| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA AN TOÀN THÔNG TIN**  Logo HvKTMM  **CƠ SỞ AN TOÀN THÔNG TIN**  **NHÓM 7 : TÌM HIỂU VỀ HONEYPOT**  Ngành: An toàn thông tin  Mã số: 7.48.02.02  *Sinh viên thực hiện*: **Phan Anh Duy AT170615**    *Người hướng dẫn*: **Nguyễn Ngọc Toàn**  Khoa An toàn thông tin – Học viện Kỹ thuật mật mã  **Hà Nội, 2023** |
| --- |

**LỜI CẢM ƠN**

Trong suốt thời gian học tập tại trường em đã nhận được rất nhiều sự quan tâm và tận tình chỉ bảo của các thầy cô. Nhờ đó mà em đã tiếp thu được không ít các kiến thức cùng kinh nghiệm quý báu trong lĩnh vực An toàn thông tin. Các kiến thức và kinh nghiệm này là một hành trang vững chắc cho em trong học tập cũng như trong công việc sau này.

Em xin chân thành cảm ơn thầy **Nguyễn Ngọc Toàn** đã tận tình hướng dẫn, truyền đạt kiến thức và chỉ bảo cho em trong suốt thời gian thực hiện đề tài để em có thể hoàn thành bài báo cáo này một cách tốt nhất. Mặc dù có nhiều cố gắng nhưng với lượng kiến thức hạn hẹp nên bài báo cáo của em không thể tránh khỏi nhiều thiếu sót. em rất mong nhận được sự góp ý, chỉ bảo của thầy để bài báo cáo của em được hoàn thiện hơn. Em xin chân thành cảm ơn!

Hà Nội, tháng 10 năm 2023

**MỤC LỤC**

[***MỞ ĐẦU***](#_heading=h.gjdgxs) 1

**DANH MỤC HÌNH VẼ………………………………………**

[***CHƯƠNG I – TỔNG QUAN VỀ HỆ THỐNG HONEYPOT***](#_heading=h.30j0zll) 3

[**1.1. Khái niệm và vai trò của hệ thống HONEYPOT** 3](#_heading=h.1fob9te)

[**1.1.1. Giới thiệu về HONEYPOT** 3](#_heading=h.3znysh7)

[**1.1.2. Ưu , nhược điểm của HONEYPOT** 6](#_heading=h.tyjcwt)

[**1.1.3. Các loại hình Honeypot** 7](#_heading=h.1t3h5sf)

[**1.2. Mạng Honeynet** 8](#_heading=h.3rdcrjn)

[**1.2.1. Khái niệm Honeynet** 8](#_heading=h.26in1rg)

[**1.2.2. Các chức năng của Honeynet** 9](#_heading=h.35nkun2)

[**1.2.3. Vai trò và ý nghĩ của Honeynet** 11](#_heading=h.2jxsxqh)

[***CHƯƠNG II : KẾ HOẠCH TRIỂN KHAI HONEYPOTS***](#_heading=h.z337ya) 12

[**2.1. Triển khai Honeypots** 12](#_heading=h.3j2qqm3)

[**2.2**. **Lôi kéo kẻ tấn công** 14](#_heading=h.1y810tw)

[**2.3. Xác định mục tiêu** 14](#_heading=h.4i7ojhp)

[**2.4. Vị trí đặt hệ thống Honeypots** 15](#_heading=h.1ci93xb)

[***CHƯƠNG III: TRIỂN KHAI – CÀI ĐẶT – THỰC NGHIỆM***](#_heading=h.3whwml4) 16

[**3.1. Kịch bản** 16](#_heading=h.2bn6wsx)

[**3.2. Mô hình thực nghiệm** 17](#_heading=h.qsh70q)

[**3.3 Sở đồ thực hành** 18](#_heading=h.3as4poj)

[**3.4 Thực hiện thực nghiệm** 18](#_heading=h.1pxezwc)

[***KẾT LUẬN***](#_heading=h.49x2ik5) 29

[***TÀI LIỆU THAM KHẢO***](#_heading=h.2p2csry) 29

# **MỞ ĐẦU**

Trong thời đại số hóa ngày càng phát triển, an ninh mạng trở thành một vấn đề cấp thiết không chỉ đối với cá nhân mà còn đối với tổ chức và doanh nghiệp trên khắp thế giới. Mạng internet không chỉ mang lại tiện ích và cơ hội, mà còn đặt ra những thách thức an ninh mạng ngày càng phức tạp. Các mối đe dọa từ các hành vi tấn công mạng đe dọa sự bảo mật của dữ liệu, thông tin cá nhân, và hoạt động kinh doanh.

Honeypot, một khái niệm trong lĩnh vực an ninh mạng, đã nổi lên như một công cụ quan trọng trong việc đối phó với các hành vi tấn công và xâm nhập vào hệ thống mạng. Honeypot không chỉ giúp phát hiện và theo dõi các tấn công mạng mà còn cho phép chúng ta nghiên cứu và hiểu rõ hơn về cách các tội phạm mạng hoạt động, từ đó cải thiện bảo mật và phòng ngừa các loại tấn công tương lai.

Khác với các hệ thống An ninh mạng khác như: Hệ thống phát hiện xâm nhập và chống xâm nhập ( IDS - IPS ), Hệ thống Firewall,…, được thiết kế làm việc thụ động trong việc phát hiện - ngăn chặn sự tấn công của tin tặc ( Hacker ) vào hệ thống mạng, thì Honeypot lại được thiết kế nhằm chủ động lôi kéo Hacker tấn công vào hệ thống giả được bố trí bên cạnh hệ thống thật với nhiều mục đích

Trong nghiên cứu này, sẽ cùng khám phá và tìm hiểu về Honeypot, một công cụ mạng đầy tiềm năng và đa dạng trong lĩnh vực an ninh mạng. đi sâu vào các khía cạnh khác nhau của Honeypot, từ loại hình và triển khai đến ứng dụng thực tế và những thách thức đặt ra trong việc sử dụng nó. Đồng thời, cũng sẽ xem xét những nghiên cứu và phát triển mới nhất trong lĩnh vực này, để hiểu rõ hơn về tương lai của Honeypot và vai trò quan trọng của nó trong việc bảo vệ an toàn mạng.

Hãy cùng khám phá thế giới đầy thách thức và cơ hội của Honeypot và nhận thức sâu hơn về tầm quan trọng của an ninh mạng trong cuộc sống hàng ngày của chúng ta.

***DANH MỤC HÌNH VẼ***

[***Hình 1.1. Hũ mật*** 3](#_heading=h.2et92p0)

[***Hình 1.2. Mô hình Honeypot*** 5](#_heading=h.3dy6vkm)

[***Hình 1.3. Mô hình các loại Honeypot*** 6](#_heading=h.4d34og8)

[***Hình 1.4. Ví dụ về BackOffice Friendly*** 7](#_heading=h.2s8eyo1)

[***Hình 1.5. Ví dụ về Honeyd*** 8](#_heading=h.17dp8vu)

[***Hình 1.6. Mô hình kiến trúc Honeynet*** 9](#_heading=h.lnxbz9)

[***Hình 1.7. Thu thập dữ liệu*** 11](#_heading=h.1ksv4uv)

[***Hình 1.8. Giao diện phân tích dữ liệu*** 12](#_heading=h.44sinio)

[***Hình 2.1. Ví dụ về một sản phẩm Honeynet*** 14](#_heading=h.2xcytpi)

# **CHƯƠNG I – TỔNG QUAN VỀ HỆ THỐNG HONEYPOT**

## **1.1. Khái niệm và vai trò của hệ thống HONEYPOT**

### **1.1.1. Giới thiệu về HONEYPOT**

Honeypot là một hệ thống tài nguyên thông tin được xây dựng với mục đích giả dạng đánh lừa những kẻ sử dụng và xâm nhập không hợp pháp, thu hút sự chú ý của chúng, ngăn không cho chúng tiếp xúc với hệ thống thật. Honeypot có thể được xem như “Mắt ong”; và tất nhiên là Honeypot cũng có phải có “Mật ngọt” – tức là có chứa các Hệ thống tài nguyên thông tin có giá trị, nhạy cảm, có tính bí mật như : thông tin về chứng khoán, thông tin tài khoản ở các ngân hàng, thông tin bí mật an ninh quốc gia…., để làm “mồi” dụ Hacker chú ý đến tấn công.



# *Hình 1.1. Hũ mật*

Hệ thống tài nguyên thông tin có nghĩa là Honeypot có thể giả dạng bất cứ loại máy chủ tài nguyên nào như là Mail Server, Domain Name Server, Web Server… được cài đặt chạy trên bất cứ Hệ điều hành nào như: Linux ( Red hat, Fedora…), Unix( Solaris), Window ( Window NT, Window 2000, Window XP, Window 2003, Vista,….. Honeypot sẽ trực tiếp tương tác với tin tặc và tìm cách khai thác thông tin về tin tặc như hình thức tấn công, công cụ tấn công hay cách thức tiến hành thay vì bị tấn công.

Thông tin tình báo thu thập được từ honeypots rất hữu ích trong việc giúp các tổ chức phát triển và nâng cao chiến lược an ninh mạng của họ nhằm đối phó với các mối đe dọa trong thế giới thực và xác định các điểm mù tiềm ẩn trong kiến ​​trúc, thông tin và an ninh mạng hiện có.

### **1.1.2. Ưu , nhược điểm của HONEYPOT**

\*\* Ưu điểm : Honeypot là một khái niệm rất đơn giản, trong đó cung cấp một số đặc điểm mạnh mẽ.

+ Phát hiện tấn công: Honeypot cho phép phát hiện các tấn công mạng và xâm nhập một cách hiệu quả. Nó thu thập dữ liệu về các hoạt động tấn công, cho phép các chuyên gia an ninh mạng nghiên cứu và phân tích chúng.

+ Học hỏi và cải thiện an ninh: Dựa trên dữ liệu từ Honeypot, tổ chức có thể cải thiện an ninh mạng của họ bằng cách hiểu rõ hơn về cách kẻ tấn công hoạt động và điều chỉnh biện pháp bảo mật.

+ Mở rộng kiến thức về tấn công: Honeypot giúp nghiên cứu và phát triển kiến thức về các mô hình tấn công, công cụ và kỹ thuật mới, giúp ngăn chặn tấn công tương lai.

+ Bảo vệ tài nguyên quan trọng: Honeypot có thể được sử dụng như một "mồi" để lôi kéo tấn công ra khỏi hệ thống chính, bảo vệ các tài nguyên quan trọng hơn.

+ Giúp xác định kẻ tấn công: Thông qua phân tích tấn công vào Honeypot, tổ chức có thể xác định nguồn gốc của các cuộc tấn công và đối phó với chúng.

\*\* Nhược điểm : Giống như nhiều công nghệ, các Honeypots cũng có những yếu điểm. Đó là do chúng không thể thay thế các công nghệ hiện tại, nhưng làm việc với các công nghệ hiện có.

+ Nguy cơ bị tấn công: Honeypot là một mục tiêu dễ bị tấn công vì nó được thiết lập để lôi kéo tấn công. Nếu không được quản lý cẩn thận, nó có thể trở thành một cửa vào cho kẻ tấn công vào hệ thống chính.

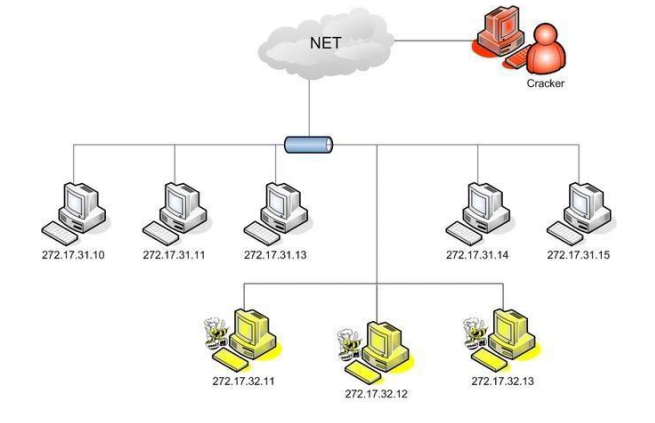
+ Tài nguyên và bảo trì: Triển khai và duy trì Honeypot đòi hỏi tài nguyên và thời gian. Nó cần sự chú ý và quản lý liên tục để đảm bảo hiệu suất và bảo mật.

+ Sự phức tạp của dữ liệu: Dữ liệu thu thập từ Honeypot có thể phức tạp và cần phân tích kỹ thuật để hiểu được. Điều này đòi hỏi sự hiểu biết và kỹ năng chuyên môn.

+ Pháp lý và quyền riêng tư: Sử dụng Honeypot có thể gây ra vấn đề pháp lý và vi phạm quyền riêng tư nếu không tuân thủ các quy định và luật pháp liên quan.

+ Khả năng nhầm lẫn: Có thể xảy ra trường hợp Honeypot nhầm lẫn và chặn truy cập từ người dùng hợp pháp, gây phiền toái và nguy cơ tiêu biểu.

Tùy thuộc vào mục tiêu và yêu cầu cụ thể, Honeypot có thể là một công cụ hữu ích trong việc bảo vệ mạng, nhưng cần được sử dụng và quản lý cẩn thận để tận dụng được ưu điểm và giảm thiểu nhược điểm.

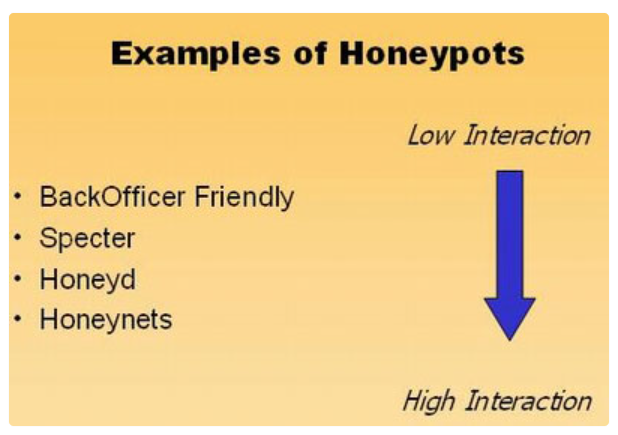
*Hình 1.2. Mô hình Honeypot*

### **1.1.3. Các loại hình Honeypot**

Honeypot được chia làm hai loại chính: Tương tác thấp và tương tác cao .

+ Tương tác thấp: Honeypot chỉ cài đặt chương trình (chẳng hạn như: Honeyd, BackOfficer Friendly, Specter,) mô phỏng giả các dịch vụ, ứng dụng, và hệ điều hành. Loại này có mức độ rủi ro thấp, dễ triển khai và bảo dưỡng nhưng lại bị giới hạn về dịch vụ.

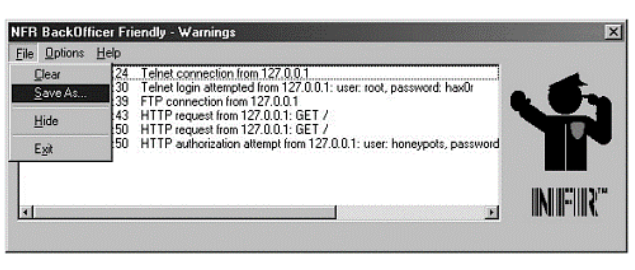
+ Tuơng tác cao: Honeypot được cài đặt, chạy các dịch vụ, ứng dụng và hệ điều hành thực ( Chẳng hạn như Honeynet ). Loại này có mức độ thông tin thu thập được cao nhưng mức độ rủi ro cao và tốn thời gian để vận hành và bảo dưỡng.



# *Hình 1.3. Mô hình các loại Honeypot*

\*\* Đặc điểm của các loại Honeypot

+ BackOfficer Friendly (BOF): là một loại hình Honeypot rất dễ vận hành và cấu hình và có thể hoạt động trên bất kì phiên bản nào của Windows và Unix nhưng nhược điểm của nó là chỉ tương tác được với một số dịch vụ đơn giản như FTP, Telnet, SMTP…

*Hình 1.4. Ví dụ về BackOfficer Friendly*

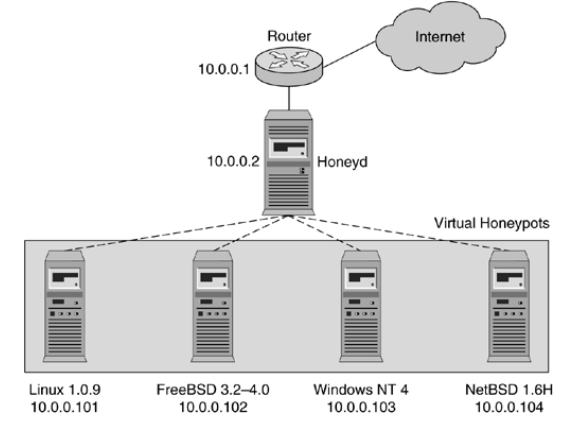
+ Specter: đây cũng là loại hình Honeypot tương tác thấp nhưng có khả năng tương tác tốt hơn so BackOfficer, loại Honeypot này có thể giả lập trên 14 cổng ( Port ); và có thể cảnh báo, quản lý từ xa. Tuy nhiên, cũng giống như BackOfficer thì Specter có nhược điểm là bị giới hạn số dịch vụ và không linh hoạt.

+ Honeyd:

- Loại Honeypot này có thể lắng nghe trên tất cả các cổng TCP và UDP, những dịch vụ mô phỏng được thiết kế với mục đích ngăn chặn và ghi lại những cuộc tấn công, tương tác với kẻ tấn công trong vai trò là một hệ thống nạn nhân.

- Hiện nay, Honeyd có nhiều phiên bản và có thể mô phỏng được khoảng 473 hệ điều hành.

- Honeyd là loại hình Honeypot tương tác thấp có nhiều ưu điểm tuy nhiên Honeyd có nhược điểm là không thể cung cấp một hệ điều hành thật để tương tác với tin tặc và không có cơ chế cảnh báo khi phát hiện hệ thống bị xâm nhập hoặc gặp phải nguy hiểm.



*Hình 1.5. Ví dụ về Honeyd*

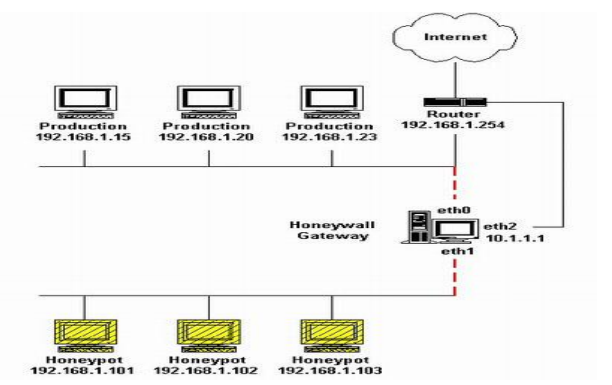
## **1.2. Mạng Honeynet**

### **1.2.1. Khái niệm Honeynet**

Honeynet (tạm gọi là “Tổ ong”) là một hình thức của honeypot tương tác cao. Khác với các honeypot khác, Honeynet là một hệ thống thật, hoàn toàn giống một mạng làm việc bình thường và Honeynet cung cấp các hệ thống, ứng dụng, các dịch vụ thật như : Web, Mail, File server,...

Honeynet khác với các hệ thống Firewall, hệ thống phát hiện và ngăn chặn xâm nhập, hệ thống mã hóa ở chỗ : các hệ thống tuy đều có khả năng bảo vệ hệ thống mạng và tài nguyên mạng nhưng các hệ thống này đều là thực hiện nhiệm vụ “Phòng thủ”, mang tính thụ động; ngược lại, Honeynet lại là hệ thống chủ động lôi kéo, thu hút sự chú ý và tấn công của Hacker nhằm thu thập các thông tin của Hacker như: Kỹ thuật tấn công của Hacker, công cụ Hacker sử dụng, các loại mã độc mới được xuất hiện,....

Nhiệm vụ quan trọng nhất khi triển khai xây dựng – cài đặt một hệ thống Honeynet chính là Honeywall. Honeywall là gateway ở giữa honeypot và mạng bên ngoài. Nó hoạt động ở tầng 2 như là Bridged.



*Hình 1.6. Mô hình kiến trúc Honeynet*

Với mô hình này Honeywall gồm có 3 card mạng là : eth0, eth1, eth2 . Card mạng eth0 thì kết nối với Production Network, card eth1 thì kết nối với các Honeypot, còn card thứ 3 kết nối với Router. Khi Hacker từ bên ngoài Internet tấn công vào hệ thống thì các Honeypot sẽ đóng vai trò là hệ thống thật tương tác với Hacker, và thực hiện thu thập các thông tin của Hacker như : địa chỉ IP của máy Hacker sử dụng, Kỹ thuật Hacker tấn công, các công cụ mà Hacker sử dụng …. Các thông tin này đều sẽ bị ghi lại trên Honeywall, và được các chuyên gia an ninh mạng sử dụng để phân tích kỹ thuật tấn công của Hacker ; qua đó, đánh giá được mức độ an toàn của hệ thống, và có biện pháp kịp thời khắc phục các điểm yếu tồn tại trong hệ thống .

### **1.2.2. Các chức năng của Honeynet**

\*\* Điều khiển dữ liệu : Nhằm ngăn chặn tin tặc sử dụng Honeynet để làm bàn đạp tấn công hệ thống mạng bên ngoài.

+ Khi các mã hiểm độc thâm nhập vào Honeynet , sẽ bị kiểm soát các hoạt động

+ Các luồng dữ liệu khi đi vào không hạn chế , nhưng khi đi ra ngoài thì sẽ bị hạn chế

\*\* Thu thập dữ liệu : Là việc giám sát và ghi lại tất cả hoạt động của các thành phần trong hệ thống Honeynet.

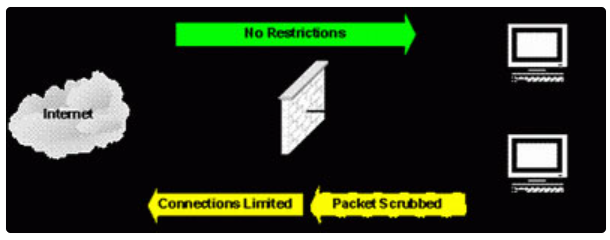
+ Honeynet định nghĩa ba lớp quan trọng của chức năng thu thập dữ liệu gồm:

- Nhật ký của tường lửa

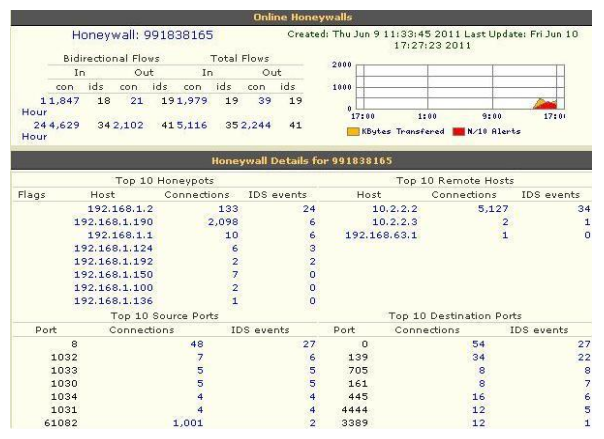
- Lưu lượng của mạng

- Các hoạt động của hệ thống

+ Khi dữ liệu đi vào thì honeynet sẽ xem xét và ghi lại tất cả các hoạt động có tính phá hoại và sau đó sẽ phân tích các động cơ hoạt động của tin tặc.

*Hình 1.7. Thu thập dữ liệu*

\*\* Phân tích dữ liệu : Mục đích chính của honeynet chính là thu thập thông tin. Khi đã có thông tin thì người dùng cần phải có khả năng để phân tích các thông tin này. Để thực hiện tốt công việc này, đòi hỏi người phân tích phải có một kiến thức rất tốt về an ninh mạng, phải am hiểu về các kỹ thuật tấn công mạng. Vì vậy, thông thường người thực hiện phân tích thường là các chuyên gia an ninh mạng.

****

# *Hình 1.8. Giao diện phân tích dữ liệu*

### **1.2.3. Vai trò và ý nghĩ của Honeynet**

Honeynet là môi trường thử nghiệm có kiểm soát an toàn giúp sớm phát hiện ra các lỗ hổng bảo mật tồn tại trên các sản phẩm công nghệ thông tin đã triển khai - cài đặt trên Hệ thống thật (Đặc biệt là các lỗ hổng Zero – day). Từ đó, sớm có biện pháp ứng phó - khắc phục kịp thời. Đồng thời, honeynet cũng giúp kiểm tra độ an toàn của hệ thống mạng, các dịch vụ mạng ( như : Web, DNS, Mail,…), và kiểm tra độ an toàn - tin cậy - chất lượng của các sản phẩm thương mại công nghệ thông tin khác (đặc biệt là các Hệ điều hành như: Unix, Linux, Window,…). Thu thập các thông tin, dấu vết của Hacker ( như : địa chỉ IP của máy Hacker sử dụng tấn công, vị trí địa lý của Hacker, thời gian Hacker tấn công,…). Từ đó, giúp chuyên gia an ninh mạng truy tìm thủ phạm.

Ý nghĩa: Qua đây, giúp bạn đọc có những hiểu biết, kiến thức cơ bản về Honeynet cũng như là Honeypot cùng với vai trò và mục đích của việc xây dựng – triển khai hệ thống này,

# **CHƯƠNG II : KẾ HOẠCH TRIỂN KHAI HONEYPOTS**

## **2.1. Triển khai Honeypots**

Để triển khai Honeypots cần có một quá trình xử lý kĩ thuật tốt cùng với việc thực hiện đúng kế hoạch sẽ giúp triển khai thành công hệ thống.

Danh sách dưới đây đưa ra các bước để thực hiện:

+ Xác nhận Honeypots là được cho phép tạo dựng trong một môi trường hệ thống đó.

+ Xác định mục tiêu Honeypots. Tại sao lại muốn chạy Honeypots?

+ Dùng nó để nghiên cứu hay là bảo vệ hệ thống tổ chức máy tính.

+ Xác định vai trò của con người trong việc tạo ra và duy trì một Honeypots. Có chuyên môn kĩ thuật để triển khai một cách chính xác và duy trì một Honeypots không? Có phần mềm và phần cứng để triển khai chưa ? thời gian hàng ngày mất để duy trì và phân tích dữ liệu như thế nào? Tiếp tục thảo luận, nghiên cứu để theo kịp những Honeypots mới và khai thác một cách hiệu quả.

+ Các loại Honeypots sẽ triển khai là nghiên cứu hoặc sản phẩm, thực hay ảo.

+ Xác định cài đặt cấu hình thiết bị mạng cần thiết để tạo ra Honeypots. Kế hoạch và cấu hình một số thành phần hỗ trợ Honeypots và tool (cảnh báo, đăng nhập, giám sát, quản lý…).

+ Thu thập các thiết lập của việc giám sát, đăng nhập và các tool phân tích hợp pháp.

+ Triển khai kế hoạch phục hồi lại. Làm thế nào để phục hồi hệ thống Honeypots nguyên bản sau khi nó được khai thác sử dụng dẫn tới việc hủy hại.

+ Triển khai Honeypots và các thành phần hỗ trợ nó, kiểm tra việc triển khai, đánh giá các công cụ phát hiện xâm nhập, thử nghiệm xem hệ thống Honeypots hoạt động tốt không.

+ Phân tích các kết quả và tìm ra những thiếu sót. Tinh chỉnh các hệ thống Honeypots dựa trên các bài đã được học và nghiên cứu. Lặp lại các bước cần thiết.

* 1. **. Lôi kéo kẻ tấn công**

Nếu để lộ ra Honeypots theo cách mà những địa chỉ IP và các port được truy xuất tới từ Internet, thì nó sẽ được truy cập một cách nhanh chóng. Trung bình hằng ngày các địa chỉ IP công khai trên Internet được thăm dò hàng chục lần. Theo số liệu thống kê của nhiều dự án của Honeypots cho thấy rằng có nhiều hơn một trăm lần thăm dò mỗi ngày và hầu hết các máy chủ lưu trữ đều xảy ra tấn công trong vòng một tuần . Các worm từ Internet sẽ quét nhiều lần trong ngày. Nhiều quản trị của Honeypots đã ghi lại thành công những tổn hại xảy ra chưa đến 20 phút.

Chính vì những nguyên nhân đó một số quản trị viên của Honeypots đã nhanh chóng và tích cực đăng vùng Honeypots của họ tới danh sách email và website của hacker. Những quản trị viên đăng các vị trí Honeypots của họ để khám phá một số tội phạm nghiêm trọng. Thu thập các thông tin, chứng cứ về cách hành vi xâm nhập trái phép. Việc tạo ra Honeypots không bao giờ nên quảng bá sự hiện diện hay mời gọi các hacker vì nó sẽ đánh bại các mục đích chính của Honeypots.

## **2.3. Xác định mục tiêu**

Để thiết kế hệ thống Honeypots cần xác định các mục tiêu, muốn chọn nơi nào để đặt Honeypots. Có rất nhiều câu hỏi cần được trả lời trước khi bắt đầu, bao gồm cả những điều sau đây:

+ Lý do muốn tạo ra hệ thống Honeypots.

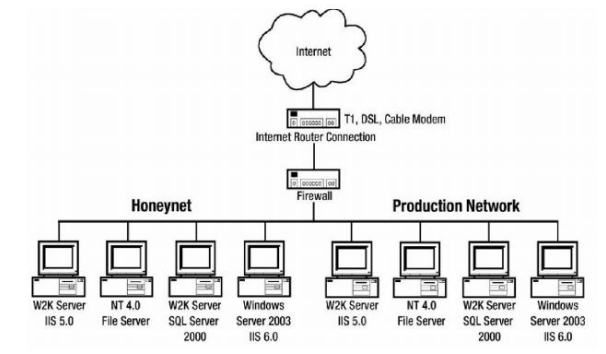
+ Môi trường OS là gì để giả lập Honeypots?

+ Giả lập những loại server hoặc service gì?

+ Muốn theo dõi các mối đe dọa từ bên trong, bên ngoài, hay cả hai?

Để có câu trả lời cho những câu hỏi này về cơ bản là cần xác định là sẽ nghiên cứu hay tạo ra các sản phẩm Honeypots và làm như thế nào? Cấu hình nó ra sao? Sản phẩm Honeypots nên mô phỏng theo các ứng dụng, dịch vụ và máy chủ đã tồn tại. Nếu làm đúng với các tương tác cao, nó sẽ gây khó khăn cho tin tặc trong việc nhận biết và tương tác với Honeypots.

Ví dụ, giả sử hệ thống mạng bao gồm máy chủ chạy HĐH Windows Server 2003 chạy IIS 6.0, Windows 2000 Server chạy Microsoft SQL Server 2000, Windows NT 4.0 Server và một Windows 2000 Server chạy IIS 6.0. Sản phẩm Honeypots sẽ cố gắng để mô phỏng giống như những cái máy chủ dịch vụ ở trên.



# *Hình 2.1. Ví dụ về một sản phẩm Honeynet*

## **2.4. Vị trí đặt hệ thống Honeypots**

Có 3 vùng chính để đặt Honeypots:

+ External Placement (Đặt ở vùng ngoài).

+ Internal Placement (Đặt ở vùng trong)

+ DMZ Placement(Đặt ở vùng DMZ)

Mỗi vùng để đặt Honeypots đều có những ưu điểm và nhược điểm tùy theo mục đích của việc tạo ra Honeypots để làm gì.

+ Đặt ở vùng ngoài: Là vùng nằm ngoài Internet với vị trí này thì sẽ không có bức tường lửa nào đứng trước Honeypots, các Honeypots và mạng lưới Honeypots sẽ chia sẻ cùng một địa chỉ IP subnet công cộng.

+ Đặt ở vùng trong: vị trí Honeypots nằm bên trong mạng và bức tường lửa ở giữa ngăn cách nó với thế giới Internet. Vị trí này là cách tốt nhất để tạo ra một hệ thống cảnh báo sớm cho biết bất kì sự khai thác từ bên ngoài vào và bảo vệ mạng nội bộ, bắt các đe dọa xảy ra cùng một lúc. Một ví dụ cho thấy khi mà worm Blaster tấn công, nhiều công ty đã triển khai Firewall và cấu hình khóa port 135 ngăn chặn an toàn từ các worm nhưng worm có thể lén đi qua firewall trên đường links và từ những máy tính laptop, thiết bị di động. Sau khi đã qua bức tường lửa, các worm có thể lây nhiễm các máy tính nội bộ chưa được vá lỗi hệ điều hành và lỗi bảo mật.

+ Đặt ở vùng DMZ: DMZ là một vùng nằm riêng lẻ so với LAN nhằm mục đích đặt những server public như web server, mail server, ftp server.

# **CHƯƠNG III: TRIỂN KHAI – CÀI ĐẶT – THỰC NGHIỆM**

## **3.1. Kịch bản**

Trong thực tế Web server có thể là hệ thống thật hoặc giả mạo . Khi các hacker tấn công vào hệ thống , Honeywall sẽ thu thập được tất cả các gói tin đến Webserver khi kết hợp với công cụ Sebek được cài đặt trên server. Người quản trị có thể giám sát thời gian thực với những dữ liệu thu thập đó . Từ đó có thể phân tích , đánh giá các thông tin cần thiết để đưa ra các phương án phòng chống , nâng cấp hợp lý

+ Honeywall là gateway ở giữa honeypot và mạng bên ngoài. Nó hoạt động ở tầng 2 như là Bridged. Các luồng dữ liệu khi vào và ra từ honeypot đều phải đi qua Honeywall. Để kiểm soát các luồng dữ liệu này, cũng như thu thập các dấu hiệu tấn công, và ngăn chặn tấn công của các Hacker thì Honeywall sử dụng hai công cụ chính là: IDS Snort và Firewall Iptables (bao gồm các luật – Rule)

+ Sebek là công cụ ghi lại các hoạt động của hacker trên các Honeypot . Sebek hoạt động theo mô hình client–server. Theo mô hình này, thành phần Sebek client được cài đặt trên các Honeypot, còn thành phần Sebek server thì được tích hợp sẵn trên Honeywall. Khi kẻ tấn công thực hành vi xâm nhập vào các Honeypot thì Sebek client sẽ thu thập toàn bộ các thông tin về hoạt động của Hacker và gửi về Sebek server ở Honeywall. Và tại đây, các thông tin thu thập được sẽ được đem ra để phân tích.

Mô tả bằng hình ảnh (Lưu ý: Đây là vẽ theo ý hiểu của em ạ)

**Kẻ tấn công**

xâm nhập

Honeypot( giả mạo Card

Webserver) cài đặt siber client

-> thu thập

## **3.2. Mô hình thực nghiệm**

Chuẩn bị bao gồm 4 máy ảo trong đó :

\* Máy ảo 1 (Honeywall):

─ Sử dụng 03 giao diện mạng:

+ Địa chỉ IP: Bridge (Kết nối mạng bên ngoài)

+ Địa chỉ IP: Host-only

+ Địa chỉ IP: VMNet2

─ RAM: 1GB, HDD: 10GB

\* Máy ảo 2 (WebServer):

─ Cài đặt hệ điều hành Windows Server 2008

─ Cài đặt dịch vụ IIS

─ Tạo 1 Website đơn giản để có thể truy cập tới Web Server

─ Địa chỉ IP: 10.0.0.20 Host-only

─ RAM: 1GB, HDD: 15GB

\* Máy ảo 3 (Manager): quản lỹ giám sát Honeypot

─ Cài đặt hệ điều hành Windows 7

─ Địa chỉ IP: 172.16.1.10 VMNet2

─ RAM: 1GB, HDD: 20GB

\* Máy ảo 4 (Hacker):

─ Cài đặt hệ điều hành Windows 10

─ Địa chỉ IP: 10.0.0.100 Host-only

─ RAM: 1GB, HDD: 20GB

\* Các công cụ cần chuẩn bị cho việc thực nghiệm :

+ File ISO cài đặt Honeywall

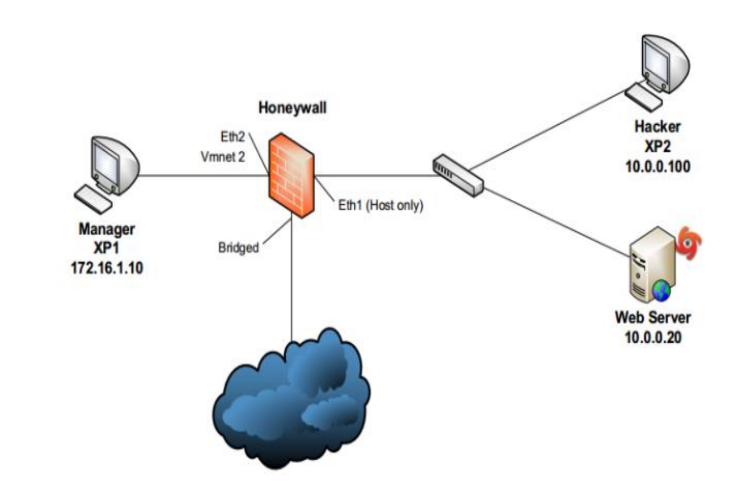
+ File ISO cài đặt Windows Server 2008

+ File ISO cài đặt Windows 7 , 10

+ File cài đặt phần mềm Nmap

+ File cài đặt phần mêm Sebek

## **3.3 Sở đồ thực hành**



+ Máy Manager đóng vai trò là một máy quản trị kết nối tới giao diện của Honeywall để quản trị

+ Máy Hacker đóng vai trò thực hiện cuộc tấn công lên máy Web Server

+ Máy Web Server đóng vai trò một Web Server giả, cho phép các hacker tấn công và két nỗi nối đến một giao diện của Honeywall

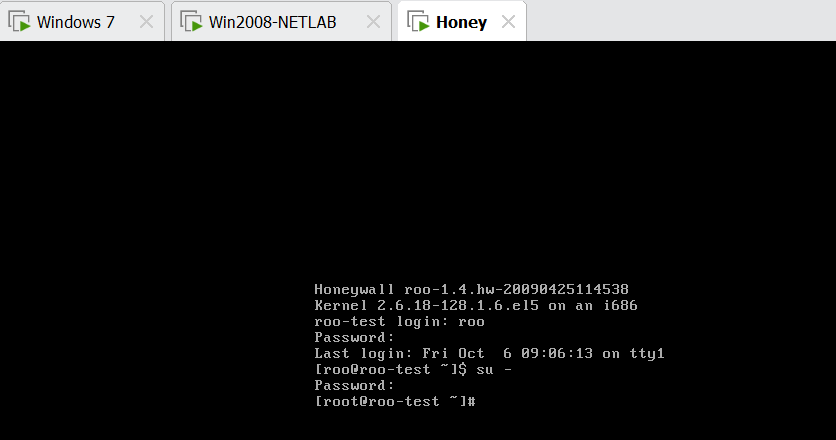
+ Giao diện mạng thứ ba của Honeywall kết nối ra ngoài Internet, với địa chỉ IP phù hợp để có thể ra mạng Internet

## **3.4 Thực hiện thực nghiệm**

**Bước 1: Cài đặt và cấu hình Honeywall**

+ Đăng nhập vào hệ thống sử dụng tài khoản : user - roo ; password – honey

+ Tiếp tục chuyển sang tài khoản root cũng với password - honey



+ Truy cập vào tệp cấu hình của Honeywall :



+ Dòng 44 định nghĩa dải mạng quản lý (dải mạng của Win7 máy quản lý honeypot)



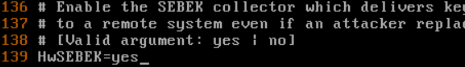
+ Dòng 76 cấu hình Honeywall khi khởi động



+ Dòng số 85 định nghĩa IP của máy chủ honeypot (webserver2008)



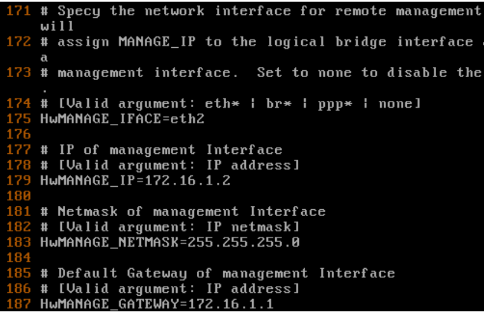
+ Dòng số 139 để cho phép nhân thông tin từ Sebek



+ Dòng số 143 cho phé truy cập quản lý thông qua trình duyệt web



+ Dòng 175 giao diện quản lý: eth2, dòng 179 địa chỉ IP của giao diện quản lý , dòng 187 gateway của mạng quản lý

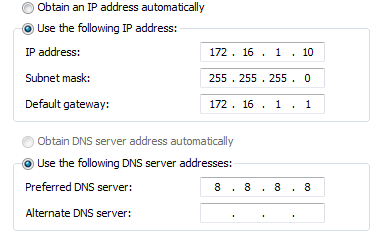


+ Cuối cùng khởi động lại Honeywall bằng lênh sau:

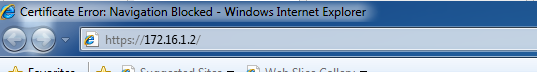


**Bước 2 : Truy cập quản lý từ xa**

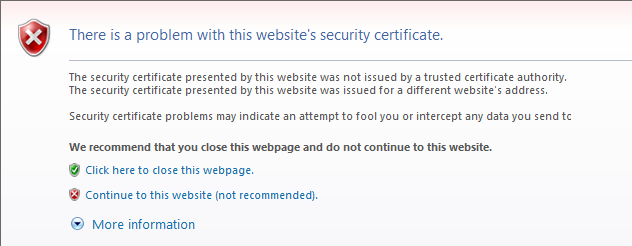
+ Cấu hình địa chỉ IP Win7 (máy manager) :



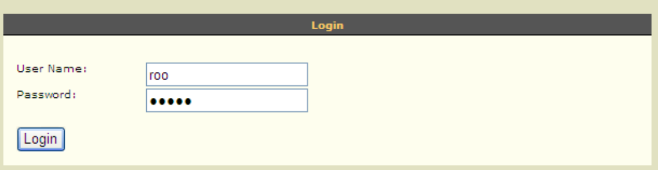
+ Từ máy ảo quản lý Windows 7 sử dụng trình duyệt web truy cập vào địa chỉ đã khai báo ở trên truy cập



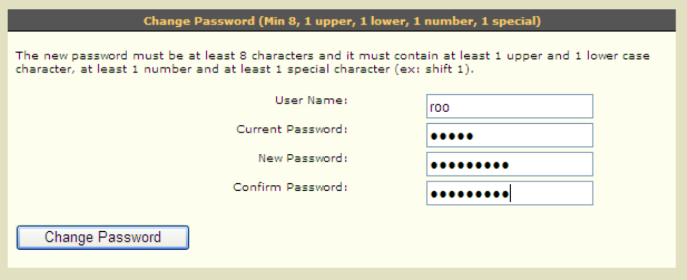
+ Khi xuất hiện cảnh báo bảo mật, lựa chọn “Continue to this website”



+ Giao diện truy cập



+ Thay đổi mật khẩu trong lần đăng nhập đầu tiên

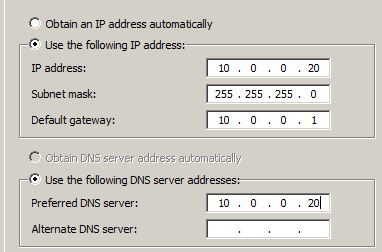


+ Giao diện quản lý của Honeywall

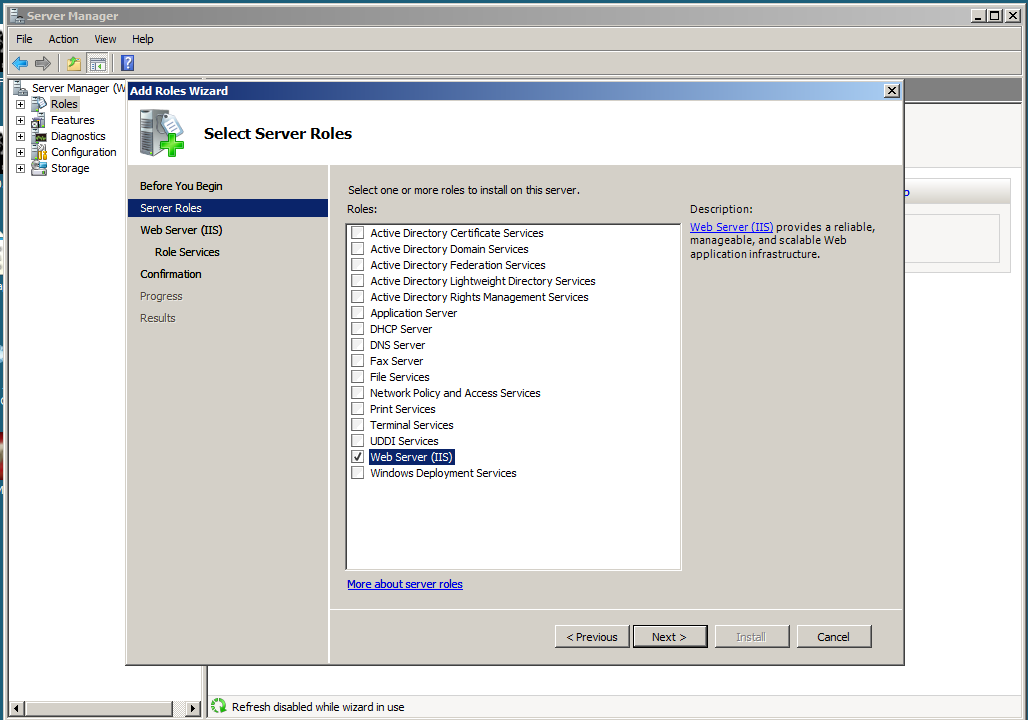


**Bước 3 : Cấu hình Sebek trên Webserver2008**

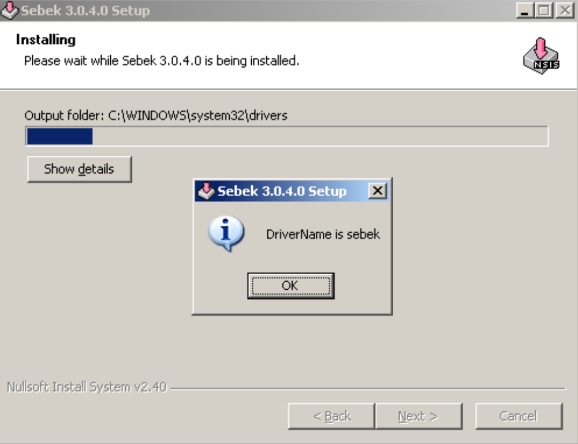
+ Cấu hình địa chỉ IP của winserver



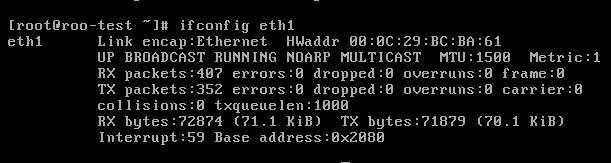
+ Cài đặt dịch vụ Web Server (IIS)



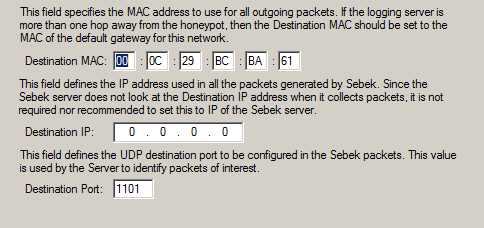
+ Cài đặt phần mềm Sebek: Setup.exe



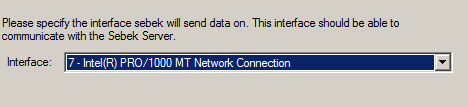
+ Xem địa chỉ MAC eth1 của Honeywall



+ Chạy chương trình: Configuration Wizard.exe để cấu hình Sebek, nhập đúng địa chỉ MAC của eth1 vào giao diện sau:

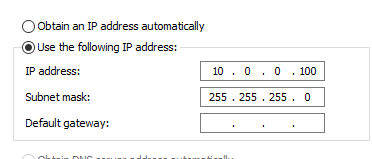


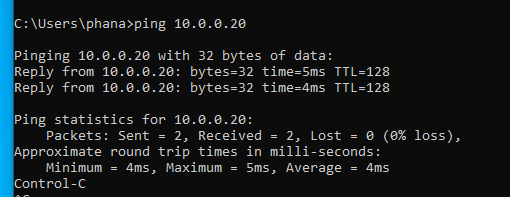
+ Chọn giao diện để Sebek chuyển tiếp thông tin



**Bước 4 : Sử dụng công cụ tấn công để phân tích hành vi**

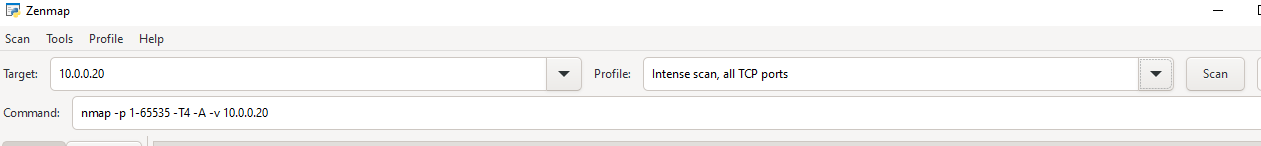
+ Cài đặt địa chỉ IP của máy win10 ( Attack )

****

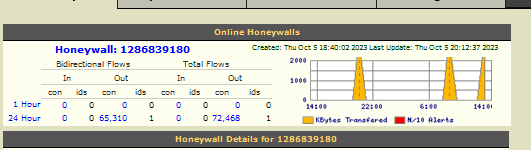
****

**-> Ping thông với máy Winserver2008**

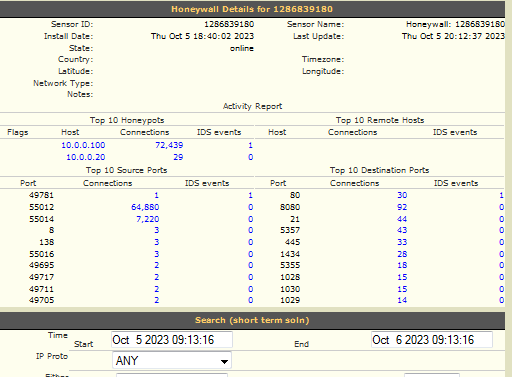
+ Sử dụng công cụ Nmap để quét cổng mở trên Webserver 2008



+ Chuyển sang giao diện quản trị



+ Xem chi tiết trong khoản thời gian nào đó



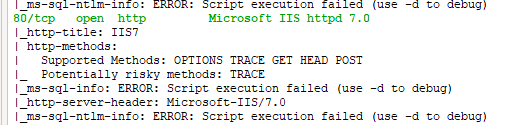
+ Phân tích



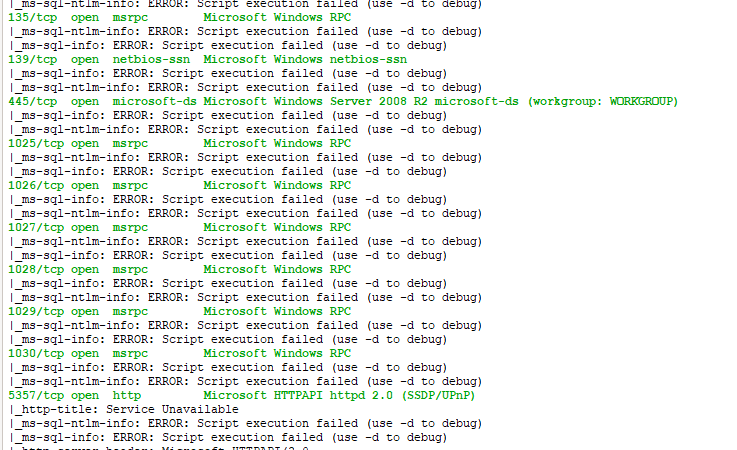
==> Từ việc phân tích các dữ liệu thu thập được ta có thể thấy đây là một cuộc tấn công quét cổng từ địa chỉ 10.0.0.100, ... biết được thời gian mà kẻ tấn công thực hiện

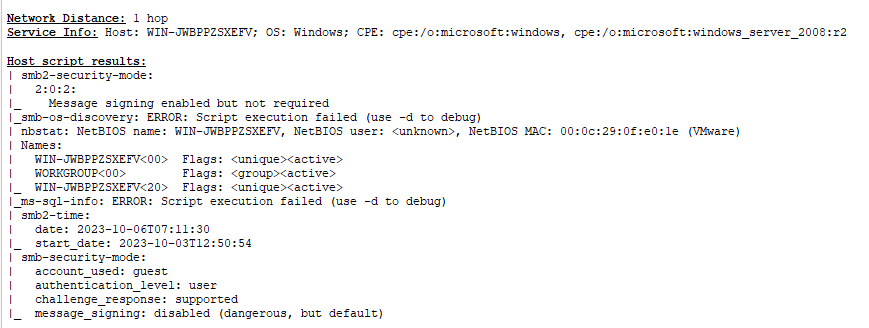
+ Một số thông tin hacker thu thập được khi thực hiện quét cổng:

Hacker có thể biết được dịch vụ IIS7 đã được cài đặt trên Web



+ Danh sách cổng đang mở





**Đánh giá :** Qua bài thực nghiệm giúp người dùng có thể hiểu hơn về :

+ Cấu trúc hệ thống Honeypot

+ Cấu hình Honeywall

+ Theo dõi, giám sát dữ liệu thu thập từ Honeywall

+ Sử dụng các công cụ phổ biến để thực hiện tấn công: rò quét...

# **KẾT LUẬN**

Tìm hiểu về Honeypot là một hành trình thú vị và quan trọng trong lĩnh vực an ninh mạng. Honeypot không chỉ là một công cụ mạng đầy tiềm năng để phát hiện và theo dõi tấn công mạng, mà còn là một cách để nghiên cứu và hiểu rõ sâu hơn về mô hình tấn công, kỹ thuật tấn công, và hành vi của kẻ tấn công. Các ưu điểm của Honeypot bao gồm khả năng nâng cao bảo mật mạng, cải thiện hiệu suất an ninh, và cung cấp thông tin quý báu cho việc phát triển biện pháp bảo mật mới. Tuy nhiên, việc triển khai và quản lý Honeypot cũng đòi hỏi sự chú tâm và sự hiểu biết chuyên môn để tránh các nguy cơ và thách thức. Cuối cùng, tìm hiểu về Honeypot không chỉ giúp bảo vệ mạng một cách hiệu quả mà còn là một cách để tiến xa trong lĩnh vực an ninh mạng và giữ bước với sự phát triển của các mối đe dọa mạng trong tương lai.

Bên cạnh những ưu điểm và thách thức, việc tìm hiểu về Honeypot cũng mở ra cơ hội cho sự học hỏi không ngừng và sáng tạo trong lĩnh vực an ninh mạng. Điều này đặc biệt quan trọng trong bối cảnh môi trường an ninh mạng ngày càng biến đổi và phức tạp. Honeypot không chỉ giúp phát hiện và đối phó với các mối đe dọa hiện tại mà còn đóng vai trò như một phòng thí nghiệm thực tế cho sự nghiên cứu và phát triển. Điều này khuyến khích cộng đồng an ninh mạng khắp nơi hợp tác để chia sẻ thông tin và kinh nghiệm, từ đó nâng cao sự hiểu biết chung và cùng nhau đối phó với các mối đe dọa ngày càng tiên tiến.

Tìm hiểu về Honeypot không chỉ là một nhiệm vụ của các chuyên gia an ninh mạng, mà còn là trách nhiệm của tất cả chúng ta trong việc bảo vệ thông tin cá nhân, tài sản và hệ thống mạng. Với sự tập trung vào sự học hỏi, nghiên cứu và cải thiện liên tục, Honeypot có thể đóng góp quan trọng cho việc xây dựng một môi trường mạng an toàn và đáng tin cậy hơn, phản ánh tầm quan trọng của an ninh mạng trong cuộc sống hàng ngày của chúng ta.

# **TÀI LIỆU THAM KHẢO**

[1]. <https://quantrimang.com/cong-nghe/tim-hieu-ve-honeypot-va-honeynet-37896>

[2[]. https://bkhost.vn/blog/honeypot/](about:blank)

[3]. <https://www.youtube.com/@maithanhthang9472>

[4]. <https://123docz.net/document/2225942-tim-hieu-ve-honeypot-va-honeynet.htm>

[5]. <https://youtube.com/watch?v=tV-uUnsIekc&ab_channel=NguyenLeVu>