BÁO CÁO BÀI TẬP LỚN

Phân tích hành vi tấn công mạng từ Cowrie Honeypot sử dụng kỹ thuật tiền xử lý và học máy

Nhóm 3

Giảng viên hướng dẫn: PGS. TS. Nguyễn Đình Hân

Học phần: An toàn hệ thống thông tin (MI4260)

Ngày 11 tháng 6 năm 2025

Mục lục

Bối cảnh ra đời

Bối cảnh ra đời

- Sự phát triển nhanh chóng của Internet (1990s): Mạng internet ngày càng phổ biến,gia tăng các cuộc tấn công mạng như: quét cổng (port scanning), brute-force, exploit lỗ hổng.
- Hạn chế của các công cụ bảo mật truyền thống:Tường lửa (firewall) và IDS thường chỉ phát hiện chứ không ghi lại chi tiết hành vi tấn công;Khó phân biệt được giữa truy cập hợp lệ và truy cập độc hại.
- Nhu cầu nghiên cứu hành vi của hacker:Cần một môi trường kiểm soát để quan sát kỹ thuật, công cụ và chiến thuật của kẻ tấn công.
  =>Honeypot ra đời.

Lịch sử hình thành Honeypot

Lịch sử hình thành Honeypot

Mốc thời gian	Sự kiện / Diễn biến chính
1990s	Khái niệm honeypot bắt đầu được biết đến trong giới an ninh mạng. Một trong những công trình đầu tiên mô tả rõ honeypot là của Clifford Stoll với vụ "The Cuckoo's Egg"– ông theo dõi hacker Đông Đức tấn công hệ thống Mỹ.
1997	Fred Cohen công bố một số tài liệu về việc sử dụng honeypot để phát hiện các hành vi tấn công. Ông được xem là một trong những người đầu tiên đưa ra mô hình honeypot có hệ thống.
1998	The Honeynet Project được thành lập – tổ chức phi lợi nhuận đầu tiên nghiên cứu chuyên sâu về honeypot, do Lance Spitzner sáng lập. Họ công bố nhiều công cụ và tài liệu giúp cộng đồng sử dụng honeypot hiệu quả.

" Nguồn:Threat Reference: Honeypot." Proofpoint, www.proofpoint.com/us/threat-reference/honeypot.

Lịch sử hình thành Honeypot

Mốc thời gian	**Sự kiện / Diễn biến chính**
2000s	Honeypot được phát triển mạnh mẽ hơn với sự xuất hiện của low-interaction và high-interaction honeypots, phục vụ cả nghiên cứu lẫn bảo vệ hệ thống thực.
2010s – nay	Honeypot được ứng dụng trong các môi trường đám mây, IoT, công nghiệp, với nhiều nền tảng mã nguồn mở (Dionaea, Cowrie, T-Pot...). Chúng cũng trở thành một phần trong chiến lược phòng thủ chủ động (active defense).

Tổng quan về Honeypot

Khái niệm về HoneyPot

Khái niệm

Honeypot là một hệ thống giả lập — có thể là máy chủ, dịch vụ hoặc dữ liệu — được thiết lập như "mồi nhử" để thu hút kẻ tấn công mạng (hacker, bot). Mục đích chính là ghi lại chi tiết các hoạt động xâm nhập, phân tích phương thức tấn công, đồng thời chuyển hướng và cô lập những mối đe dọa này khỏi hệ thống thực sự của tổ chức.

Một số thuật ngữ cơ bản

Thuật ngữ

- Zero-day (0-day) là một lỗ hổng bảo mật chưa được nhà phát triển phần mềm phát hiện hoặc vá lỗi, nhưng hacker đã biết và đang khai thác.
- APT là một hình thức tấn công mạng có chủ đích, có tổ chức, và kéo dài lâu dài, thường do các nhóm hacker chuyên nghiệp hoặc nhà nước tài trợ, nhằm vào các tổ chức lớn, chính phủ hoặc tập đoàn.
  "Advanced" – Sử dụng công cụ/phương pháp tiên tiến. "Persistent" – Duy trì hiện diện trong hệ thống trong thời gian dài. "Threat" – Là mối nguy thực sự, không phải giả lập.
- Dữ liệu forensic: Dữ liệu forensic là tập hợp các chứng cứ điện tử được trích xuất từ máy tính, thiết bị mạng, thiết bị lưu trữ, ứng dụng hoặc môi trường số khác nhằm: Phân tích nguyên nhân sự cố, Truy tìm dấu vết kẻ tấn công, Phục vụ cho quy trình tố tụng pháp luật.

Phân loại HoneyPot

Phân loại

Low-Interaction Honeypot: mô phỏng một phần nhỏ các dịch vụ hoặc ứng dụng thật, cho phép kẻ tấn công tương tác hạn chế mà không thực sự truy cập được vào hệ điều hành hoặc hệ thống thật sự.

High-Interaction Honeypot: cung cấp một môi trường tương tác đầy đủ và chân thực, cho phép kẻ tấn công tương tác sâu (khai thác lỗ hổng, tải file, cài mã độc, tạo shell) như thể đang khai thác một hệ thống thật, từ đó ghi lại toàn bộ hành vi, công cụ, và chiến thuật tấn công.

Mid-Interaction Honeypot:cung cấp tương tác ở mức trung bình, mô phỏng hành vi hệ thống sâu hơn so với low-interaction nhưng không đầy đủ như high-interaction. Nó cho phép kẻ tấn công đi xa hơn trong quá trình khai thác, nhưng vẫn trong giới hạn an toàn do không có hệ điều hành thật sự phía sau.

Phát hiện sớm các mối đe dọa (scan, brute-force, malware...):

Phát hiện các hành vi bất thường như quét cổng, brute-force, khai thác lỗ hổng... trước khi kẻ tấn công đến hệ thống thật. Vì honeypot không phục vụ mục đích sử dụng thực tế, mọi truy cập vào nó đều bị xem là đáng ngờ.

Ví dụ: Một honeypot SSH phát hiện hàng loạt truy cập từ một IP – cảnh báo rằng hệ thống đang bị dò quét hoặc tấn công từ botnet.

Chức năng Honeypot

Cung cấp thông tin chi tiết về kỹ thuật tấn công:

- Ghi lại chi tiết các lệnh, payload, công cụ mà hacker sử dụng.
- Phân tích chiến thuật – kỹ thuật – quy trình tấn công (Tactics, Techniques, Procedures – TTPs).
- Phát hiện mã độc mới, backdoor, rootkit...

Dữ liệu thu được có thể dùng để:

- Huấn luyện hệ thống phát hiện xâm nhập (IDS/IPS).
- Cập nhật cơ sở dữ liệu virus, signatures.
- Nghiên cứu APT và các cuộc tấn công nhắm mục tiêu.

Chức năng Honeypot

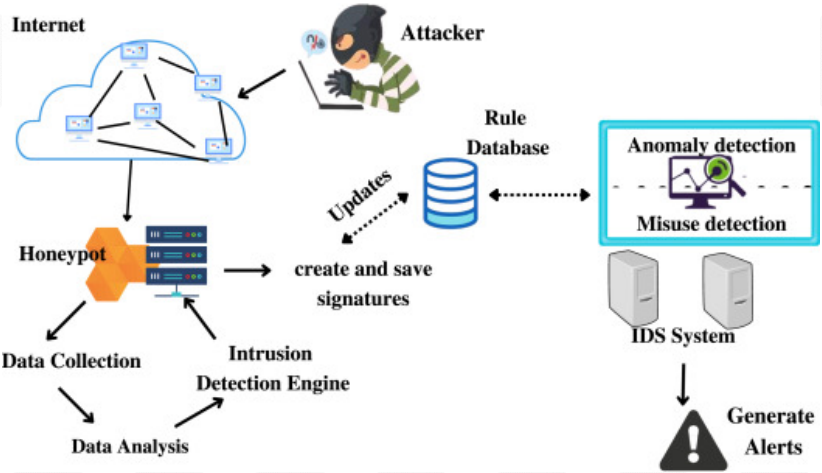
Tăng cường hệ thống phòng thủ:

- Đóng vai trò như lớp phòng thủ phụ, thu hút và làm chậm kẻ tấn công.
- Cho phép các hệ thống an ninh khác (firewall, IDS, SIEM...) có thêm thời gian phản ứng.

Hỗ trợ huấn luyện phân tích mã độc:

- Cho phép các nhà nghiên cứu mô phỏng tấn công mạng an toàn mà không gây rủi ro thật.
- Dùng để kiểm thử công cụ bảo mật, hệ thống giám sát, IDS...

Phương thức hoạt động



" Nguồn: Alshamrani et al. (2023), Journal of Network and Computer Applications, https://doi.org/10.1016/j.jnca.2023.103637

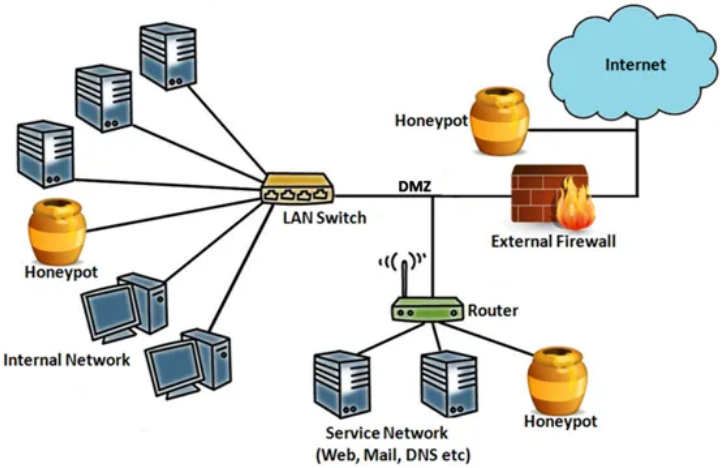
So sánh IDS/IPS – Honeypot

Tiêu chí	IDS	IPS	Honeypot
Chức năng chính	Phát hiện xâm nhập,hành vi đáng ngờ	Ngăn chặn xâm nhập,hành vi độc hại	Dụ dỗ, ghi nhận công cụ,kỹ thuật tấn công
Phản ứng	Thụ động (cảnh báo)	Chủ động (chặn)	Thụ động (ghi nhận)
Cách hoạt động	Giám sát lưu lượng, so khớp chữ ký	Tương tự IDS, có thể can thiệp	Giả lập hệ thống mồi nhử attacker
Vị trí triển khai	Sau firewall hoặc song song với mạng	Giữa firewall và hệ thống chính	Trong DMZ hoặc mạng nội bộ

So sánh IDS/IPS – Honeypot

Tiêu chí	IDS	IPS	Honeypot
Phát hiện Zero-day	Có (nếu dùng phân tích hành vi)	Có thể (tùy cấu hình)	Tốt (ghi nhận hành vi mới)
Can thiệp tấn công	Không	Có	Không
Cảnh báo sai	Trung bình đến cao	Trung bình đến cao	Rất thấp
Chi phí duy trì	Trung bình	Cao	Thấp đến cao (tùy loại)
Ứng dụng chính	Cảnh báo sớm, giám sát	Bảo vệ chủ động, ngăn chặn	Phân tích tấn công, đánh lạc hướng

Ứng dụng Honeypot trong hệ thống mạng



" Nguồn: Cyberhoot(Craig Taylor,2020)

Honeypot trong mạng nội bộ (Internal Network)

Honeypot trong mạng nội bộ là một hệ thống giả lập (hoặc thiết bị ảo) được cài đặt bên trong mạng LAN của tổ chức để phát hiện các mối đe dọa nội bộ hoặc các cuộc tấn công đã vượt qua hàng rào bảo vệ bên ngoài (firewall, IDS/IPS).

Ưu điểm:

- Phát hiện được các mối đe dọa bên trong tổ chức, như các nội gián,...
- Theo dõi hoạt động của mã độc, virus nếu một thiết bị nội bộ bị lây nhiễm.
- Giúp xác định APT đã vượt qua firewall và đang hoạt động bên trong.
- Cung cấp dữ liệu forensic cho phân tích sau tấn công.

Nhược điểm:

- Nếu không cấu hình đúng, có thể trở thành điểm yếu giúp hacker mở rộng tấn công.
- Dễ bị phát hiện hơn vì môi trường ít nhiễu hơn, hacker "già"có thể nghi ngờ.

Honeypot trong DMZ

Honeypot trong DMZ là hệ thống bẫy giả lập được triển khai trong vùng DMZ – vùng trung lập giữa mạng nội bộ và Internet,giúp phát hiện các cuộc tấn công từ bên ngoài trước khi chúng xâm nhập vào mạng nội bộ. DMZ thường là nơi đặt các dịch vụ công khai như web server, mail server, DNS server,...

Ưu điểm:

- Thích hợp để phân tích tấn công vào dịch vụ công khai như Web, Mail, DNS...
- Thu thập được các mẫu tấn công có mục tiêu cụ thể như brute-force, SQLi, scanning...
- Có thể giảm thiểu rủi ro thực sự đối với server thật bằng cách đóng vai trò "mồi nhử".

Nhược điểm:

- Có thể trở thành lỗ hổng bảo mật nếu không cách ly tốt.
- DMZ thường có nhiều truy cập thật $\rightarrow$ khó tách biệt hành vi đáng ngờ với bình thường.
- Cần phối hợp chặt chẽ với firewall/IDS để tránh nhầm lẫn log.

Honeypot đối diện Internet

Honeypot đối diện Internet là một hệ thống bẫy được triển khai công khai trên Internet, không nằm sau firewall nội bộ hoặc DMZ. Nó có địa chỉ IP công cộng và thường mô phỏng các dịch vụ dễ bị tấn công như: SSH (port 22), HTTP (port 80), RDP (3389), FTP (21), v.v.

Ưu điểm:

- Thu thập được nhiều kiểu tấn công từ mọi nơi trên thế giới: scanning, DDoS, malware distribution...
- Cực kỳ hữu ích cho nghiên cứu bảo mật, threat intelligence, phân tích xu hướng.
- Phát hiện các chiến dịch tấn công mới, botnet,zero day...

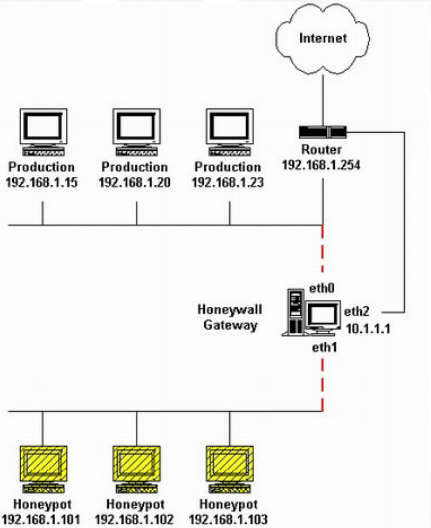
Nhược điểm:

- Rất nguy hiểm nếu không cô lập kỹ: hacker có thể chiếm quyền điều khiển honeypot và sử dụng nó để tấn công hệ thống khác.
- Không đại diện cho hệ thống thật nên dữ liệu thu được có thể không sát thực tế tổ chức.
- Dễ bị nhận diện là honeypot vì không giống server thông thường.

Rủi ro khi sử dụng HoneyPot

- Không bảo vệ hoàn toàn: Honeypot không đảm bảo bảo vệ toàn diện.Nếu bị phát hiện, kẻ tấn công có thể chuyển mục tiêu.
- Cấu hình sai: Honeypot cấu hình sai có thể khiến kẻ tấn công dễ dàng xác định và di chuyển sang các phần khác của mạng, gây nguy cơ cao hơn.
- Thông tin sai lệch: Kẻ tấn công có thể cố tình cung cấp thông tin sai lệch, làm nhầm lẫn trong phân tích.
- Tăng nguy cơ xâm nhập: Nếu honeypot chạy trên môi trường thực với các dịch vụ thật, nó có thể trở thành mục tiêu tấn công thực sự nếu không được quản lý cẩn thận.

HoneyNet



Honeynets là viết tắt của "Honeypot Networks"– tức là một mạng gồm nhiều honeypot được cấu trúc, phối hợp chặt chẽ, nhằm mô phỏng một hệ thống mạng thật để thu hút và giám sát hành vi của kẻ tấn công.

Honeywall là gateway ở giữa honeypots và mạng bên ngoài. Nó hoạt động ở tầng 2 như là Bridged. Các luồng dữ liệu khi vào và ra từ honeypots đều phải đi qua honeywall.
Chức năng: Giám sát toàn bộ lưu lượng đến/đi, ghi log, ngăn chặn tấn công lan rộng.

Data Control trong HoneyNet:

Data Control trong honeynet là việc kiểm soát:
Dữ liệu vào: Giới hạn truy cập vào các dịch vụ mà honeynet giả lập.
Dữ liệu ra: Giới hạn hành vi độc hại như:

- Gửi spam.
- Tấn công máy khác.
- Kết nối ra Internet để tải malware hoặc điều khiển C2 (Command , Control).

VD:Giả sử trong honeynet:
Một attacker tấn công máy giả lập (SSH port 22).
Hắn đăng nhập thành công, cài botnet và dùng nó tấn công IP khác qua port 80.
Honeywall sẽ ghi lại toàn bộ hành động,ngoài ra nó cho phép một số hành động nhỏ ra ngoài để dụ attacker "chơi tiếp",nhưng sẽ drop hoặc redirect các gói tin tấn công ra ngoài .

Honeypot của Hacker là gì?

- Không chỉ các chuyên gia bảo mật, hacker cũng tạo honeypot.
- Honeypot của hacker là hệ thống/file/dịch vụ giả mạo để:

  Đánh lừa và gây nhiễu chuyên gia điều tra
  Bẫy và tấn công ngược lại chuyên gia
  Theo dõi quá trình điều tra

Mục đích của Honeypot Hacker

Mục đích	**Giải thích**
Đánh lạc hướng	Dẫn nhà phân tích đi sai hướng điều tra
Phân tích phản ứng	Xem chuyên gia điều tra tới đâu, tìm thấy gì
Làm sạch dấu vết	Giả dạng log hoặc file config nhằm che giấu phần mềm thật sự nằm sâu bên dưới
Tấn công ngược	Nhúng mã độc vào file log hoặc môi trường sandbox

Các kiểu Honeypot của Hacker

- **Thư mục giả chứa mã độc:** tạo ra thư mục hoặc tập tin trông có vẻ độc hại như malware.exe, thật ra chỉ là script đánh lừa
- **Reverse Honeypot (phản bẫy):**

  Giả dạng malware
  Khi chuyên gia mở để phân tích $\rightarrow$ mã độc kích hoạt
  Gửi dữ liệu ngược về hacker
- **Fake C&C Server:**

  Khi hệ thống sandbox cố kết nối
  Gửi lại dữ liệu sai hoặc mã độc hóa học

Cách Phát Hiện Honeypot của Hacker

Dấu hiệu	**Mô tả**
File/service quá lộ liễu	Ví dụ: malware.zip đặt giữa desktop
Hành vi vòng lặp	Process chạy theo pattern lặp bất thường
Không kết nối thực tế	Không log, không gửi đến server thật
Macro lạ, shellcode ẩn	Nhắm trực tiếp vào analyst

Cách hacker sử dụng Honeypot

- Tạo file, log hoặc dịch vụ giả mạo có vẻ quan trọng.
- Nhúng mã độc (shell script, macro, reverse shell) vào mồi nhử.
- Đặt tên hấp dẫn như `passwords.txt`, `malware.zip`.
- Khi nhà phân tích mở $\rightarrow$ mã độc được kích hoạt ngầm.
- Honeypot gửi dữ liệu về máy chủ của hacker.
- Hacker theo dõi hành vi để cải tiến kỹ thuật ẩn mình.

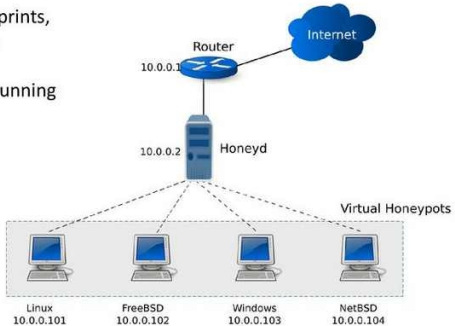
So sánh Honeypot của hacker và mã độc thông thường

Tiêu chí	Honeypot của Hacker	Mã độc Thông thường
Mục tiêu chính	Đánh lừa, bẫy, hoặc phân tích hành vi của chuyên gia bảo mật	Gây thiệt hại, chiếm quyền, trộm dữ liệu hoặc phá hoại
Tính chất nguy hiểm	Gián tiếp: dụ nhà phân tích tự kích hoạt mã độc hoặc sai lầm	Trực tiếp: thực thi mã phá hoại, trộm cắp hoặc mã hóa dữ liệu
Cách thức hoạt động	Giả mạo là file hợp lệ, log, server... nhưng chứa trap tinh vi	Là chương trình thực thi hành vi ác ý ngay khi chạy
Khả năng phát hiện	Khó hơn, vì thường được ngụy trang rất khéo léo	Có thể bị nhận diện bởi chữ ký, hành vi bất thường hoặc sandbox
Tác động tâm lý	Gây nhiễu, làm phân tích viên mất niềm tin vào dấu vết	Tác động tiêu cực trực tiếp đến người dùng hoặc hệ thống
Ví dụ điển hình	Fake log, shell script ngụy danh, C&C server giả, reverse honeypot	Trojan, ransomware, keylogger, worm, spyware

Một số công cụ HoneyPot

Low-interaction honeypots: Honeyd

- Receive and responds to packets routed to unused IP address range.
- Personalities and service scripts are assigned to unused addresses.
- Personality defines traffic fingerprints, i.e., response appear to be from specific OS.
- Service script emulate services running on these addresses.
- Other honeypots available
  - Kippo, ...



Một số công cụ HoneyPot

1. Honeyd

Giới thiệu về Honeyd

Honeyd là một công cụ Low-Interaction Honeypot mã nguồn mở, được thiết kế để mô phỏng nhiều máy tính ảo (ảo hóa cấp IP), mỗi máy có thể chạy các dịch vụ giả, hệ điều hành giả, trên cùng một máy vật lý hoặc máy ảo.

Phát triển bởi Niels Provos – nhà nghiên cứu bảo mật tại Google.

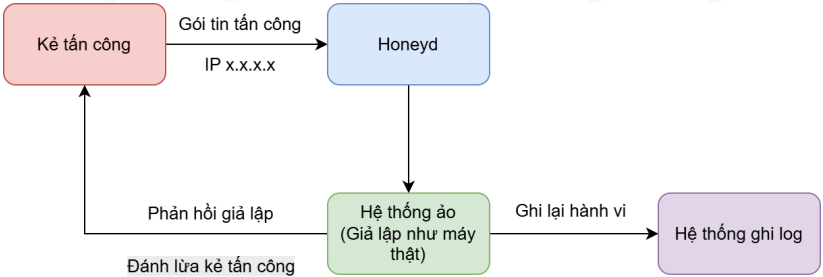
Các tính năng nổi bật của Honeyd

1. Honeyd

Tính năng	Mô tả
Mô phỏng nhiều host cùng lúc	Giả lập hàng trăm IP/máy tính ảo trên một máy thực
Giả dịch vụ	Có thể giả lập các dịch vụ như FTP, SSH, HTTP, Telnet, SMTP,...
Giả hệ điều hành	Gây nhiễu các công cụ quét như Nmap bằng cách cung cấp fingerprint giả
Ghi log chi tiết	Ghi lại mọi tương tác từ attacker như địa chỉ IP, port, và dịch vụ được truy cập
Tùy biến dễ dàng	Cấu hình đơn giản qua file `.conf`, có thể mở rộng thêm nhiều script

Cách thức hoạt động của Honeyd

1. Honeyd



Ưu và nhược điểm của Honeyd

1. Honeyd

Ưu điểm	**Nhược điểm**
Nhẹ, dễ cấu hình	Không tương tác sâu với attacker
Mô phỏng đa dạng IP & dịch vụ	Có thể bị nhận diện bởi attacker có kinh nghiệm
Ghi log tốt, dễ tích hợp	Không phân tích sâu mã độc như high-interaction honeypot

Ứng dụng thực tế của Honeyd

1. Honeyd

Ứng dụng thực tế của Honeyd

- Phát hiện tấn công mạng:Giám sát IP không dùng, phát hiện quét cổng và tấn công; ghi lại hành vi nghi vấn.
- Phân tích spammer: Mô phỏng proxy/mail server để thu hút spammer, ghi lại chuyển email rác cho phân tích.
- Bẫy và làm chậm attacker:Tạo dịch vụ "tarpit" phản hồi chậm, giữ kết nối lâu nhằm tiêu hao tài nguyên kẻ tấn công.
- Huấn luyện và kiểm thử:Tạo mạng ảo với nhiều máy giả phục vụ đào tạo và thử nghiệm an ninh mạng.

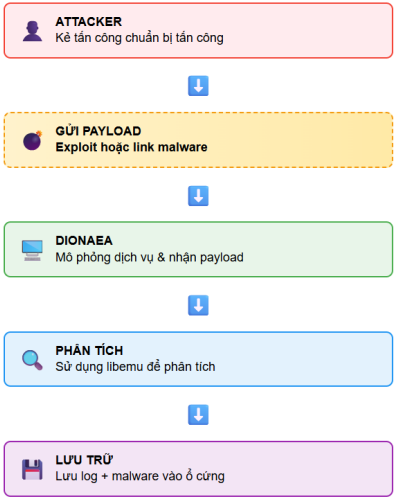
2. Dionaea

Giới thiệu về Dionaea

Dionaea là một low-to-medium interaction honeypot chuyên dùng để thu hút, bẫy và ghi nhận các loại malware – thường được triển khai để phân tích các botnet, ransomware, sâu mạng (worms), v.v.

Viết bằng Python và C, sử dụng nhiều module mạnh như libemu (phân tích shellcode), Python bindings, SQLite để lưu log.

Cách thức hoạt động của Dionaea



Tính năng nổi bật của Dionaea

2. Dionaea

Tính năng	**Mô tả**
Thu hút malware tự động tải xuống	Mô phỏng các dịch vụ như SMB, FTP, HTTP, MSSQL...
Phân tích hành vi shellcode	Tích hợp `libemu` để phân tích nội dung shellcode gửi đến
Lưu mẫu mã độc thực	Malware bị bẫy sẽ được lưu lại dưới dạng file thực để phân tích
Giao diện phân tích log	Có thể tích hợp với ELK stack hoặc MHN để theo dõi log trực quan
Giả IP và dịch vụ dễ dàng	Chạy đa cổng, thu hút nhiều giao thức

Một số giao thức giả lập phổ biến

2. Dionaea

Dionaea hỗ trợ giả lập nhiều dịch vụ, thu hút tấn công đa dạng:

- **SMB (port 445)**: Thu hút khai thác như EternalBlue, ransomware.
- **HTTP (port 80)**: Bẫy malware tải về thông qua web.
- **FTP, TFTP**: Thu hút brute-force và loader gửi mã độc.
- **MSSQL, MySQL**: Dò password, tấn công chèn payload.
- **SIP**: Ghi nhận hoạt động scanner VoIP.

Ứng dụng thực tế của Dionaea Honeypot

2. Dionaea

- **Thu thập mẫu mã độc thực tế:**

  Dionaea có khả năng thu hút và lưu trữ các mẫu mã độc từ các cuộc tấn công thực tế, đặc biệt là qua các giao thức như SMB, FTP, HTTP, MSSQL, SIP.

- **Phân tích hành vi tấn công:**

  Tích hợp với `libemu` để phân tích shellcode và hành vi của mã độc, giúp hiểu rõ hơn về phương thức tấn công.

- **Tích hợp với hệ thống giám sát:**

  Có thể kết hợp với các công cụ như ELK Stack hoặc MHN để trực quan hóa và phân tích dữ liệu log thu thập được.

- **Phát hiện lỗ hổng và tấn công zero-day:**

  Bằng cách mô phỏng các dịch vụ dễ bị tấn công, Dionaea giúp phát hiện các lỗ hổng mới và các cuộc tấn công chưa được biết đến.

- **Giáo dục và đào tạo an ninh mạng:**

  Cung cấp môi trường thực tế để sinh viên và chuyên gia an ninh mạng thực hành và nghiên cứu các kỹ thuật tấn công và phòng thủ.

3. Kippo

Giới thiệu về Kippo

Kippo là một honeypot SSH tương tác trung bình, được viết bằng Python, mô phỏng một hệ thống shell giả để ghi lại toàn bộ quá trình tương tác của attacker. Sau khi attacker đăng nhập thành công qua SSH, Kippo cung cấp một môi trường giả lập hệ thống Linux, cho phép attacker thực hiện các hành động như:

- Gõ lệnh và nhận phản hồi giả lập.
- Duyệt qua hệ thống tập tin giả.
- Tải xuống tệp bằng các công cụ như `wget` hoặc `curl`.

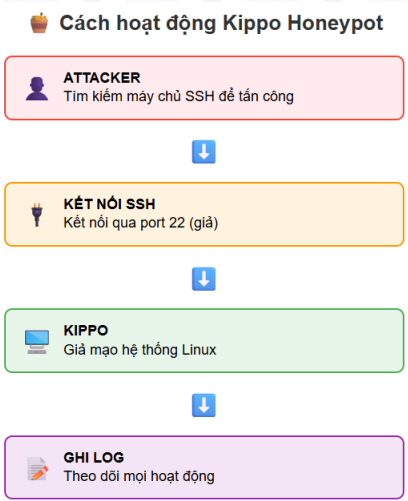
Tính năng nổi bật của Kippo

3. Kippo

Tính năng	Mô tả
Giả dịch vụ SSH thật	Nghe trên cổng 22 (hoặc 2222), phản hồi như một SSH server thật.
Shell ảo đầy đủ	Cung cấp môi trường shell giả cho attacker, cho phép thực thi lệnh và nhận phản hồi.
Giả hệ thống tập tin	Mô phỏng cấu trúc thư mục và tệp tin của hệ thống Linux, cho phép attacker "khám phá".
Log chi tiết	Ghi lại mọi hoạt động của attacker dưới dạng văn bản và ttylog (dạng video).
Bẫy tải file	Lưu lại các tệp mà attacker tải xuống bằng `wget` hoặc `curl` để phân tích sau.

Cách thức hoạt động của Kippo

3. Kippo



4. Cowrie

Giới thiệu về Cowrie

Cowrie là một honeypot tương tác trung bình đến cao (medium-to-high interaction) chuyên mô phỏng các dịch vụ SSH (cổng 22) và Telnet (cổng 23). Mục tiêu chính của Cowrie là thu hút, ghi lại và phân tích các hành vi tấn công từ xa của hacker.

Cowrie được phát triển dựa trên Kippo , nhưng bổ sung nhiều tính năng mạnh hơn.

Cơ chế hoạt động của Cowrie

Cowrie – Honeypot SSH/Telnet hoạt động theo các bước:

- **Giả lập dịch vụ**
- **Tiếp nhận kết nối**
- **Ghi lại lệnh và hành vi**
- **Theo dõi tệp tải lên/tải xuống**
- **Lưu trữ và phân tích dữ liệu**

Tính năng nổi bật của Cowrie

4. Cowrie

Tính năng	Mô tả
Giả lập dịch vụ SSH và Telnet	Mô phỏng các dịch vụ thường xuyên bị tấn công để thu hút kẻ tấn công.
Ghi lại chi tiết hoạt động	Ghi lại các lệnh đã thử và thực thi, cũng như các mẫu tương tác của kẻ tấn công.
Hỗ trợ tải lên và tải xuống tệp	Ghi lại các tệp mà kẻ tấn công tải lên và tải xuống để phân tích sau.
Phiên làm việc tương tác	Mô phỏng các phiên làm việc dòng lệnh tương tác để ghi lại hành vi của kẻ tấn công.
Cấu hình động	Cho phép điều chỉnh cấu hình để mô phỏng các môi trường và thiết lập khác nhau.

Ứng dụng thực tế của Cowrie

4. Cowrie

- **Phân tích hành vi tấn công:** Thu thập dữ liệu về các kỹ thuật tấn công, hỗ trợ phát triển các biện pháp phòng ngừa hiệu quả.
- **Phát hiện và ngăn chặn tấn công:** Giả lập các dịch vụ SSH và Telnet để phát hiện sớm các cuộc tấn công và ngăn chặn chúng trước khi ảnh hưởng đến hệ thống thực tế.
- **Giảm thiểu rủi ro:** Sử dụng Cowrie giúp giảm thiểu rủi ro bị tấn công trực tiếp vào hệ thống thực tế bằng cách "dẫn dụ"kẻ tấn công vào các máy chủ ảo.

Hạn chế của Cowrie

4. Cowrie

- **Khả năng tương tác hạn chế:** Là một honeypot mức trung bình, Cowrie chỉ mô phỏng một phần của hệ điều hành, do đó khả năng tương tác của kẻ tấn công với hệ thống bị giới hạn.
- **Khó khăn trong việc cấu hình:** Việc cấu hình Cowrie đòi hỏi kiến thức kỹ thuật cao và có thể gặp khó khăn đối với người mới bắt đầu.
- **Không hỗ trợ giao thức mới:** Cowrie có thể không hỗ trợ một số giao thức hoặc dịch vụ mới, do đó có thể bỏ sót một số cuộc tấn công sử dụng các giao thức này.

So sánh các công cụ Honeypot (1/2)

3.5. So sánh các công cụ Honeypot (Phần 1)

Tiêu chí	Honeyd	Dionaea	Kippo	Cowrie
Loại Honeypot	Low-Interaction	Low-to-Medium Interaction	Medium-to-High Interaction	Medium-to-High Interaction
Mục tiêu chính	Mô phỏng mạng, gây nhiễu	Thu thập malware, phân tích botnet	Ghi lại tương tác shell SSH	Ghi lại tương tác SSH/Telnet nâng cao
Dịch vụ giả lập	FTP, SSH, HTTP, SMTP,...	SMB, HTTP, FTP, MSSQL, SIP	SSH	SSH, Telnet
Mức độ tương tác	Nhẹ (phản hồi tĩnh)	Trung bình (xử lý payload)	Cao (shell giả tương tác)	Cao (shell giả tương tác cải tiến)
Phân tích mã độc	Không hỗ trợ	Lưu file + phân tích shellcode	Hạn chế (lưu file tải về)	Hạn chế (lưu file tải về)

So sánh các công cụ Honeypot (2/2)

3.5. So sánh các công cụ Honeypot (Phần 2)

Tiêu chí	Honeyd	Dionaea	Kippo	Cowrie
Độ phức tạp triển khai	Dễ (file .conf)	Trung bình (Python/C modules)	Trung bình (Python)	Trung bình - Phức tạp
Tài nguyên yêu cầu	Thấp (mô phỏng 100+ IP)	Trung bình (xử lý payload)	Trung bình	Trung bình - Cao
Khả năng tích hợp	Log cơ bản	ELK, MHN, SQLite	Log text/ttylog	ELK, MHN, JSON/SQL
Ưu điểm chính	Nhẹ, mô phỏng đa IP	Bẫy malware tự động + lưu mẫu	Ghi video terminal	Mô phỏng shell thực tế
Nhược điểm chính	Dễ bị phát hiện, không xử lý payload	Giới hạn giao thức giả lập	Môi trường giả lập hạn chế	Cấu hình phức tạp

Mục tiêu và phạm vi mô phỏng

Mục tiêu đề tài

- Hiểu và triển khai Cowrie Honeypot trên hệ thống Ubuntu để ghi nhận các hoạt động tấn công mạng.
- Thu thập, xử lý và trích xuất thông tin có giá trị từ các log thu được từ Cowrie.
- Ứng dụng các kỹ thuật tiền xử lý dữ liệu (pandas, ipaddress, GeoIP) để làm sạch và chuẩn hóa log.
- Phân tích hành vi tấn công qua biểu đồ trực quan (Plotly Express) và kỹ thuật phân cụm không giám sát (DBSCAN).
- Đánh giá khả năng nhận diện nhóm tấn công tiềm ẩn dựa trên đặc trưng mạng (IP, geolocation, thời gian, lệnh gõ...).

Phạm vi đề tài

- Sử dụng Cowrie Honeypot với giao diện web HTML/CSS đơn giản nhằm đánh lừa attacker truy cập.
- Triển khai honeypot trên môi trường Ubuntu nội bộ, không triển khai thực tế trên Internet công cộng.
- Phân tích tập dữ liệu log có sẵn (hoặc sinh ra trong quá trình thử nghiệm) với số lượng 82.000 dòng.
- Chỉ áp dụng thuật toán phân cụm DBSCAN, không triển khai hệ thống cảnh báo hay học sâu (Deep Learning).
- Mục tiêu chính là mô phỏng quy trình phân tích log và rút trích hành vi, không nhằm mục đích phòng thủ thực tế.

Hệ thống thực hiện

Sơ đồ tổng quan hệ thống

Hình 2 – Sơ đồ tổng quan hệ thống.

- Hệ thống gồm 3 giai đoạn chính:
  - Ghi nhận hành vi tấn công qua Cowrie Honeypot
  - Tiền xử lý và phân tích log
  - Trực quan hóa và phân cụm hành vi

Tổng kết và đánh giá

Tổng kết và đánh giá

- Đề tài đã trình bày cách cài đặt, cấu hình và vận hành hệ thống Honeypot sử dụng Cowrie để thu thập log các hành vi tấn công mạng.
- Các log thu thập được đã được tiền xử lý: chuyển về dạng CSV, làm sạch, phân tích địa lý và kỹ thuật mạng.
- Ứng dụng các thư viện Python như `pandas`, `ipaddress`, `plotly.express`, và `sklearn.cluster` để trực quan hóa và phân cụm dữ liệu.
- Xây dựng được giao diện web login giả để thu hút hacker, đóng vai trò như một lớp bẫy trực quan.
- Qua phân tích, đề tài rút ra được những xu hướng và mô hình tấn công cơ bản từ các IP độc hại.
- Kết quả hỗ trợ nâng cao nhận thức và chuẩn bị giải pháp phòng thủ mạng phù hợp hơn.

Trân trọng cảm ơn!

Mọi ý kiến đóng góp nhóm xin được ghi nhận
để bài làm có thể hoàn thiện hơn trong tương lai.