính như Phương trình (4).

$$(\text{tấn công thành công}) = \sum_{=0}^{h} \sum_{=1}^{1} \frac{( )(h) \quad (+))}{((h + +)} \tag{4}$$

Do đó, người bảo vệ mạng có thể đưa ra quyết định tốt nhất để lựa chọn phương pháp lừa dối thích hợp bằng cách thay đổi giá trị của các biến trong Phương trình (4) và kiểm tra xác suất của đối thủ chiến thắng.

Các mô hình URN trước đây không xem xét quá trình thăm dò kẻ thù thực hiện trước khi tung ra các cuộc tấn công. Do đó, Fraun-holz và Schotten (2018b) đã đề xuất một mô hình trò chơi cũng mô phỏng

Bảng 5

So sánh các nghiên cứu trong lĩnh vực lừa đảo trong mạng lưới mật ong.

Nghiên cứu	Mục đích	Đặc điểm chính	Chiến lược tối ưu cho người phòng thủ	Kiểu mẫu
TBM (Rowe và cộng sự, 2007)	Tối ưu hóa	Xem xét sự khoan dung của đối thủ	Tính toán chi phí dự kiến tối đa cho đối thủ và cố gắng làm cho chi phí tấn công cao hơn chi phí đó. Đặt số lượng honeypot theo Phương trình (2).	Mô hình toán học
URN (Crouse, 2012)	Tối ưu hóa	Xem xét các máy chủ an toàn trong mô hình	Tính toán xác suất tấn công thành công và cố gắng giảm xác suất đó xuống. Đặt số lượng honeypot theo Phương trình (3).	Mô hình toán học
URNt (Crouse và cộng sự, 2015)	Tối ưu hóa	Xem xét các máy chủ an toàn và ngưỡng để kết nối với honeypot	Tính toán xác suất tấn công thành công và cố gắng giảm xác suất đó xuống. Đặt số lượng honeypot theo Phương trình (4).	Mô hình toán học
GBO (Fraunholz và Schotten, 2018b)	Tối ưu hóa	Xem xét số lượng thăm dò trước khi tấn công	Tạo ra tình huống mà đối thủ không muốn tấn công. Tính số lượng honeypot theo Phương trình (5).	Trò chơi chung dành cho hai người chơi
HSGp (Píbil và cộng sự, 2012)	Đa dạng hóa	Chỉ định cho mỗi máy chủ một giá trị quan trọng về số	Lập mô hình mạng với trò chơi được gợi ý và tìm chiến lược tối ưu bằng cách sử dụng cân bằng Nash.	Trò chơi tổng bằng không
HSG (Kiekintveld và cộng sự, 2015)	Đa dạng hóa	Sử dụng biểu đồ tấn công mạng để tìm giá trị quan trọng của máy chủ	Lập mô hình mạng với trò chơi được gợi ý và tìm chiến lược tối ưu bằng cách sử dụng cân bằng Nash.	Trò chơi tổng bằng không
DHG (Durkota và cộng sự, 2015a)	Đa dạng hóa	Chỉ định các giá trị quan trọng hạn chế cho các máy chủ	Tìm chiến lược tối ưu của đối thủ và cố gắng khiến nó không thể đạt được bằng cân bằng Stackelberg.	Trò chơi chung dành cho hai người chơi
DHGu (Durkota và cộng sự, 2015b)	Đa dạng hóa	Giả sử rằng đối thủ không biết các loại honeypot để thực tế hơn	Tính toán giới hạn trên cho chi phí của đối thủ và giải quyết trò chơi một cách gần đúng bằng cách sử dụng cân bằng Stackelberg.	Trò chơi tổng hợp
DHD (Sarr và cộng sự, 2020)	Đa dạng hóa	Xem xét các kỹ thuật phát hiện honeypot	Đa dạng hóa mạng lưới để giảm khả năng phát hiện bẫy mật khi phát hiện ra một trong số chúng. Sử dụng phương pháp xấp	Trò chơi tổng bằng không
POSG (Anwar và cộng sự, 2019)	Định vị	Xem xét mức độ an toàn của biểu đồ tấn công chưa biết đối với người bảo vệ	xỉ hoặc thuật toán POMDP để giải quyết trò chơi và tìm ra chiến lược tối ưu.	Trò chơi tổng bằng không
POSGm (Anwar và cộng sự, 2020)	Định vị	Cho phép người bảo vệ đặt nhiều honeypot trên biểu đồ tấn công	Kiểm tra tất cả các chiến lược và tìm ra chiến lược tối ưu theo hàm phần thưởng bằng thuật toán tiến bộ. Nói dối càng nhiều	Trò chơi tổng bằng không
DD (Cài và cộng sự, 2009)	Động lực hóa	Giả sử các honeypot nằm liền kề nhau	càng tốt	Trò chơi chung dành cho hai người chơi
SGM (Carroll và Tổng, 2011)	Động lực hóa	Xem xét các cuộc tấn công có và không có thăm dò	Trong các điều kiện được đề cập trong Phương trình (6) đến Phương trình (8), hiển thị máy chủ được thăm dò như một máy chủ thực sự và nếu không, hiển thị nó như một honeypot	Trò chơi báo hiệu
SGMd (Çeker và cộng sự, 2016)	Động lực hóa	Tập trung vào các cuộc tấn công từ chối dịch vụ Làm cho	các máy chủ thực sự nói sự thật trong các điều kiện được đề cập trong Phương trình (9) đến Phương trình (14). Làm cho các honeypot nói sự thật trong các điều kiện được đề cập trong Phương trình (11) đến Phương trình (16). Trong các tình huống khác, hãy nói dối.	Trò chơi báo hiệu
HDG (Garg và Grosu, 2007)	Động lực hóa	Xem xét nhiều cuộc thăm dò cho đối thủ	Trả lời sao cho khả năng nhận được sự thật và lời nói dối là như nhau.	Trò chơi dạng mở rộng
CSG (Pawlick và Zhu, 2015)	Động lực hóa	Xem xét bằng chứng thu thập được của đối phương	Tìm chiến lược tối ưu bằng cân bằng Bayesian Nash hoàn hảo Ở trạng thái	Trò chơi báo hiệu
SGE (Pawlick và cộng sự, 2018)	Động lực hóa	Xem xét bằng chứng thu thập được của đối phương dựa trên hoạt động của chủ nhà	trội, làm cho tất cả các host thực và honeypot có vẻ giống nhau. Ở trạng thái nặng, làm cho tất cả các honeypot có vẻ giống như các host thực. Ở trạng thái giữa, làm cho một nửa số honeypot hoạt động như các host thực và chỉ một số ít host thực hoạt động như honeypot.	Trò chơi báo hiệu
eHDG (Bilinski và cộng sự, 2018)	Động lực hóa	Giả sử rằng cả đối thủ và người dùng hợp pháp đều có thể thăm dò mạng để trở nên thực tế hơn	Nói dối là điều cần thiết đối với người bảo vệ.	Trò chơi chung dành cho hai người chơi
BRL (Limouchi và Mahgoub, 2021)	Động lực hóa	Sử dụng máy học dựa trên các hàng xóm độc hại để tìm ra chiến lược tối ưu	Hoạt động như một honeypot khi phát hiện có hơn hai hàng xóm độc hại	Học tăng cường
IoTCandyJar (Luo và cộng sự, 2017)	Động lực hóa	Sử dụng máy học để tạo ra honeypot tương tác thông minh	Chiến lược tối ưu được tìm thấy dựa trên mô hình đã được đào tạo	Học máy
MDRL (Huang và Zhu, 2019)	Động lực hóa	Sử dụng máy học để tìm ra chiến lược tối ưu, đặc biệt là để lựa chọn hoạt động như một honeypot tương tác thấp hoặc cao	Chiến lược tối ưu được tìm thấy dựa trên mô hình đã được đào tạo	Học tăng cường
DTG (Ren và Zhang, 2020)	Tạo hình	Chỉ định các nhiệm vụ khác nhau cho các nút có đặc điểm cấu trúc khác nhau	Sử dụng số mũ cao hơn cho mạng không có tỷ lệ.	Trò chơi vi phân
VTG (Ren và cộng sự, 2021)	Tạo hình	Xem xét các cấu trúc mạng khác nhau	Giữ mức độ của vật chủ lớn nhất ở mức thấp.	Mô hình toán học

quá trình thăm dò và nó được giải quyết dựa trên cuộc thi Stackelberg, trong đó đối thủ và bên phòng thủ cố gắng sử dụng chiến lược tốt nhất sau chiến lược của người chơi trước. Vì mô hình này sử dụng các khái niệm lý thuyết trò chơi để tối ưu hóa số lượng honeypot, chúng tôi gọi nó là GBO (viết tắt của Game-Base Optimizer). Mô hình trò chơi này cố gắng tìm số lượng honeypot tối ưu cần triển khai trong mạng.

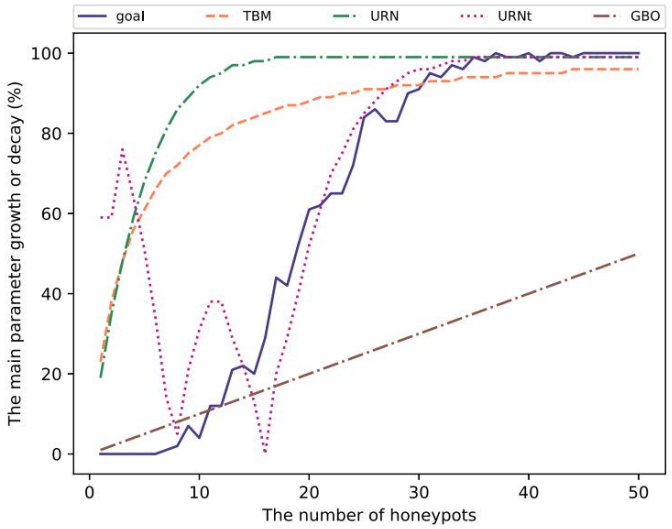
Hai kịch bản được định nghĩa trong mô hình này. Trong kịch bản đầu tiên, kẻ thù không thăm dò các máy chủ trước khi tấn công chúng. Do đó, mô hình đề xuất thiết lập số lượng honeypot sao cho phần thưởng tấn công bằng với phần thưởng không tấn công. Trong tình huống này, đối thủ buộc phải không tấn công máy chủ. Theo điều kiện này, số lượng honeypot tối thiểu (h) có thể được tính theo Phương trình (5).

$$h = \frac{\times}{\quad} \tag{5}$$

Trong kịch bản thứ hai, quá trình thăm dò cũng được xem xét. Một phương trình tuyến tính được trình bày để tìm ra phần thưởng của mỗi chiến lược, và sau đó, một thuật toán tìm kiếm được đề xuất để tìm ra chiến lược tốt nhất.

Thuật toán 1 Quá trình tấn công của đối thủ trong các mô phỏng để so sánh các nghiên cứu đư ợc tiến hành nhằm tối ư u hóa các bẫy mật.

```
h                danh sách các nút honeypot
h    danh sách các nút máy chủ thực
     h          + h
          danh sách trống
 h   danh sách trống
     0
        _    = 20 × h   _     + 4 × h        _
trong khi True làm
    nếu size( ) = 20 thì
        ghi lại một cuộc tấn công thành công
        phá vỡ
    nếu size( h ) = size( log một cuộc            ) sau đó
        tấn công không thành công
        phá vỡ
    ~          >            _       sau đó
        ghi lại một cuộc tấn công không thành công
        phá vỡ
           một nút ngẫu nhiên từ                  h
    thêm       đến h
    nếu        h            sau đó
                    + h        _
    khác
                + h          _
        thêm vào       ĐẾN
```



Hình 11. So sánh các nghiên cứu về tối ư u hóa số lư ợng honeypot.

Để so sánh hiệu suất của các nghiên cứu đư ợc đề cập trong này phần (tức là TBM, URN, URNt và GBO), chúng tôi đã mô phỏng một số ngẫu nhiên mạng lư ới với các đặc điểm khác nhau trong Python và áp dụng tối ư u số liệu đư ợc đề xuất bởi mỗi mô hình. Mỗi mạng có tổng số 100 nút và số lư ợng honeypot thay đổi từ 0 đến 50 trong mỗi nút kịch bản. Kẻ thù thăm dò mạng và nhấm mục tiêu thỏa hiệp tại ít nhất 20 máy chủ thực trong mạng. Kết nối với hơn 4 honey-pot dẫn đến thất bại của đối thủ. Kịch bản tấn công của đối thủ chi tiết đư ợc trình bày trong Thuật toán 1.

Kết quả đư ợc thể hiện trong Hình 11. Những thay đổi về số lư ợng các cuộc tấn công thành công, đư ợc biểu thị bằng "thành công", và những thay đổi về bốn số liệu của mô hình đư ợc thể hiện trong hình này. Sự tăng trư ởng và suy giảm của các số liệu so sánh với số liệu thành công của đối thủ giải thích rằng sử dụng Phư ơng trình (4), đư ợc trình bày bởi mô hình URNt, có thể có đư ợc kết quả tốt hơn hơn ba mô hình khác trong các kịch bản của chúng tôi. Có vẻ như Phư ơng trình (4) đạt đư ợc kết quả tốt hơn vì sử dụng các số liệu quan trọng nhất, đặc biệt là số lư ợng kết nối tối đa có thể chấp nhận đư ợc tới honeypot (tức là h).

5.2. Đa dạng hóa các honeypot

Loại honeypot nằm trong mạng là một tham số chính khác ảnh hư ởng đến hiệu suất honeynet. Có nhiều loại khác nhau của honeypots với nhiều khả năng khác nhau. Do đó, mạng lư ới bảo vệ phải đặt các loại phù hợp theo chi phí triển khai của chúng. Hơn nữa, sự đa dạng này giúp ngư ời bảo vệ ngăn chặn nhiều phát hiện honeypot hơn tấn công. Trên thực tế, nếu đối thủ tìm ra cách phát hiện ra một honeypot loại , các loại honeypot khác có thể đư ợc phát hiện tư ơng tự. Như ng nếu các honeypot có các loại khác nhau, việc phát hiện một trong các honeypot có thể không dẫn đến việc phát hiện tất cả chúng một cách đơn giản.

Píbil et al. (2012) đã đề xuất một mô hình trò chơi tổng bằng không, đư ợc gọi là HSG (viết tắt của Honeypot Selection Game) cho một mạng lư ới mật ong với các loại khác nhau của honeypots. Trò chơi này gán một giá trị số cho mỗi máy chủ thực và honeypot, cho thấy tầm quan trọng của nó trong mạng. Ví dụ, máy chủ cơ sở dữ liệu là một trong những tài sản quan trọng trong mạng và nó là có khả năng là mục tiêu của kẻ thù. Các giá trị quan trọng cho honeypots là giả mạo vì chúng giả vờ quan trọng đến vậy. Trong HSG, Ngư ời bảo vệ mạng và kẻ thù là những ngư ời chơi trò chơi. kẻ thù có mục đích tấn công một máy chủ thực sự. Đồng thời, ngư ời phòng thủ triển khai tối ư u một số lư ợng honeypot cố định với các loại khác nhau (các giá trị quan trọng khác nhau) để tăng khả năng tấn công honey-pot. Trong HSG, đối thủ không thể thăm dò máy chủ trư ớc khi tấn công chúng. Do đó, một mô hình khác gọi là HSGp đư ợc đề xuất trong cùng một nghiên cứu để hỗ trợ quá trình thăm dò. Trong HSGp, nguồn lực của đối thủ bị hạn chế và chỉ có thể thăm dò một số lư ợng cụ thể của máy chủ. Thông tin thu đư ợc từ các đầu dò này không phải lúc nào cũng hợp lệ. Nghiên cứu này gợi ý tìm ra chiến lư ợc tối ư u cho ngư ời phòng thủ bằng cách Khái niệm cân bằng Nash (Kreps, 1989).

Vì tầm quan trọng của máy chủ mạng không chỉ đơn thuần là một con số, Kiekintveld et al. (2015) đã sử dụng mô hình HSG với các giá trị quan trọng đư ợc tính toán từ biểu đồ tấn công mạng. Biểu đồ tấn công có thể chỉ định lỗ hổng lư u trữ và trình bày các đư ờng tấn công có khả năng xảy ra nhất có thể gán một giá trị quan trọng cho mỗi máy chủ.

Giá trị quan trọng của các máy chủ trong mạng đư ợc chọn từ một danh sách cụ thể. Do đó, chỉ những số cụ thể mới đư ợc phép gán cho honeypot. Do đó, Durkota et al. (2015a) đã đề xuất một mô hình trò chơi để trình bày một mạng lư ới mật ong với các loại hon-eypot khác nhau như ng hạn chế. Chúng tôi đặt tên cho mô hình này là DHG (viết tắt của Diversifying Honeynet) Trò chơi). Kẻ thù và ngư ời bảo vệ mạng là những ngư ời chơi của trò chơi này trò chơi. Ngư ời phòng thủ có thể đặt một số lư ợng cụ thể các honeypot trong mạng, như ng các loại của chúng là tùy chỉnh. Đối thủ không biết máy chủ là honeypot. Do đó, nó tạo ra biểu đồ tấn công của honeynet và phân tích nó để tìm ra con đư ờng tấn công tối ư u. Theo tối ư u chiến lư ợc của đối thủ, chiến lư ợc phòng thủ tốt nhất có thể đư ợc tính toán theo cân bằng Stackelberg. Trong trò chơi này, đối thủ phải trả một chi phí cụ thể khi tấn công một honeypot, và mặt khác, nó nhận đư ợc một phần thư ởng cho việc tấn công thành công một vật chủ thực sự.

Vì DHG cho rằng đối thủ biết các loại bẫy mật ong, nên một mô hình khác đư ợc Durkota và cộng sự (2015b) đề xuất cho một mô hình tư ơng tự kịch bản, như ng với giả định rằng đối thủ không biết về các loại bẫy mật ong. Chúng tôi gọi mô hình này là DHGu (viết tắt của DHG với đối thủ). Mô hình này trình bày một mạng lư ới các loại honeypot khác nhau với một trò chơi tổng hợp. Ngư ời phòng thủ và đối thủ là hai ngư ời chơi của trò chơi này. Ngư ời bảo vệ mạng thực hiện động thái đầu tiên để đặt các loại honeypot khác nhau vào mạng một cách tối ư u. Triển khai những honeypot này có thể có chi phí khác nhau và mang lại mức độ bảo mật khác nhau cấp độ. Kẻ thù biết số lư ợng honeypot, như ng không có bất kỳ thông tin nào về loại và vị trí của chúng. Tuy nhiên, nó chọn một máy chủ để thỏa hiệp bằng cách tính toán xác suất truy cập một honeypot và chi phí cho cuộc tấn công thành công của nó. Nghiên cứu này đề xuất các giải pháp gần đúng để tìm ra chiến lư ợc tốt nhất cho mỗi ngư ời chơi và cũng trình bày một phư ơng trình tuyến tính để tính toán giới hạn trên của tiện ích chức năng trong trò chơi này.

Để phân tích các cuộc tấn công phát hiện honeypot, Sarr et al. (2020) đã đề xuất một mô hình trò chơi tổng bằng không, trong đó bên phòng thủ cố gắng giảm

cơ hội thành công của các cuộc tấn công phát hiện honeypot bằng cách tăng chi phí phát hiện tất cả các loại honeypot. Chúng tôi gọi mô hình này là DHD (viết tắt để Đa dạng hóa nhằm giảm thiểu Phát hiện Honeypot). Ngư ời bảo vệ phải đặt một số lư ợng cụ thể các honeypot trong mạng. Tuy nhiên, đư ợc phép chọn các loại honeypot tùy chỉnh. Ngư ời bảo vệ trả một số tiền cụ thể chi phí triển khai từng loại honeypot. Mặt khác, đối thủ nhận đư ợc phần thư ởng bằng cách phát hiện ra honeypot, như ng phải trả cùng một khoản chi phí triển khai của một loại honeypot như chi phí phát hiện. Ví dụ, nếu ngư ời bảo vệ sử dụng hai loại honeypot, tư ơng tác thấp và tư ơng tác cao, chi phí triển khai của loại thứ nhất và thứ hai là $_1$ Và 2, tư ơng ứng, và phát hiện cũng phải trả 1 và $_2$ để detect loại thứ nhất và loại thứ hai, tư ơng ứng. Điểm trong trò chơi này là nếu đối thủ trả 1 để phát hiện ra một honeypot loại thứ hai, anh ta sẽ không thành công. Nghiên cứu này đề xuất không triển khai cùng một loại honeypot và đa dạng hóa chúng một cách ngẫu nhiên trong mạng lư ới để giảm khả năng bị phát hiện bởi honeypot.

5.3. Xác định vị trí các honeypot

Ngoài số lư ợng honeypot, vị trí của chúng cũng rất quan trọng trong việc lừa dối đối thủ và lãng phí thời gian. Hai mạng lư ới mật ong với cùng một số lư ợng honeypot có thể có hiệu suất phòng thủ khác nhau theo chiến lư ợc bố trí đư ợc triển khai để định vị honeypots. Biểu đồ tấn công của một mạng có thể đư ợc sử dụng để tìm vị trí thích hợp cho các honeypot. Biểu đồ tấn công là một biểu đồ có hư ớng đồ thị biểu diễn trạng thái bắt đầu và kết thúc của các trạng thái khác nhau xâm nhập vào mạng. Các cạnh trong biểu đồ này hiển thị quá trình khai thác các lỗ hổng. Ví dụ, nếu đối thủ có thể để xâm phạm máy chủ $h1$ chỉ sau khi xâm phạm máy chủ $h2$, trong cuộc tấn công đồ thị chúng ta có $h1$ và $h2$ là hai nút và có một cạnh từ $h2$ đến $h1$. Các honeypot phải đư ợc đặt giữa hai nút của đồ thị này đư ợc kết nối với một cạnh, theo cách đạt đến trạng thái cuối cùng (tức là, mục tiêu của kẻ thù) thông qua chúng là không tốn kém cho kẻ thù. Do đó, nó sẽ giao tiếp với các honeypot và sẽ bị lệch khỏi mục tiêu tấn công. Nói cách khác, chúng tôi cố gắng cho thấy mạng dễ bị tổn thư ơng hơn với các honeypot ở những vị trí thích hợp. Hơn nữa, đặt các honeypot ở đúng vị trí có thể giúp chúng ta theo dõi kẻ thù. Giao tiếp với honeypot cho thấy kẻ thù đã khai thác các nút tiên quyết để đạt tới nút hiện tại.

Anwar et al. (2019) đã mô hình hóa vấn đề đặt honeypot trong một mạng lư ới như một trò chơi ngẫu nhiên tổng bằng không giữa ngư ời phòng thủ và đối thủ. Mô hình trò chơi đư ợc gọi là POSG. Cả hai ngư ời chơi đều biết đồ thị tấn công trong POSG, tuy nhiên, đối thủ không biết nút mạng là một honeypot, và ngư ời bảo vệ không biết điều đó điểm yếu đã bị kẻ thù khai thác. Trong mỗi bư ớc, Ngư ời bảo vệ có thể chọn đặt một honeypot duy nhất trên một cạnh cụ thể của biểu đồ tấn công mạng hoặc không làm gì cả, và kẻ thù chọn một máy chủ để khai thác. Khai thác honeypot tốn kém cho kẻ thù và ngư ời bảo vệ nhận đư ợc phần thư ởng. Như ng nếu đối thủ thăm dò một máy chủ thực sự, nó nhận đư ợc phần thư ởng và ngư ời bảo vệ phải trả một chi phí cụ thể. Các nhà nghiên cứu POSG không đề cập đến một chiến lư ợc cụ thể cho ngư ời chơi và họ đề xuất sử dụng các phư ơng pháp gần đúng hoặc thuật toán POMDP, đư ợc sử dụng đối với các mô hình trò chơi tư ơng tự, để tìm ra chiến lư ợc tối ư u.

Vì ngư ời bảo vệ chỉ có thể đặt một honeypot duy nhất ở mỗi bư ớc của POSG, Anwar et al. (2020) đã đề xuất một mô hình trò chơi tổng bằng không khác dựa trên biểu đồ tấn công mạng, trong đó ngư ời bảo vệ có thể đặt nhiều honeypots như nó muốn trong mỗi bư ớc. Chúng tôi gọi mô hình này là POSGm (viết tắt của POSG với nhiều honeypot). Ngư ời bảo vệ phải trả một chi phí cụ thể để định vị từng honeypot trong mạng và nhận đư ợc một phần thư ởng nếu nó có thể theo dõi kẻ thù. Mặt khác, chi phí cho kẻ thù phải bị phát hiện và phần thư ởng là khai thác một máy chủ thực sự lỗ hổng. Trong mô hình trò chơi này, đầu tiên, một phư ơng trình tuyến tính đư ợc đề xuất để tính toán hàm phần thư ởng của ngư ời chơi, một thuật toán tiến bộ là đề xuất kiểm tra tất cả các trạng thái trò chơi có thể có trong các bư ớc tiếp theo và tìm ra chiến lư ợc tốt nhất.

5.4. Làm cho honeypot trở nên năng động

Một trong những kỹ thuật lừa dối có thể đư ợc sử dụng trong mạng lư ới mật ong là thay đổi hành vi của máy chủ thực sự hoặc honeypot và phản hồi lại đối thủ một cách năng động. Trong trư ờng hợp này, khi một đối thủ thăm dò một trong các máy chủ, ngư ời bảo vệ mạng quyết định có hiển thị máy chủ đó hay không một máy chủ thực sự hoặc như một honeypot. Kỹ thuật này làm tăng khả năng của đối thủ sự không chắc chắn về các loại máy chủ. Ví dụ, nếu đối thủ tìm thấy một máy chủ có nhiều cổng mở, cho thấy dấu hiệu của một honeypot, sẽ không chắc chắn về loại máy chủ đó. Máy chủ đó có thể thực sự một honeypot hoặc đó là một máy chủ thực sự giả vờ là một honeypot. Đối với điều này lý do, việc tạo ra honeynet động có thể dẫn đến hiệu suất lừa đảo cao hơn. Như ng, có một sự đánh đổi giữa mức độ lừa đảo thu đư ợc bằng cách nói dối và chi phí cấu hình một cơ chế liên quan. Do đó, điều này tính năng động phải đư ợc tạo ra với ranh giới thích hợp.

Cai et al. (2009) đã đề xuất một mô hình trò chơi hai ngư ời chơi, trong đó honeypots đư ợc đặt liền kề trong không gian địa chỉ của mạng. Ngư ời bảo vệ mạng và kẻ thù là những ngư ời chơi của trò chơi này. kẻ thù thăm dò các máy chủ mong muốn của nó. Nếu máy chủ đó là máy chủ thực sự, nó sẽ nhận đư ợc phản ứng bình thư ờng. Như ng nếu đối thủ thăm dò một honeypot, ngư ời phòng thủ quyết định nói dối hay nói thật về danh tính của honeypot đó. Số lư ợng lời nói dối trong mô hình này là có hạn. Do đó, ngư ời bảo vệ phải áp dụng chiến lư ợc thông minh để dụ kẻ thù. Kẻ thù cố gắng tìm ra khối honeypots có số lư ợng đầu dò thấp nhất có thể và ngư ời bảo vệ có mục đích tăng số lư ợng các đầu dò này. Nghiên cứu này đề xuất những ngư ời bảo vệ sử dụng một chiến lư ợc đư ợc gọi là Trì hoãn-Trì hoãn (DD), trong mà những kẻ lừa đảo luôn nói dối cho đến khi giới hạn của chúng bị vư ợt quá. Vì chiến lư ợc tối ư u trong mô hình này đư ợc gọi là DD, chúng tôi cũng đặt tên là mô hình như DD.

Các honeypot không phải lúc nào cũng nằm liền kề trong không gian địa chỉ quảng cáo. Chúng có thể nằm trong các địa chỉ ngẫu nhiên. Do đó, Carroll và Grosu (2011) đã đề xuất một mô hình khác dựa trên các trò chơi tín hiệu, trong mà mạng lư ới sử dụng các honeypot ở những nơi tùy chỉnh. Chúng tôi đặt tên mô hình này là SGM (viết tắt của Signaling Game Model). Ngư ời bảo vệ mạng và đối thủ là ngư ời gửi và ngư ời nhận trong SGM, tư ơng ứng. Một số lư ợng cụ thể các honeypot đư ợc đặt trong mạng, như ng ngư ời bảo vệ có thể trả lời các cuộc thăm dò của đối thủ bằng các phản ứng khác nhau. Nói cách khác, nếu máy chủ là honeypot và đối thủ thăm dò nó, ngư ời bảo vệ quyết định xem có nên phản ứng với nó như một ngư ời chủ thực sự hay như một honeypot. Ngư ời bảo vệ cố gắng che giấu danh tính của honeypot và khiến đối thủ tấn công họ. Mặt khác, đối thủ nhằm mục đích chọn một máy chủ thực sự để tấn công. Khi kẻ thù thăm dò một máy chủ, ngư ời bảo vệ có thể trả lời bằng 'h' hoặc 'r' để cho thấy máy chủ đư ợc thăm dò là một honeypot hoặc một hệ thống thực sự, tư ơng ứng. Trong tình huống này, đối thủ có ba lựa chọn: tấn công máy chủ đó, tấn công máy chủ sau khi thăm dò nó, hoặc kết thúc trò chơi mà không tấn công. SGM gợi ý rằng các chiến lư ợc tối ư u là luôn phản ứng bằng 'h' hoặc luôn phản ứng với 'r'. Nghiên cứu này cũng nêu rằng chiến lư ợc ngẫu nhiên hóa phản ứng tư ơng đư ơng với hai chiến lư ợc này. Trong bất kỳ điều kiện nào đư ợc đề cập trong Phư ơng trình (6), Phư ơng trình (7) và Phư ơng trình (8), phư ơng pháp tối ư u chiến lư ợc là luôn luôn trả lời bằng 'r'. Hơn nữa, chiến lư ợc tối ư u trong điều kiện khác là luôn trả lời bằng 'h'.

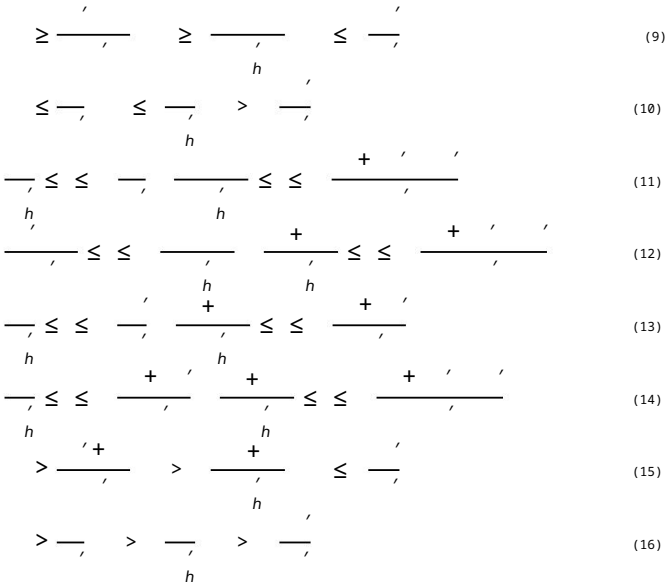
$$\frac{h}{h++} \le \frac{h}{+} \quad \frac{h}{h++} \le \frac{}{+} \tag{6}$$

$$\frac{h}{h++} \ge \frac{h}{+} \quad \frac{h}{h++} \le \frac{h}{} \tag{7}$$

$$\frac{h}{h++} \ge \frac{}{+} \quad \frac{h}{h++} \ge \frac{h}{} \tag{8}$$

Ç eker et al. (2016) đã đề xuất một mô hình trò chơi báo hiệu để trình bày một honeynet, gần giống với SGM. Tuy nhiên, mô hình này tập trung vào việc ngăn chặn các cuộc tấn công DoS trong honeynet. Ngư ời bảo vệ mạng là ngư ời gửi trong mô hình này và cố gắng cấu hình honeynet một cách tối ư u vẫn phục vụ ngư ời dùng hợp pháp trong một cuộc tấn công DoS. Vì mô hình này là giống như SGM và đư ợc sử dụng cho các cuộc tấn công DoS, chúng tôi đặt tên cho nó là SGMd (viết tắt của SGM trong các cuộc tấn công DoS). Kẻ thù là ngư ời chơi tiếp nhận và thực hiện

một trong những hành động này khi giao tiếp với máy chủ: tấn công máy chủ đó chủ nhà, quan sát hoặc kết thúc trò chơi mà không tấn công. Nghiên cứu này đề nghị những ngư ời chủ thực sự nói sự thật trong những điều kiện đã nêu trong Phư ơng trình (9) đến Phư ơng trình (14), và trong các điều kiện khác, nó là tối ư u để báo hiệu lời nói dối. Các honeypot cũng gợi ý nói dối trong các điều kiện đư ợc đề cập trong Phư ơng trình (11) đến Phư ơng trình (16), và sự thật trong các điều kiện khác.



Trong SGM và SGMd, kẻ thù chỉ có thể thăm dò một máy chủ duy nhất trong mỗi bư ớc, trong khi thực tế, kẻ thù có thể thăm dò nhiều máy chủ trư ớc quyết định tấn công một trong số chúng. Do đó, Garg và Grosu (2007) đã đề xuất một mô hình trò chơi khác, đư ợc gọi là HDG, để đại diện tốt hơn cho honeynet trong các tình huống nói dối. HDG là một trò chơi dạng mở rộng với mạng lư ới hậu vệ và đối thủ lần lư ợt là ngư ời chơi thứ nhất và thứ hai. Những ngư ời chơi trong HDG di chuyển xen kẽ cho đến khi đối thủ thăm dò số lư ợng máy chủ cụ thể. Ở bư ớc cuối cùng của trò chơi này, đối thủ quyết định tấn công một trong những máy chủ hay không. HDG đề xuất rằng ngư ời phòng thủ để phản ứng theo cách mà khả năng nhận đư ợc câu trả lời đúng hoặc sai phản ứng là như nhau.

Một số đối thủ thông minh tìm kiếm bằng chứng để kiểm tra xác suất cho dù phản hồi là lời nói dối hay sự thật. Ví dụ, một honeypot có thể mô phỏng chuyển động của chuột để hoạt động bình thư ờng. Tuy nhiên, đối thủ có thể tìm ra chuyển động giả với các mẫu không phổ biến. Hai mô hình đư ợc các nhà nghiên cứu đề xuất sau khi xem xét bằng chứng của đối thủ. Mô hình đầu tiên đư ợc đề xuất bởi Pawlick và Zhu (2015). Mô hình này là dựa trên các trò chơi tín hiệu nói chuyện rẻ tiền, trong đó mạng lư ới bảo vệ và đối thủ lần lư ợt là ngư ời gửi và ngư ời nhận. Chúng tôi gọi mô hình này là CSG (viết tắt của Cheap-talk Signaling Game). Kẻ thù có thể tìm thấy bằng chứng về sự lừa dối đư ợc sử dụng trong mạng lư ới, và sau đó nhận đư ợc thông điệp từ ngư ời phòng thủ, quyết định có nên tấn công hay không. CSG đề xuất tìm chiến lư ợc tối ư u bằng cách sử dụng Bayesian hoàn hảo Cân bằng Nash. Tuy nhiên, một chiến lư ợc tối ư u chính xác vẫn chư a đư ợc xác định. Do đó, Pawlick và cộng sự (2018) đã đề xuất một trò chơi khác mô phỏng một mạng lư ới hon-eynet với hai loại phản ứng nói dối và sự thật. Mô hình này dựa trên trên các trò chơi tín hiệu nói chuyện rẻ tiền và cho rằng mạng lư ới bảo vệ và đối thủ là ngư ời gửi và ngư ời nhận trong trò chơi này, tư ơng ứng. Tin nhắn đư ợc trao đổi giữa ngư ời gửi và ngư ời nhận trong trò chơi cụ thể này là mức độ hoạt động của máy chủ. Máy chủ có mức độ hoạt động cao có thể là máy chủ thực sự, và mức độ hoạt động thấp là chính đặc điểm của honeypot. Mặc dù vậy, ngư ời phòng thủ có thể thay đổi mức độ hoạt động để dụ kẻ thù. Vì mô hình này dựa trên Signaling Trò chơi có bằng chứng, chúng tôi gọi là SGE. Chiến lư ợc tối ư u cho ngư ời bảo vệ trong SGE là làm cho bằng chứng của đối thủ trở nên vô dụng. Do đó, mô hình này xem xét các trạng thái khác nhau cho một mạng lư ới mật ong và đề xuất chiến lư ợc tối ư u của de-fender ở mỗi trạng thái. Các trạng thái và chiến lư ợc là như sau:

- Trạng thái thống trị: Trong trư ờng hợp số lư ợng honeypot hoặc số lư ợng máy chủ thực sự cực kỳ thấp (tức là gần như bằng không), chiến lư ợc tối ư u là tạo ra tất cả các hệ thống (tức là các honeypot và máy chủ thực sự) có mức độ hoạt động tư ơng tự. Nói cách khác, tất cả các hệ thống phải ở mức độ hoạt động cao hoặc tất cả chúng phải có mức độ hoạt động thấp mức độ hoạt động.
- Trạng thái nặng: Khi số lư ợng honeypot không gần bằng 0 như ng nó ít hơn các máy chủ thực sự, chiến lư ợc tối ư u là giữ nguyên thực tế mức độ hoạt động của máy chủ cao và làm cho các honeypot xuất hiện với một mức độ hoạt động cao. Trong trư ờng hợp số lư ợng máy chủ thực tế không phải là gần bằng không như ng ít hơn honeypot, chiến lư ợc tối ư u là giống nhau.
- Trạng thái trung gian: Nếu số lư ợng honeypot và máy chủ thực tế gần bằng nhau bằng nhau, chiến lư ợc tối ư u là làm cho một nửa số honeypot hoạt động hoạt động, và một nửa còn lại ở mức độ hoạt động thấp. Hầu hết các máy chủ thực sự cũng phải đư ợc giữ ở mức hoạt động cao và những máy chủ khác về hoạt động ở mức độ thấp.

Các mô hình đã đề cập trư ớc đó trong phần này chỉ giả định rằng kẻ thù thăm dò mạng. Trong các tình huống thực tế, một số máy chủ lành tính cũng thăm dò mạng lư ới và giao tiếp với những ngư ời khác. Do đó, Bilinski et al. (2018) mở rộng mô hình HDG và đề xuất một mô hình trò chơi Bayesian, trong đó ngư ời chơi đầu tiên là ngư ời bảo vệ mạng và ngư ời chơi thứ hai là một nút chung. Ngư ời chơi thứ hai là một đối thủ có một xác suất và nếu không, nó là một nút lành tính. Chúng tôi gọi mô hình này là eHDG (viết tắt của HDG mở rộng). Ngư ời bảo vệ trong eHDG có thể đặt lên đến các máy chủ trong mạng và đối thủ sẽ thắng trò chơi nếu có thể thực hiện một cuộc tấn công thành công vào ít nhất một máy chủ thực sự. Mục đích của trò chơi này là để chỉ ra rằng chiến lư ợc nói dối của ngư ời phòng thủ là cần thiết. Nếu không có lời nói dối này, bên phòng thủ sẽ thua hầu hết thời gian. Chiến lư ợc đư ợc đề xuất là cân bằng số lư ợng lời nói dối giữa tất cả chủ nhà.

Học tăng cư ờng đư ợc sử dụng bởi Limouchi và Mahgoub (2021) để tối ư u hóa các honeypot trong môi trư ờng IoT. Vì điều này mô hình sử dụng thuật toán Bayesian kết hợp với học tăng cư ờng, chúng tôi gọi mô hình này là BRL (Bayesian Reinforcement Learning). Một honey-pot có thể hoạt động như một máy chủ thực hoặc giả trong nghiên cứu này. Khi honeypot có nhiều hơn một ngư ỡng số lư ợng hàng xóm độc hại, nó phải hành động như một honeypot. Nếu không, nó có thể chuyển sang một máy chủ thực sự. Nghiên cứu này cho thấy giá trị ngư ỡng 2 dẫn đến chiến lư ợc tối ư u cho hậu vệ.

Ngư ời ta có thể coi quá trình động lực hóa là thay đổi hành vi của honeypot dựa trên mức độ tư ơng tác của chúng. Luo et al. (2017) gọi những honeypot này là honeypot tư ơng tác thông minh. Trong nghiên cứu này, trạng thái của các thiết bị trong mạng IoT liên tục đư ợc giám sát và sau đó một mô hình học máy đư ợc đào tạo để tìm ra chiến lư ợc tối ư u. Kiến trúc honeypot đư ợc đề xuất trong nghiên cứu này, IoTCandyJar, quyết định dựa trên mô hình học tập để hoạt động như một mức thấp hoặc tư ơng tác cao. Huang và Zhu (2019) đã đề xuất một sự củng cố mô hình học tập để thúc đẩy hiệu quả mạng lư ới mật ong bằng cách thay đổi mức độ tư ơng tác của honeypots. Ngư ời bảo vệ trong mô hình học tập này có thể thực hiện bốn hành động khác nhau: loại bỏ kết nối của đối thủ, ghi lại tất cả thông tin của đối thủ, hoạt động như một tư ơng tác thấp honeypot và hoạt động như một honeypot có tư ơng tác cao. Mô hình này sử dụng quá trình quyết định bán Markov để tìm ra chiến lư ợc tối ư u. Chúng tôi gọi mô hình này MDRL (Markov Decision-based Reinforcement Learning).

Để so sánh các mô hình chính đư ợc đề cập trong phần này (tức là DD, SGM, HDG và SGE), chúng tôi đã mô phỏng một số tình huống trong Python. Chúng tôi áp dụng chiến lư ợc tối ư u của mỗi mô hình trong bốn mô hình này. Mỗi mạng mô phỏng nằm trong một trong các trạng thái đư ợc giới thiệu trong SGE: Chiếm ư u thế, Nặng và Trung bình. Mỗi mạng chứa 100 nút, trong đó 5, 20 và 50 nút là honeypots ở trạng thái thống trị, nặng và trung bình, tư ơng ứng. Chúng tôi đã mô phỏng bốn loại kịch bản. Trong lần đầu tiên kịch bản, kẻ thù quét mạng một cách ngẫu nhiên (RandomScan), và các honeypot đư ợc phân phối ngẫu nhiên trong mạng (Vị trí ngẫu nhiên). Kịch bản này đư ợc gọi là RS-RL. Trong kịch bản thứ hai,

Thuật toán 2 Quá trình của kịch bản mô phỏng để so sánh nghiên cứu về việc thúc đẩy các honeypot.

```
danh sách các nút mạng
h  danh sách trống
danh sách trống
từ 1 đến 40 làm
    một nút ngẫu nhiên từ h
    thêm vào đến h
    thăm dò( , )
    một số ngẫu nhiên giữa 0 và 100
    nếu < _ _ sau đó
        nếu = một máy chủ thực sự sau đó
            thêm vào ĐẾN
        khác
            nếu = một cái bẫy mật ong
            thêm ) ĐẾN
    nếu kích thước( > 0 sau đó
        một nút ngẫu nhiên từ
        nếu là một máy chủ thực sự sau đó
            ghi lại một cuộc tấn công thành công
        khác
            ghi lại một cuộc tấn công không thành công
    khác
        ghi lại một cuộc tấn công không thành công
```

honeypots được phân phối tuần tự (SequentialLocation). Vì vậy, chúng tôi gọi kịch bản này là RS-SL. Kịch bản thứ ba sử dụng quét tuần tự Phương pháp (SequentialScan) với honeypot phân phối ngẫu nhiên. Vì vậy, chúng tôi gọi nó là SS-RL. Cuối cùng, kịch bản cuối cùng được gọi là SS-SL, vì nó sử dụng quét tuần tự và các honeypot được đặt tuần tự trong không gian mạng. Kẻ thù thăm dò tới 40 máy chủ và mạng người bảo vệ có thể nói dối nhiều nhất 30 lần trong các tình huống của chúng tôi. Cuối cùng, đối thủ chọn một mục tiêu trong số các máy chủ được thăm dò và phát động một cuộc tấn công chống lại nó. Nếu mục tiêu là máy chủ thực sự, cuộc tấn công sẽ thành công, nếu không, kẻ thù thất bại. Quá trình chi tiết của các kịch bản mô phỏng được giải thích trong Thuật toán 2. Hàm probe() được đề cập trong Thuật toán 2 là loại nút mục tiêu, có thể là lời nói dối hoặc sự thật, tùy thuộc vào mô hình động lực học.

Kết quả của mỗi kịch bản được thể hiện trong Hình 12. Chúng ta có thể thấy rằng trung bình, DD và SGM có hiệu suất cao hơn HDG và SGE trong các kịch bản của chúng tôi. Điều này có thể được quy cho thực tế là tần số của những thay đổi trong phản ứng ở DD và SGM thấp hơn HDG và SGE.

5.5. Định hình lưới mật ong

Cấu trúc mạng lưới mật ong là một yếu tố khác cần được xem xét khi phân tích hiệu suất của nó. Các kết nối giữa các máy chủ có thể có ảnh hưởng đáng kể đến sức mạnh lừa dối. Ví dụ, trong một mạng có đầy đủ cấu trúc lưới, tất cả các máy chủ được kết nối trực tiếp và sự lan truyền của phần mềm độc hại trong mạng như vậy là nhanh chóng. Do đó, trình bảo vệ mạng phải chú ý đến cấu trúc mạng honeynet để có hiệu suất tốt hơn.

Cấu trúc mạng lưới mật ong ảnh hưởng đến khả năng của một honeypot duy nhất. Ren và Zhang (2020) đã đề xuất một trò chơi khác biệt giữa honeynet và đối thủ để phân tích hiệu ứng này. Chúng tôi đặt tên cho mô hình trò chơi này là Trò chơi tôpô vi phân (DTG). Trong trò chơi này, đối thủ cố gắng tìm ra tỷ lệ lây nhiễm tốt nhất cho các máy chủ mạng để khởi chạy một cuộc tấn công DDoS. Mặt khác, honeynet cố gắng giảm tỷ lệ lan truyền phần mềm độc hại của đối thủ với chi phí thấp nhất. Nó được nêu trong nghiên cứu này rằng mức độ của mỗi honeypot có thể ảnh hưởng đáng kể đến hiệu suất của nó. Ví dụ, honeypot có mức độ cao hơn có thể bắt được nhiều cuộc tấn công hơn so với các cuộc tấn công cấp độ thấp hơn. Tuy nhiên, các honeypot cấp độ thấp hơn phù hợp hơn cho các quy trình phục hồi. Điều này nghiên cứu cũng cho thấy rằng số mũ cao hơn sẽ hiệu quả hơn trong việc ngăn chặn các cuộc tấn công cho các mạng không có quy mô, trong đó các cấp độ tuân theo một phân phối luật lũy thừa.

Ngoài các mạng không có quy mô, có thể có các cấu trúc khác có thể định hình honeynet. Do đó, ảnh hưởng của một số kiểu

Thuật toán 3 Quá trình lan truyền phần mềm độc hại trong các mô phỏng cho so sánh các nghiên cứu về việc định hình mạng lưới mật ong.

```
h  danh sách các nút honeypot
danh sách các nút bị nhiễm
cho mỗi khoảng thời gian nhiễm trùng làm
    cho làm
        h danh sách các nút lân cận của nút
        một số ngẫu nhiên giữa 0 và 10
        nếu < _ × 10 sau đó
            cho h LÀ M
                nếu h sau đó
                    xóa khỏi phần ngất
                thêm vào
```

cấu trúc mạng về hiệu suất lừa dối được nghiên cứu trong Ren et al. (2021), đề xuất một mô hình trong đó honeynet bị nhiễm một phần phần mềm độc hại và tốc độ lây lan của phần mềm độc hại này được kiểm tra trong các cấu trúc mạng khác nhau như hình tròn, hình sao, hình cây và không có thang đo cấu trúc mạng. Kết quả nghiên cứu này nêu rằng nếu giá trị đặc trưng tối đa của ma trận kề honeynet ( ) nhỏ hơn tỷ lệ giữa tốc độ phục hồi của các máy chủ bị nhiễm với tốc độ lây nhiễm phần mềm độc hại, honeynet có thể đạt được hiệu suất cao. Họ đã tính toán các ranh giới của như được đưa ra trong Phương trình (17), trong đó

$$= h + + .$$

$$\frac{}{\sqrt{\sqrt{\sqrt{}}}\ 1} \quad {}^{2} \leq \quad \leq \text{phút}\left(, \frac{1}{} \right) \qquad (17)$$

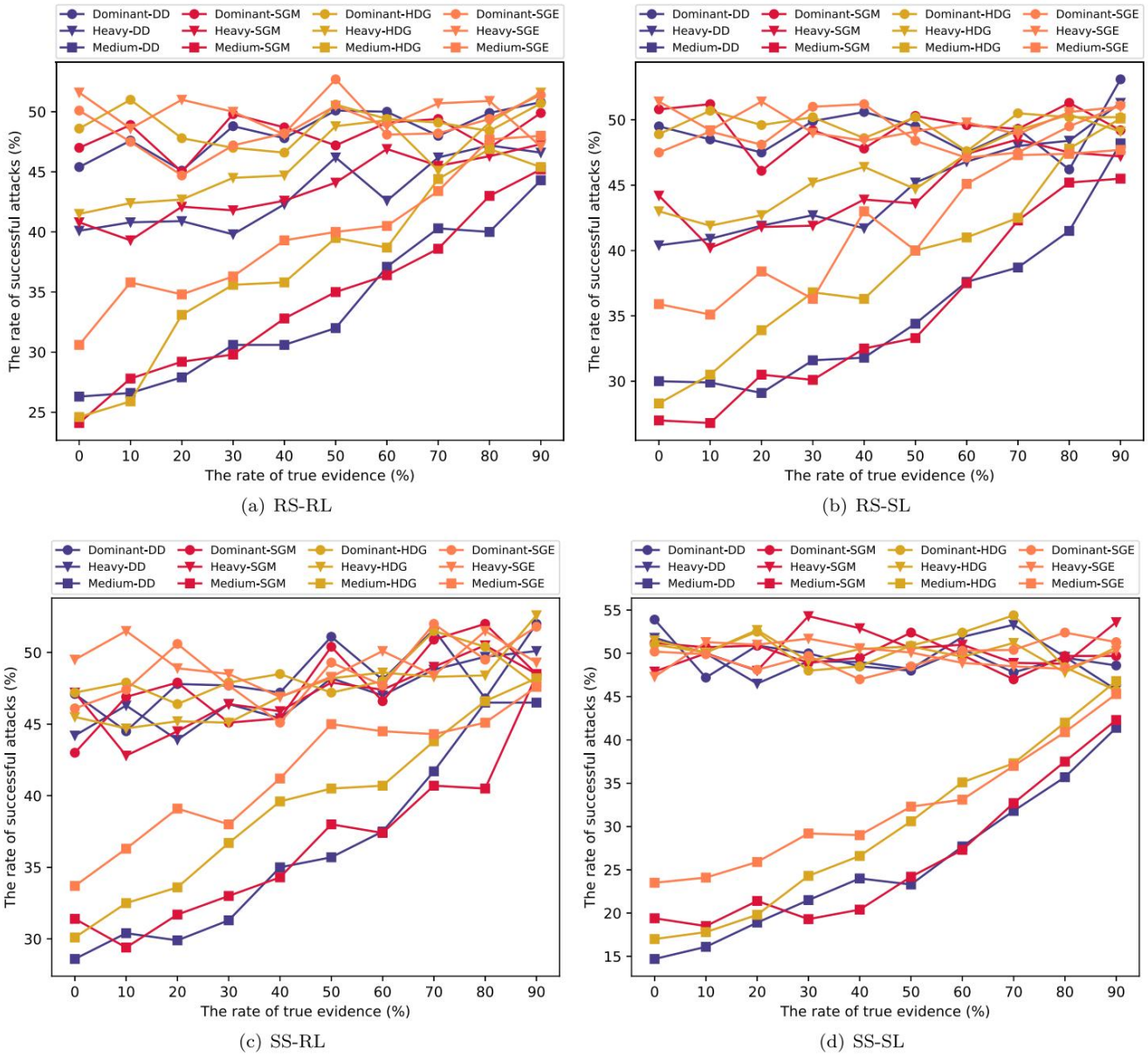
Xét phương trình (17) và điều kiện được đề cập để nghiên cứu đề xuất giữ , cái mức độ vật chủ lớn nhất ở mức thấp để có một mạng lưới mật ong hiệu quả. Vì mô hình xem xét nhiều cấu trúc khác nhau để mô hình hóa Trò chơi, chúng tôi gọi nó là VTG.

Để phân tích các nghiên cứu được thực hiện trong lĩnh vực cấu trúc mạng honeynet, chúng tôi đã mô phỏng sáu mạng trong Python với các cấu trúc mạng khác nhau bị nhiễm phần mềm độc hại. Các mạng này được hiển thị trong Hình 13. và 1, 2, 3 sử dụng cấu trúc vòng, sao và cây tương ứng. 4 sử dụng cấu trúc k-regular cấu trúc mạng, trong đó tất cả các nút đều có bảy nút lân cận. Cuối cùng, và 6 là mạng không có thang đo, trong đó có số mũ thấp hơn 5 hơn 6. 5 Tất cả các mạng mô phỏng có 50 nút, trong đó có 10 các nút là honeypots và phần mềm độc hại ban đầu lây nhiễm năm nút. honeypots và các máy chủ bị nhiễm ban đầu được đặt ngẫu nhiên trong mạng và được hiển thị bằng các nút màu vàng và đỏ trong Hình 13 . Các máy chủ bị nhiễm có thể kết nối với các máy chủ bình thường và khai thác chúng bằng một xác suất cụ thể. Nếu một máy chủ bị nhiễm kết nối với một honeypot, nó sẽ được phục hồi. Chi tiết về quá trình lan truyền phần mềm độc hại được đề cập trong Thuật toán 3.

Kết quả của các mô phỏng này được thể hiện trong Hình 14. Như thể hiện trong Hình 14, mạng có số lượng máy chủ bị nhiễm thấp nhất và nó có thể ngăn chặn tốt hơn sự lây lan của phần mềm độc hại trong các tình huống của chúng 6 tôi. Vì và 5 là các mạng không có quy mô và số mũ trong cao hơn, chúng tôi 6 có thể nói rằng đề xuất của mô hình DTG trong các kịch bản của chúng tôi là có thể chấp nhận được. Mặt khác, theo Phương trình (17), các giá trị của đối với 4 là hai và bảy, và đối với giá trị này lớn hơn 1 Và 2 bảy. for lớn hơn hai và nhỏ hơn bảy. Tuy nhiên, một 3 mối quan hệ trực tiếp giữa và số lượng cuối cùng của các máy chủ bị nhiễm là không quan sát được.

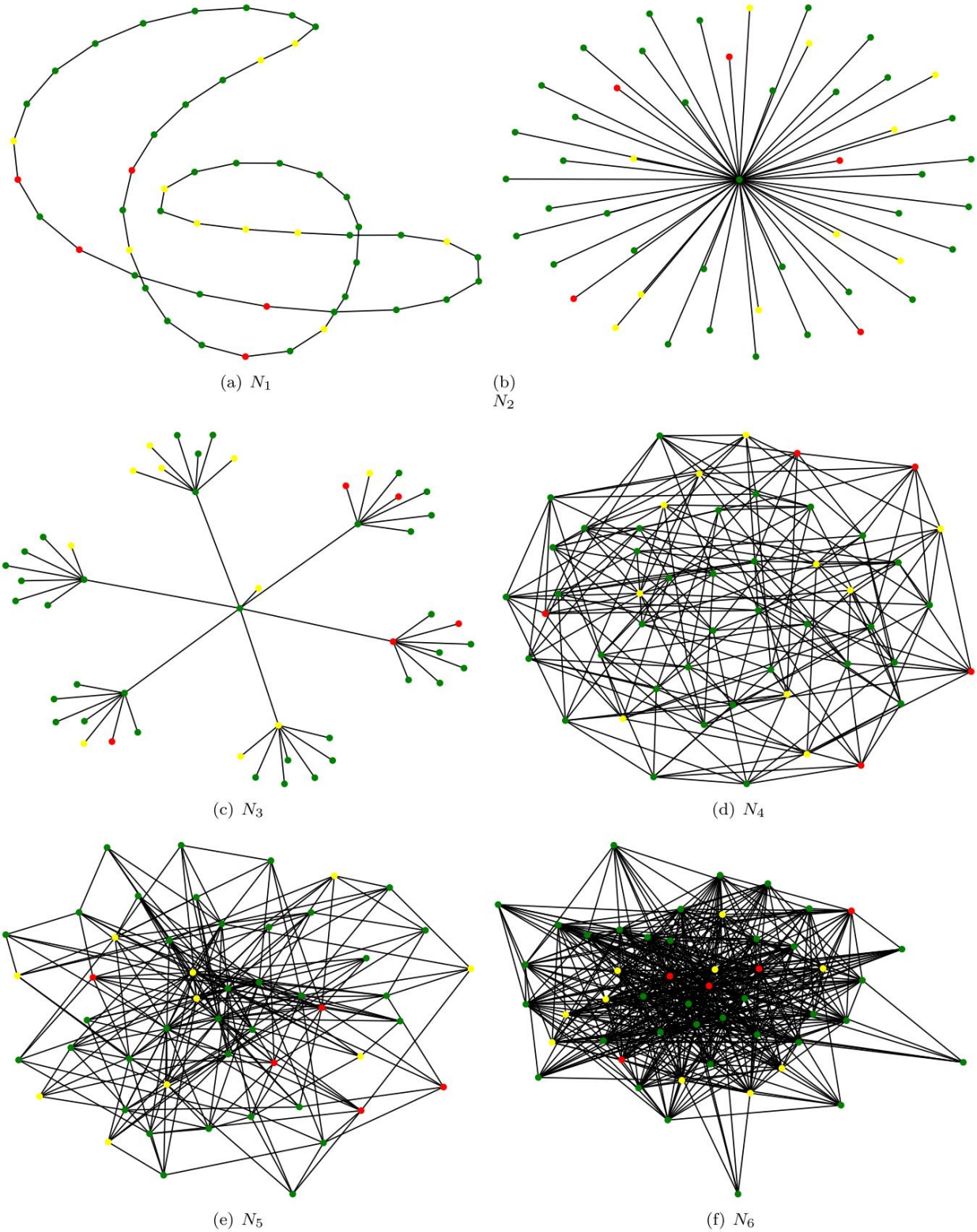
5.6. Mô phỏng - che giấu: nâng cao sự lừa dối của honeypot lên tầm cao mới

Mô phỏng - Che giấu là một kỹ thuật lừa dối đại diện cho đỉnh cao của sự tinh vi trong lĩnh vực bảo mật honeypot. Mục tiêu chính của nó là đạt được một kỳ tích đáng chú ý – làm cho honeypot gần như không thể phân biệt được với các tài sản mạng đích thực. Kỹ thuật này không chỉ đơn thuần là mời gọi những kẻ tấn công; nó khéo léo bẫy chúng vào một mạng lưới ảo tương phức tạp, nơi ranh giới giữa thực tế và sự lừa dối trở nên quá mờ nhạt đến nỗi ngay cả những kẻ thù sáng suốt nhất



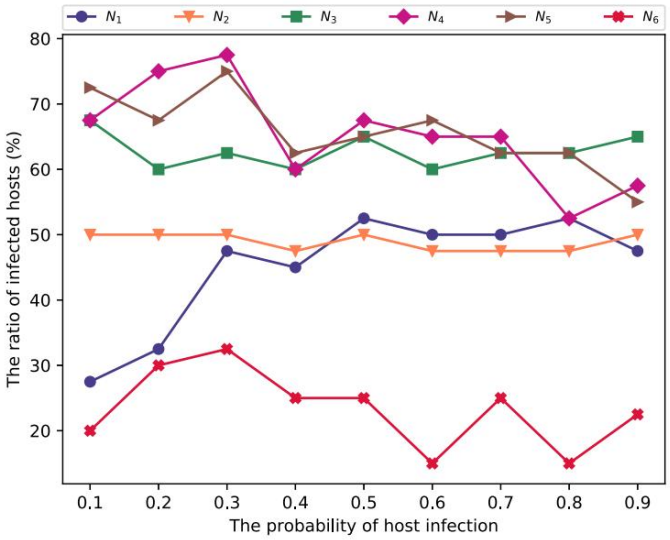
Hình 12. So sánh hiệu suất của các chiến lư ợc DD, SGM, HDG và SGE trong các tình huống khác nhau.

thấy khó để phân biệt. Về bản chất, Mô phỏng - Che giấu dựa vào nghệ thuật che giấu. Honeypot đư ợc thiết kế tỉ mỉ để mô phỏng các đặc điểm, thuộc tính và hành vi của tài sản mạng thực sự. Sự mô phỏng này mở rộng đến nhiều chi tiết, bao gồm cả việc thay đổi biểu ngữ hệ thống để phù hợp với các dịch vụ thực tế, sao chép một cách tỉ mỉ hành vi dịch vụ và phản ánh các giao thức thư ờng thấy trong môi trư ờng mạng. Kết quả là một honeypot có thể mô phỏng chính xác một mục tiêu hợp pháp, có giá trị đối với con mắt không đư ợc đào tạo của kẻ tấn công. Sự thành công của Mô phỏng - Che giấu phụ thuộc vào khả năng thu hút kẻ tấn công và thuyết phục chúng về tính xác thực của honeypot. Honeypot, đư ợc ngụy trang hoàn hảo, dụ kẻ tấn công giao chiến với nó, thuyết phục họ rằng nó đại diện cho một cơ hội vàng. Sự lừa dối này đặt những kẻ tấn công vào một vị trí bấp bênh khi họ tư ơng tác với những gì họ tin rằng đó là một tài sản hợp pháp. Trong tư ơng tác này, honeypot quản trị viên có đư ợc sự hiểu biết sâu sắc về chiến thuật, kỹ thuật và động cơ của kẻ tấn công. Điều làm cho việc che giấu trở nên khác biệt là tác động tâm lý nó đòi hỏi những kẻ tấn công. Những kẻ tấn công phải điều hư ớng một môi trư ờng đầy rẫy với sự không chắc chắn khi chúng đi qua mạng lư ới. Không có khả năng phân biệt honeypots từ tài sản hữu hình gây gánh nặng cho kẻ tấn công bằng sự phân ly nhận thức nance, khiến họ phải suy nghĩ lại mọi hành động của mình. Nhận thức này tải thư ờng dẫn đến sự do dự, sai lầm và phát hiện, cung cấp cho ngư ời bảo vệ thời gian phản ứng vô giá. Triển khai các kỹ thuật che giấu trong honeypots là một hình thức nghệ thuật đòi hỏi sự chính xác và hiểu biết sâu sắc về kiến trúc mạng. Cấu hình honeypot phải liền mạch tích hợp với môi trư ờng mạng rộng hơn, tạo ra một ảo ảnh liền mạch mà ngay cả những kẻ tấn công tinh ranh cũng không thể xâm nhập. Các địa điểm như công cộng Các vùng Wi-Fi và phân đoạn mạng mở, đư ợc biết đến với khả năng thu hút nhiều đối tư ợng khác nhau hành vi của ngư ời dùng, đóng vai trò là địa điểm triển khai lý tư ởng cho các honeypot đư ợc che giấu. Trong các thiết lập này, honeypots mô phỏng các hành vi mạng đích thực, nắm bắt các kỹ thuật và hành vi phức tạp nhất của kẻ tấn công. Tóm lại, Mô phỏng-che mặt là minh chứng cho sự tinh vi vô song của công nghệ honeypot. Nó thể hiện bản chất của sự lừa dối honeypot bằng cách tạo ra một môi trư ờng nơi ranh giới giữa thực tế và ảo tư ởng đư ợc làm mờ một cách tỉ mỉ. Khi đư ợc sử dụng khéo léo bởi những ngư ời bảo vệ có kỹ năng, kỹ thuật này không chỉ củng cố các thế trận an ninh mạng mà còn vạch trần sự yếu đuối của tâm lý con ngư ời trư ớc sự lừa dối liên tục bối cảnh đang phát triển của các mối đe dọa mạng (Argyratos, 2021; Graham và cộng sự, 2016; Heckman và cộng sự, 2015; Wang và cộng sự, 2022). Trong suốt phần này-



(a) N_1 (b) N_2 (c) N_3 (d) N_4 (e) N_5 (f) N_6

Hình 13. Các mạng mô phỏng với các cấu trúc mạng khác nhau. (Để giải thích màu sắc trong hình, người đọc được giới thiệu phiên bản web của bài viết này.)



Hình 14. So sánh quá trình phát tán phần mềm độc hại trong các tình huống khác nhau.

tion, chúng tôi đã khám phá kỹ lư ng nghiên cứu honeynet, bao gồm một phạm vi rộng
phạm vi các chủ đề liên quan. Chúng tôi bắt đầu bằng cách giải thích các khái niệm cơ bản
của honeynet, cung cấp cho ngư i đọc một nền tảng vững chắc trong
khu vực này. Sau đó, chúng tôi trình bày một mô hình toàn diện cho
trình bày có hệ thống về honeynet, cung cấp một khuôn khổ có cấu trúc để nâng cao sự hiểu
biết và đánh giá các hệ thống phòng thủ mạng này. Tiếp tục khám phá, chúng tôi đi sâu vào
lĩnh vực
các kỹ thuật lừa dối, đóng vai trò then chốt trong việc tăng cư ng hiệu suất của lư i mật
ong. Các kỹ thuật này đư c phân loại một cách chu đáo
thành năm lớp riêng biệt: tối ư u hóa, đa dạng hóa, dựa trên vị trí
chiến lư c, động lực và định hình honeypot. Mỗi danh mục đư c phân tích trong bối cảnh
của mô hình chung đư c đề xuất, cho phép so sánh có ý nghĩa giữa các kỹ thuật này và tạo
điều kiện cho việc hiểu sâu hơn
hiểu rõ ư u điểm và như c điểm của từng loại.

Để cung cấp những hiểu biết thực nghiệm về hiệu quả của các kỹ thuật này,
chúng tôi đã tiến hành các thí nghiệm mô phỏng bằng Python. Những mô phỏng này
bao gồm một loạt các tình huống và cho phép chúng tôi đánh giá định lư ng
việc thực hiện các kỹ thuật lừa dối khác nhau trong bối cảnh
honeynets. Thông qua các mô phỏng này, chúng tôi đã thu đư c dữ liệu và quan sát có giá
trị, đóng vai trò quan trọng trong việc tinh chỉnh sự hiểu biết của chúng tôi về
các kỹ thuật nổi bật nhất trong lĩnh vực này. Sử dụng Python làm nền tảng mô phỏng đảm bảo
rằng các thí nghiệm của chúng tôi vừa nghiêm ngặt vừa
có thể tái tạo, góp phần tăng thêm độ tin cậy cho những phát hiện của chúng tôi.

5.7. Mô phỏng - đóng gói lại

Đóng gói lại là một kỹ thuật tinh vi và mang tính chiến lư c giúp tăng cư ng đáng kể
hiệu quả của honeypot trong cuộc chiến không ngừng nghỉ
chống lại những kẻ tấn công mạng. Phư ng pháp này tận dụng khuynh hư ng tin tư ng vào
các nguồn lực có vẻ hợp pháp của kẻ tấn công, thư ng khai thác sự tò mò và tìm kiếm tài
sản có giá trị của họ. Đây là một nghệ thuật đư c tinh chỉnh, đòi hỏi
những ngư i bảo vệ trở nên thành thạo trong việc nắm vững kỹ thuật nhúng các yếu tố lừa
dối tinh vi như ng cực kỳ hiệu quả vào các nguồn tài nguyên xác thực.
Các thành phần lừa đảo này đư c xây dựng cẩn thận và có khả năng có nhiều hình thức khác
nhau, chẳng hạn như các tập lệnh ẩn, các tệp thực thi đã sửa đổi hoặc
thậm chí cả những thay đổi phức tạp trong cấu trúc dữ liệu. Những yếu tố này là chiến lư c
đư c sắp xếp hợp lý để kích hoạt các phản ứng hoặc hành động cụ thể khi đư c truy cập bởi
những kẻ tấn công không hề hay biết, thực sự khiến họ rơi vào bẫy lừa đảo của honeypot.

Sự đa dạng về tài nguyên là một đặc điểm xác định của Mô phỏng -
Đóng gói lại. Ngư i bảo vệ có khả năng linh hoạt để chuyển đổi một loạt các
tài nguyên vào các honeypot thu hút kẻ tấn công. Kỹ thuật này mở rộng
ngoài các tài liệu và ứng dụng thông thư ng cho các trang web, cơ sở dữ liệu,
và thậm chí cả tin nhắn email, đóng vai trò như những cái bẫy tiềm tàng. Khả năng thích ứng này
cho phép những ngư i bảo vệ dụ dỗ những kẻ tấn công bằng những thông tin đa dạng, có vẻ có giá trị
tài sản, tăng khả năng tham gia. Sức mạnh thực sự của Sim-ulation - Repackaging nằm ở khả
năng cảnh báo sớm của nó – khi kẻ tấn công
tư ng tác với các nguồn tài nguyên lừa đảo này, kỹ thuật này sẽ thu thập đư c một loạt
dữ liệu có giá trị về hành động của chúng trong giai đoạn đầu
của sự tham gia. Dữ liệu này cung cấp cho những ngư i bảo vệ một cửa sổ quý giá để hiểu
đư c ý định độc hại, cho phép họ phản ứng chủ động trư c
một cuộc tấn công leo thang thành một vụ vi phạm an ninh toàn diện.

Việc tạo ra một chiến lư c mô phỏng - đóng gói lại thành công đòi hỏi
sự chú ý tỉ mỉ đến từng chi tiết và cam kết không lay chuyển đối với chủ nghĩa hiện thực.
Môi trư ng Honeypot phải đư c thiết kế tỉ mỉ để sao chép hoàn hảo các nguồn lực và dịch
vụ hợp pháp của một tổ chức. Điều này
sao chép đảm bảo rằng kẻ tấn công gặp phải tài nguyên đư c đóng gói lại
mà không gây ra sự nghi ngờ ngay lập tức, góp phần vào hiệu quả
của honeypot. Tùy chỉnh là tối quan trọng, với mỗi lần triển khai honeypot đư c điều chỉnh
để phù hợp với bối cảnh mối đe dọa độc đáo và cụ thể
mục tiêu của tổ chức. Đây là một quá trình năng động đòi hỏi phải điều chỉnh liên tục.

Tuy nhiên, việc điều hư ng các khía cạnh đạo đức và pháp lý của việc triển khai
honeypot, đặc biệt là những honeypot sử dụng Mô phỏng - Đóng gói lại,
là rất quan trọng. Những ngư i bảo vệ phải giải quyết những mối quan tâm này một cách cẩn thận và nghiêm ngặt
tuân thủ luật pháp địa phư ng và các nguyên tắc đạo đức. Sự minh bạch và tuân thủ các
tiêu chuẩn đạo đức là điều cần thiết để bảo vệ một tổ chức
uy tín và duy trì lòng tin của các bên liên quan.

Ngoài chức năng cảnh báo sớm, những hiểu biết sâu sắc đư c trích xuất từ Sim-ulation
- Repackaging sẽ đóng vai trò là bàn đạp để củng cố
thế trận an ninh của một tổ chức. Điều này bao gồm lỗ hổng kịp thời
vá lỗi, cập nhật chính sách bảo mật và cải tiến liên tục
của các thủ tục ứng phó sự cố. Trong bối cảnh năng động của an ninh mạng, nơi những kẻ tấn
công liên tục thích nghi và phát triển chiến thuật của chúng,
Mô phỏng - Đóng gói lại nổi lên như một ngư i bảo vệ khéo léo và chủ động,
trao quyền cho các tổ chức với tầm nhìn xa và các công cụ cần thiết để củng cố hiệu quả
các biện pháp phòng thủ an ninh mạng của họ. Bằng cách kết hợp nghệ thuật
lừa dối với kế hoạch tỉ mỉ và cân nhắc về mặt đạo đức, những ngư i bảo vệ có thể chủ động
đánh bại kẻ thù trên mạng và luôn đi đầu trong
cuộc chiến đang diễn ra vì an ninh kỹ thuật số (De Faveri và Moreira, 2016;
(De Faveri và cộng sự, 2018).

5.8. Mô phỏng - đóng gói lại

Mô phỏng - Dazzling là một kỹ thuật lừa dối tinh vi và đư c thiết kế khéo léo, tỏa
sáng rực rỡ trong thế giới của honeypot. Nó
vư t qua các quan niệm truyền thống về sự lừa dối bằng cách tạo ra môi trư ng bẫy mật
không chỉ đánh lừa những kẻ tấn công tiềm năng mà còn làm chúng lóa mắt.
Hãy tư ng tư ng nó như một cảnh tư ng kỹ thuật số, nơi ranh giới giữa ảo ảnh và
thực tế mờ nhạt, khiến những kẻ thù mạng phải kinh ngạc. Về cốt lõi, Simulation-Dazzling
xoay quanh nghệ thuật chế tạo tài sản honeypot
không chỉ lừa dối mà còn gây ấn tư ng mạnh về mặt thị giác và hấp dẫn sâu sắc
những kẻ tấn công tiềm năng. Những honeypot này không chỉ là những cái bẫy; chúng là những
tủ trư ng bày kỹ thuật số đư c trang trí bằng những yếu tố khiến chúng nổi bật như
kho báu hiếm có trong bối cảnh mạng lư i. Chúng giống như những thứ lấp lánh
đá quý, không thể cư ng lại đối với những ngư i tìm kiếm cơ hội trong thế giới kỹ thuật số
miền. Một nguyên tắc cơ bản của Simulation-Dazzling là việc triển khai chiến lư c các tài
sản mồi nhử đư c thiết kế để trở nên đặc biệt
hấp dẫn. Những mồi nhử này có nhiều dạng khác nhau, từ các tệp có tên hấp dẫn hứa hẹn nội
dung có giá trị đến các thư mục đư c thiết kế để
hấp dẫn khám phá hoặc các dịch vụ mạng có sức hấp dẫn không thể cư ng lại.
Đư c đặt chính xác trong môi trư ng honeypot, các tài sản này hoạt động
như những mồi nhử tử tính, thu hút những kẻ tấn công bằng lời hứa về những gì có vẻ như
để trở thành một giải độc đắc kỹ thuật số. Sự thành công của Simulation-Dazzling không chỉ nằm ở
trong việc thu hút sự chú ý của kẻ tấn công như ng lại chiếm hết sự tập trung của chúng. Với
sức hấp dẫn về mặt thị giác và tâm lý của chúng, những honeypots chói lọi này thư ng trở
thành ư u tiên hàng đầu của kẻ tấn công, bị hiểu nhầm là mục tiêu có giá trị cao. Sự chuyển
hư ng sự chú ý khỏi các tài sản thực sự này mang lại
những ngư i bảo vệ một lợi thế chiến thuật quan trọng. Hơn nữa, mô phỏng-Dazzling

không chỉ là về sức hấp dẫn trực quan; nó còn thúc đẩy tác động tâm lý đến lợi thế của nó. Sự hiện diện của những mồi nhử nổi bật này tạo ra cảm giác sâu sắc về sự bất hòa nhận thức trong những kẻ tấn công. Họ phải đối mặt với sự bối rối khi đánh giá tầm quan trọng đư ợc nhận thức của những điều này tài sản, thư ờng dẫn đến sự do dự, tư ơng tác kéo dài trong môi trư ờng honeypot, và cuối cùng là thu thập dữ liệu mở rộng cho de-fenders. Triển khai mô phỏng - Dazzling trong honeypots đòi hỏi hiểu biết sâu sắc về tâm lý của kẻ tấn công và một con mắt tinh tư ờng cho thiết kế. Ngư ời quản lý Honeypot phải tỉ mỉ chế tạo trực quan tấn công các tài sản honeypot, định vị chúng một cách chiến lư ợc trong mạng. Các máy chủ công khai, thư ờng là mục tiêu chính của kẻ tấn công, tạo ra địa điểm lý tư ởng để triển khai các honeypot sáng chói. Các honeypot sáng chói như những ngọn hải đăng không thể cư ỡng lại trong những bối cảnh này, dễ dàng hư ớng dẫn những kẻ tấn công hư ớng tới họ. Khai thác sức mạnh của sự quyến rũ thị giác và sự hấp dẫn về mặt tâm lý lôi kéo những kẻ tấn công vào mạng lư ới lừa dối đầy mê hoặc của nó. Điều này kỹ thuật này không chỉ chuyển hư ớng sự chú ý của kẻ tấn công khỏi tài sản thực sự như ng cũng trang bị cho ngư ời bảo vệ một góc nhìn độc đáo để quan sát, phân tích và hiểu đư ợc hành vi của kẻ tấn công trong bối cảnh luôn thay đổi của các mối đe dọa mạng. Thông qua sự sáng chói lừa dối của nó, Simulation-Dazzling làm sáng tỏ con đư ờng hư ớng tới an ninh mạng mạnh mẽ và chủ động hơn (Almeshekah và Spafford, 2014; De Faveri và cộng sự, 2018; Heckman và cộng sự và cộng sự, 2015).

5.9. Sự che giấu - bịa ra sự lừa dối ngoài mong đợi

Phát minh đại diện cho đỉnh cao của sự đổi mới trong lĩnh vực này của các kỹ thuật lừa đảo honeypot, đẩy mạnh ranh giới của an ninh mạng với cách tiếp cận tiên tiến và đầy sáng tạo. Nó đứng như một minh chứng cho khả năng khéo léo và trí tư ởng tư ợng của con ngư ời, định nghĩa lại bản chất của honeypots. Hãy tư ởng tư ợng nó như một hành động tạo ra một câu chuyện kỹ thuật số hấp dẫn, nơi ranh giới giữa thực tế và sự sáng tạo hòa lẫn vào một tấm thảm lừa dối tinh vi đầy quyến rũ.

Về bản chất, Dissimulation - Inventing là một quá trình khéo léo của việc triệu hồi tài sản mật ong chỉ tồn tại trong thế giới hư cấu, như ng đư ợc thiết kế tỉ mỉ với mức độ chi tiết và tinh tế vô song.

Những chiếc lọ mật ong này vư ợt ra ngoài định nghĩa thông thư ờng của mồi nhử; chúng là những câu chuyện hoàn chỉnh, những nhân vật đư ợc phát triển đầy đủ hoặc thậm chí là toàn bộ thế giới ảo thế giới mà những kẻ tấn công tiềm năng có thể tình cờ gặp phải trong quá trình bất hợp pháp của họ đột nhập vào lĩnh vực kỹ thuật số. Một nguyên tắc cơ bản làm nền tảng

Sự che giấu - Phát minh là nghệ thuật kể chuyện sâu sắc. Những ngư ời quản lý mật ong đảm nhận vai trò là ngư ời kể chuyện kỹ thuật số, đan xen những câu chuyện phức tạp hoặc tạo ra những nhân vật hư cấu để thu hút và quyến rũ những kẻ tấn công tiềm năng. Những cấu trúc sáng tạo này biểu hiện dư ới nhiều hình thức khác nhau, từ việc tạo ra các tài khoản ngư ời dùng giả mạo có cốt truyện hấp dẫn sự khởi đầu của các môi trư ờng kỹ thuật số hoàn toàn đư ợc chế tạo hoặc thậm chí triệu hồi các lỗ hổng bảo mật phức tạp đư ợc nhúng một cách chiến lư ợc trong môi trư ờng honeypot. Chiến thắng thực sự của Dissimulation - Phát minh nằm ở khả năng vô song của nó không chỉ thu hút sự chú ý của kẻ tấn công mà còn khiến chúng đắm chìm trong một thế giới kỹ thuật số hấp dẫn. thế giới. Những kẻ tấn công, bị thu hút bởi sự quyến rũ của những câu chuyện hoặc bị mê hoặc bởi tạo ra các lỗ hổng, đầu tư nhiều thời gian và công sức vào các tư ơng tác của họ với các honeypot này, hoàn toàn tin tư ởng rằng họ đã vấp phải những mục tiêu xác thực. Sự đắm chìm này mang lại cho những ngư ời bảo vệ một cơ hội vô giá để xem xét kỹ lư ỡng các phư ơng pháp, động cơ của kẻ tấn công, và quyết tâm chặt chẽ. Hơn nữa, Sự che giấu - Phát minh vư ợt qua phạm vi lừa dối kỹ thuật để khám phá sự phức tạp của tâm lý con ngư ời. Những câu chuyện hấp dẫn và trải nghiệm đắm chìm đư ợc thiết kế tỉ mỉ bằng kỹ thuật này có thể gợi lên những phản ứng cảm xúc ở những kẻ tấn công, nuôi dư ỡng cảm giác gắn bó và cam kết với họ tư ơng tác trong môi trư ờng honeypot. Sự đầu tư cảm xúc này thư ờng dẫn đến thời gian lư u trú kéo dài, thu thập dữ liệu mở rộng và hiểu biết sâu sắc hơn về đặc điểm hành vi của kẻ tấn công. Thực hiện che giấu - Phát minh trong honeypot đòi hỏi một sự kết hợp giữa thiên tài sáng tạo và sự hiểu biết sâu sắc về kẻ tấn công tâm lý học. Ngư ời quản lý Honeypot phải tạo ra những câu chuyện kỹ thuật số hấp dẫn và đảm bảo những honeypot giàu trí tư ởng tư ợng này phù hợp liền mạch với lợi ích và mục tiêu của những kẻ tấn công tiềm năng. Những honeypot sáng tạo này đư ợc đặt ở vị trí chiến lư ợc trong môi trư ờng mạng, thư ờng ở những khu vực phù hợp với lộ trình khám phá tự nhiên mà kẻ tấn công có xu hư ớng thực hiện để theo dõi. Sự che giấu - Phát minh đại diện cho đỉnh cao của sự sáng tạo trong bối cảnh honeypot. Khai thác sức mạnh mê hoặc của kể chuyện và xây dựng thế giới giàu trí tư ởng tư ợng thu hút những kẻ tấn công tiềm năng vào mạng lư ới lừa dối hấp dẫn của nó. Kỹ thuật này thu hút sự chú ý của kẻ tấn công và trang bị cho ngư ời phòng thủ một điểm quan sát đặc biệt để giải mã những sự phức tạp tinh vi của hành vi kẻ tấn công trong thế giới luôn thay đổi và đa dạng của các mối đe dọa mạng. Sự che giấu - Phát minh định nghĩa lại giới hạn của cải tiến honeypot, thúc đẩy nghệ thuật lừa dối vư ợt xa những mong đợi thông thư ờng (Cantella, 2021; Từ Faveri và Moreira, 2016).

5.10. Sự che giấu - bất chư ớc

Sự che giấu - Bất chư ớc là một kỹ thuật lừa dối phi thư ờng và cực kỳ hiệu quả, là đỉnh cao của sự xuất sắc trong miền của honeypots. Nó đại diện cho đỉnh cao của sự mô phỏng, nơi honeypot đư ợc thiết kế tỉ mỉ để mô phỏng hình thức và hành vi của các tài sản mạng thực ở mức độ đáng kinh ngạc, tư ơng tự như việc chế tạo một bản sao kỹ thuật số khiến những kẻ tấn công hoàn toàn tin rằng họ đã tình cờ tìm thấy nguồn tài nguyên xác thực.

Về bản chất, việc giả vờ bất chư ớc đòi hỏi sự khéo léo tỉ mỉ của honeypots hầu như không thể phân biệt đư ợc với mạng lư ới thực sự nguồn lực. Những honeypot này vư ợt xa sự bắt chư ớc hời hợt, mạo hiểm đi sâu vào trái tim của sự lừa dối bằng cách sao chép mọi khía cạnh của tài sản hợp pháp. Điều này bao gồm các biểu ngữ hệ thống phản chiếu, bắt chư ớc tỉ mỉ các hành vi dịch vụ và thậm chí tái tạo hoàn hảo các mẫu lư u lư ợng mạng. Kết quả là một honeypot, với con mắt tinh tư ờng của kẻ tấn công không chỉ có vẻ ngoài xác thực mà còn hoàn toàn là một phần không thể thiếu của mạng lư ới.

Một nguyên tắc cơ bản làm nền tảng cho việc ngụy trang-bắt chư ớc là tính xác thực không lay chuyển. Ngư ời quản lý Honeypot tham gia vào các chi tiết tỉ mỉ để đảm bảo rằng các tài sản bắt chư ớc của họ là chính xác hoàn hảo. Điều này đòi hỏi phải tạo ra các honeypot mô phỏng hoàn hảo các cấu hình chính xác của các dịch vụ mạng, phản ánh các giao thức theo các sắc thái tinh tế nhất và tạo ra lư u lư ợng không thể phân biệt đư ợc với mạng hợp pháp. hoạt động.

Thành công vang dội của việc ngụy trang-bắt chư ớc nằm ở khả năng vô song của nó trong việc thuyết phục những kẻ tấn công rằng chúng thực sự đang tư ơng tác với các nguồn lực xác thực. Những kẻ tấn công, khi chúng tham gia vào những honeypots, thư ờng không thể phân biệt đư ợc chúng với tài sản hữu hình mà họ nhiệt thành tìm cách thỏa hiệp. Mức độ sâu sắc này của sự lừa dối đặt những kẻ tấn công vào một vị trí bấp bênh khi chúng vô tình tiết lộ chiến thuật, kỹ thuật và động cơ của mình trong môi trư ờng bẫy mật, nơi những ngư ời bảo vệ cảnh giác sẵn sàng quan sát và phản ứng. Hơn nữa, việc bắt chư ớc ngụy trang thư ờng xuyên mang lại lợi thế tâm lý của sự bất hòa nhận thức đối với những kẻ tấn công. Vì họ điều hư ớng mạng lư ới mô phỏng, kẻ tấn công thư ờng xuyên gặp phải những bẫy mật hấp dẫn đến mức chúng nghi ngờ tính xác thực của mọi thứ xung quanh họ. Gánh nặng nhận thức này có thể dẫn đến sự do dự, sai lầm và phát hiện, cung cấp cho ngư ời bảo vệ phản ứng vô giá thời gian và hiểu biết sâu sắc về hành vi của kẻ tấn công. Thực hiện che giấu - Việc bắt chư ớc trong honeypot đòi hỏi sự chú ý vô song đến từng chi tiết và hiểu biết toàn diện về kiến trúc mạng. Cấu hình honeypot phải đư ợc tích hợp tỉ mỉ vào phạm vi rộng hơn môi trư ờng mạng để tạo ra ảo ảnh gần như hoàn hảo. Những hon-eypot này đư ợc triển khai hiệu quả nhất trong các phân đoạn mạng quan trọng nơi mà tính xác thực của chúng sẽ thuyết phục nhất đối với những kẻ tấn công tiềm năng. Sự giả vờ-bắt chư ớc là đỉnh cao của sự tinh vi của bẫy mật, thể hiện bản chất của sự lừa dối bằng cách tạo ra một môi trư ờng nơi những kẻ tấn công phải kinh ngạc về tính xác thực của tài sản mà họ gặp gỡ. Kỹ thuật này không chỉ giúp củng cố các thế trận an ninh mạng mà còn mang đến cho những ngư ời bảo vệ một cơ hội phi thư ờng để hiểu và ngăn chặn sự phức tạp của hành vi tấn công trong

cảnh quan liên tục phát triển của các mối đe dọa mạng. Nó đại diện cho đỉnh cao của sự đổi mới honeypot, nơi sự lừa dối hoàn hảo được mài giũa đến mức mức độ thành thạo vô song (Whaley, 1982; Pawlick và cộng sự, 2019; Heck-man và cộng sự, 2015).

5.11. Sự che giấu - sự dụ dỗ

Sự che giấu - Mồi nhử là một trò lừa bịp đầy mê hoặc và cực kỳ tinh vi kỹ thuật lừa dối xuất hiện như một kiệt tác quyến rũ trong lĩnh vực của honeypots. Nó xoay quanh nghệ thuật phức tạp của việc xây dựng honeypots vượt qua sự lừa dối đơn thuần để trở nên phức tạp ảo tưởng, được thiết kế để gây hoang mang và đánh lừa những kẻ tấn công tiềm năng. Hình ảnh nó giống như việc dàn dựng một vũ hội hóa trang lớn nơi những chiếc mặt nạ được đeo bởi những người tham gia không chỉ là ngụy trang mà còn là những câu đố phức tạp, dẫn đến một mê cung của sự hấp dẫn.

Về bản chất, Dissimulation - Decoying đòi hỏi kỹ thuật tạo ra những chiếc lọ mật ong có hình dạng như mê cung, chứa đầy mồi nhử. các yếu tố được bố trí tỉ mỉ để đánh lạc hướng và làm kẻ tấn công bối rối. Những honeypot này giống như những mê cung phức tạp, nơi kẻ tấn công phải điều hướng qua một loạt các mồi nhử tinh vi trước khi truy cập vào thông tin có giá trị hoặc tài sản mạng thực sự. Một nguyên tắc cơ bản neo giữ sự ngụy trang-mồi nhử là nghệ thuật đánh lạc hướng. Những người quản lý Honeypot đầu tư nhiều công sức để đảm bảo môi trường Honeypot là đầy rẫy những mồi nhử bắt chước tài sản thật một cách thuyết phục. Những mồi nhử có nhiều hình thức khác nhau, từ các tập tin giả có tên gọi đánh lừa và thông tin xác thực giả mạo cho các dịch vụ mạng gây hiểu lầm. Chúng được đặt một cách khéo léo trong môi trường bẫy mật ong để cám dỗ, đánh lạc hướng và đánh lạc hướng những kẻ tấn công. Sự thành công vang dội của Dissimulation - Decoying nằm ở khả năng làm cho kẻ tấn công bối rối và vướng vào, dẫn họ xuống một con đường quanh co của sự lừa dối. Những kẻ tấn công, khi họ tham gia vào những chiếc lọ mật ong này, sớm thấy mình bị mắc kẹt trong một mạng lưới mồi nhử, phung phí thời gian và nguồn lực quý báu vào những gì họ tin là mục tiêu có giá trị cao. Sự chuyển hướng chiến lược này cung cấp cho những người bảo vệ một chỉ huy lợi thế khi kẻ tấn công sử dụng các tài sản quan trọng để điều hướng mê cung lừa dối. Hơn nữa, sự che giấu - lừa dối thường xuyên gây ra tác động tâm lý lên những kẻ tấn công, gây ra sự thất vọng khi họ gặp phải một mồi nhử sau một mồi nhử khác. Sự mất phương hướng và chán nản ngày càng tăng này có thể dẫn đến sai sót và phát hiện. Tác động tâm lý trở thành đồng minh mạnh mẽ cho những người bảo vệ. Thực hiện việc che giấu - Đánh lừa trong honeypot đòi hỏi khả năng sáng tạo để đánh lạc hướng và hiểu biết sâu sắc về tâm lý của kẻ tấn công. Honeypot người quản lý phải tỉ mỉ tạo ra môi trường honeypot chứa đầy với những mồi nhử không chỉ thuyết phục mà còn gây bối rối. Những cái bẫy mật ong này thường được đặt một cách chiến lược trong các phân đoạn mạng nơi kẻ tấn công có khả năng khám phá nhưng không phải là một phần không thể thiếu của chức năng cốt lõi của mạng. Sự che giấu - Mồi nhử đại diện cho một khía cạnh hấp dẫn của sự lừa dối mật ong quyến rũ kẻ tấn công bằng sự phức tạp của nó, dẫn họ vào một mê cung ảo tưởng khó hiểu. Kỹ thuật này không chỉ làm cho kẻ tấn công bối rối và khó xử nhưng cũng trao quyền cho người phòng thủ điểm quan sát đặc biệt để quan sát, phân tích và hiểu được những phức tạp đa dạng của hành vi của kẻ tấn công trong cảnh quan đang phát triển của các mối đe dọa mạng. Đó là một minh chứng cho nghệ thuật của sự lừa dối, nơi mà các bẫy mật ong trở thành những bức tranh phức tạp về sự đánh lạc hướng và âm mưu (Cantella, 2021; Han và cộng sự, 2018; Heckman và cộng sự, 2015).

6. Khám phá hiệu quả của honeypot thông qua đánh giá

Lĩnh vực honeypots đặt ra một thách thức độc đáo trong việc đánh giá hiệu quả của chúng, xét đến mục tiêu kép của chúng là đánh lừa các cuộc tấn công tự động và thao túng quá trình ra quyết định của con người. Một đánh giá nghiêm ngặt phương pháp luận là cần thiết để đo lường tác động của chúng một cách toàn diện. Điều này phần này đi sâu vào các phương pháp được sử dụng trong tài liệu để đánh giá hiệu quả của honeypot, đặc biệt tập trung vào ý nghĩa của thí nghiệm nhóm đỏ.

- Bối cảnh đánh giá đa chiều: Đánh giá honeypots bao gồm việc điều hướng một bối cảnh đa diện mở rộng ra ngoài các số liệu an ninh mạng thông thường. Trong khi các chuẩn mực kỹ thuật như tỷ lệ phát hiện xâm nhập và thời gian tham gia của kẻ tấn công là rất quan trọng, phạm vi đánh giá sẽ mở rộng khi xem xét ảnh hưởng của honeypots trên những kẻ tấn công con người. Quyết định của con người, thường được thúc đẩy bằng cảm xúc, thành kiến và quá trình nhận thức, đưa ra một chiều hướng độc đáo đòi hỏi những cách tiếp cận đánh giá sáng tạo (Priya và Chakkaravarthy, 2023).
- Các thí nghiệm Red-Teaming: Đi đầu trong việc đánh giá honeypot phương pháp luận là các thí nghiệm nhóm đỏ, mô phỏng thế giới thực các tình huống liên quan đến kẻ thù là con người. Các bài tập nhóm đỏ sao chép động cơ, chiến lược và quá trình ra quyết định thực sự của kẻ tấn công, cho phép các nhà nghiên cứu đánh giá hiệu quả của honeypot một cách toàn diện. Những thí nghiệm này thu hẹp khoảng cách giữa khả năng kỹ thuật và tâm lý con người, cung cấp cái nhìn sâu sắc về cách honeypot tương tác với và ảnh hưởng đến hành vi của kẻ tấn công (Drew và Heinen, 2022).
- Các chiều kích kỹ thuật và tâm lý: Các thí nghiệm nhóm đỏ bao gồm cả các chiều hướng kỹ thuật và tâm lý. Về mặt kỹ thuật, các đánh giá này đo lường mức độ hiệu quả của honeypot ngăn chặn các cuộc tấn công do những kẻ tấn công là con người thực hiện (Sethuraman và cộng sự, 2023). Họ cũng làm sáng tỏ các chiến lược mà kẻ tấn công sử dụng để điều hướng honeypot môi trường. Tuy nhiên, điều phân biệt các thí nghiệm nhóm đỏ là khám phá của họ về động lực tâm lý. Bằng cách bắt chước các tác nhân kích hoạt cảm xúc, thành kiến nhận thức và các chiến thuật kỹ thuật xã hội được sử dụng bởi những kẻ tấn công, những thí nghiệm này cho thấy mức độ mà honeypot thao túng quá trình ra quyết định của con người.
- Thông tin chi tiết về Honeypot toàn diện: Kết hợp các thí nghiệm nhóm đỏ vào bộ công cụ đánh giá cung cấp một góc nhìn toàn diện về honeypot hiệu quả. Những thí nghiệm như vậy cho thấy những lỗ hổng trong kỹ thuật các khía cạnh của honeypot và khả năng ảnh hưởng đến hành động của kẻ tấn công và quyết định. Nhận thức toàn diện này trang bị cho các nhà nghiên cứu và người bảo vệ với sự hiểu biết toàn diện về bối cảnh mối đe dọa đang phát triển, cho phép họ tăng cường các chiến lược bẫy mật ong giải quyết cả những thách thức về mặt kỹ thuật và con người (Maesschalck và cộng sự, 2022; Kan-danaarachchi và cộng sự, 2022).
- Làm giàu cho Honeypot Arsenal: Khi bối cảnh an ninh mạng phát triển, vai trò của các thí nghiệm nhóm đỏ trở nên ngày càng quan trọng. Chúng thu hẹp khoảng cách giữa các cuộc tấn công mô phỏng và phức tạp hành vi của những kẻ tấn công thực sự. Bằng cách kết hợp các phương pháp nhóm đỏ vào quá trình đánh giá, hiệu quả của honeypot có thể được tinh chỉnh để phản ánh sự tương tác năng động giữa các cuộc tấn công tự động và tâm lý con người. Sự hiểu biết phong phú này trao quyền cho những người bảo vệ để xây dựng các chiến lược lừa dối mạnh mẽ hơn nhằm chống lại hiệu quả các mối đe dọa đa chiều (Chung và cộng sự, 2023).
- Việc kết hợp khám phá các phương pháp đánh giá, đặc biệt là các thí nghiệm nhóm đỏ, trong bài báo sẽ tăng cường chiều sâu của nó bằng cách làm nổi bật sự giao thoa giữa sự lừa dối về mặt kỹ thuật và sự phức tạp tâm lý của kẻ thù con người. Sự tích hợp này phản ánh bản chất phát triển của các chiến lược an ninh mạng và nhấn mạnh tầm quan trọng của các kỹ thuật lừa dối lấy con người làm trung tâm trong việc củng cố khả năng an ninh mạng hình ảnh.
- Tiết lộ vai trò của tâm lý con người trong lừa đảo trực tuyến Chiến lược:

Các chiến lược lừa dối trong an ninh mạng vượt ra khỏi phạm vi công nghệ và đi sâu vào phạm vi phức tạp của tâm lý con người. Nhận ra rằng mục tiêu cuối cùng của sự lừa dối là tác động đến con người việc ra quyết định bổ sung thêm một lớp chiều sâu vào việc đánh giá an ninh biện pháp. Nhận thức này trở nên đặc biệt thích hợp khi kiểm tra hiệu quả của honeypot, vì thành công của chúng phụ thuộc vào khả năng của chúng để thao túng hành vi của kẻ thù là con người. Trong khi thông thường số liệu an ninh mạng cung cấp những hiểu biết vô giá, nhưng chúng thường không đầy đủ của việc nắm bắt sự tương tác phức tạp giữa công nghệ và con người bản chất. Sự xuất hiện của các thí nghiệm nhóm đỏ như một phương pháp đánh giá nổi bật cho thấy nỗ lực có ý thức nhằm thu hẹp khoảng cách này (Gonzalez et al., 2022). Những thí nghiệm này, mô phỏng các tình huống thực tế

với động cơ thực tế của kẻ tấn công và quá trình nhận thức, cung cấp một ống kính độc đáo để kiểm tra sự tương tác giữa các chiến lược lừa dối và tâm lý con người. Trong bối cảnh của honeypots, sự nhấn mạnh vào các thí nghiệm nhóm đó phản ánh bối cảnh phát triển của các biện pháp phòng thủ an ninh mạng. Ngoài khả năng kỹ thuật của họ, các thí nghiệm này khám phá cách honeypot có thể khai thác những thành kiến nhận thức, kích hoạt cảm xúc, và các chiến thuật kỹ thuật xã hội để thao túng hành vi của con người. Bằng cách làm sáng tỏ cách những kẻ tấn công phản ứng với những thao túng tâm lý này, các nhà nghiên cứu có được hiểu biết sâu sắc để tinh chỉnh các chiến lược honeypot, làm nổi bật mối quan hệ cộng sinh giữa công nghệ và tâm lý con người. Như lĩnh vực an ninh mạng tiếp tục phát triển, nó ngày càng trở nên bằng chứng là hiệu quả của các kỹ thuật lừa dối phụ thuộc vào chúng khả năng ảnh hưởng và đánh lừa những kẻ tấn công là con người. Bằng cách làm nổi bật khía cạnh lừa dối lấy con người làm trung tâm, các phương pháp đánh giá được lựa chọn, đặc biệt là các thí nghiệm nhóm đó, làm phong phú thêm sự hiểu biết về cách các chiến lược an ninh mạng phải thích ứng với sự tương tác năng động giữa công nghệ và tâm lý con người (Ferguson-Walter và cộng sự, 2023). Trong theo quan điểm này, honeypots không chỉ là công cụ kỹ thuật đơn thuần và nổi lên như những công cụ mạnh mẽ khai thác những điểm yếu của con người để củng cố tư thế an ninh mạng tổng thể. Việc kết hợp thảo luận này làm giảm sự kết nối không thể thiếu giữa sự lừa dối, công nghệ và hành vi của con người, do đó cung cấp cái nhìn toàn diện về các chiến lược an ninh mạng trong bối cảnh mối đe dọa không ngừng thay đổi (Cranford và cộng sự, 2023).

7. Các vấn đề mở

Sau khi xem xét các kỹ thuật và phương pháp đã đề cập, chúng tôi đã xác định được một số lỗ hổng nghiên cứu trong lĩnh vực honeypot và honeynet. các nhà nghiên cứu có thể tiếp tục điều tra những khoảng cách này để có được hiệu quả hơn honeypot và honeynet. Gợi ý của chúng tôi như sau.

7.1. Đánh giá honeypot

Theo đuổi một khuôn khổ chính xác và thực tế cho toàn diện đánh giá các hệ thống honeypot có nhiều kỹ thuật lừa dối khác nhau vẫn là một lĩnh vực chín muồi để khám phá. Trong khi chúng tôi đã phác thảo chung số liệu trong phần 3, định nghĩa chính xác của chúng cần được tinh chỉnh thêm. Để giải quyết nhu cầu này, chúng tôi đề xuất sử dụng mô hình học máy kết hợp các số liệu được đề xuất làm tham số đầu vào. Bằng cách sử dụng mô hình này, các nhà phát triển có thể đánh giá khách quan hiệu suất của hệ thống honeypot của họ và chủ động giải quyết những thiếu sót của họ. Việc điều hướng những phức tạp của đánh giá honeypot đưa chúng ta đến một thách thức ngã tư đường: ưu tiên các số liệu trong các tình huống khác nhau. Ví dụ, một mạng lưới công nghiệp. Ở đây, tầm quan trọng của dữ liệu thu thập được có thể nhạt nhòa so với nhu cầu tối quan trọng là giảm thiểu rủi ro bị xâm phạm. Việc bảo vệ tính toàn vẹn của các thiết bị được ưu tiên hơn những chi tiết nhỏ của việc phân tích các mối đe dọa để phân tích tiếp theo. Do đó, các nhà nghiên cứu đối mặt với nhiệm vụ quan trọng là xác định các số liệu có liên quan và xác định các ưu tiên của họ. Khai thác sức mạnh của một cỗ máy mô hình học tập cung cấp một khuôn khổ thích ứng phản ứng với các sắc thái ngữ cảnh. Khả năng xử lý nhiều số liệu và các ưu tiên tương ứng của họ trang bị cho các nhà phát triển một công cụ mạnh mẽ để đánh giá hiệu quả của honeypot trong các tình huống khác nhau. Tuy nhiên, hành trình để có một khuôn khổ đánh giá honeypot toàn diện đòi hỏi phải có một cái nhìn sâu sắc hơn khám phá các mô hình hành vi của kẻ tấn công và động lực theo ngữ cảnh. Nghiên cứu liên tục là điều cần thiết để khám phá các chiến lược liên tục thay đổi của các đối thủ mạng và các biện pháp thích ứng tương ứng được yêu cầu trong các phương pháp đánh giá. Cuối cùng, sự tích hợp hiệp lực của học máy, số liệu được xác định rõ ràng và hiểu biết sâu sắc về những sự tinh tế theo ngữ cảnh sẽ mở đường cho một sự kiên cường và thích nghi mô hình đánh giá honeypot. Khi an ninh mạng tiến triển, việc áp dụng kỹ thuật đánh giá sáng tạo là một cách tiếp cận mang tính chuyển đổi định hình lại cách chúng ta định lượng hiệu quả của honeypot. Cách tiếp cận này trao quyền các nhà phát triển để khuếch đại sức mạnh của hệ thống honeypot của họ và giảm thiểu chủ động khai thác điểm yếu của họ, qua đó thúc đẩy một bối cảnh mạng mạnh mẽ hơn.

7.2. Các số liệu chính được sử dụng để đánh giá honeypot

Một đánh giá toàn diện về honeypot đòi hỏi phải áp dụng nhiều loại số liệu khác nhau để cùng nhau làm sáng tỏ chúng hiệu suất và tác động. Các số liệu này đóng vai trò là chuẩn mực định lượng hướng dẫn quá trình đánh giá. Tỷ lệ phát hiện xâm nhập (IDR) đo lường hiệu quả của honeypot trong việc xác định và cảnh báo kịp thời về các nỗ lực truy cập trái phép. Tỷ lệ tham gia định lượng mức độ tương tác giữa kẻ tấn công và honeypot, phản ánh khả năng quyến rũ kẻ thù của nó. Thời gian thỏa hiệp đánh giá hiệu quả của honeypot trong việc ngăn chặn và trì hoãn những kẻ tấn công bằng cách kéo dài thời gian vi phạm. Dữ liệu đã thu thập đánh giá sự phong phú và khối lượng thông tin thu thập được từ các tương tác của kẻ tấn công (Santhosh Kumar et al., 2023). Tỷ lệ dương tính giả cho biết tần suất người dùng hợp pháp kích hoạt cảnh báo, đảm bảo tính liên tục của hoạt động. Tấn công Thuộc tính đo lường độ chính xác mà honeypot xác định kẻ tấn công, tăng cường thông tin tình báo về mối đe dọa. Chỉ số Độ phức tạp của cuộc tấn công cung cấp thông tin chi tiết về mức độ tinh vi của các cuộc tấn công đã thực hiện. Lừa dối Độ sâu đánh giá mức độ thành công của honeypot trong việc khuyến khích sự tham gia sâu sắc bằng cách thu hút những kẻ tấn công. Sự đa dạng tương tác đo lường sự đa dạng của các chiến lược kẻ tấn công sử dụng trong môi trường honeypot. Sớm Cảnh báo đo lường tốc độ phát hiện và giao tiếp của honeypot mối đe dọa mới nổi. Việc sử dụng tài nguyên đánh giá tác động của mật ong đối với cơ sở hạ tầng và khả năng thu hút kẻ tấn công của nó. Cuộc tấn công Chỉ số hiệu quả đẩy lùi cho thấy honeypot khéo léo như thế nào trong việc đánh lạc hướng kẻ tấn công khỏi các tài sản quan trọng. Tác động đến hành vi của kẻ tấn công phân tích xem honeypot có ảnh hưởng đến kẻ tấn công để điều chỉnh chiến thuật của chúng hay không. Threat Intelligence Yield định lượng giá trị của dữ liệu được thu thập trong việc đưa ra các chiến lược an ninh mạng rộng hơn. Cuối cùng, Honeypot Resilience đánh giá độ bền của honeypot trong việc duy trì vẻ ngoài lừa dối của nó đang bị tấn công. Các số liệu này cùng nhau cho phép một khuôn khổ đánh giá toàn diện xem xét cả kỹ thuật và lấy con người làm trung tâm như - các khía cạnh, làm phong phú thêm sự hiểu biết về hiệu quả của honeypot (Eriksson, 2023). Các số liệu này cùng nhau cung cấp cái nhìn toàn diện về honeypot hiệu suất, tác động của nó đến bối cảnh mối đe dọa và những đóng góp của nó để cải thiện các chiến lược an ninh mạng và ứng phó sự cố. Việc lựa chọn và diễn giải các số liệu phải phù hợp với các mục tiêu cụ thể của việc triển khai honeypot và kết quả mong muốn của đánh giá quy trình. Mô tả cho từng mục có thể được tìm thấy ở phần sau.

- Tỷ lệ phát hiện xâm nhập (IDR): Tỷ lệ phát hiện xâm nhập đo lường hiệu quả của honeypot trong việc xác định và cảnh báo về các nỗ lực truy cập trái phép. IDR cao hơn cho thấy cơ chế phát hiện của hon-eypot nhận ra các hoạt động đáng ngờ, giúp những người bảo vệ phản ứng nhanh chóng với các mối đe dọa tiềm tàng (Raharjo và cộng sự, 2022).
- Tỷ lệ tham gia: Tỷ lệ tham gia biểu thị mức độ tương tác giữa kẻ tấn công và honeypot. Tỷ lệ tham gia cao hơn cho thấy honeypot đã thành công trong việc thu hút và nắm bắt sự chú ý của những kẻ tấn công, tạo điều kiện thu thập dữ liệu và hiểu biết sâu sắc hơn về chúng chiến thuật và ý định (Panda et al., 2022).
- Thời gian thỏa hiệp: Chỉ số này đo lường thời gian kẻ tấn công mất để phá vỡ hàng phòng thủ của honeypot. Thời gian thỏa hiệp dài hơn cho thấy honeypot kéo dài hiệu quả nỗ lực của kẻ tấn công, cấp người bảo vệ có nhiều thời gian hơn để xác định, phân tích và phản ứng với sự xâm nhập (Hobert và cộng sự, 2023).
- Dữ liệu được thu thập: Dữ liệu được thu thập đánh giá số lượng và chất lượng thông tin được thu thập trong quá trình tương tác với kẻ tấn công. Điều này bao gồm lưu lượng mạng, lệnh được ban hành, các tệp được truy cập và các hành động khác được thực hiện bởi những kẻ tấn công trong môi trường honeypot (Ikuomenisan và Morgan, 2022).
- Tỷ lệ dương tính giả: Tỷ lệ dương tính giả tính toán tần suất với những người dùng hợp pháp hoặc hệ thống tự động kích hoạt cảnh báo hoặc tham gia vào honeypot. Giảm thiểu Tỷ lệ dương tính giả đảm bảo honeypot không cản trở hoạt động bình thường hoặc tiêu thụ tài nguyên một cách không cần thiết (Kandanaarachchi và cộng sự, 2022).
- Phân bổ tấn công: Phân bổ tấn công đánh giá mức độ chính xác của honeypot xác định nguồn gốc và danh tính của kẻ tấn công. Bắt buộc tại-

sự đóng góp cung cấp những hiểu biết có giá trị về vị trí địa lý của kẻ tấn công, mối quan hệ và động cơ tiềm ẩn (Crochelet và cộng sự, 2022).

• Độ phức tạp của tấn công: Chỉ số này đo lường mức độ tinh vi của các cuộc tấn công hướng vào honeypot. Các cuộc tấn công phức tạp có thể chỉ ra rằng honeypot thu hút những kẻ thù có kỹ năng, trong khi những cuộc tấn công trực tiếp hơn có thể phản ánh những nỗ lực cơ hội từ những mối đe dọa ít tinh vi hơn diễn viên (Yang và cộng sự, 2023).

• Độ sâu lừa dối: Độ sâu lừa dối đo lường mức độ hiệu quả của honeypot tạo ra một môi trường dụ kẻ tấn công tham gia sâu sắc. Độ sâu lừa dối cao cho thấy kẻ tấn công đầu tư nhiều thời gian và công sức, tiết lộ nhiều hơn về ý định và kỹ thuật của chúng (Sumadi và cộng sự, 2022).

• Sự đa dạng tương tác: Sự đa dạng tương tác đánh giá sự đa dạng của cách kẻ tấn công tương tác với honeypot. Một loạt các tương tác cung cấp thông tin chi tiết về chiến lược và mục tiêu của kẻ tấn công, từ việc thăm dò đến thử nhiều phương án tấn công khác nhau (Srinivasa và cộng sự, 2022).

• Cảnh báo sớm: Cảnh báo sớm đo lường tốc độ của honeypot phát hiện và cảnh báo cho người bảo vệ về các mối đe dọa mới nổi. Phát hiện nhanh chóng trao quyền cho các nhóm an ninh mạng phản ứng kịp thời, giảm thiểu khả năng rủi ro trước khi chúng leo thang (Salimova, 2022).

• Sử dụng tài nguyên: Sử dụng tài nguyên đánh giá tác động của honeypot trên cơ sở hạ tầng cơ bản. Sử dụng tài nguyên cao có thể chỉ ra rằng honeypot thực sự thu hút và lôi kéo những kẻ tấn công, tiêu tốn thời gian và nguồn lực của chúng (Abdulqadder và cộng sự, 2023).

• Hiệu quả chống tấn công: Chỉ số này đánh giá mức độ hiệu quả của honeypot chuyển hướng kẻ tấn công khỏi mục tiêu là các hệ thống sản xuất thực tế. Một chiến lược chống tấn công thành công sẽ chuyển hướng những kẻ tấn công khỏi những mục tiêu có giá trị cao mục tiêu, giảm thiểu rủi ro cho các tài sản quan trọng (Yamin và Katt, 2022).

• Tác động đến Hành vi của Kẻ tấn công: Tác động đến Hành vi của Kẻ tấn công phân tích xem honeypot có ảnh hưởng đến kẻ tấn công để thay đổi chiến thuật của chúng hay không hoặc kỹ thuật. Việc xác định những thay đổi trong hành vi có thể cung cấp thông tin cho những người bảo vệ về các mối đe dọa đang phát triển và các chiến lược thích ứng của kẻ tấn công (Tabari et và cộng sự, 2023).

• Threat Intelligence Yield: Threat Intelligence Yield định lượng cách dữ liệu thu thập được từ honeypot góp phần vào tổ chức tình báo đe dọa. Những hiểu biết có giá trị thu được từ honeypot thông báo chiến lược an ninh mạng tổng thể và ra quyết định (Tan et al., 2023).

• Khả năng phục hồi của Honeypot: Đánh giá khả năng chịu đựng các cuộc tấn công và duy trì vẻ ngoài lừa dối của honeypot. Một honeypot có khả năng phục hồi vẫn hoạt động mặc dù bị giám sát chặt chẽ, tiếp tục tham gia và thu thập dữ liệu từ những kẻ tấn công (Alyas và cộng sự, 2022).

7.3. Honeypot công nghiệp

Trong bối cảnh an ninh mạng không ngừng thay đổi, nơi các mối đe dọa leo thang với tốc độ chưa từng có, việc triển khai chiến lược các honeypot đã nổi lên như một chiến lược phòng thủ then chốt. Các lần lặp lại chuyên biệt của honeypot đã xuất hiện trong môi trường năng động này để giải quyết những thách thức do bối cảnh công nghệ phát triển nhanh chóng đặt ra. Các honeypot không dây đã nổi lên như những công cụ đáng gờm, chế tạo một cách chiến lược mạng Wi-Fi mô phỏng để thu hút những kẻ tấn công tiềm năng và làm sáng tỏ lỗ hổng độc đáo của môi trường không dây. Những honeypot này làm sáng tỏ sự phức tạp của các điểm truy cập trái phép, các nỗ lực nghe lén, và các kết nối trái phép, cung cấp những hiểu biết vô giá quan trọng cho bảo vệ mạng không dây. Song song với đó, sự gia tăng tự động hóa và các hệ thống kết nối đã tạo ra các bẫy mật công nghiệp, sao chép hệ thống điều khiển công nghiệp và kiểm soát giám sát và dữ liệu mạng lưới mua lại. Những cấu trúc ảo này vẫy gọi kẻ thù, mời họ đi qua những cảnh quan lừa dối phản ánh sự phức tạp lĩnh vực công nghiệp hiện đại. Khi câu chuyện diễn ra, bài báo này khám phá những loại honeypot chuyên biệt này, làm sáng tỏ các chiến lược đằng sau chúng triển khai, những lợi thế riêng biệt của họ và những hiểu biết sâu sắc mà họ cung cấp vào lĩnh vực lừa đảo và phòng thủ mạng (Pashaei et al., 2022).

Đi sâu hơn vào lĩnh vực honeypot không dây và công nghiệp:

• Honeypots không dây: Điều hướng Cyber Shadows trong sóng vô tuyến

Các honeypot không dây đã nổi lên như là các biện pháp phòng thủ chiến lược trong bối cảnh của các mạng không dây phổ biến. Các honeypot này được thực hiện một cách tỉ mỉ mô phỏng mạng Wi-Fi đích thực, thu hút kẻ tấn công một cách có chiến lược và phát hiện ra những lỗ hổng vốn có của hệ thống không dây. Vai trò của họ mở rộng đến việc phát hiện các điểm truy cập trái phép, ngăn chặn các nỗ lực kết nối bất hợp pháp và phát hiện các trường hợp nghe lén không dây. Bằng cách phân biệt giữa hành vi hợp pháp của người dùng và hành động độc hại, honeypot không dây cung cấp những hiểu biết vô song về các phương pháp được kẻ tấn công sử dụng để khai thác các điểm yếu trong mạng không dây môi trường (Soundararajan và cộng sự, 2022). Việc triển khai của họ đòi hỏi sự chú ý tỉ mỉ đến cấu hình mạng, nhiễu tín hiệu và cường độ tín hiệu. Đáng chú ý là các khu vực Wi-Fi công cộng, nhộn nhịp với nhiều người dùng khác nhau hoạt động, đóng vai trò là nền tảng lý tưởng để triển khai các honeypot này. Bằng cách phản ánh các hành vi mạng thực sự, các honeypot này nắm bắt và phân tích tỉ mỉ các chiến lược tấn công mà kẻ thù có thể sử dụng để xâm phạm dữ liệu người dùng hoặc xâm nhập vào hệ thống tổ chức.

• Honeypots công nghiệp: Bảo vệ cốt lõi của ngành công nghiệp hiện đại

Khi các ngành công nghiệp áp dụng tự động hóa và các hệ thống kết nối, sự thay đổi cơ bản đã xảy ra trong môi trường công nghiệp. Sự chuyển đổi này sự hình thành đã báo trước sự cần thiết của các biện pháp an ninh mạng chuyên biệt, được thể hiện bằng sự ra đời của các honeypot công nghiệp. Những honeypot này mô phỏng khéo léo sự phức tạp của các hệ thống kiểm soát công nghiệp (ICS) và mạng lưới điều khiển giám sát và thu thập dữ liệu (SCADA), mời những kẻ tấn công tiết lộ chiến thuật và cách điều động của chúng. Hoạt động như chiến trường ảo, bẫy mật công nghiệp cho thấy kẻ thù có thể mục tiêu cơ sở hạ tầng quan trọng. Bằng cách mô phỏng các thành phần độc đáo của mạng công nghiệp, chẳng hạn như bộ điều khiển logic lập trình (PLC) và giao diện người-máy (HMI), các honeypot này nắm bắt các trường hợp của sự xâm nhập, lệnh kiểm soát trái phép và các hoạt động độc hại khác (Conti et al., 2022; Apruzzese et al., 2023). Ngoài ra, họ đóng góp vào việc phát triển thông tin tình báo về mối đe dọa có mục tiêu cụ thể các ngành công nghiệp như năng lượng, sản xuất và vận tải. Đó là điều quan trọng cần lưu ý là việc triển khai honeypot công nghiệp đòi hỏi một hiểu biết sâu sắc về các quy trình công nghiệp, giao thức và các mô hình truyền thông. Các chuyên gia bảo mật phải sao chép một cách tỉ mỉ sự phức tạp của các hệ thống này để xây dựng các môi trường lừa dối phản ánh chính xác bối cảnh công nghệ vận hành.

• Thu hẹp khoảng cách và tăng cường phòng thủ mạng

Việc kết hợp các cuộc thảo luận chuyên sâu về honey-pot không dây và công nghiệp trong bài báo của chúng tôi là một nỗ lực thu hẹp khoảng cách giữa những thách thức về an ninh mạng đang phát triển và việc triển khai các giải pháp tiên tiến chiến lược lừa dối. Bằng cách làm nổi bật các thuộc tính đặc biệt của những các loại honeypot chuyên dụng, công việc của chúng tôi đạt được sự liên quan cao hơn, phù hợp hoàn hảo với trọng tâm hiện đại về bảo vệ mạng không dây mạng lưới và bảo vệ cơ sở hạ tầng công nghiệp quan trọng (Jha, 2023). Việc khám phá những phức tạp trong triển khai, các vectơ tấn công và những lợi thế đa dạng của các honeypot này cung cấp cho bài báo của chúng tôi một cái nhìn toàn diện và toàn cảnh về lĩnh vực đa dạng của honeypot. công nghệ.

7.4. Honeypots dựa trên SDN

Trong bối cảnh của Mạng được xác định bằng phần mềm (SDN) và đám mây tính toán, quản lý tài nguyên hiệu quả và bảo mật mạnh mẽ là rất quan trọng, khiến việc kết hợp honeypot trở nên quan trọng hơn nữa (Javadpour và Wang, 2022; Javadpour và cộng sự, 2023b). Đáng chú ý là trong khi một số loại của nghiên cứu đã khám phá kỹ thuật bắt chước tiên tiến, như được giới thiệu trong tiểu mục 3.1, nhiều nghiên cứu trong số này chủ yếu là tập trung vào việc mô phỏng các chức năng của máy móc trong truyền thống mạng. Thật không may, họ bỏ qua các dịch vụ riêng biệt và các lỗ hổng chỉ có ở môi trường SDN và điện toán đám mây. Một của các tính năng đặc trưng của môi trường SDN và điện toán đám mây mạng là thành phần điều khiển trung tâm của chúng, thường được gọi là SDN bộ điều khiển hoặc bộ điều phối đám mây. Sự tập trung này mang đến một cơ hội hấp dẫn để triển khai các cơ chế lừa dối nhằm bảo vệ mạng lưới. Chúng tôi khuyến nghị các nhà nghiên cứu hướng nỗ lực của họ vào

phát triển các honeypot được thiết kế để mô phỏng chính xác các chức năng của bộ điều khiển SDN và bộ điều phối đám mây. Cách tiếp cận chiến lược này có thể tạo điều kiện cho việc phân tích toàn diện hơn các cuộc tấn công nhắm vào SDN bộ điều khiển và hệ thống quản lý đám mây và đóng góp vào việc phát triển các biện pháp bảo mật chủ động trong mạng điện toán đám mây. HAI CÁC MỐI ĐE DỌA ĐÁNG CHÚ Ý NỔI BẬT trong SDN, điện toán đám mây và giao điểm của chúng: ngộ độc cấu trúc (Adjou et al., 2022; Khoa et al., 2023) và các cuộc tấn công Từ chối dịch vụ phân tán (DDoS) nhắm vào bộ điều khiển hoặc bộ điều phối đám mây. Trong các cuộc tấn công đầu độc cấu trúc, kẻ thù thao túng dữ liệu liên quan đến cấu trúc được trao đổi giữa các công tắc Open-Flow và bộ điều khiển SDN hoặc bộ điều phối đám mây, hiệu quả ngụy trang cấu trúc mạng. Để có được cái nhìn sâu sắc hơn vào chiến thuật được sử dụng trong các cuộc tấn công này, chúng tôi khuyên bạn nên phát triển Các công tắc OpenFlow giả được thiết kế như honeypot. Các công tắc honeypot dễ bị tấn công này sẽ tự nguyện phơi bày bản thân trước các cuộc tấn công đầu độc topol-ogy, cung cấp cho các nhà nghiên cứu thông tin tình báo có giá trị về những mối đe dọa này. Hơn nữa, kẻ thù có thể phát động các cuộc tấn công DDoS chống lại bộ điều khiển SDN, bộ điều phối đám mây hoặc tài nguyên đám mây để làm họ mất khả năng bằng cách áp đảo các kênh truyền thông của họ. Để phân tích và chủ động giảm thiểu các cuộc tấn công như vậy, chúng tôi đề xuất triển khai môi trường SDN với nhiều bộ điều khiển, như minh họa bởi công trình của Javadpour (2020) và nhiều nhà điều phối đám mây trong mạng điện toán đám mây. Sau đó, triển khai bộ điều khiển giả và những người điều phối cùng với những người hợp pháp, với tư cách là người điều khiển và điều phối bẫy, có thể tăng cường khả năng phòng thủ của mạng. Những kẻ điều khiển và điều phối honeypot này có thể tạo ra những thông tin giả mạo lừa đảo các quy tắc về các công tắc và tài nguyên đám mây hoặc tạo ra các công tắc và tài nguyên đám mây để truyền tải các thông điệp trạng thái giả mạo đến họ. Điều này chiến lược chủ động cho phép phát hiện sớm các nỗ lực DDoS và thúc đẩy sự hiểu biết sâu sắc hơn về các chiến thuật được kẻ thù sử dụng nhắm mục tiêu vào bộ điều khiển SDN và bộ điều phối đám mây trong điện toán đám mây mạng lưới. Tóm lại, tích hợp honeypots phù hợp với nhu cầu của môi trường SDN, mạng điện toán đám mây và sự hội tụ hứa hẹn to lớn cho việc nâng cao quản lý tài nguyên và bảo mật trên đám mây. Bằng cách mô phỏng trung thực các bộ điều khiển SDN, các công cụ điều phối đám mây và các thành phần liên quan cũng như triển khai chiến lược các honeypot để chống lại tình trạng đầu độc cấu trúc mạng và các mối đe dọa DDoS, các nhà nghiên cứu và quản trị viên mạng có thể có được những hiểu biết sâu sắc về các lỗ hổng tiềm ẩn và đưa ra các biện pháp đối phó hiệu quả để củng cố mạng điện toán đám mây chống lại các mối đe dọa mạng đang phát triển (Anwar et al., 2022).

7.5. Honeypot dựa trên 5G

Mở rộng việc sử dụng honeypot để tăng cường bảo mật mạng 5G, nó là điều cần thiết để đi sâu hơn vào các lỗ hổng cụ thể liên quan với mỗi thành phần mạng và những lợi ích tiềm năng của việc sử dụng kỹ thuật bắt chước. Đầu tiên và quan trọng nhất, mạng lưới cốt lõi hình thành xương sống của các dịch vụ 5G, bao gồm một loạt các cơ sở hạ tầng vật lý quan trọng. Những máy móc này là mạch sống của kết nối 5G và bất kỳ sự gián đoạn hoạt động của họ có thể gây ra hậu quả sâu rộng. Bằng cách triển khai các honeypot có hiệu quả bắt chước các lõi thiết yếu này các thành phần mạng, chúng ta có thể chuyển hướng sự tập trung của những kẻ thù tiềm tàng tránh xa tài sản thực sự. Sự chuyển hướng này là một biện pháp ngăn chặn và cung cấp một cơ hội duy nhất để thu thập thông tin tình báo về các mối đe dọa tiềm tàng, phương pháp tấn công và kẻ thù. Di chuyển mạng truy cập vô tuyến đại diện cho một liên kết quan trọng trong chuỗi 5G, bao gồm các kết nối và giao diện không dây. Mặc dù đã có một số sự công nhận về nhu cầu để bảo đảm khía cạnh này của mạng, các chiến lược triển khai chi tiết và đánh giá hiệu suất vẫn còn thiếu (Javadpour et al., 2023c; Benzaïd và cộng sự, 2022). Điều này nhấn mạnh tầm quan trọng của việc tiếp tục nghiên cứu và phát triển trong lĩnh vực này. Honeypots được thiết kế để các thành phần mạng truy cập vô tuyến bắt chước có thể vô cùng hữu ích trong việc bảo vệ các thành phần này và hiểu rõ hơn về cách kẻ thù nhắm mục tiêu chúng. Hơn nữa, vai trò của honeypot phía máy khách trong việc xác định các lỗ hổng trong các thiết bị đầu cuối không thể bị đánh giá thấp. Những thiết bị này, thường được coi là điểm tương tác cuối cùng trong mạng 5G, dễ bị tổn thương trước nhiều mối đe dọa bảo mật khác nhau. Honeypot phía máy khách có thể mô phỏng những điều này thiết bị, tạo ra một vùng đệm chống lại các cuộc tấn công tiềm ẩn và thu thập dữ liệu về các chiến thuật được sử dụng bởi những kẻ xấu. Việc tích hợp các honeypot chuyên dụng, được thiết kế để mô phỏng các thành phần mạng 5G khác nhau, cung cấp một cách tiếp cận đa diện để tăng cường bảo mật mạng. Bằng cách giải quyết toàn diện các lỗ hổng ở nhiều cấp độ khác nhau của 5G kiến trúc, chúng tôi củng cố mạng lưới chống lại các mối đe dọa tiềm ẩn và đạt được hiểu biết sâu sắc hơn về bối cảnh mối đe dọa đang phát triển. Kiến thức này sau đó có thể được sử dụng để tinh chỉnh các biện pháp bảo mật và cuối cùng đảm bảo sự mạnh mẽ và khả năng phục hồi của mạng 5G trong thời đại công nghệ phát triển nhanh chóng và thách thức an ninh mạng ngày càng tăng (Kheir và cộng sự, 2022).

7.6. Honeypot và botnet

Trong tiểu mục 3.2, chúng tôi đã trình bày nghiên cứu về honeypot hợp tác với kẻ thù và giả vờ giúp đỡ kẻ thù. Tuy nhiên, các honeypot được đề cập với kỹ thuật lừa dối hợp tác có thể được cải thiện nhiều hơn nữa. Các botnet và các mối đe dọa phức tạp là ngày càng phát triển, cung cấp cho chúng ta nhiều thông tin hơn về hành vi của chúng. các nhà nghiên cứu có thể sử dụng thông tin này để thiết kế các honeypot mạnh mẽ lừa dối trong việc hợp tác với kẻ thù. Các honeypot có thể là được thiết kế để cung cấp cho kẻ thù sự trợ giúp giả mạo trong các giai đoạn khác nhau vòng đời của botnet.

Có thể rất khó để hợp tác với một botmaster. Bởi vì một số botnet rất phức tạp và có nhiều loại thành viên khác nhau. Do đó, chúng tôi đề xuất các nhà nghiên cứu xác định các thành viên botnet khác nhau trong một mạng lưới và vai trò của họ để hợp tác hiệu quả với họ. Ví dụ, một trong những thành viên trong mạng botnet dựa trên trình tải, chẳng hạn như Mirai, là trình tải. Các bot thăm dò toàn bộ mạng và sau đó báo cáo tên người dùng và mật khẩu máy chủ bị xâm nhập. Sau đó, trình tải sẽ lây nhiễm máy chủ với tập lệnh phần mềm độc hại. Trong các mạng bot như vậy, chúng tôi đề xuất các honey-pot hoạt động như một bot và báo cáo các cặp thông tin xác thực của một honeypot khác đến bộ nạp. Trong điều kiện này, thông tin xác thực là hợp lệ và bộ nạp tin rằng honeypot đang ở bên cạnh mình.

7.7. Honeypot phân tán

Kỹ thuật chuyển hướng lưu lượng (được trình bày trong tiểu mục 3.6) là được triển khai rộng rãi trong các mạng lừa đảo khác nhau. Tuy nhiên, tình trạng tắc nghẽn giao thông hướng đến các honeypot không được phân tích. Để cải thiện hiệu suất của honeypots trong một mạng lưới có chi phí hạn chế, chúng tôi đề xuất các nhà nghiên cứu làm việc trên các cơ chế ảo hóa như mạng ảo các khái niệm nhúng công việc, được Javadpour và Wang sử dụng (2022) và Javadpour (2019), để phân phối hiệu quả các chức năng của honeypot và lưu lượng truy cập của nó giữa các nút mạng khác nhau và đường dẫn tương ứng. Điều này sẽ giúp họ sử dụng lượng tài nguyên tối thiểu có thể. Trước tiên, phải phân tích lưu lượng truy cập và sau đó chuyển hướng đến nút thích hợp.

Việc đồng bộ hóa các honeypot phân tán và bảo mật kết nối của chúng là một thách thức. Do đó, các nhà nghiên cứu phải làm việc trên các kênh truyền thông được bảo vệ, chẳng hạn như blockchain, để đồng bộ hóa các honeypot được phân phối một cách an toàn.

7.8. Học honeynet

Đa dạng hóa các honeypot và định vị chúng trong mạng lưới honeynet (được đề cập trong tiểu mục 5.2 và tiểu mục 5.3) là hai kỹ thuật đánh lừa mà chúng tôi cho rằng có thể được cải thiện bằng các phương pháp học máy.
Chúng tôi đề xuất các nhà nghiên cứu thu thập thông tin hữu ích để tạo ra một mô hình học tập có thể dự đoán các dịch vụ thường được nhắm mục tiêu bởi mối đe dọa hiện tại lan truyền trên mạng. Dự đoán này giúp các honeypot để mô phỏng các dịch vụ có thể thu hút kẻ thù tại một tỷ lệ cao hơn.

Điểm đầu tiên cần lưu ý là một số máy học các mô hình dễ bị tấn công mạng (Benzaïd và Taleb, 2020). Nếu những mô hình này không được thiết kế dựa trên các yếu tố bảo mật, chúng có thể gây rủi ro honeypots extra. Do đó, các nhà nghiên cứu phải xem xét các cơ chế bảo vệ trong việc phát triển các mô hình máy học honeypot.
Điểm khác là việc đào tạo mô hình không được gây ra thêm trên cao đến một mạng lưới mật ong. Các mô hình nhẹ là lựa chọn tốt cho đang được sử dụng trong mạng lưới mật ong.

Gợi ý khác là thay đổi vị trí của các hon-eypot trong mạng lưới mật ong một cách linh hoạt, dẫn đến chi phí triển khai thấp hơn và hiệu quả cao hơn trong việc lãng phí thời gian của đối thủ. Ngược lại ta có thể sử dụng Di chuyển Các khái niệm Phòng thủ Mục tiêu (MTD) để thay đổi tập hợp tối ưu của honey-pot. Các phương pháp MTD cố gắng thay đổi bề mặt tấn công bằng cách thay đổi vị trí của các mục tiêu của đối thủ. Tuy nhiên, sử dụng các khái niệm MTD là thách thức vì những thay đổi có thể cảnh báo đối thủ về các sự kiện bất thường trong mạng. Do đó, các nhà phát triển phải chú ý đến tần số xáo trộn của honeypot để che giấu những thay đổi từ đối thủ. Các mô hình học máy có thể được đào tạo để tìm tần số xáo trộn tối ưu. Một điều khác có thể được xem xét đối với honeypots là vị trí của chúng trong mạng vệ tinh. Theo cách này, triển khai các honeypot khác nhau có thể ngăn chặn các cuộc tấn công DoS và DDoS. Và khi sử dụng phương pháp MTD, tỷ lệ chấp nhận vào mạng sẽ giảm.

7.9. Hiểu các loại lỗ hổng trong an ninh mạng

Trong bối cảnh năng động của an ninh mạng, điều bắt buộc là phải nhận ra rằng không phải tất cả các lỗ hổng đều được tạo ra như nhau. Tầm quan trọng và sức hấp dẫn của một điểm yếu đối với những kẻ thù tiềm năng có thể khác nhau đáng kể, và khía cạnh sắc thái này có ý nghĩa sâu sắc đối với các chiến lược an ninh mạng. Trong khi nghiên cứu của chúng tôi tập trung vào hiệu suất và tối ưu hóa trong bối cảnh của honeynet, chúng tôi thừa nhận một điều quan trọng chiều hướng cần được kết hợp - ảnh hưởng của tính dễ bị tổn thương các loại động cơ và hành vi của kẻ tấn công. Sự bổ sung này có thể cung cấp hiểu biết toàn diện hơn về hiệu quả của honeynet trong việc phòng thủ chống lại các loại lỗ hổng cụ thể (Jones, 2022; McCoy, 2022).

• Tích hợp các loại lỗ hổng (Agarwal, 2022): Để giải quyết vấn đề này khía cạnh quan trọng, chúng tôi đề xuất mở rộng khuôn khổ nghiên cứu của chúng tôi để kết hợp các loại lỗ hổng như một yếu tố trong phân tích của chúng tôi. Đáng chú ý, các lỗ hổng như EternalBlue và Log4j có mức độ hấp dẫn khác nhau đối với những kẻ tấn công tiềm năng do các yếu tố như khả năng khai thác, tiềm năng để có tác động rộng rãi và các ưu đãi tài chính. Phân tích của chúng tôi sẽ hướng tới để phân biệt giữa các loại lỗ hổng này và khi làm như vậy, cung cấp những hiểu biết có giá trị về cách hiệu quả của honeynet có thể thay đổi trước những lợi ích đối nghịch rõ ràng.

• Liên quan đến Nghiên cứu Hiện tại: Trong khi nghiên cứu của chúng tôi đã đặt ra nền tảng để tối ưu hóa honeynet, xem xét các đối thủ khác nhau lợi ích dựa trên các loại lỗ hổng là một thành phần thiết yếu cho một hiểu biết toàn diện về hiệu suất honeynet. Phần mở rộng này không chỉ làm tăng thêm chiều sâu cho cuộc điều tra của chúng tôi mà còn củng cố tính thực tế khả năng áp dụng các phát hiện của chúng tôi. Bằng cách đưa vào chiều hướng này, chúng tôi hướng tới cung cấp một góc nhìn sắc thái hơn về hiệu quả của mạng lưới mật ong trong bối cảnh an ninh mạng đang không ngừng phát triển (Rich, 2023).

• Việc kết hợp chiều hướng này vào nghiên cứu của chúng tôi sẽ liên quan đến việc phân loại các lỗ hổng thành các loại riêng biệt dựa trên mức độ hấp dẫn của chúng đối với những kẻ thù tiềm năng. Sau đó chúng tôi sẽ tiến hành phân tích tập trung trên các danh mục này, đánh giá cách thức hoạt động của honeynet và có thể được tối ưu hóa khác nhau cho từng loại lỗ hổng. Phương pháp luận của chúng tôi sẽ kết hợp dữ liệu thực tế và mô phỏng để chứng minh những phát hiện của chúng tôi.

• EternalBlue: EternalBlue là một lỗ hổng phần mềm khét tiếng đã trở nên khét tiếng do có liên quan đến cuộc tấn công ransomware WannaCry toàn cầu vào năm 2017. Ban đầu được Cơ quan An ninh Quốc gia Hoa Kỳ (NSA) xác định, lỗ hổng này nhắm vào Windows hệ điều hành. EternalBlue cho phép những kẻ xấu khai thác một Lỗ hổng giao thức Server Message Block (SMB), cho phép chúng lan truyền phần mềm độc hại và thực thi mã tùy ý từ xa trên các hệ thống dễ bị tấn công. Tác động đáng kể và sự lây lan nhanh chóng của WannaCry đã làm sáng tỏ nhu cầu cấp thiết về việc vá lỗi phần mềm kịp thời và an ninh mạng hiệu quả biện pháp (Riggs và cộng sự, 2023; Ibrahim và cộng sự, 2023).

• Log4j: Log4j, trước đây được gọi là Apache Log4j, là một thư viện ghi nhật ký nguồn mở cho các ứng dụng Java. Vào tháng 12 năm 2021, một lỗ hổng bảo mật nghiêm trọng, thường được gọi là “Log4Shell” hoặc “Log4j lỗ hổng bảo mật,” đã được phát hiện trong Log4j. Lỗ hổng bảo mật này, được theo dõi như CVE-2021-44228, cho phép kẻ tấn công thực thi mã tùy ý từ xa bằng cách khai thác khả năng xử lý các mục nhật ký của thư viện. Lỗ hổng Log4j đã gây ra những lo ngại đáng kể trong cộng đồng an ninh mạng do nó được sử dụng rộng rãi trong các ứng dụng Java, được sử dụng trong nhiều hệ thống và dịch vụ quan trọng. Nó nhấn mạnh tầm quan trọng của việc vá lỗi nhanh chóng và quản lý lỗ hổng trước sự xuất hiện các mối đe dọa (Rossotti, 2022; Feng và Lubis, 2022).

8. Kết luận và đề xuất

Cuộc khảo sát này cung cấp một cuộc khám phá chi tiết về nghiên cứu honeypot trên hai thập kỷ qua. Chúng tôi bắt đầu bằng cách giải thích các khái niệm cơ bản làm nền tảng cho honeypot, đóng vai trò là cơ sở để phân loại và phân tích các cơ chế bảo mật này dựa trên mục đích, chế độ của chúng của tương tác, phương pháp thực hiện, hoạt động vận hành, các bên liên quan tham gia, tính nhất quán và đồng nhất. Các danh mục này cung cấp một khuôn khổ có cấu trúc để hiểu các honeypot và cung cấp thông tin chi tiết cho các nhà phát triển cần chọn loại phù hợp nhất cho nhu cầu bảo mật cụ thể của họ. Khi chúng tôi nỗ lực cải thiện hiệu quả của honeypot, chúng tôi đã tiến hành một cuộc điều tra kỹ lưỡng về các kỹ thuật lừa dối có thể nâng cao hiệu suất của từng honeypot. Các kỹ thuật này có thể được tổ chức thành sáu nhóm, mỗi nhóm với các chiến lược độc đáo có thể được sử dụng để tránh bị phát hiện và thu hút mối đe dọa tiềm ẩn. Sáu nhóm bao gồm bắt chước nâng cao, hợp tác giả mạo, thao túng Cơ sở dữ liệu lừa đảo, gián đoạn tinh vi, honeytoken baiting và chuyển hướng lưu lượng truy cập. Để đánh giá hiệu quả của các kỹ thuật bảo mật, chúng tôi đề xuất một bộ số liệu đo lường được thiết kế để mạnh mẽ và thiết thực trong nhiều tình huống khác nhau. Chúng tôi cũng kiểm tra các kỹ thuật lừa dối khác nhau được sử dụng trong honeynet và cách chúng có thể nâng cao hiệu suất của chúng. Các kỹ thuật này được nhóm thành các danh mục dựa trên mục đích của chúng: tối ưu hóa, đa dạng hóa, vị trí, động hóa và định hình honeypots trong mạng. Chúng tôi tóm tắt các nghiên cứu và mô hình có liên quan trong từng danh mục để cho phép phân tích so sánh. Để đơn giản hóa quá trình này, chúng tôi đề xuất một mô hình chung để giúp lựa chọn cách tiếp cận phù hợp nhất cho một mục đích nhất định bối cảnh. Để khám phá tính thực tiễn của các kỹ thuật lừa dối quan trọng, chúng tôi tiến hành các kịch bản mô phỏng bằng Python. Các mô phỏng này cung cấp những hiểu biết có giá trị về các kết quả tiềm năng và hiệu quả của việc triển khai cơ chế lừa dối trong môi trường mạng. Sau khi khảo sát kết luận, chúng tôi nhấn mạnh các vấn đề và thách thức còn bỏ ngỏ cần được giải quyết thêm điều tra trong khi cung cấp các khuyến nghị chiến lược cho bối cảnh phát triển của các kỹ thuật lừa đảo honeypot và honeynet. Điều này tài liệu tổng hợp là một nguồn tài nguyên có giá trị cho các nhà nghiên cứu và học viên trong lĩnh vực an ninh mạng đang không ngừng phát triển, phục vụ mục đích thông tin và truyền cảm hứng những tiến bộ.

Tuyên bố đóng góp tác giả CRediT

Amir Javadpour: Khái niệm hóa, Quản lý dữ liệu, Phân tích chính thức, Thu hút tài trợ, Điều tra, Phương pháp luận, Quản lý dự án, Tài nguyên, Phần mềm, Giám sát, Xác thực, Hình dung, Viết – bản thảo gốc, Viết – đánh giá & biên tập. Forough Ja'-fari: Quản lý dữ liệu, Phương pháp luận, Giám sát, Viết – bản thảo gốc. Tarik Taleb: Tài nguyên, Viết – bản thảo gốc, Viết – đánh giá & biên tập. Mohammad Shojafar: Điều tra, Viết – bản thảo gốc, Viết – đánh giá & biên tập. Chafika Benzaïd: Quản lý dữ liệu, Điều tra, Hình ảnh hóa, Viết – đánh giá & biên tập.

Tuyên bố về lợi ích cạnh tranh

Các tác giả tuyên bố rằng họ không có bất kỳ mối quan hệ cá nhân hoặc lợi ích tài chính cạnh tranh nào có thể ảnh hưởng đến công trình được trình bày trong bài báo này.

Tính khả dụng của dữ liệu

Không có dữ liệu nào được sử dụng cho nghiên cứu được mô tả trong bài viết.

Sự thừa nhận

Công trình nghiên cứu này được hỗ trợ một phần bởi chương trình nghiên cứu và đổi mới Horizon Europe của Liên minh châu Âu HORIZON-JU-SNS-2022 theo dự án RIGOUROUS (Số tài trợ 101095933). Bài báo chỉ phản ánh quan điểm của tác giả. Ủy ban không chịu trách nhiệm về bất kỳ việc sử dụng nào có thể được thực hiện đối với thông tin mà bài báo có.

Tài liệu tham khảo

Abay, NC, Akcora, CG, Zhou, Y., Kantarcioglu, M., Thuraisingham, B., 2019. Sử dụng học sâu để tạo honeydata quan hệ. Trong: Lừa đảo mạng tự động. Springer, trang. 3–19.

Abdulqadder, IH, Zou, D., Aziz, IT, 2023. Chuỗi khối dag: honeypot hỗ trợ biên an toàn để phát hiện tấn công và cân bằng tải dựa trên nhiều bộ điều khiển trong sdn 5g. Hệ thống máy tính thế hệ tương lai 141, 339–354.

Achleitner, S., La Porta, TF, McDaniel, P., Sugrim, S., Krishnamurthy, SV, Chadha, R., 2017. Đánh lừa trinh sát mạng bằng cách sử dụng các cấu trúc mạng ảo dựa trên sdn. IEEE Trans. Netw. Serv. Manag. 14 (4), 1098–1112.

Ackerman, P., 2020. Thực hành an ninh mạng hiện đại: Khám phá và triển khai các khuôn khổ và chiến lược an ninh mạng linh hoạt cho tổ chức của bạn. Ấn phẩm BPB.

Adjou, ML, Benzaïd, C., Taleb, T., 2022. Topotrust: khám phá cấu trúc mạng an toàn và không cần tin cậy dựa trên blockchain trong sdns. Trong: 2022 International Wireless Communications and Mobile Computing (IWCMC), tr. 1107–1112.

Agarwal, Y., 2022. Khung ghi nhật ký Apache Log4j và lỗ hổng của nó.

Akingbola, Dahunsi, Alese, Adewale, Ogundele, 2015. Cải thiện khả năng lừa dối trong honeynet thông qua thao tác dữ liệu. J. Công nghệ Internet Bảo vệ. Bản dịch 4, 373–379.

Akiyama, M., Yagi, T., Hariu, T., Kadobayashi, Y., 2018. Honeycirculator: phân phối thông tin xác thực honeytoken để tự kiểm tra chu kỳ tấn công dựa trên web. Int. J. Inf. Secur. 17 (2), 135–151.

Almeshekah, MH, Spafford, EH, 2014. Lên kế hoạch và tích hợp sự lừa dối vào các biện pháp phòng thủ an ninh máy tính. Trong: Biên bản Hội thảo về các mô hình an ninh mới năm 2014 , trang 127–138.

Almeshekah, MH, Spafford, EH, 2016. Lừa đảo an ninh mạng. Trong: Lừa đảo mạng. Springer, trang. 25–52.

Almeshekah, MH, Spafford, EH, Atallah, MJ, 2013. Cải thiện an ninh bằng cách lừa dối. Trung tâm Giáo dục và Nghiên cứu Đảm bảo và An ninh Thông tin, Đại học Purdue, Tech. Rep. CERIAS Tech Report, tập 13. trang 2013.

Alosefer, Y., Rana, O., 2010. Honeyware: một honeypot khách hàng tương tác thấp dựa trên web. Trong: Hội nghị quốc tế lần thứ ba năm 2010 về thử nghiệm phần mềm, xác minh và xác thực. IEEE, trang 410–417.

Althonayan, A., Andronache, A., 2019. Khả năng phục hồi dưới tầm nhìn chiến lược: tác động của quản lý an ninh mạng và sự liên kết quản lý rủi ro doanh nghiệp. Trong: Hội nghị quốc tế năm 2019 về Nhận thức tình huống mạng, Phân tích dữ liệu và Đánh giá (Cyber SA). IEEE, trang 1–9.

Alyas, T., Alissa, K., Alqahtani, M., Faiz, T., Alsaif, SA, Tabassum, N., Naqvi, HH, 2022. Khung bảo mật tích hợp đa đám mây sử dụng honeypot. Mob. Inf. Syst. 2022, 1–13.

Anwar, AH, Kamhoua, C., Leslie, N., 2019. Một khuôn khổ lý thuyết trò chơi cho sự lừa dối mạng động trong Internet của các vật thể chiến trường. Trong: Biên bản báo cáo của Hội nghị quốc tế EAI lần thứ 16 về Hệ thống di động và phổ biến: Máy tính, Mạng và Dịch vụ, trang 522–526.

Anwar, AH, Kamhoua, C., Leslie, N., 2020. Phân bổ Honeypot trên biểu đồ tấn công trong trò chơi lừa đảo mạng. Trong: Hội nghị quốc tế về máy tính, mạng và truyền thông năm 2020 (ICNC). IEEE, trang 502–506.

Anwar, AH, Kamhoua, CA, Leslie, NO, Kiekintveld, C., 2022. Phân bổ Honeypot cho lừa đảo trên mạng trong điều kiện không chắc chắn. IEEE Trans. Netw. Serv. Manag. 19 (3), 3438–3452.

http://dx.doi.org/10.1037/0021-843X.102.2.23 Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopou- los, AV, Di Franco, F., 2023. Vai trò của máy học trong an ninh mạng. Chữ số. Xử lý Res. Pract. 4 (1), 1–38.

Argyratos, T., 2021. Phân tích lý thuyết thông tin về sự lừa dối và quyết định trong mạng lưới. Luận án tiến sĩ. Đại học Aristotle ở Thessaloniki.

Ayeni, O., Alese, B., Omotosho, L., 2013. Thiết kế và triển khai một phương tiện truyền thông hành động honeypot. Int. J. Comput. Appl. 975, 8887.

Badr, Y., Hariri, S., Youssif, A.-N., Blasch, E., 2015. Các dịch vụ hệ thống ứng dụng dữ liệu động (dddas) đáng tin cậy và linh hoạt cho môi trường quản lý khủng hoảng . Proc. Comput. Sci. 51, 2623–2637.

Bedi, HS, Roy, S., Shiva, S., 2011. Cơ chế phòng thủ dựa trên lý thuyết trò chơi chống lại các cuộc tấn công ddos vào các luồng thân thiện với tcp/tcp. Trong: Hội nghị chuyên đề IEEE năm 2011 về Trí tuệ tính toán trong An ninh mạng (CICS). IEEE, trang 129–136.

Benzaïd, C., Taleb, T., 2020. AI cho mạng lưới vượt ra ngoài 5g: phòng thủ an ninh mạng hoặc công cụ hỗ trợ hàng rào? IEEE Netw. 34 (6), 140–147.

Benzaïd, C., Taleb, T., Song, J., 2022. Kiến trúc quản lý bảo mật tự động và có thể mở rộng dựa trên AI để phân chia mạng an toàn trong b5g. IEEE Netw. 36 (6), 165–174.

Bercovitch, M., Renford, M., Hasson, L., Shabtai, A., Rokach, L., Elovici, Y., 2011. Honey -gen: một trình tạo honeytokens tự động. Trong: Biên bản báo cáo Hội nghị quốc tế IEEE năm 2011 về tin học tình báo và an ninh. IEEE, trang 131–136.

Biedermann, S., Mink, M., Katzenbeisser, S., 2012. Honeypots trích xuất động nhanh trong điện toán đám mây. Trong: Biên bản Hội thảo ACM năm 2012 về Hội thảo bảo mật điện toán đám mây, trang 13–18.

Bilinski, M., Gabrys, R., Mauger, J., 2018. Vị trí tối ưu của honeypot để bảo vệ mạng. Trong: Hội nghị quốc tế về Quyết định và Lý thuyết trò chơi cho An ninh. Springer, trang 115–126.

Bowen, BM, Hershkop, S., Keromytis, AD, Stolfo, SJ, 2009. Nhử kẻ tấn công bên trong bằng cách sử dụng tài liệu mồi nhử. Trong: Bảo mật và quyền riêng tư trong mạng truyền thông: Hội nghị quốc tế ICST lần thứ 5. SecureComm 2009, Athens, Hy Lạp, ngày 14–18 tháng 9 năm 2009, Các bài báo đã chọn đã sửa đổi 5. Springer, trang 51–70.

Bringer, ML, Chelmecki, CA, Fujinoki, H., 2012. Một cuộc khảo sát: những tiến bộ gần đây và xu hướng tương lai trong nghiên cứu honeypot. Int. J. Comput. Netw. Inf. Secur. 4 (10), 63.

Cai, J.-Y., Yegneswaran, V., Alfeld, C., Barford, P., 2009. Một trò chơi tấn công-phòng thủ cho lừa đảo mật ong. Trong: COCOON. Springer, trang 7–16.

Cantella, E., 2021. Phong cách kiến trúc: Biến dạng khi triển khai và quản lý công nghệ lừa dối trong hệ thống phần mềm. Học viện công nghệ Rochester.

Carroll, TE, Grosu, D., 2011. Một cuộc điều tra lý thuyết trò chơi về sự lừa dối trong bảo mật mạng. Secur. Commun. Netw. 4 (10), 1162–1172. Çeker, H., Zhuang, J.,

Upadhyaya, S., La, QD, Soong, B.-H., 2016. Phương pháp tiếp cận lý thuyết trò chơi dựa trên sự lừa dối để giảm thiểu các cuộc tấn công dos. Trong: Hội nghị quốc tế về Quyết định và Lý thuyết trò chơi cho Bảo mật. Springer, trang 18–38.

Chakraborty, T., Jajodia, S., Katz, J., Picariello, A., Sperli, G., Subrahmanian, V., 2019. Forge: công cụ tạo kho lưu trữ trực tuyến giả mạo để lừa đảo trên mạng. IEEE Trans. Máy tính an toàn đáng tin cậy.

Chen, TM, Buford, J., 2009. Cân nhắc thiết kế cho honeypot cho các cuộc tấn công tiêm nhiễm SQL. Trong: Hội nghị IEEE lần thứ 34 năm 2009 về Mạng máy tính cục bộ. IEEE, trang 915–921.

Chung, M.-H., Yang, Y., Wang, L., Cento, G., Jerath, K., Raman, A., Lie, D., Chignell, MH, 2023. Triển khai phòng thủ chống rò rỉ dữ liệu tại chỗ: khảo sát các biện pháp đối phó và sự tham gia của con người. ACM Comput. Surv.

Conti, M., Trolese, F., Turrin, F., 2022. Icspot: honeypot tương tác cao cho các hệ thống điều khiển công nghiệp. Trong: Hội nghị chuyên đề quốc tế năm 2022 về mạng, máy tính và truyền thông (ISNCC). IEEE, trang 1–4.

Cranford, E., Ou, H.-C., Gonzalez, C., Tambe, M., Lebiere, C., 2023. Kế toán cho Un- sự chắc chắn trong việc phát tín hiệu lừa đảo nhằm mục đích an ninh mạng.

Crochelet, P., Neal, C., Cuppens, NB, Cuppens, F., 2022. Quy kết kẻ tấn công thông qua suy luận đặc điểm sử dụng dữ liệu honeypot. Trong: Hội nghị quốc tế về an ninh mạng và hệ thống. Springer, trang 155–169.

Crouse, M., Prosser, B., Fulp, EW, 2015. Phân tích hiệu suất xác suất của phòng thủ trinh sát mục tiêu di động và đánh lừa. Trong: Biên bản Hội thảo ACM lần thứ hai về Phòng thủ mục tiêu di động. ACM, trang 21–29.

Crouse, MB, 2012. Phân tích hiệu suất của lừa đảo trên mạng bằng cách sử dụng các mô hình xác suất . Luận văn thạc sĩ. Trường sau đại học về nghệ thuật và khoa học của Đại học Wake Forest, Winston-Salem, Bắc Carolina.

Dahbul, R., Lim, C., Purnama, J., 2017. Tăng cường khả năng đánh lừa honeypot thông qua dấu vân tay dịch vụ mạng. Trong: Tạp chí Vật lý: Chuỗi hội nghị, tập 801. Nhà xuất bản IOP, trang 012057.

Dalamagkas, C., Sarigiannidis, P., Ioannidis, D., Iturbe, E., Nikolis, O., Ramos, F., Rios, E., Sarigiannidis, A., Tzovaras, D., . Trong: Hội nghị IEEE năm 2019 về Phần mềm hóa mạng (Net- Soft). IEEE, trang 1-12. 93–100.

Dantu, R., Cangussu, JW, Patwardhan, S., 2007. Ngăn chặn gian nhanh bằng cách sử dụng phản hồi kiểm soát. IEEE Trans. Máy tính an toàn đáng tin cậy. 4 (2), 119–136.

De Faveri, C., Moreira, A., 2016. Thiết kế các chiến lược lừa dối thích ứng. Trong: Hội nghị quốc tế IEEE năm 2016 về chất lượng phần mềm, độ tin cậy và bảo mật Companion (QRS-C). IEEE, trang 77–84.

De Faveri, C., Moreira, A., Amaral, V., 2018. Mô hình lừa dối đa mô hình cho phòng thủ mạng. J. Syst. Softw. 141, 32–51.

de Nobrega, K., 2023. Năng lực và khả năng phòng thủ mạng:: Quan điểm từ Ngành tài chính của một quốc gia nhỏ.

Domingue, MJ, Lakhtakia, A., Pulsifer, DP, Hall, LP, Badding, JV, Bischof, JL, Martín-Palma, RJ, Imrei, Z., Janik, G., Mastro, VC, et al., 2014. Các đặc điểm thị giác được sao chép sinh học của mồi nhử bọ cánh cứng buprestid được chế tạo bằng nano gợi lên các chuyến bay giao phối khuôn mẫu của con đực . Proc. Natl. Acad. Sci. 111 (39), 14 106–14 111.

Doubleday, H., Maglaras, L., Janicke, H., 2016. Ssh Honeypot: Xây dựng, Triển khai và Phân tích.

Dowling, S., Schukat, M., Barrett, E., 2018. Sử dụng học tăng cư ờng để che giấu chức năng honeypot. Trong: Hội nghị chung châu Â u về học máy và khám phá kiến thức trong cơ sở dữ liệu. Springer, trang 341–355.

Drew, SK, Heinen, CW, 2022. Kiểm tra sự lừa dối bằng một công cụ thư ơng mại mô phỏng không gian mạng. Luận án tiến sĩ, Monterey, CA; Trư ờng Sau đại học Hải quân.

Durkota, K., Lisy,` V., Bošansky,` B., Kiekintveld, C., 2015a. Tăng cư ờng bảo mật mạng tối ư u bằng cách sử dụng trò chơi đồ thị tấn công. Trong: Hội nghị chung quốc tế lần thứ hai mư ơi bốn về trí tuệ nhân tạo.

Durkota, K., Lisy,` V., Bošansky,` B., Kiekintveld, C., 2015b. Các giải pháp gần đúng cho trò chơi đồ thị tấn công với thông tin không hoàn hảo. Trong: Hội nghị quốc tế về Quyết định và Lý thuyết trò chơi cho An ninh. Springer, trang 228–249.

Erguler, I., 2016. Đạt đư ợc sự phẳng: chọn mật khẩu từ mật khẩu ngư ời dùng hiện có. IEEE Trans. Máy tính bảo mật đáng tin cậy. 13 (2), 284–295.

Eriksson, O., 2023. Đánh giá Honeypot với Kubernetes tư ơng thích.

Fan, W., Fernández, D., 2017. Một cơ chế chuyển giao kết nối tcp tàng hình dựa trên sdn mới cho các hệ thống honeypot lai. Trong: Hội nghị IEEE năm 2017 về phần mềm hóa mạng (NetSoft). IEEE, trang 1–9.

Fan, W., Du, Z., Fernández, D., 2015. Phân loại các giải pháp honeynet. Trong: 2015 SAI Hội nghị Hệ thống thông minh (IntelliSys). IEEE, trang 1002–1009.

Fan, W., Du, Z., Fernández, D., Villagra, VA, 2017a. Cho phép xem giải phẫu để điều tra các hệ thống honeypot: một cuộc khảo sát. IEEE Syst. J. 12 (4), 3906–3919.

Fan, W., Fernández, D., Du, Z., 2017b. Khung quản lý honeynet ảo đa năng . Thông tin bảo mật của IET 11 (1), 38–45.

Fan, W., Du, Z., Smith-Creasey, M., Fernandez, D., 2019. Honeydoc: kiến trúc honeypot hiệu quả cho phép thiết kế toàn diện. IEEE J. Sel. Areas Commun. 37 (3), 683–697.

Faveri, CD, 2022. Mô hình hóa sự lừa dối trong an ninh mạng.

Feng, S., Lubis, M., 2022. Chiến lư ợc bảo mật phòng thủ chuyên sâu trong phân tích lỗ hổng log4j . Trong: Hội nghị quốc tế năm 2022 về sự tiến bộ trong khoa học dữ liệu, học tập điện tử và hệ thống thông tin (ICADEIS). IEEE, trang 01–04.

Ferguson-Walter, KJ, Major, MM, Johnson, CK, Muhleman, DH, 2021. Kiểm tra hiệu quả của trò lừa đảo mạng dựa trên mồi nhử và tâm lý. Trong: Hội nghị chuyên đề bảo mật USENIX lần thứ 30 (USENIX Security 21), trang 1127–1144.

Ferguson-Walter, KJ, Major, MM, Johnson, CK, Johnson, CJ, Scott, DD, Gutzwiller, RS, Shade, T., 2023. Phản hồi của chuyên gia an ninh mạng: kinh nghiệm, kỳ vọng và ý kiến về lừa đảo trên mạng. Comput. Secur. 130, 103268.

Ferretti, P., Pogliani, M., Zanero, S., 2019. Đặc trư ng tiếng ồn nền trong lư u lư ợng ics thông qua một tập hợp các honeypot tư ơng tác thấp. Trong: Biên bản Hội thảo ACM về An ninh & Quyền riêng tư của Hệ thống mạng vật lý, trang 51–61.

Fraunholz, D., Schotten, HD, 2018a. Bảo vệ máy chủ web bằng cách đánh lừa, gây mất tập trung và che giấu. Trong: Hội nghị quốc tế về máy tính, mạng và truyền thông năm 2018 (ICNC). IEEE, trang 21–25.

Fraunholz, D., Schotten, HD, 2018b. Phòng thủ và tấn công chiến lư ợc trong an ninh mạng dựa trên sự lừa dối. Trong: Hội nghị quốc tế về mạng thông tin năm 2018 (ICOIN). IEEE, trang 156–161.

Fraunholz, D., Krohmer, D., Anton, SD, Schotten, HD, 2017. Điều tra tội phạm mạng đư ợc thực hiện bằng cách lạm dụng mật khẩu yếu hoặc mặc định với honeypot tư ơng tác trung bình . Trong: Hội nghị quốc tế năm 2017 về an ninh mạng và bảo vệ dịch vụ kỹ thuật số (An ninh mạng). IEEE, trang 1–7.

Fraunholz, D., Anton, SD, Lipps, C., Reti, D., Krohmer, D., Pohl, F., Tammen, M., Schotten, HD, 2018. Làm sáng tỏ công nghệ lừa dối: một cuộc khảo sát. Bản in trư ớc của arXiv. arXiv:1804.06196.

Ganesarathinam, R., Prabakar, MA, Singaravelu, M., Fernandez, AL, 2020. Phân tích chi tiết các hoạt động của kẻ xâm nhập trong mạng thông qua thử nghiệm honeynet ảo thời gian thực . Trong: Trí tuệ nhân tạo và tính toán tiến hóa trong hệ thống kỹ thuật. Springer, trang 39–53.

Garg, N., Grosu, D., 2007. Lừa dối trong honeynet: phân tích lý thuyết trò chơi. Trong: Hội thảo về bảo mật và đảm bảo thông tin IEEE SMC năm 2007. IEEE, trang 107–113.

Gautam, R., Kumar, S., Bhattacharya, J., 2015. Honeynet ảo đư ợc tối ư u hóa với việc triển khai máy chủ như honeywall. Trong: Hội nghị thư ơng niên IEEE Ấn Độ năm 2015 (INDICON). IEEE, trang 1–6.

Gjermundrød, H., Dionysiou, I., 2015. Cloudhoneycy-một khuôn khổ honeypot tích hợp cho cơ sở hạ tầng đám mây. Trong: Hội nghị quốc tế lần thứ 8 về Tiện ích và Điện toán đám mây (UCC) của IEEE/ACM năm 2015. IEEE, trang 630–635.

Gonzalez, C., Aggarwal, P., Cranford, EA, Lebiere, C., 2022. Phòng thủ mạng thích ứng với sự lừa dối: một cách tiếp cận nhận thức của con ngư ời-ai. Trong: Sự lừa dối trên mạng: Kỹ thuật, Chiến lư ợc và Khía cạnh của con ngư ời, trang 41–57.

Graham, J., Olson, R., Howard, R., 2016. Những điều cơ bản về an ninh mạng. CRC Press.

Guerra Manzanares, A., 2017. Honeyio4: xây dựng honeypot iot ảo, tư ơng tác thấp . Luận văn thạc sĩ. Đại học Bách khoa Catalonia.

Han, Q., Molinaro, C., Picariello, A., Sperli, G., Subrahmanian, VS, Xiong, Y., 2021. Tạo tài liệu giả bằng đồ thị logic xác suất. IEEE Trans. Máy tính bảo mật đáng tin cậy.

Han, W., Zhao, Z., Doupé, A., Ahn, G.-J., 2016. Honeymix: hư ớng tới honeynet thông minh dựa trên sdn . Trong: Biên bản Hội thảo quốc tế ACM năm 2016 về Bảo mật trong Mạng đư ợc xác định bằng phần mềm & Ảo hóa chức năng mạng, trang 1–6.

Han, X., Kheir, N., Balzarotti, D., 2018. Các kỹ thuật lừa dối trong bảo mật máy tính: góc nhìn nghiên cứu. ACM Comput. Surv. 51 (4), 1–36.

Hayatle, O., Otrok, H., Youssef, A., 2012. Một cuộc điều tra lý thuyết trò chơi cho honeypot tư ơng tác cao. Trong: Hội nghị quốc tế về truyền thông IEEE năm 2012 (ICC). IEEE, trang 6662–6667.

Heckman, KE, Stech, FJ, Thomas, RK, Schmoker, B., Tsow, AW, 2015. Từ chối mạng, lừa dối và phản lừa dối. Adv. Inf. Secur. 64.

Hedayati, R., Mostafavi, S., 2021. Một thuật toán mã hóa hình ảnh nhẹ cho truyền thông an toàn trong Internet vạn vật đa phư ơng tiện. Wirel. Pers. Commun., 1–23.

Hirata, A., Miyamoto, D., Nakayama, M., Esaki, H., 2015. Intercept+: Hỗ trợ Sdn cho honeypots dựa trên di chuyển trực tiếp. Trong: Hội thảo quốc tế lần thứ 4 năm 2015 về Xây dựng bộ dữ liệu phân tích và thu thập dữ liệu kinh nghiệm để bảo mật (BADGERS). IEEE, trang 16–24.

Hobert, K., Lim, C., Budiarto, E., 2023. Tăng cư ờng khả năng quy kết tội phạm mạng thông qua phát hiện hành vi tư ơng tự trên honeypot shell Linux với khuôn khổ att&ck. Trong: Hội nghị quốc tế IEEE năm 2023 về mật mã, tin học và an ninh mạng (ICoCIC). IEEE, trang 139–144.

Huang, L., Zhu, Q., 2019. Sự tham gia của honeypot thích ứng thông qua việc học tăng cư ờng các quá trình quyết định bán Markov. Trong: Hội nghị quốc tế về Quyết định và Lý thuyết trò chơi cho An ninh. Springer, trang 196–216.

Huang, M., Fan, W., Huang, W., Cheng, Y., Xiao, H., 2020. Nghiên cứu về việc xây dựng cơ sở dữ liệu lỗ hổng có thể khai thác cho ứng dụng đám mây gốc. Hội nghị lần thứ 4 về công nghệ thông tin, mạng, điện tử và điều khiển tự động hóa (ITNEC) của IEEE năm 2020, tập 1. IEEE, trang 758–762.

Ibrahim, A., Tariq, U., Ahamed Ahanger, T., Tariq, B., Gebali, F., 2023. Trả đũa phần mềm tống tiền trong hệ thống pureos hỗ trợ đám mây. Toán học 11 (1), 249.

Ikuomenisan, G., Morgan, Y., 2022. Đánh giá có hệ thống các phư ơng pháp trực quan đồ họa trong phân tích dữ liệu tấn công honeypot. J. Inf. Secur. 13 (4), 210–243.

Izagirre, M., 2017. Chiến lư ợc lừa dối để bảo mật ứng dụng web: Phư ơng pháp tiếp cận ở lớp ứng dụng và nền tảng thử nghiệm.

Ja'fari, F., Mostafavi, S., Mizanian, K., Jafari, E., 2021. Một phư ơng pháp chặn botnet thông minh trong các mạng đư ợc xác định bằng phần mềm sử dụng honeypot. J. Ambient Intell. Humaniz. Máy tính. 12 (2), 2993–3016.

Javadpour, A., 2019. Cải thiện quản lý tài nguyên trong ảo hóa mạng bằng cách sử dụng mạng dựa trên phần mềm. Wirel. Pers. Commun. 106 (2), 505–519.

Javadpour, A., 2020. Cung cấp một cách để tạo sự cân bằng giữa độ tin cậy và độ trễ trong mạng sdn bằng cách sử dụng vị trí đặt bộ điều khiển thích hợp. Wirel. Pers. Com- mun. 110 (2), 1057–1071.

Javadpour, A., Wang, G., 2022. cTMvSDN: cải thiện quản lý tài nguyên bằng cách kết hợp quá trình Markov và tdma trong mạng đư ợc xác định bằng phần mềm. J. Supercom- put. 78, 3477–3499.

Javadpour, A., Abharian, SK, Wang, G., 2017. Lựa chọn tính năng và phát hiện xâm nhập trong môi trư ờng đám mây dựa trên các thuật toán học máy. Trong: Hội nghị chuyên đề quốc tế IEEE năm 2017 về Xử lý song song và phân tán với các ứng dụng và Hội nghị quốc tế IEEE năm 2017 về Điện toán và Truyền thông phổ biến (ISPA/IUCC). IEEE, tr. 1417–1421.

Javadpour, A., Ja'fari, F., Taleb, T., Shojafar, M., 2022b. Một cách tiếp cận mtd tiết kiệm chi phí cho các cuộc tấn công ddos trong các mạng đư ợc xác định bằng phần mềm. Trong: GLOBECOM 2022-2022 IEEE Global Communications Conference. IEEE, trang 4173–4178.

Javadpour, A., Ja'fari, F., Taleb, T., Shojafar, M., Yang, B., 2022a. SCEMA: một phư ơng pháp tiếp cận MTD dựa trên cạnh tiết kiệm chi phí theo định hư ớng SDN. IEEE Trans. Inf. Forensics Se- cur. 18, 667–682.

Javadpour, A., Ja'fari, F., Taleb, T., Benzaıd, C., 2023b. Một mô hình toán học để phân tích honeynet và các kỹ thuật lừa đảo mạng của chúng. Trong: Hội nghị quốc tế lần thứ 27 năm 2023 về Kỹ thuật hệ thống máy tính phức tạp (ICECCS). IEEE Computer Society, trang 81–88.

Javadpour, A., Ja'fari, F., Taleb, T., Benzaïd, C., 2023c. Phân tách lát cắt dựa trên học tăng cư ờng chống lại các cuộc tấn công ddos trong các mạng ngoài 5g. IEEE Trans. Netw. Serv. Quản lý

Javadpour, A., Pinto, P., Ja'fari, F., Zhang, W., 2023a. Dmaidps: hệ thống phát hiện và ngăn chặn xâm nhập đa tác nhân phân tán cho môi trư ờng IoT đám mây. Clust. Com -put. 26 (1), 367–384.

Jha, RK, 2023. Đánh giá chuyên sâu về các phư ơng pháp tiếp cận lai trong điện toán mềm cho nhận dạng kỹ thuật xã hội. J. Soft Comput. Paradig. 5 (3), 232–248.

Jiang, X., Hao, Z., Wang, Y., 2010. Một hệ thống thu thập và theo dõi mẫu phần mềm độc hại. Trong: Đại hội thế giới lần thứ hai về Kỹ thuật phần mềm năm 2010, tập 1. IEEE, trang 69–72.

Jones, A., 2022. Tư thế an ninh: Đánh giá có hệ thống về các mối đe dọa mạng và chủ động Bảo vệ.

Jones, MJ, 2016. Thủ đoạn mờ ám hay chiến thuật hợp pháp - các viên chức thực thi pháp luật có thể sử dụng tài khoản mạng xã hội giả để tư ơng tác với nghi phạm không. Am. J. Trial Advoc. 40, 69.

Jonsson, D., Marteni, A., 2022. Cơ chế xác thực đa yếu tố dựa trên trình duyệt Dấu vân tay và Honeytokens đồ họa.

Juels, A., Rivest, RL, 2013. Honeywords: làm cho việc bẻ khóa mật khẩu có thể phát hiện đư ợc. Trong: Biên bản báo cáo Hội nghị ACM SIGSAC về Bảo mật máy tính và truyền thông năm 2013, tập 11. ACM, trang 145–160.

Kandanaarachchi, S., Ochiai, H., Rao, A., 2022. Honeyboost: tăng cư ờng hiệu suất honeypot với hợp nhất dữ liệu và phát hiện bất thư ờng. Expert Syst. Appl. 201, 117073.

Khan, ZA, Abbasi, U., 2020. Quản lý danh tiếng bằng cách sử dụng honeypot để phát hiện xâm nhập trong Internet vạn vật. Điện tử 9 (3), 415.

Kheir, N., Abdelrazek, L., Daniel, C., 2022. Bài báo trình diễn: caught in my radio net- thử nghiệm với honeypots trong mạng truy cập vô tuyến. Trong: Hội nghị lần thứ 25 năm 2022 về Đổi mới trong Đám mây, Internet và Mạng (ICIN). IEEE, trang 1–3.

Khoa, NH, Do Hoang, H., Ngo-Khanh, K., Duy, PT, Pham, V.-H., 2023. Triển khai lừa đảo mạng dựa trên Sdn cho chiến lược phòng thủ chủ động bằng cách sử dụng mật ong của vạn vật và tình báo về mối đe dọa mạng. Trong: Hội nghị quốc tế về tình báo vạn vật. Springer, trang 269–278.

Kiekintveld, C., Lisý, V., Píbil, R., 2015. Nền tảng lý thuyết trò chơi cho việc sử dụng chiến lược honeypot trong bảo mật mạng. Trong: Chiến tranh mạng. Springer, trang 81–101.

Kolias, C., Kambourakis, G., Stavrou, A., Voas, J., 2017. Ddos trong IoT: Mirai và các mạng botnet khác. Máy tính 50 (7), 80–84.

Koziol, J., 2003. Phát hiện xâm nhập bằng Snort. Nhà xuất bản Sams.

Kreps, DM, 1989. Cân bằng Nash. Trong: Lý thuyết trò chơi. Springer, trang 167–177.

Kumar, S., Sehgal, R., Bhatia, J., 2012. Khung honeypot lai để thu thập và phân tích phần mềm độc hại. Trong: Hội nghị quốc tế lần thứ 7 về hệ thống công nghiệp và thông tin (ICIIS) của IEEE năm 2012. IEEE, trang 1–5.

La, QD, Quek, TQ, Lee, J., Jin, S., Zhu, H., 2016. Trò chơi tấn công và phòng thủ lừa đảo trong mạng sử dụng honeypot cho Internet vạn vật. IEEE Int. Things J. 3 (6), 1025–1035.

Lackner, P., 2021. Cách chế nhạo một con gấu: Honeypot, Honeynet, Honeywall & Honeytoken: Một cuộc khảo sát.

Limouchi, E., Mahgoub, I., 2021. Tối ưu hóa ngưỡng hỗ trợ học tăng cường cho việc thích ứng honeypot động để tăng cường bảo mật mạng iobt. Trong: Chuỗi hội thảo IEEE năm 2021 về Trí tuệ tính toán (SSCI). IEEE, trang 1–7.

Luo, T., Xu, Z., Jin, X., Jia, Y., Ouyang, X., 2017. Iotcandyjar: hướng tới một honeypot tương tác thông minh cho các thiết bị iot. Black Hat, 1–11.

Maesschalck, S., Giotsas, V., Green, B., Race, N., 2022. Đừng để bị đốt, hãy phủ mật ong lên IC của bạn: honeypot phù hợp như thế nào với bảo mật hệ thống điều khiển công nghiệp. Máy tính. Bảo mật. 114, 102598.

Marble, JL, Lawless, WF, Mittu, R, Coyne, J, Abramson, M, Sibley, C, 2015 . Trong: Chiến tranh mạng: Xây dựng nền tảng khoa học, trang 107-111. 173–206.

McCarthy, A., Ghadafi, E., Andriotis, P., Legg, P., 2022. Học máy đối kháng bảo toàn chức năng để phân loại mạnh mẽ trong lĩnh vực an ninh mạng và phát hiện xâm nhập: một cuộc khảo sát. J. Cybersecur. Priv. 2 (1), 154–190.

McCoy, CG, 2022. Một mô hình liên quan để xếp hạng các lỗ hổng an ninh mạng theo mối đe dọa. Luận án tiến sĩ. Đại học Old Dominion.

Mohan, PV, Dixit, S., Gyaneshwar, A., Chadha, U., Srinivasan, K., Seo, JT, 2022. Đòn bẩy - các kỹ thuật trí tuệ tính toán lão hóa để đánh lừa phòng thủ: một bài đánh giá, những tiến bộ gần đây, các vấn đề chưa có lời giải và định hướng tương lai. Cảm biến 22 (6), 2194.

Mokube, I., Adams, M., 2007. Honeypots: khái niệm, cách tiếp cận và thách thức. Trong: Biên bản Hội nghị khu vực Đông Nam thường niên lần thứ 45, trang 321-326.

Msaad, M., Srinivasa, S., Andersen, MM, Audran, DH, Orji, CU, Vasilomanolakis, E., 2022. Honeysweeper: hướng tới các kỹ thuật lấy dấu vân tay honeytoken bí mật. Trong: Hội nghị Bắc Âu về Hệ thống CNTT an toàn. Springer, trang 101–119.

Naeem, NA, Batchelder, M., Hendren, L., 2007. Các số liệu để đo lường hiệu quả của trình dịch ngược và trình làm tối nghĩa. Trong: Hội nghị quốc tế lần thứ 15 của IEEE về Hiểu chương trình (ICPC'07). IEEE, trang 253–258.

Naik, N., Shang, C., Jenkins, P., Shen, Q., 2020. D-fri-honeypot: một hoạt động sting an toàn để hack tin tặc bằng cách sử dụng nội suy quy tắc mờ động. IEEE Trans. Emerg. Đứng đầu. Tính toán. Trí tuệ.

Nazario, J., 2009. Phoneyc: honeypot của khách hàng ảo. LEET 9, 911–919.

Nelson, BA, Wilson, JO, Rosen, D., Yen, J., 2009. Các số liệu tinh chỉnh để đo lường hiệu quả của ý tưởng. Des. Stud. 30 (6), 737–743.

Om Kumar, C., Sathia Bhama, PR, 2019. Phát hiện và đối phó với các cuộc tấn công chớp nhoáng từ botnet iot. J. Supercomput. 75, 8312–8338.

Pa, YMP, Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., Rossow, C., 2016 . Tạp chí J. Inf. Quá trình. 24(3), 522–533.

Panda, S., Rass, S., Moschoyiannis, S., Liang, K., Loukas, G., Panaousis, E., 2022. Honeycar: một khuôn khổ để cấu hình lỗ hổng honeypot trên Internet của xe cộ. Truy cập IEEE 10, 104 671–104 685.

Papaspirou, V., Maglaras, L., Ferrag, MA, Kantzavelou, I., Janicke, H., Douligeris, C., 2021. Một cơ chế xác thực honeytoken hai yếu tố mới. Trong: Hội nghị quốc tế về truyền thông máy tính và mạng (ICCCN) năm 2021. IEEE, trang 1–7.

Park, B., Dang, SP, Noh, S., Yi, J., Park, M., 2019. Honeypot mạng ảo động. Trong: Hội nghị quốc tế năm 2019 về sự hội tụ của công nghệ thông tin và truyền thông (ICTC). IEEE, trang 375–377.

Park, Y., Stolfo, SJ, 2012. Mồi nhử phần mềm cho mối đe dọa nội gián. Trong: Biên bản Hội nghị chuyên đề ACM lần thứ 7 về An ninh thông tin, máy tính và truyền thông, trang 93–94.

Pashaei, A., Akbari, ME, Lighvan, MZ, Charmin, A., 2022. Hệ thống phát hiện xâm nhập sớm sử dụng honeypot cho mạng lưới điều khiển công nghiệp. Kết quả Eng. 16, 100576.

Pauna, A., Iacob, A.-C., Bica, I., 2018. Qrassh-một honeypot ssh tự thích ứng được điều khiển bởi q-learning. Trong: Hội nghị quốc tế về truyền thông (COMM) năm 2018. IEEE, trang 441–446.

Pawlick, J., Zhu, Q., 2015. Lừa dối theo thiết kế: trò chơi báo hiệu dựa trên bằng chứng cho mạng bảo vệ công trình. bản in trước arXiv. arXiv:1503.05458.

Pawlick, J., Colbert, E., Zhu, Q., 2018. Mô hình hóa và phân tích sự lừa dối rò rỉ bằng cách sử dụng trò chơi tín hiệu có bằng chứng. IEEE Trans. Inf. Forensics Secur. 14 (7), 1871–1886.

Pawlick, J., Colbert, E., Zhu, Q., 2019. Phân loại lý thuyết trò chơi và khảo sát về sự lừa dối phòng thủ cho an ninh mạng và quyền riêng tư . ACM Comput. Surv. 52 (4), 1–28.

Pawlick, J., Zhu, Q., et al., 2021. Lý thuyết trò chơi cho lừa đảo trên mạng. Mùa xuân.

Perevozchikov, VA, Shaymardanov, TA, Chugunkov, IV, 2017. Các kỹ thuật mới phát hiện phần mềm độc hại bằng hệ thống honeypot ftp. Trong: Hội nghị IEEE năm 2017 của các nhà nghiên cứu trẻ ngườ ời Nga về Kỹ thuật Điện và Điện tử (EIConRus). IEEE, trang 204–207.

Píbil, R., Lisý, V., Kiekintveld, C., Bošansky, B., Pechou ˇ cek, ˇ M., 2012. Mô hình lý thuyết trò chơi về lựa chọn honeypot chiến lược trong mạng máy tính. Trong: Hội nghị quốc tế về Quyết định và Lý thuyết trò chơi cho An ninh. Springer, trang 201–220.

Popli, NK, Girdhar, A., 2019. Phân tích hành vi của các phần mềm tống tiền gần đây và dự đoán các cuộc tấn công trong tương lai bằng phần mềm tống tiền đa hình và biến hình. Trong: Trí tuệ tính toán: Lý thuyết, Ứng dụng và Hướng đi trong tương lai - Tập II. Springer, trang 65–80.

Priya, VD, Chakkaravarthy, SS, 2023. Lừa đảo honeypot dựa trên đám mây chứa container để theo dõi những kẻ tấn công. Sci. Rep. 13 (1), 1437.

Qin, X., Jiang, F., Cen, M., Doss, R., 2023. Chiến lược phòng thủ mạng kết hợp sử dụng honey-x: một cuộc khảo sát. Comput. Netw., 109776.

Raharjo, DHK, Nurmala, A., Pambudi, RD, Sari, RF, 2022. Đánh giá hiệu suất của hệ thống phát hiện xâm nhập để phát hiện bất thường về lưu lượng dựa trên các quy tắc danh tiếng IP đang hoạt động. Trong: Hội nghị quốc tế lần thứ 3 năm 2022 về Kỹ thuật điện và Tin học (ICon EEI). IEEE, trang 75–79.

Rahmatullah, DK, Nasution, SM, Azmi, F., 2016. Triển khai honeypot máy chủ web tương tác thấp bằng cách sử dụng cubieboard. Trong: Hội nghị quốc tế năm 2016 về Kiểm soát, Điện tử, Năng lượng tái tạo và Truyền thông (ICCEREC). IEEE, trang 127–131.

Razali, MF, Razali, MN, Mansor, FZ, Muruti, G., Jamil, N., 2018. Iot honeypot: đánh giá từ góc nhìn của nhà nghiên cứu. Trong: Hội nghị IEEE năm 2018 về Ứng dụng, Thông tin và An ninh mạng (AINS). IEEE, trang 93–98.

Ren, J., Zhang, C., 2020. Một phương pháp trò chơi khác biệt chống lại các cuộc tấn công trong honeynet không đồng nhất. Comput. Secur. 97, 101870.

Ren, J., Zhang, C., Hao, Q., 2021. Một phương pháp lý thuyết để đánh giá hiệu lực của mạng lưới mật ong. Hệ thống máy tính thế hệ tương lai 116, 76–85.

Rich, MS, 2023. Phân tích theo chiều dọc các chiến thuật và kỹ thuật đối đầu trên mạng.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, MA, Amir, A., Vuda, KV, Sarwat, AI, 2023. Tác động, lỗ hổng và chiến lược giảm thiểu cho cơ sở hạ tầng quan trọng an toàn mạng. Cảm biến 23 (8), 4060.

Rossotti, A., 2022. Khung phát hiện dị thường và kỹ thuật học sâu cho Tấn công Zero-Day trong môi trường dựa trên container.

Rowe, NC, 2006. Đo lường hiệu quả của honeypot chống lừa đảo. Trong: Biên bản Hội nghị quốc tế Hawaii lần thứ 39 về khoa học hệ thống (HICSS'06), tập 6. IEEE, trang 129c–129c.

Rowe, NC, Custy, EJ, Duong, BT, 2007. Bảo vệ không gian mạng bằng honeypot giả. J. Tính toán 2 (2), 25–36.

Sahin, M., Hébert, C., Cabrera Lozoya, R., 2022. Một cách tiếp cận để tạo ra các tham số http thực tế cho sự lừa dối ở lớp ứng dụng. Trong: Hội nghị quốc tế về mật mã ứng dụng và an ninh mạng. Springer, trang 337–355.

Salimova, HR, 2022. Một khuôn khổ honeypot ảo. Cent. Asian Res. J. Interdiscip. Nghiên cứu. 2 (5), 479–486.

Sangaiah, AK, Javadpour, A., Ja'fari, F., Pinto, P., Zhang, W., Balasubramanian, S., 2023a. Lựa chọn tính năng trí tuệ nhân tạo dựa trên chẩn đoán kết hợp cho các bộ phân loại phát hiện xâm nhập trong đám mây vạn vật. Cụm. Máy tính. 26 (1), 599–612.

Sangaiah, AK, Javadpour, A., Pinto, P., 2023b. Hướng tới đánh giá bảo mật dữ liệu bằng mô hình bảo mật ids cho các thành phố thông minh mạng vật lý. Inf. Sci., 119530.

Santhosh Kumar, S., Selvi, M., Kannan, A., et al., 2023. Một khảo sát toàn diện về các hệ thống phát hiện xâm nhập dựa trên máy học để giao tiếp an toàn trong Internet vạn vật. Comput. Intell. Neurosci. 2023.

Sardana, A., Joshi, R., 2009. Kiến trúc honeypot tự động phản hồi để phân bổ tài nguyên động và điều chỉnh qos trong mạng bị tấn công ddos. Comput. Com- mun. 32 (12), 1384–1399.

Sarr, AB, Anwar, AH, Kamhoua, C., Leslie, N., Acosta, J., 2020. Sự đa dạng của phần mềm cho lừa đảo trên mạng. Trong: GLOBECOM 2020-2020 Hội nghị truyền thông toàn cầu IEEE. IEEE, trang 1–6.

Selvaraj, R., Kuthadi, VM, Marwala, T., 2016. Honey pot: một kỹ thuật chính để phát hiện xâm nhập. Trong: Biên bản Hội nghị quốc tế lần thứ hai về Công nghệ máy tính và truyền thông. Springer, trang 73–82.

Sethuraman, SC, Jadapalli, TG, Sudhakaran, DPV, Mohanty, SP, 2023. Phương pháp honeypot chứa dựa trên luồng để phân tích lưu lượng mạng: một nghiên cứu thực nghiệm. Tạp chí Khoa học Máy tính, số 50, 100600.

Seungjin, L., Abdullah, A., Jhanjhi, N., 2020. Đánh giá về các mô hình phát hiện botnet dựa trên honeypot cho nhà máy thông minh. Int. J. Adv. Comput. Sci. Appl. 11 (6), 418–435.

Shabtai, A., Bercovitch, M., Rokach, L., Gal, Y., Elovici, Y., Shmueli, E., 2016. Nghiên cứu hành vi của người dùng khi tương tác với honeytokens đang hoạt động. ACM Trans. Inf. Syst. Điều 18 (3), 1–21.

Shakarian, P., Paulo, D., Albanese, M., Jajodia, S., 2014. Giữ cho những kẻ xâm nhập không bị phát hiện: một phương pháp tiếp cận dựa trên lý thuyết đồ thị để giảm khả năng xâm nhập mạng thành công. Trong: Hội nghị quốc tế lần thứ 11 về an ninh và mật mã (SECRYPT) năm 2014. IEEE, trang 1–12.

Shi, L., Jiang, L., Liu, D., Han, X., 2012. Mimicry honeypot: giới thiệu tóm tắt. Trong: Hội nghị quốc tế lần thứ 8 năm 2012 về truyền thông không dây, mạng và điện toán di động. IEEE, trang 1–4.

Shin, B., Lowry, PB, 2020. Đánh giá và giải thích lý thuyết về 'năng lực tình báo đe dọa mạng (cti)' cần
được bồi dưỡng ở những người thực hành an ninh thông tin và cách thức thực hiện điều này. Comput.
Secur. 92, 101761.
Shumakov, IU, Troitskiy, SS, Silnov, DS, 2017. Tăng sức hấp dẫn của thông tin sai lệch
các đối tượng tấn công trên máy chủ web. Trong: Hội nghị quốc tế lần thứ 18 năm 2017
Chuyên gia trẻ về công nghệ vi mô/nano và thiết bị điện tử (EDM). IEEE,
trang 195–198.
Siniosoglou, I., Efstathopoulos, G., Pliatsios, D., Moscholios, ID, Sarigiannidis, A., Sakel-lari, G.,
Loukas, G., Sarigiannidis, P., 2020. Neuralpot: một triển khai honeypot công nghiệp dựa trên mạng nơ-
ron sâu. Trong: Hội nghị chuyên đề về máy tính của IEEE năm 2020
và Truyền thông (ISCC). IEEE, trang 1–7.
Soundararajan, R., Rajagopal, M., Muthuramalingam, A., Hossain, E., Lloret, J., 2022.
Mô hình đóng khung honeypot xen kẽ với các chính sách mac an toàn cho mạng cảm biến không
dây . Cảm biến 22 (20), 8046.
Srinivasa, S., Pedersen, JM, Vasilomanolakis, E., 2020. Hướng tới honeytoken có hệ thống
dấu vân tay. Trong: Hội nghị quốc tế lần thứ 13 về an ninh thông tin và mạng , trang 1–5.

Srinivasa, S., Pedersen, JM, Vasilomanolakis, E., 2022. Tương tác là vấn đề: phân tích toàn diện và tập
dữ liệu về honeypot iot/ot lai. Trong: Biên bản báo cáo của Hội nghị lần thứ 38
Hội nghị ứng dụng bảo mật máy tính thường niên, trang 742–755.
Steingartner, W., Galinec, D., Kozina, A., 2021. Phòng thủ mối đe dọa: phương pháp tiếp cận lừa đảo trên mạng
và giáo dục về khả năng phục hồi trong mô hình mối đe dọa lai. Đối xứng 13 (4), 597.
Sumadi, FDS, Widagdo, AR, Reza, AF, et al., 2022. Tích hợp Sd-honeypot để giảm thiểu tấn công ddos bằng
cách sử dụng các phương pháp học máy. JOIV: Int. J. Inform. Vis. 6
(1), 39–44.
Sun, J., Sun, K., Li, Q., 2020. Hướng tới một hệ thống mồi nhử đáng tin cậy: phát lại các hoạt động mạng
từ hệ thống thực. Trong: Hội nghị IEEE năm 2020 về Truyền thông và Mạng
Bảo mật (CNS). IEEE, trang 1–9.
Sun, R., Yuan, X., Lee, A., Bishop, M., Porter, DE, Li, X., Gregio, A., Oliveira, D., 2017.
Liều lượng tạo nên chất độc—tận dụng sự không chắc chắn để phát hiện phần mềm độc hại hiệu quả.
Trong: Hội nghị IEEE năm 2017 về Máy tính đáng tin cậy và an toàn. IEEE, trang 123–130.
Suratkar, S., Shah, K., Sood, A., Loya, A., Bisure, D., Patil, U., Kazi, F., 2021. Một honeypot thích ứng
sử dụng q-learning với trình phân tích mức độ nghiêm trọng. J. Ambient Intell. Humaniz.
Máy tính, 1–12.
Suryawanshi, BD, Tayade, PB, Patil, AV, Patil, JB, Rajput, DV, 2017. Tăng cường
bảo mật sử dụng honeywords. Trong: Tạp chí quốc tế về nghiên cứu sáng tạo và công nghệ sáng tạo, tập
2. IJIRCT.
Tabari, AZ, Liu, G., Ou, X., Singhal, A., 2023. Tiết lộ hành vi của kẻ tấn công con người bằng cách sử dụng
hệ sinh thái honeypot Internet vạn vật thích ứng. Trong: Hội nghị quốc tế IFIP
về Khoa học pháp y kỹ thuật số. Springer, trang 73–90.
Tan, RR, Eng, S., How, KC, Zhu, Y., Jyh, PWH, 2023. Honeypot cho an ninh mạng
tình báo về mối đe dọa. Trong: IRC-SET 2022: Biên bản Hội nghị IRC lần thứ 8 về Khoa học, Kỹ thuật và
Công nghệ, tháng 8 năm 2022, Singapore. Springer, trang 587–598.
Tian, DJ, Bates, A., Butler, K., 2015. Bảo vệ chống lại phần mềm USB độc hại bằng
goodusb. Trong: Biên bản Hội nghị Ứng dụng Bảo mật Máy tính thường niên lần thứ 31 , trang 261–270.

Toor, JS, Bhandari, EA, 2017. Honeypot: một cái bẫy lừa đảo. Int. J. Eng. Technol. Manag.
Khoa học ứng dụng
Valero, JMJ, Pérez, MG, Celdrán, AH, Pérez, GM, 2020. Nhận dạng và phân loại các mối đe dọa mạng thông qua
hệ thống honeypot ssh. Trong: Sổ tay nghiên cứu về
Hệ thống phát hiện xâm nhập. IGI Global, trang 105–129.
Voris, JA, Jermyn, J., Keromytis, AD, Stolfo, S., 2013. Mồi nhử và chỉ điểm: Bảo vệ sự đồng lõa
Hệ thống máy tính có mồi nhử.
Wagener, G., Dulaunoy, A., Engel, T., et al., 2009. Honeypots tương tác cao tự thích ứng được thúc đẩy
bởi lý thuyết trò chơi. Trong: Hội thảo về Hệ thống tự ổn định. Springer,
trang 741–755.
Wang, H., Wu, B., 2019. Honeypot lai dựa trên Sdn để bắt giữ tấn công. Trong: 2019 IEEE 3rd
Hội nghị Công nghệ thông tin, Mạng, Điện tử và Điều khiển tự động
(ITNEC). IEEE, trang 1602–1606.
Wang, H., He, H., Zhang, W., Liu, W., Liu, P., Javadpour, A., 2022. Sử dụng honeypot để
mô hình tấn công botnet vào Internet của các thiết bị y tế. Comput. Electr. Eng. 102,
108212.
Wang, K., Du, M., Maharjan, S., Sun, Y., 2017. Mô hình trò chơi honeypot chiến lược cho các cuộc tấn công
từ chối dịch vụ phân tán trong lưới điện thông minh. IEEE Trans. Smart Grid 8 (5),
2474–2482.
Wang, M., Santillan, J., Kuipers, F., 2018. Thingpot: một hon- eypot tương tác về Internet vạn
vật. Bản in trước arXiv. arXiv:1807.04114.
Wang, S.-H., 2022. Quan sát về an ninh camera thông minh.
Wegerer, M., Tjoa, S., 2016. Đánh bại kẻ thù cơ sở dữ liệu bằng cách lừa dối - mysql
honeypot cơ sở dữ liệu. Trong: Hội nghị quốc tế năm 2016 về bảo mật và đảm bảo phần mềm (ICSSA).
IEEE, trang 6–10.
Whaley, B., 1982. Hướng tới một lý thuyết chung về sự lừa dối. J. Strateg. Stud. 5 (1), 178–192.
White, J., Park, JS, Kamhoua, CA, Kwiat, KA, 2014. Mô phỏng tấn công mạng xã hội
với honeytokens. Mạng xã hội. Anal. Min. 4, 1–14.
Yamin, MM, Katt, B., 2022. Sử dụng các tác nhân tấn công và phòng thủ mạng trong phạm vi mạng: a
nghiên cứu tình huống. Comput. Secur. 122, 102892.
Yang, X., Yuan, J., Yang, H., Kong, Y., Zhang, H., Zhao, J., 2023. Một tương tác cao
cách tiếp cận dựa trên honeypot để quản lý mối đe dọa mạng. Internet trong tương lai 15 (4),
127.
You, J., Lv, S., Zhao, L., Niu, M., Shi, Z., Sun, L., 2020. Một vật lý tương tác cao có khả năng mở rộng
khuôn khổ honeypot cho bộ điều khiển logic lập trình. Trong: Hội nghị công nghệ xe cộ IEEE lần thứ 92
năm 2020 (VTC2020-Mùa thu). IEEE, trang 1–5.
Zarras, A., 2014. Nghệ thuật bảo động giả trong trò lừa bịp: tận dụng các lọ mật ong giả để tăng cường an
ninh. Trong: Hội nghị quốc tế Carnahan về an ninh năm 2014
Công nghệ (ICCST). IEEE, trang 1–6.
Zhang, L., Thing, VL, 2021. Ba thập kỷ các kỹ thuật lừa dối trong hoạt động mạng
phòng thủ-hồi tưởng và triển vọng. Comput. Secur. 106, 102288.
Zhu, M., Anwar, AH, Wan, Z., Cho, J.-H., Kamhoua, CA, Singh, MP, 2021. Một cuộc khảo sát
của sự lừa dối phòng thủ: các phương pháp tiếp cận sử dụng lý thuyết trò chơi và máy học. IEEE
Gia sư cộng đồng. 23 (4), 2460–2493.
Zhuge, J., Holz, T., Han, X., Guo, J., Zou, W., 2007. Đặc điểm của botnet dựa trên irc
Hiện tượng. Báo cáo kỹ thuật của China Honeynet.
Zobal, L., Kolár, D., Fujdiak, R., 2019. Tình trạng hiện tại của honeypot và các chiến lược lừa dối
trong an ninh mạng. Trong: Đại hội quốc tế lần thứ 11 năm 2019 về Hệ thống và Hội thảo Viễn
thông và Điều khiển Siêu hiện đại (ICUMT). IEEE, trang 1–9.

Amir Javadpour đã lấy bằng Thạc sĩ Kỹ thuật Công nghệ Thông tin Y tế từ Đại học Tehran, Iran,
vào năm 2014. Ông nhận bằng Tiến sĩ Khoa học máy tính/Toán học/An ninh mạng
từ Đại học Quảng Châu, Trung Quốc. Ngoài ra, ông đã xuất bản các bài báo cùng
với các đồng nghiệp của mình trong các tạp chí được xếp hạng cao
các tạp chí và một số hội nghị được xếp hạng về nhiều chủ đề, bao gồm Điện
toán đám mây, Mạng được xác định bằng phần mềm (SDN),
Dữ liệu lớn, Hệ thống phát hiện xâm nhập (IDS) và Internet
Vạn vật (IoT), Phòng thủ mục tiêu di động (MTD), Học máy
(ML) và các thuật toán tối ưu hóa. Ngoài ra, ông đã xem xét các bài báo cho
một số địa điểm có uy tín như IEEE Transactions on Cloud Computing, IEEE
Giao dịch về Khoa học và Kỹ thuật Mạng, Giao dịch ACM về Công nghệ Internet, Tạp chí Siêu máy tính, một số
tạp chí của Springer và Elsevier, v.v.
là thành viên của Ủy ban Chương trình Kỹ thuật (TCP) của nhiều hội nghị khác nhau.

Forough Ja'fari là Nhà nghiên cứu cao cấp về an ninh mạng và
khoa học máy tính. Cô đã nhận được bằng Cử nhân của Sharif
Đại học Công nghệ và bằng Thạc sĩ Máy tính
Kỹ thuật mạng từ Đại học Yazd, Iran. Cô ấy là một
học giả nghiên cứu tại Đại học Quảng Châu, Trung Quốc. Điện toán đám mây,
Mạng được xác định bằng phần mềm (SDN), lừa đảo trên mạng, Hệ thống phát
hiện xâm nhập (IDS), Internet vạn vật (IoT), Di chuyển
Target Defence (MTD) và Machine Learning là một số sở thích nghiên cứu của
cô. Cô hiện là Biên tập viên khách mời (GE) của Cluster
Tạp chí Máy tính (CLUS) và là người đánh giá cho một số tạp chí
và hội nghị.

Tarik Taleb Giáo sư Tarik Taleb hiện là Giáo sư chính thức
tại Khoa Kỹ thuật Điện và Công nghệ Thông tin, Đại học Ruhr Bochum, Đức, và
là giáo sư tại
Trung tâm truyền thông không dây, Đại học Oulu,
Phần Lan. Ông là người sáng lập và giám đốc của Phòng thí nghiệm MOSAIC
(www.mosaic-lab.org). Từ tháng 10 năm 2014 đến tháng 12 năm 2021, anh ấy
là Phó Giáo sư tại Khoa Kỹ thuật Điện, Đại học Aalto, Phần Lan. Trước đó,
ông làm việc như
một Nhà nghiên cứu cao cấp và Chuyên gia về Tiêu chuẩn 3GPP tại NEC Châu Âu
Ltd, Heidelberg, Đức. Trước khi gia nhập NEC và cho đến tháng 3 năm 2009,
ông đã làm việc như một trợ lý giáo sư tại Trường Cao học Khoa học Thông tin,
Đại học Tohoku, Nhật Bản, trong một phòng thí nghiệm được tài trợ hoàn toàn bởi KDDI, nhà điều hành di động lớn
thứ hai tại Nhật Bản. Từ tháng 10 năm 2005 đến tháng 3 năm 2006, ông làm việc với tư cách là nghiên cứu viên tại
Viện nghiên cứu vũ trụ thông minh, Sendai, Nhật Bản. Ông nhận bằng Cử nhân Kỹ thuật thông tin với bằng
xuất sắc, bằng Thạc sĩ và Tiến sĩ Khoa học thông tin
từ Đại học Tohoku, vào các năm 2001, 2003 và 2005. Các mối quan tâm nghiên cứu của Giáo sư Taleb nằm trong
lĩnh vực điện toán đám mây viễn thông, phần mềm hóa mạng và phân chia mạng, dựa trên AI
bảo mật được xác định bằng phần mềm, truyền thông nhập vai, phát trực tuyến đa phương tiện di động và
mạng di động thế hệ tiếp theo. Giáo sư Taleb cũng đã trực tiếp tham gia vào việc phát triển và chuẩn hóa
Hệ thống gói Evolved với tư cách là thành viên của Hệ thống 3GPP
Nhóm làm việc về kiến trúc 2. Giáo sư Taleb phục vụ tại Hiệp hội truyền thông IEEE
Ban Phát triển Chương trình Chuẩn hóa. Giáo sư Taleb giữ chức chủ tịch chung
của phiên bản năm 2019 của Hội nghị Mạng và Truyền thông Không dây IEEE
(WCNC'19) được tổ chức tại Marrakech, Morocco. Ông là tổng biên tập khách mời của IEEE
JSAC Series về phần mềm hóa mạng và các công cụ hỗ trợ. Ông là thành viên ban biên tập của
các tạp chí và báo chí IEEE khác nhau. Cho đến tháng 12 năm 2016, ông giữ chức chủ tịch Ủy ban Kỹ thuật
Truyền thông Không dây, ủy ban lớn nhất tại IEEE ComSoC. Giáo sư Taleb là
người nhận Giải thưởng công nhận của Ủy ban kỹ thuật truyền thông không dây IEEE ComSoc năm 2021 (tháng
12 năm 2021), Giải thưởng phần mềm truyền thông IEEE ComSoc năm 2017
Giải thưởng Thành tựu Kỹ thuật (tháng 12 năm 2017) cho những đóng góp nổi bật của ông cho mạng lưới
phần mềm hóa. Ông cũng là người (đồng) nhận giải thưởng IEEE Communications Society năm 2017
Giải thưởng Fred W. Ellersick (tháng 5 năm 2017), giải thưởng Nhà nghiên cứu trẻ xuất sắc nhất Châu Á - Thái
Bình Dương của IEEE ComSoc năm 2009 (tháng 6 năm 2009), Giải thưởng Công nghệ Hệ thống VIỄN THÔNG năm 2008 từ
Quỹ Phát triển Viễn thông (tháng 3 năm 2008), Quỹ Funai 2007
Giải thưởng Xúc tiến Khoa học (tháng 4 năm 2007), Chi nhánh Nhật Bản của Hiệp hội Máy tính IEEE năm 2006
Giải thưởng Tác giả trẻ (tháng 12 năm 2006), Giải thưởng Tưởng niệm Niwa Yasujirou (tháng 2 năm 2005) và
Giải thưởng khuyến khích nhà nghiên cứu trẻ từ chi nhánh Nhật Bản của Hiệp hội công nghệ xe cộ IEEE (VTS)
(tháng 10 năm 2003). Một số công trình nghiên cứu của Giáo sư Taleb đã được
được trao giải bài báo hay nhất tại các hội nghị uy tín do IEEE tổ chức.

Chafika Benzaïd hiện là nghiên cứu viên cao cấp tại Đại học Oulu, Phần Lan. Từ tháng 11 năm 2018 đến tháng 12 năm 2021, bà là nghiên cứu viên cao cấp tại Đại học Aalto. Trư ớc đó, bà làm phó giáo sư tại Đại học Khoa học và Công nghệ Houari Boumediene (USTHB). Bà có bằng Kỹ sư , Thạc sĩ và "Tiến sĩ Khoa học" từ USTHB. Các mối quan tâm nghiên cứu của bà nằm trong lĩnh vực 5G/6G, SDN, Bảo mật mạng, Bảo mật AI và AI/ML để quản lý bảo mật không cần chạm.

Cô ấy là thành viên chuyên nghiệp của ACM.

Mohammad Shojafar (Thành viên cao cấp, IEEE) là Giảng viên cao cấp (Phó giáo sư) về an ninh mạng và là Nhà đổi mới của Intel, thành viên ACM chuyên nghiệp và Diễn giả xuất sắc của ACM, Viện sĩ của Viện Hàn lâm Giáo dục Đại học và Cựu sinh viên Marie Curie, làm việc tại Trung tâm Đổi mới 5G & 6G (5GIC & 6GIC), Viện Hệ thống Truyền thông (ICS), tại Đại học Surrey, Vư ơng quốc Anh. Trư ớc đó, ông là Nhà nghiên cứu cao cấp và là Viện sĩ Marie Curie trong nhóm Nghiên cứu Bảo mật và Quyền riêng tư SPRITZ tại Đại học Padua, Ý. Tiến sĩ Mohammad đã bảo đảm đư ợc 310.000 bảng Anh cho dự án ESKMARALD do GCHQ tài trợ, Anh, năm 2022. Ngoài ra, ông là PI của AUTOTRUST, một nền tảng quản lý giao thông tự động an toàn dựa trên 5G mà Cơ quan Vũ trụ Châu Â u đã hỗ trợ với số tiền khoảng 750.000 euro vào năm 2021. Ngoài ra, Mohammad là PI của dự án PRISENODE, một dự án Marie Curie Horizon 2020 trị giá 275.000 euro về bảo mật mạng và lập lịch tác vụ/nguồn lực Fog hợp tác tại Đại học Padua. Ông cũng là PI về bảo mật và quyền riêng tư SDN của Ý (60.000 euro) đư ợc Đại học Padua hỗ trợ vào năm 2018 và là Đồng PI về một dự án Anh-Ecuador về phân bổ nguồn lực IoT và Công nghiệp 4.0 (20.000 đô la) vào năm 2020. Ông đã đóng góp cho một số dự án của Ý trong lĩnh vực viễn thông, như GAUChO, SAMMClouds và SC2. Ông đã nhận bằng Tiến sĩ về CNTT từ Đại học Sapienza ở Rome, Rome, Ý vào năm 2016 với bằng "Xuất sắc". Ông là Biên tập viên cộng tác của IEEE Transactions on Network and Service Management, IEEE Transactions on Intelligent Transportation Systems, Tạp chí IEEE Consumer Electronics, Tạp chí IEEE Systems và Mạng máy tính.