BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG**

---


# ĐỒ ÁN TỐT NGHIỆP

**NGÀNH : CÔNG NGHỆ THÔNG TIN**

**Sinh viên : Nguyễn Hữu Mạnh**

**Giảng viên hướng dẫn : TS Hồ Văn Canh**

**HẢI PHÒNG – 2023**

BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG**

---

# TÌM HIỂU VỀ MẠNG MÁY TÍNH VÀ GIẢI PHÁP BẢO MẬT THÔNG TIN CHO MẠNG MÁY TÍNH CỦA CÔNG TY CMC

**ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY**

**NGÀNH: CÔNG NGHỆ THÔNG TIN**

**Sinh viên : Nguyễn Hữu Mạnh**

**Giảng viên hướng dẫn : TS. Hồ Văn Canh**

**HẢI PHÒNG – 2023**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG**

---

# NHIỆM VỤ ĐỀ TÀI TỐT NGHIỆP

**Sinh viên:** Nguyễn Hữu Mạnh **Mã SV:** 1812111011

**Lớp :** CT2201M

**Ngành :** Công nghệ thông tin

**Tên đề tài**: Tìm hiểu về mạng máy tính và giải pháp bảo mật thông tin cho mạng máy tính của Công ty CMC

# NHIỆM VỤ ĐỀ TÀI

## 1.Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp.

a. Nội dung

- Tổng quan mạng máy tính

- Các hệ thống phát hiện và ngăn chặn xâm nhập

- Ứng dụng giải pháp bảo mật cho mạng máy tính của công ty CMC.

b. Các yêu cầu cần giải quyết

-Trình bày tổng quan về mạng máy tính và vấn đề an toàn cho Mạng.

-Trình bày về các hệ thống phát hiện xâm nhập mạng đã tìm hiểu.

-Khảo sát hiện trạng máy tính của đơn vị.

-Triển khai giải pháp bảo vệ an ninh cho hệ thống mạng.

## 2.Các tài liệu cần thiết

[1] Hồ Văn Canh, Lê Danh Cường (2018): Mật mã và an toàn thông tin: Lý thuyết và ứng dụng. NXB: Thông tin và Truyền thông – 8/2018.

[2] Mennezes, Paul C. Van Oorschot, S cott A. Vanstone (1999): Handbook of Applied Cryptography. CRC Press: Boca Raton, New York, London, Tokyo.

[3] Neal Koblitz (2000): A Course in Number Theory and Cryptography.

Springer-Verlag Press: New York, Berlin Heidelberg, London, Pái, and Tokyo (2000).

[4] Phan Đình Diệu (2002): Mật mã và an toàn thông tin. NXB Đại học Quốc gia Hà Nội năm 2002

.[5] Trịnh Nhật Tiến ( 2003): Mật mã và an toàn CSDL. NXB ĐHQG Hà Nội năm 2003.

## 3.Địa điểm thực tập tốt nghiệp

Công ty CMC TELECOM

**CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP**

Họ và tên : Hồ Văn Canh

Học hàm, học vị : Đại Tá-Tiến Sĩ

Cơ quan công tác : Học Viện Kỹ Thuật Mật Mã

**Nội dung hướng dẫn:**

Nội dung dự kiến

- Tổng quan mạng máy tính
- Các hệ thống phát hiện và ngăn chặn xâm nhập
- Ứng dụng giải pháp bảo mật cho mạng máy tính của công ty CMC.

Đề tài tốt nghiệp được giao ngày 07 tháng 11 năm 2022

Yêu cầu phải hoàn thành xong trước ngày 18 tháng 02 năm 2023

| **Đã nhận nhiệm vụ ĐTTN** | **Đã giao nhiệm vụ ĐTTN** |
|---|---|
| Sinh viên | Giảng viên hướng dẫn |
| **Nguyễn Hữu Mạnh** | **TS. Hồ Văn Canh** |

Hải Phòng, ngày ….. tháng….. năm 2022

**TRƯỞNG KHOA**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**Độc lập - Tự do - Hạnh phúc**

# PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN TỐT NGHIỆP

Họ và tên giảng viên: Hồ Văn Canh

Đơn vị công tác: Cục Kỹ thuật Nghiệp Vụ-CBA

Họ và tên sinh viên: Nguyễn Hữu Mạnh  Ngành: Công nghệ thông tin

Đề tài tốt nghiệp:Tìm hiểu về mạng máy tính và giải pháp bảo mật thông tin cho mạng máy tính của công ty CMC.

**1. Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp**

……

…….

…….

…….

**2. Đánh giá chất lượng của đồ án/khóa luận(so với nội dung yêu cầu đã đề ra trong nhiệm vụ Đ.T. T.N trên các lý luận, thực tiễn, tính toán số liệu…)**

…….

…….

…….

…….

**3. Ý kiến của giảng viên chấm phản biện**

Được bảo vệ  Không được bảo vệ  Điểm…….

Hải Phòng, ngày  tháng  năm 2023

Giảng viên chấm phản biện

(Ký và ghi rõ họ tên)

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**Độc lập - Tự do - Hạnh phúc**

# PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN CHẤM PHẢN BIỆN

Họ và tên giảng viên:

Đơn vị công tác:

Họ và tên sinh viên: Nguyễn Hữu Mạnh Ngành: Công nghệ thông tin

Đề tài tốt nghiệp: **Tìm hiểu về mạng máy tính và giải pháp bảo mật thông tin cho mạng máy tính của công ty CMC.**

**1. Phần nhận xét của giảng viên chấm phản biện**

…….

…….

…….

…….

**2. Những mặt còn hạn chế**

…….

…….

…….

…….

**3. Ý kiến của giảng viên chấm phản biện**

Được bảo vệ Không được bảo vệ Điểm……

Hải Phòng, ngày tháng năm 2023

**Giảng viên chấm phản biện**

(Ký và ghi rõ họ tên)

# LỜI CẢM ƠN

Lời đầu tiên, em xin gửi lời cảm ơn chân thành đến các Thầy Cô trong Khoa Công Nghệ Thông, Trường Đại học Quản Lý và Công Nghệ Hải Phòng đã giảng dạy, chỉ bảo cho em kiến thức và kinh nghiệm quý báu trong suốt 4 năm học tại trường để em có thể thực hiện đồ án tốt nghiệp này. Đặc biệt em xin gửi lời cảm ơn sâu sắc tới Thầy Hồ Văn Canh người đã trực tiếp hướng dẫn và tận tình giúp đỡ em hoàn thành tốt đồ án tốt nghiệp của mình. Em cũng xin cảm ơn Cô Nguyễn Thị Xuân Hương – Lãnh đạo Khoa Công Nghệ Thông Tin đã luôn tạo điều kiện cho em và các bạn trong suốt quá trình học cũng như thực hiện các công tác tốt nghiệp.

Em xin trân trọng cảm ơn Ban lãnh đạo, các Thầy Cô ở các phòng ban của Trường ĐH Quản Lý và Công Nghệ Hải Phòng đã cho em môi trường học tập tốt nhất có thể từ khi em bắt đầu đặt chân vào giảng đường và cho đến khi hoàn thành đồ án tốt nghiệp quan trọng nhất trong cuộc đời sinh viên.

Trong quá trình thực tập, cũng như là trong quá trình làm đồ án tốt nghiệp em không tránh khỏi những thiếu sót về trình độ lý luận cũng như kinh nghiệm thực tiễn nên em rất mong sự đóng góp ý kiến và chỉ bảo từ Thầy, Cô để em tiến bộ hơn và có thêm nhiều kinh nghiệm và kiến thức để có thể góp ích cho những công việc sau này.

**Em xin chân thành cảm ơn!**

# LỜI CAM ĐOAN

Em xin cam đoan rằng đề tài này được tiến hành một cách minh bạch, công khai. Mọi thứ được dựa trên sự cố gắng cũng như sự nỗ lực của bản thân cùng với sự giúp đỡ của thầy Hồ Văn Canh.

Các số liệu và kết quả nghiên cứu được đưa ra trong đồ án là trung thực và không sao chép hay sử dụng kết quả của bất kỳ đề tài nghiên cứu nào tương tự. Nếu như phát hiện rằng có sự sao chép kết quả nghiên cứu đề những đề tài khác bản thân em xin chịu hoàn toàn trách nhiệm.

Hải Phòng, ngày 20 tháng 10 năm 2022

**Sinh viên**

(Ký và ghi rõ họ tên)

# MỤC LỤC

# DANH MỤC HÌNH

# DANH MỤC TỪ VIẾT TẮT

| Từ viết tắt | Tiếng Anh | Tiếng Việt |
|---|---|---|
| CERT | Computer Emegency Response | Trung tâm khẩn cấp máy tính |
| PC | Personal computer | Máy tính cá nhân |
| WAN | Wide Area Network | Mạng diện rộng |
| LAN | Local Area Network | Mạng cục bộ |
| MAN | Metropolitan Area Network | Mạng khu vực đô thị |
| WWW | World Wide Web | World Wide Web |
| FTP | File Transfer Protocol | Giao thức truyền tệp tin |
| VOIP | Voice over Internet Protocol | Dịch vụ thoại qua Internet |
| WAP | Wireless Application Protocol Denial of Service | Giao thức ứng dụng không dây |
| DoS | Denial Of Service | Từ chối dịch vụ |
| DdoS | Distributed Denial of Service | Từ chối dịch vụ phân tán |
| WAF | Web application firewall | Tường lửa ứng dụng Wed |
| OSI | Open Systems Interconnection | Kết nối hệ thống mở |
| HTTP | Hypertext Transfer Protocol | Giao thức truyền siêu văn bản |
| HTTP/S | Hypertext Transfer Protocol Secure | Giao sức truyền siêu văn bản bảo mật |
| UTM | Urchin Tracking Module | Modul theo dõi Urchin |
| ATP | Advanced Persistent Threat | Mối đe doạ liên tục nâng cao |
| OTP | One-time password | Mật khẩu dùng 1 lần |
| IDS | Intrusion Detection Systems | Hệ thống phát hiện xâm nhập |
| SSL | Secure Sockets Layer | Lớp ở ổ cắm an toàn |
| NIDS | Network-based IDS | Hệ thống phát hiện xâm nhập mạng |
| HIDS | Host-based IDS | Hệ thống phát hiện xâm nhập máy chủ |
| IPS | Intrusion Prevention System | Hệ thống ngăn chặn xâm phạm |
| NIPS | Address Resolution Protocol | Hệ thống ngăn chặn xâm nhập mạng |
| HIPS | Interio Gateway Routing Protocol | Hệ thống ngăn chặn xâm nhập máy chủ |
| DMZ | Open Shortest Path First | Khu trung lập |
| VPN | Routing Information Protocol | Mạng riêng ảo |
| VLAN | Internetwork Packet Exchange | Mạng cục bộ ảo |

| | | |
|---|---|---|
| NAC | Internet Message Access Protocol | Kiểm soát truy cập mạng |
| SNMP | Post Office Protocol version 3 | Giao thức quản lý mạng đơn giản |
| ICMP | Network Mapper | Giao thức thông báo kiểm soát Internet |
| ASCII | Terms Of Service | Mã tiêu chuẩn hoa kì để trao đổi thông tin |
| ARP | Address Resolution Protocol | Giao thức phân giải địa chỉ |
| IGRP | Interio Gateway Routing Protocol | Giao thức định tuýeen cổng Interio |
| OSPF | Open Shortest Path First | Giao thức định tuyến OSPF |
| RIP | Routing Information Protocol | Giao thức định tuyến |
| IPX | Internetwork Packet Exchange | Trao đổi gói Internetwork |
| CIDR | Classless Inter Domain Routing | Định tuyến liên miền phân lớp |
| IMAP | Internet Message Access Protocol | Giao thức truy cập tin nhắn Internet |
| POP3 | Post Office Protocol version 3 | Giao thức tầng ứng dụng phiên bản 3 |
| NMAP | Network Mapper | Người nập bản đồ mạng |
| TOS | Terms Of Service | Điều khoản dịch vụ |

# MỞ ĐẦU

Thông tin là một tài sản vô cùng quý giá của chính phủ, tổ chức, doanh nghiệp hay bất cứ một cá nhân nào. Ngày nay, nhờ có Internet và mạng máy tính nên việc trao đổi thông tin được thực hiện ngày càng dễ dàng, thuận tiện và nhanh chóng hơn bao giờ hết. Tuy nhiên, việc trao đổi thông tin trên các thiết bị điện từ và mạng máy tính lại tồn tại rủi ro mất an toàn thông tin. Thông tin quan trọng nằm ở kho dữ liệu hay đang trên đường truyền có thể bị trộm cắp, có thể bị làm sai lệch hoặc có thể bị giả mạo. Điều đó sẽ làm ảnh hưởng tới hoạt động của các tổ chức, công ty hay cả một quốc gia. Những bí mật kinh doanh, tài chính là mục tiêu của các đối thủ cạnh tranh. Tin tức về an ninh quốc gia cũng luôn là mục tiêu của các tổ chức tình báo trong và ngoài nước. Chính vì vậy việc giữ bí mật thông tin là một vấn đề rất quan trọng đối với tổ chức và cá nhân.

Theo số liệu của CERT (Computer Emegency Response Team), số lượng các vụ tấn công trên Internet mỗi ngày một nhiều, quy mô của chúng mỗi ngày một lớn và phương pháp tấn công ngày càng hoàn thiện.

Trước những vấn đề thực tiễn đặt ra như vậy, luận văn: “Mạng máy tính và giải pháp bảo mật thông tin cho mạng máy tính của công ty CMC Telecom” tập trung vào nghiên cứu các phương pháp bảo mật mạng thông tin dữ liệu với những tính năng an toàn cao hiện nay. Luận văn trình bày những vấn đề kĩ thuật quan trọng về bảo mật mạng, bao gồm cả IDS/IPS và đề xuất giải pháp bảo mật phù hợp với yêu cầu và điều kiện thực tế cho hệ thống mạng máy tính của công ty CMC Telecom.

# CHƯƠNG I: TỔNG QUAN VỀ MẠNG MÁY TÍNH VÀ VẤN ĐỀ

## 1.1. Tổng quan đề tài

### 1.1.1. Khái quát về mạng máy tính

Mạng máy tính là một hệ thống các máy tính đơn lẻ được kết nối với nhau thông qua các thiết bị kết nối mạng và phương tiện truyền thông (giao thức mạng và môi trường truyền dẫn) theo một kiến trúc nào đó và các máy tính này trao đổi thông tin qua lại với nhau. Nếu một máy tính này có thể gửi hoặc nhận dữ liệu đến từ một máy tính khác từ xa, thì hai máy tính này được cho là trong một mạng.

Mạng là một nhóm các thiết bị được kết nối với nhau. Mạng có thể được phân loại thành nhiều đặc điểm khác nhau, chẳng hạn như phương tiện được sử dụng để vận chuyển dữ liệu, giao thức truyền thông được sử dụng, quy mô, cấu trúc liên kết, lợi ích và phạm vi tổ chức. Mạng máy tính bao gồm hai hoặc nhiều máy tính được liên kết để chia sẻ tài nguyên như máy in, các thiết bị khác, chương trình,… trao đổi tệp hoặc cho phép giao tiếp điện tử. Các máy tính trong mạng máy tính có thể được liên kết thông qua cáp, đường dây điện thoại, sóng vô tuyến, vệ tinh hoặc chùm ánh sáng hồng ngoại.

Ứng dụng của mạng máy tính:

- Một mạng cung cấp phương tiện để trao đổi dữ liệu giữa các máy tính và cung cấp các chương trình và dữ liệu cho mọi người

- Nó cho phép chia sẻ tài nguyên của máy

- Kết nối mạng cũng cung cấp chức năng sao lưu.

- Kết nối mạng cung cấp một môi trường mạng linh hoạt. Các máy tính đặt xa nhau cũng có thể kết nối trao đổi dữ liệu cho nhau thông qua mạng.

### 1.1.2. Các thành phần cơ bản

Để một hệ thống an ninh mạng hoạt động tốt nó bao gồm rất nhiều thành phần, hoạt động trên các nền tảng và môi trường khác nhau như:

- Các thiết bị đầu cuối: Máy tính, điện thoại, máy quét, máy in… các thiết bị này được kết nối với nhau qua thiết bị kết nối hoặc môi trường truyền dẫn.
- Môi trường truyền dẫn: Gồm các thiết bị kết nối không dây như bộ truyền tín hiệu, bộ phát sóng, sóng điện từ…

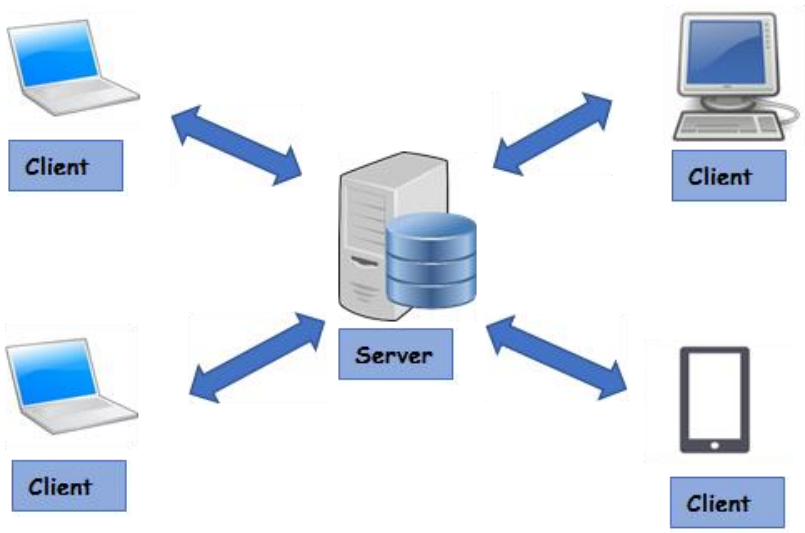
- Thiết bị kết nối vật lý: Dây nối, modun,…. được kết nối trực tiếp từ thiết bị đầu cuối này sang thiết bị đầu cuối khác.

- Phần mềm cho phép thực hiện việc trao đổi thông tin giữa các máy tính: Là những ứng dụng, chương trình được cài đặt trên các thiết bị đầu cuối và có chức năng chia sẻ dữ liệu qua các đường truyền không dây.

### 1.2. Kiến trúc mạng máy tính và các dịch vụ

#### 1) Kiến trúc khách/chủ (Client/Server):

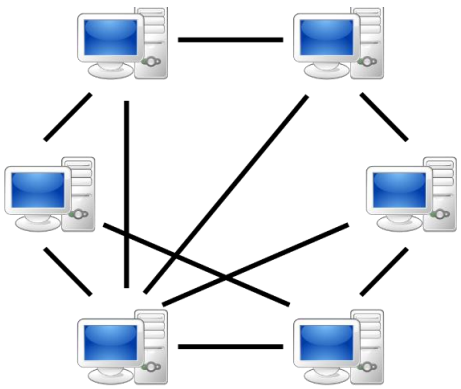
Là một loại mô hình mạng máy tính bao gồm 2 thành phần là máy chủ và máy tính.Trong đó máy chủ đóng vai trò cung cấp các dịch vụ theo yêu cầu của máy khách.




Hình 1.1: Mô hình mạng khách/chủ(Client/Server)

#### 2)Kiến trúc mạng hàng ngang(peer-to-peer)

Mạng hàng ngang là một mô hình mạng máy tính bình đẳng. Tất cả các máy tính trong mạng đều có quyền và nghĩa vụ như nhau.Chúng vừa là máy chủ vừa là máy khách.



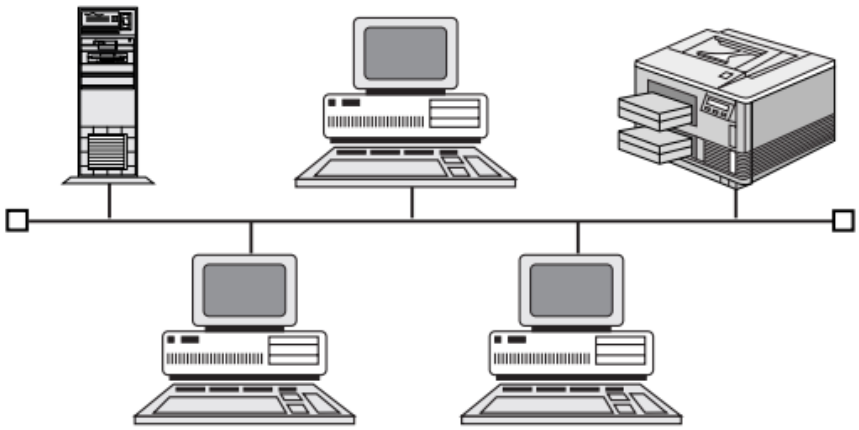
Hình 1.2: Mô hình mạng mạng hàng ngang(peer-to-peer)

### 1.2.1. Cấu trúc liên kết mạng

Cấu trúc liên kết mạng biểu thị cách thức mà các thiết bị trong mạng nhìn thấy mối quan hệ logic hoặc vật lý của chúng với nhau. Mạng máy tính có thể được phân loại theo cấu trúc liên kết mạng mà mạng dựa trên. Sau đây là một số cấu trúc điển hình.

**1) Mạng tuyến tính (Bus network)**

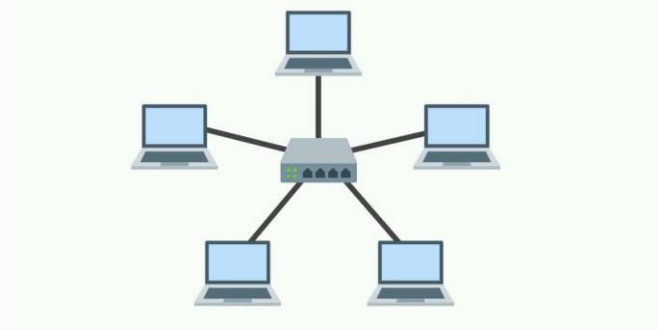
Cấu trúc mạng ở dạng liên kết điểm – đa điểm. Tất cả các thiết bị được kết nối với cáp và giao tiếp qua một kênh chia sẻ duy nhất trên một mạch điện dùng chung. Mỗi đoạn cáp được giới hạn trong một khoảng độ dài nào đó do các vấn đề về suy hao tín hiệu ở tần số sóng mang.



Hình 1.3: Cấu trúc mạng tuyến tính (Bus network)

**2) Mạng hình sao (Star network)**

Mạng hình sao là mạng cục bộ (LAN) trong đó tất cả các nút (máy trạm hoặc các thiết bị khác) được kết nối trực tiếp với một máy tính trung tâm chung. Các máy trạm được kết nối gián tiếp với nhau thông qua máy tính trung tâm. Trong một số mạng hình sao, máy tính trung tâm cũng có thể hoạt động như một máy trạm.

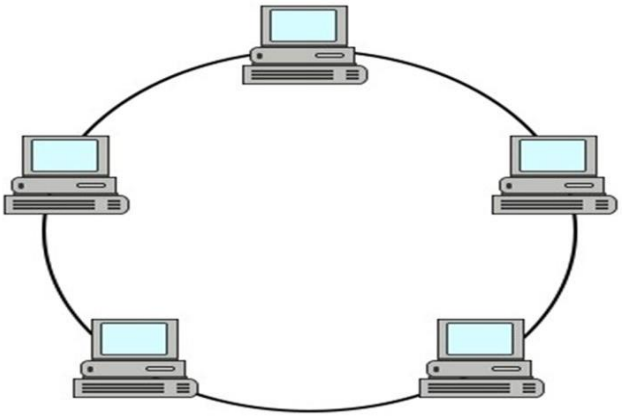


Hình 1.4: Cấu trúc mạng hình sao (Star network)

### 3) Mạng hình vòng (Ring network)

Cấu trúc liên kết vòng là một cấu hình mạng nơi các kết nối thiết bị tạo ra một đường dẫn dữ liệu hình tròn. Mỗi thiết bị được nối mạng được kết nối với hai thiết bị khác, giống như các điểm trên một vòng tròn. Cùng với nhau, các thiết bị trong cấu trúc liên kết vòng được gọi là mạng vòng.

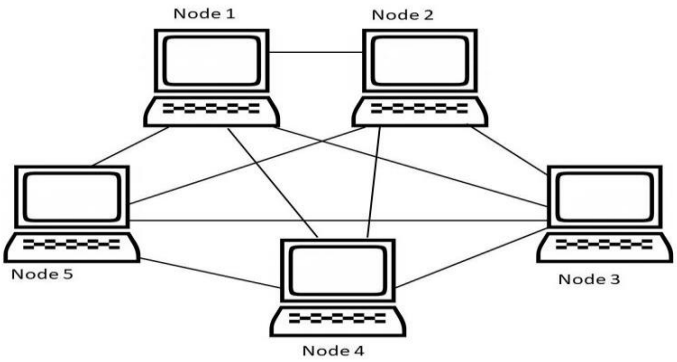
Trong mạng vòng, các gói dữ liệu di chuyển từ thiết bị này sang thiết bị khác cho đến khi chúng đến đích. Hầu hết các cấu trúc liên kết vòng cho phép các gói chỉ di chuyển theo một hướng, được gọi là mạng vòng một hướng. Một số khác cho phép dữ liệu di chuyển theo một trong hai hướng, được gọi là hai chiều.



Hình 1.5: Cấu trúc mạng hình vòng (Ring network)

### 4) Mạng hình lưới (Mesh network)

Là một mạng mà trong đó tất cả máy tính và thiết bị mạng được kết nối với nhau. Thiết lập cấu trúc liên kết này cho phép hầu hết các đường truyền được phân phối ngay cả khi một trong các kết nối gặp sự cố. Nó là một cấu trúc liên kết thường được sử dụng cho các mạng không dây. Dưới đây là một ví dụ trực quan về thiết lập máy tính đơn giản trên mạng sử dụng cấu trúc liên kết lưới.




Hình 1.6: Cấu trúc mạng hình lưới (Mesh network)

**5) Mạng cấu trúc liên kết cây hoặc phân cấp**

Cấu trúc liên kết cây có thể được bắt nguồn từ cấu trúc liên kết hình sao. Cấu trúc hình cây có một hệ thống phân cấp của các chùm khác nhau, giống như các nhánh trong một cái cây.

### 1.2.2. Các dịch vụ của mạng Internet

**1) E-mail**

Đây là dịch vụ gửi thư điện tử phổ biến trên trên Internet. Nó cho phép người dùng gửi, nhận, chuyển tiếp các thư điện tử (kể cả thư có tệp đính kèm).

**2) WWW (World Wide Web)**

Là hệ thống cung cấp thông tin dựa trên siêu văn bản. Nó có thể coi như là dịch vụ tin đa phương tiện, nó cho phép người dùng trình duyệt, tìm kiếm, truyền và tổ chức liên kết các trang web trên internet.

**3) FTP (File Transfer Protocol)**

Là dịch vụ truyền tệp (file) trên mạng. Các file được truyền được định dạng dưới dạng văn bản, hình ảnh, video..., các phần mềm ứng dụng có thể sử dụng miễn phí hoặc thử nghiệm.

**4) Telnet**

Là dịch vụ truy nhập từ xa. Đây là một công cự cơ bản của Internet. Telnet cho phép người sử dụng có thể truy cập vào một máy tính và khai thác các tài nguyên của máy đó hoàn toàn giống như đang ngồi trước máy của mình.

**5) Chat**

Là dịch vụ cho phép hội thoại trực tuyến (gồm có: text chat, voice chat, video chat). Chat là phương tiện thời gian thực, nghĩa là những từ bạn gõ vào máy tính sẽ xuất hiện gần như tức thời trên màn hình của người nhận và trả lời của họ cũng sẽ xuất hiện trên màn hình của bạn như vậy.

**6) NewsGroup**

Là dịch vụ cho phép một nhóm người sử dụng mạng để trao đổi thông tin xung quanh một đề tài.

**7) Usenet**

Là dịch vụ cho phép tập hợp vài ngàn nhóm NewsGroup. Những nhóm trao đổi tin tức theo những chủng loại chuyên môn nhất định (máy tính, khoa học, tin tức,..).

Giống như bản tin một người có thể gửi đi để những người khác có thể đọc và trả lời hay tranh luận.

**8)VoIP**

Là dịch vụ điện thoại truyền qua giao thức Internet.

**9) Video Conference**

Là dịch vụ truyền hình hội nghị. Dịch vụ này đã giúp cho những người ở các vị trí địa lí cách xa nhau có thể nhìn thấy hình ảnh của nhau, nói chuyện được với nhau thông qua một phòng họp ảo.

**10) WAP (Wireless Application Protocol)**

Là giao thức truyền thông mang lại rất nhiều ứng dụng thiết bị đầu cuối di động như E-mail, wed, mua bán trực tuyến,ngân hàng trực tuyến,thông tin chứng khoán.

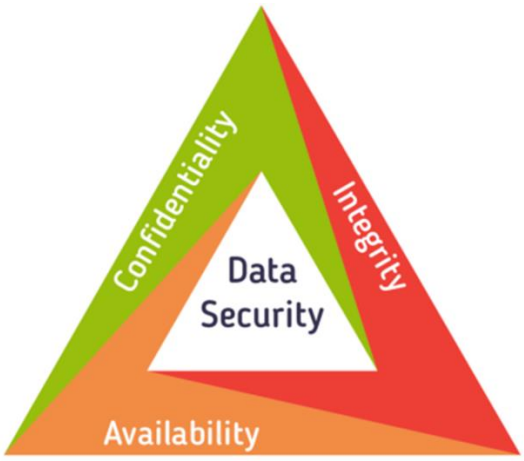
### 1.3. Các nguyên tắc nền tảng của an ninh mạng

Đối với nhiều tổ chức, doanh nghiệp, cá nhân thì thông tin và dữ liệu đóng một vai trò hết sức quan trọng trong đời sống và có khi ảnh hưởng tới sự tồn vong của họ. Vì vậy, việc bảo mật những thông tin và dữ liệu đó là điều vô cùng cần thiết, nhất là trong bối cảnh hiện nay các hệ thống thông tin ngày càng được mở rộng và trở nên phức tạp dẫn đến tiềm ẩn nhiều nguy cơ không lường trước được.

Điều này cho thấy vai trò cốt yếu của an ninh mạng trong việc bảo hệ hệ thống mạng. Và nền tảng quan trọng của an ninh mạng bao gồm 3 yếu tố:

- Confidentiality (Tính bí mật)
- Integrity (Tính toàn vẹn)
- Availability (Tính sẵn sàng)

Tùy thuộc vào ứng dụng và hoàn cảnh cụ thể, mà một trong ba nguyên tắc này sẽ quan trọng hơn những cái khác.




Hình 1.7. Mô hình bộ ba CIA

Confidentiality, Integrity, Availability, được gọi là: Mô hình bộ ba CIA. Ba nguyên tắc cốt lõi này phải dẫn đường cho tất cả các hệ thống an ninh mạng. Bộ ba CIA cũng cung cấp một công cụ đo (tiêu chuẩn để đánh giá) đối với các thực hiện an ninh. Mọi vi phạm bất kỳ một trong ba nguyên tắc này đều có thể gây hậu quả nghiêm trọng đối với tất cả các thành phần có liên quan.

### 1.3.1. Tính bí mật

Bí mật là sự ngăn ngừa việc tiết lộ trái phép những thông tin quan trọng, nhạy cảm. Đó là khả năng đảm bảo mức độ bí mật cần thiết được tuân thủ và thông tin quan trọng, nhạy cảm đó được che giấu với người dùng không được cấp phép. Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập về cả mặt vật lý, ví dụ như tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó hoặc logic, ví dụ như truy cập thông tin đó từ xa qua môi trường mạng. Sau đây là một số cách thức như vậy:

- Khóa kín và niêm phong thiết bị.
- Yêu cầu đối tượng cung cấp credential, ví dụ, cặp username + password hay đặc điểm về sinh trắc để xác thực.
- Sử dụng firewall hoặc ACL trên router để ngăn chặn truy cập trái phép.
- Mã hóa thông tin sử dụng các giao thức và thuật toán mạnh: SSL/TLS, AES, …

Đối với an ninh mạng thì tính bí mật rõ ràng là điều đầu tiên được nói đến và nó thường xuyên bị tấn công nhất.

### 1.3.2. Tính toàn vẹn

Toàn vẹn là sự phát hiện và ngăn ngừa việc sửa đổi trái phép về dữ liệu, thông tin và hệ thống, do đó đảm bảo được sự chính xác của thông tin và hệ thống. Có ba mục đích chính của việc đảm bảo tính toàn vẹn:

- Ngăn cản sự làm biến dạng nội dung thông tin của những người sử dụng không được phép.

- Ngăn cản sự làm biến dạng nội dung thông tin không được phép hoặc không chủ tâm của những người sử dụng được phép.

- Duy trì sự toàn vẹn dữ liệu cả trong nội bộ và bên ngoài.

Đảm bảo tính toàn vẹn của thông tin, tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi. Về điểm này, nhiều người thường hay nghĩ tính "integrity" đơn giản chỉ là đảm bảo thông tin không bị thay đổi (modify) là chưa đầy đủ. Ngoài ra, một giải pháp "data integrity" có thể bao gồm thêm việc xác thực nguồn gốc của thông tin này (thuộc sở hữu của đối tượng nào) để đảm bảo thông tin đến từ một nguồn đáng tin cậy và ta gọi đó là tính "authenticity" của thông tin. Sau đây là một số trường hợp tính "integrity" của thông tin bị phá vỡ:

- Thay đổi giao diện trang chủ của một website.

- Chặn đứng và thay đổi gói tin được gửi qua mạng.

- Chỉnh sửa trái phép các file được lưu trữ trên máy tính.

- Do có sự cố trên đường truyền mà tín hiệu bị nhiễu hoặc suy hao dẫn đến thông tin bị sai lệch.

### 1.3.3. Tính sẵn sàng

Tính sẵn sàng bảo đảm các người sử dụng hợp pháp của hệ thống có khả năng truy cập đúng lúc và không bị ngắt quãng tới các thông tin trong hệ thống và tới mạng. Tính sẵn sàng có liên quan đến độ tin cậy của hệ thống. Để tăng khả năng chống chọi với các cuộc tấn công cũng như duy trì độ sẵn sàng của hệ thống ta có thể áp dụng một số kỹ thuật như: Load Balancing, Clustering, Redudancy, Failover…

Mọi hệ thống thông tin đều phục vụ mục đích riêng của nó và thông tin phải luôn luôn sẵn sàng khi cần thiết. Điều đó có nghĩa rằng hệ thống tính toán sử dụng để lưu trữ và xử lý thông tin, có một hệ thống điều khiển bảo mật sử dụng để bảo vệ nó, và kênh kết nối sử dụng để truy cập nó phải luôn hoạt động chính xác. Hệ thống có tính sẵn sàng cao hướng đến sự sẵn sàng ở mọi thời điểm, tránh được những rủi ro cả về phần cứng, phần mềm như: sự cố mất điện, hỏng phần cứng, cập nhật, nâng cấp hệ thống… đảm bảo tính sẵn sàng cũng có nghĩa là tránh được tấn công từ chối dịch vụ.

## 1.4. Các kiểu tấn công mạng

### 1.4.1. Vấn đề bảo mật mạng

Bảo mật mạng là quá trình thực hiện các biện pháp phòng ngừa để bảo vệ cơ sở hạ tầng mạng bên dưới khỏi bị truy cập trái phép, sử dụng sai, hoạt động sai, sửa đổi, phá hủy hoặc tiết lộ không đúng cách. Vấn đề bảo mật mạng luôn là một vấn đề bức thiết khi ta nghiên cứu một hệ thống mạng. Hệ thống mạng càng phát triển thì vấn đề bảo mật mạng càng được đạt lên hàng đầu.

Khi nghiên cứu một hệ thống mạng chúng ta cần phải kiểm soát vấn đề bảo mật mạng ở các cấp độ sau:

• Mức mạng: Ngăn chặn kẻ xâm nhập bất hợp pháp vào hệ thống mạng.

• Mức server: Kiểm soát quyền truy cập, các cơ chế bảo mật, quá trình nhận dạng người dùng, phân quyền truy cập, cho phép các tác vụ

• Mức cơ sở dữ liệu: Kiểm soát ai, được quyền như thế nào với mỗi cơ sở dữ liệu

• Mức trường thông tin: Trong mỗi cơ sở dữ liệu kiểm soát được mỗi trường dữ liệu chứa thông tin khác nhau sẽ cho phép các đối tượng khác nhau có quyền truy cập khác nhau.

• Mức mật mã: Mã hoá toàn bộ file dữ liệu theo một phương pháp nào đó và chỉ cho phép người có " chìa khoá" mới có thể sử dụng được file dữ liệu.

### 1.4.2 Các giai đoạn tấn công

- Thăm dò (Reconnaissace): Thăm dò mục tiêu là một trong những bước quan trọng để biết những thông tin trên hệ thống mục tiêu. Hacker sử dụng kỹ thuật này để khám phá hệ thống mục tiêu đang chạy trên hệ điều hành nào, có bao nhiêu dịch vụ đang chạy trên các dịch vụ đó, cổng dịch vụ nào đang đóng và cổng nào đang mở, gồm hai loại:

• Passive: Thu thập các thông tin chung như vị trí địa lý, điện thoại, email của các cá nhân, người điều hành trong tổ chức.

• Active: Thu thập các thông tin về địa chỉ IP, domain, DNS, ... của hệ thống.

- Quét hệ thống (Scanning): Quét thăm dò hệ thống là phương pháp quan trọng mà Attacker thường dùng để tìm hiểu hệ thống và thu thập các thông tin như địa chỉ IP cụ thể, hệ điều hành hay các kiến trúc hệ thống mạng. Một vài phương pháp quét thông dụng như: quét cổng, quét mạng và quét các điểm yếu trên hệ thống.

- Chiếm quyền điều khiển (Gainning access): Đến đây hacker đã bắt đầu dần dần xâm nhập được hệ thống và tấn công nó, đã truy cập được nó bằng các lệnh khai thác. Các lệnh khai thác luôn ở bất cứ không gian nào, từ mạng LAN cho tới INTERNET và đã lan rộng ra mạng không dây. Hacker có thể chiếm quyền điều khiển tại:

• Mức hệ điều hành/mức ứng dụng.

• Mức mạng.

• Từ chối dịch vụ

- Duy trì điều khiển hệ thống (Maitaining access): Đến đây hacker bắt đầu phá hỏng làm hại, hoặc có thể cài trojan, rootkit, backdoor để lấy thông tin thêm. Thường được thấy sử dụng để đánh cắp tài khoản tín dụng, ngân hàng.

- Xoá dấu vết (Clearning tracks): Được đề cập đến hoạt động được thực hiện bằng cách hacker cố tình che dấu hành động xâm nhập của mình. Hacker phải tìm cách xóa đi dấu vết mỗi khi đột nhập bằng các phương thức như Steganography, tunneling, andaltering log file.

### 1.4.3. Các hình thức tấn công mạng phổ biến hiện nay

**1) Tấn công bằng phần mềm độc hại (Malware Attack)**

- Tấn công Malware là một trong những hình thức tấn công qua mạng phổ biến nhất hiện nay. Malware bao gồm:

- Spyware (phần mềm gián điệp)
- Ransomware (mã độc tống tiền)
- Virus
- Worm (phần mềm độc hại lây lan với tốc độ nhanh)

Thông thường, Hacker sẽ tiến hành tấn công người dùng thông qua các lỗ hổng bảo mật. Hoặc lừa người dùng Click vào một đường Link hoặc Email (Phishing) để cài phần mềm độc hại tự động vào máy tính. Một khi được cài đặt thành công, Malware sẽ gây ra những hậu quả nghiêm trọng:

- Chặn các truy cập vào hệ thống mạng và dữ liệu quan trọng (Ransomware).
- Cài đặt thêm phần mềm độc hại khác vào máy tính người dùng.
- Đánh cắp dữ liệu (Spyware).
- Phá hoại phần cứng, phần mềm, làm hệ thống bị tê liệt, không thể hoạt động.


Hình 1.8. Tấn công bằng malware

Giải pháp

- Sao lưu dữ liệu thường xuyên: Việc này sẽ giúp bạn không phải lo lắng khi dữ liệu bị phá hủy.

- Thường xuyên cập nhật phần mềm: Các bản cập nhật của phần mềm (trình duyệt, hệ điều hành, phần mềm diệt Virus,…) sẽ vá lỗi bảo mật còn tồn tại trên phiên bản cũ, đảm bảo an toàn thông tin cho người dùng.

- Cẩn thận với các Link hoặc File lạ: Đây là phương thức lừa đảo khá phổ biến của Hacker. Chúng sẽ gửi Email hoặc nhắn tin qua Facebook, đính kèm Link Download và nói rằng đó là File quan trọng hoặc chứa nội dung hấp dẫn. Khi tải về, các File này thường nằm ở dạng .docx, .xlxs, .pptx hay .pdf, nhưng thực chất là File .exe (chương trình có thể chạy được). Ngay lúc người dùng Click mở File, mã độc sẽ lập tức bắt đầu hoạt động.

**2) Tấn công giả mạo (Phishing Attack)**

Phishing (tấn công giả mạo**)** là hình thức tấn công mạng bằng giả mạo thành một đơn vị uy tín để chiếm lòng tin và yêu cầu người dùng cung cấp thông tin cá nhân cho chúng.


Hình 1.9 Tấn công phishing

Thông thường, Hacker sẽ giả mạo là ngân hàng, ví điện tử, trang giao dịch trực tuyến hoặc các công ty thẻ tín dụng để lừa người dùng chia sẻ các thông tin cá nhân như: tài khoản & mật khẩu đăng nhập, mật khẩu giao dịch, thẻ tín dụng và các thông tin quan trọng khác.

Phương thức tấn công này thường được thực hiện thông qua việc gửi Email và tin nhắn. Người dùng khi mở Email và Click vào đường Link giả mạo sẽ được yêu cầu đăng nhập. Nếu "cắn câu", tin tặc sẽ có được thông tin cá nhân của người dùng ngay tức khắc.

**Các phương thức tấn công:**

**Giả mạo Email:**

Đây là hình thức Phishing khá căn bản. Tin tặc sẽ gửi Email đến người dùng dưới danh nghĩa của một đơn vị/tổ chức uy tín nhằm dẫn dụ người dùng truy cập đến Website giả mạo

Những Email giả mạo thường rất tinh vi và rất giống với Email chính chủ, khiến người dùng nhầm lẫn và trở thành nạn nhân của cuộc tấn công. Dưới đây là một số cách mà tin tặc thường ngụy trang:

- Địa chỉ người gửi (VD: Địa chỉ đúng là **sales.congtyA@gmail.com** thì sẽ được giả mạo thành **sale.congtyA@gmail.com**)
- Thiết kế các cửa sổ Pop-up giống hệt bản gốc (cả màu sắc, Font chữ,…)
- Sử dụng kỹ thuật giả mạo đường dẫn để lừa người dùng (VD: đường dẫn là **congtyB.com** nhưng khi nhấn vào thì điều hướng đến **contyB.com**)
- Sử dụng hình ảnh thương hiệu của các tổ chức lớn để tăng độ tin cậy.

**Giả mạo Website**

Giả mạo Website trong tấn công Phishing là làm giả một trang chứ không phải toàn bộ Website. Trang được làm giả thường là trang đăng nhập để cướp thông tin của người dùng.

Website giả thường có những đặc điểm sau:

- Thiết kế giống đến 99% so với Website gốc.
- Đường dẫn chỉ khác một kí tự duy nhất: VD: facebook.com và fakebook.com, microsoft.com và mircosoft.com…)
- Luôn có những thông điệp khuyến khích người dùng cung cấp thông tin cá nhân.

**Cách phòng chống tấn công Phishing**

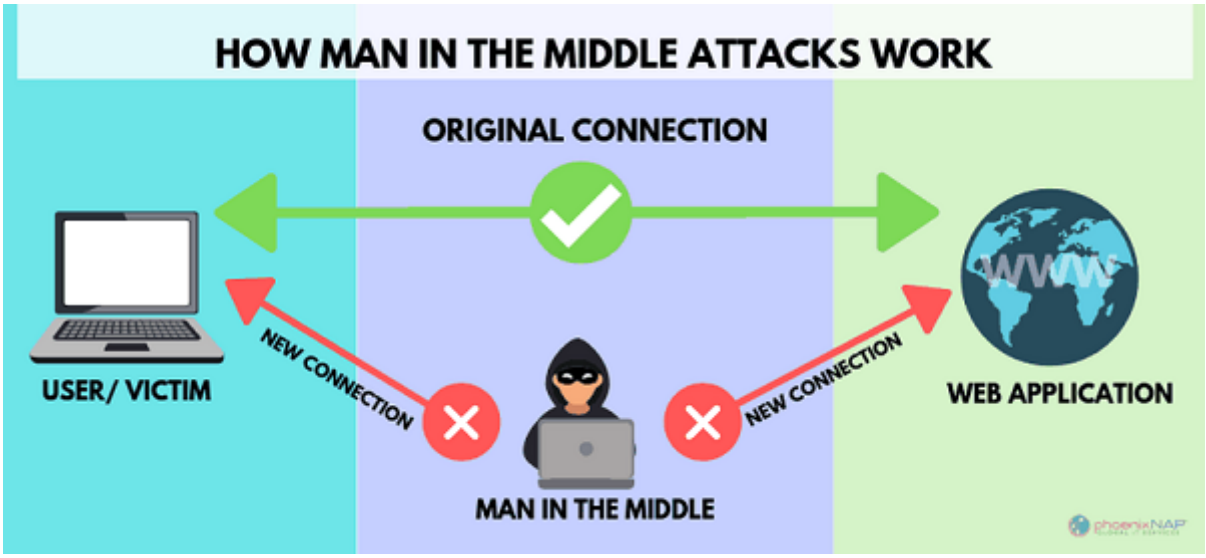
- Cảnh giác với các Email có xu hướng thúc giục bạn nhập thông tin cá nhân, thông tin nhạy cảm (thông tin thẻ tín dụng, thông tin tài khoản,..)
- Không Click vào các đường dẫn được gửi đến Email nếu không chắc chắn an toàn.
- Không trả lời những thư rác, lừa đảo.
- Luôn cập nhật phần mềm, ứng dụng đề phòng các lỗ hổng bảo mật có thể bị tấn công.

**Công cụ hạn chế phishing**

- SpoofGuard: Đây là một Plugin trình duyệt tương thích với Microsoft Internet Explorer. SpoofGuard sẽ đặt "cảnh báo" trên thanh công cụ của trình duyệt. Nó sẽ chuyển từ màu xanh sang màu đỏ nếu bạn vô tình truy cập vào Website giả mạo Phishing. Nếu bạn cố nhập các thông tin quan trọng vào một trang giả mạo, SpoofGuard sẽ lưu dữ liệu của bạn và đưa ra cảnh báo.
- Anti-phishing Domain Advisor: Thực chất đây là một Toolbar (thanh công cụ) giúp cảnh báo những trang web lừa đảo, dựa theo dữ liệu của công ty Panda Security.
- Netcraft Anti-phishing Extension: Netcraft là đơn vị uy tín trong việc cung cấp các dịch vụ bảo mật. Trong số đó, tiện ích mở rộng chống Phishing của Netcraft được đánh giá rất tốt với nhiều tính năng cảnh báo thông minh cho người dùng.

### 3) Tấn công trung gian (Man in the middle attack)

Tấn công trung gian (MitM), còn gọi là tấn công nghe lén, xảy ra khi kẻ tấn công xâm nhập vào một giao dịch/sự giao tiếp giữa 2 đối tượng. Một khi đã chen vào thành công, chúng có thể đánh cắp dữ liệu trong giao dịch đó.




Hình 1.10. Tấn công trung gian

**Các hình thức tấn công trung gian.**

- Sniffing: Sniffing hoặc Packet Sniffing là kỹ thuật được sử dụng để nắm bắt các gói dữ liệu vào và ra của hệ thống. Packet Sniffing cũng tương tự với việc nghe trộm trong điện thoại. Sniffing được xem là hợp pháp nếu được sử dụng đúng cách. Doanh nghiệp có thể thực hiện để tăng cường bảo mật.

- Packet Injection: Kẻ tấn công sẽ đưa các gói dữ liệu độc hại vào với dữ liệu thông thường. Bằng cách này, người dùng thậm chí không nhận thấy tệp/phần mềm độc hại bởi chúng đến như một phần của luồng truyền thông hợp pháp. Những tập tin này rất phổ biến trong các cuộc tấn công trung gian cũng như các cuộc tấn công từ chối dịch vụ.

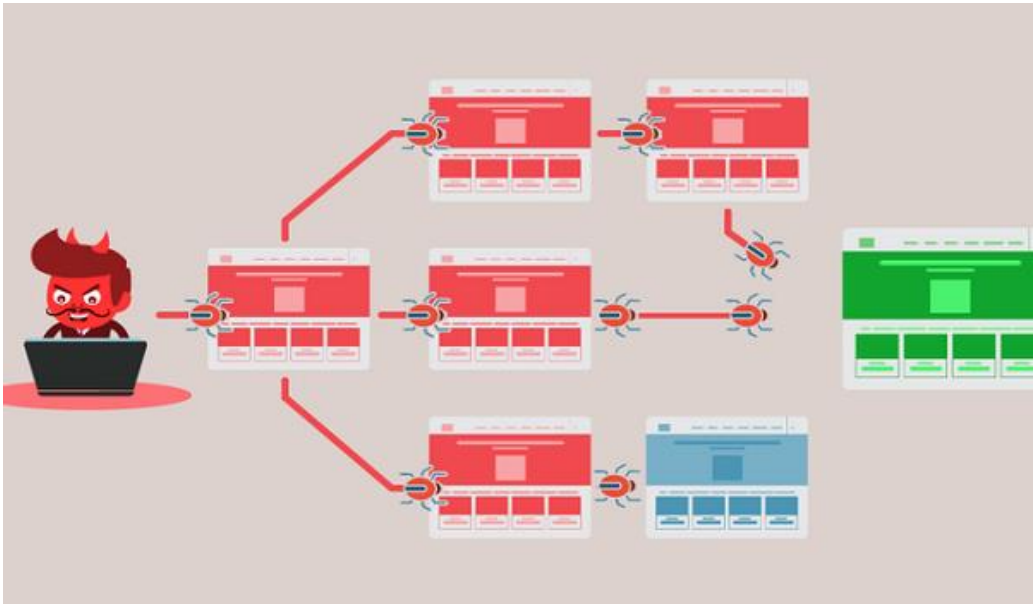
- Loại bỏ SSL: SSL Stripping hoặc SSL Downgrade Attack là một loài hiếm khi nói đến các cuộc tấn công MiTM, nhưng cũng là một trong những nguy hiểm nhất. Chứng chỉ SSL/TLS giữ liên lạc của chúng tôi an toàn trực tuyến thông qua mã hóa. Trong các cuộc tấn công SSL, kẻ tấn công loại bỏ kết nối SSL/TLS và chuyển giao thức từ HTTPS an toàn sang HTTP không an toàn.

**Cách phòng chống tấn công trung gian.**

- Đảm bảo các Website bạn truy cập đã cài SSL.
- Không mua hàng hoặc gửi dữ liệu nhạy cảm khi dùng mạng công cộng.
- Không nhấp vào Link hoặc Email độc hại.
- Có các công cụ bảo mật thích hợp được cài đặt trên hệ thống của bạn.
- Tăng cường bảo mật cho hệ thống mạng của gia đình bạn.

**4) Tấn công từ chối dịch vụ (DoS & DDoS)**

- DoS (Denial of Service**)** là "đánh sập tạm thời" một hệ thống, máy chủ hoặc mạng nội bộ. Để thực hiện được điều này, các Hacker thường tạo ra một lượng Traffic/Request khổng lồ ở cùng một thời điểm, khiến cho hệ thống bị quá tải. Theo đó, người dùng sẽ không thể truy cập vào dịch vụ trong khoảng thời gian mà cuộc tấn công DoS diễn ra.



Hình 1.11.Tấn công từ chối dịch vụ

- Một hình thức biến thể của DoS là DDoS (Distributed Denial of Service)**:** Tin tặc sử dụng một mạng lưới các máy tính (Botnet) để tấn công người dùng.vấn đề ở đây là chính các máy tính thuộc mạng lưới Botnet sẽ không biết bản thân đang bị lợi dụng trở thành công cụ tấn công.

**Một số hình thức tấn công DDoS**

Tấn công gây nghẽn mạng (UDP Flood và Ping Flood)

- Mục tiêu: Gây quá tải hệ thống mạng bằng lượng truy cập lớn đến từ nhiều nguồn để chặn các truy cập thực của người dùng.

- Phương thức: Gây nghẽn đối tượng bằng các gói UDP và ICMP.

Tấn công SYN flood (TCP)

- Mục tiêu: Gây cạn tài nguyên máy chủ, ngăn chặn việc nhận các yêu cầu kết nối mới.

- Phương thức: Lợi dụng quá trình "bắt tay" 3 chặng TCP, gửi đi yêu cầu SYN đến máy chủ và được phản hồi bằng một gói SYN-ACK. Nhưng không gửi lại gói ACK, điều này khiến cho tài nguyên máy chủ bị sử dụng hết vào việc đợi gói ACK gửi về.

Tấn công khuếch đại DNS

- Mục tiêu: Làm quá tải hệ thống bằng phản hồi từ các bộ giải mã DNS.

- Phương thức: Mạo danh địa chỉ IP của máy bị tấn công để gửi yêu cầu nhiều bộ giải mã DNS. Các bộ giải mã hồi đáp về IP của máy có kích thước gói dữ liệu có thể lớn hơn kích thước của yêu cầu tới 50 lần.

**Cách phòng chống tấn công DDoS**

- Theo dõi lưu lượng truy cập của bạn: Với cách này, bạn có thể phát hiện được các vụ tấn công DDoS nhỏ mà tin tặc vẫn thường dùng để Test năng lực của mạng lưới trước khi tấn công thật sự.

- Nếu bạn có thể xác định được địa chỉ của các máy tính thực hiện tấn công: có thể tạo một ACL (danh sách quản lý truy cập) trong tường lửa để thực hiện chặn các IP này.

**5) SQL Injection – Tấn công cơ sở dữ liệu**

SQL Injection là hình thức tấn công trong đó tin tặc chèn một đoạn mã độc hại vào server. Sau đó sử dụng ngôn ngữ SQL để lấy cắp thông tin.

Hậu quả nghiêm trọng nhất do SQL Injection gây ra là làm lộ dữ liệu quan trọng. Thông tin khách hàng, bí mật kinh doanh hay tài sản trí tuệ khi bị phát tán hoặc tống tiền sẽ gây ra thiệt hại vô cùng nặng nề cho doanh nghiệp.


Hình 1.12. Tấn công cơ sở dữ liệu

**Cách phòng chống hình thức tấn công mạng cơ sở dữ liệu**

- Không sử dụng SQL động và không xây dựng câu truy vấn với dữ liệu nhập vào từ người dùng
- Bỏ những database function không cần thiết để giảm bớt lỗ hổng tin tặc có thể lợi dụng
- Sao lưu dữ liệu thường xuyên trên đám mây

**6) Khai thác lỗ hổng Zero Day (Zero Day Attack)**

Lỗ hổng zero-day (0-day Vulnerability) thực chất là những lỗ hổng bảo mật của phần mềm hoặc phần cứng mà người dùng chưa phát hiện ra. Chúng tồn tại trong nhiều môi trường khác nhau như: Website, Mobile Apps, hệ thống mạng doanh nghiệp, phần mềm – phần cứng máy tính, thiết bị IoT, Cloud, …


Hình 1.13.Khai thác lỗ hổng Zero Day

Sự khác nhau giữa một lỗ hổng bảo mật thông thường và một lỗ hổng Zero-day nằm ở chỗ: Lỗ hổng Zero-day là những lỗ hổng chưa được biết tới bởi đối tượng sở hữu hoặc cung cấp sản phẩm chứa lỗ hổng.

Thông thường ngay sau khi phát hiện ra lỗ hổng 0-day, bên cung cấp sản phẩm sẽ tung ra bản vá bảo mật cho lỗ hổng này để người dùng được bảo mật tốt hơn. Tuy nhiên trên thực tế, người dùng ít khi cập nhật phiên bản mới của phần mềm ngay lập tức. Điều đó khiến cho Zero-day được biết đến là những lỗ hổng rất nguy hiểm. Có thể gây thiệt hại nghiêm trọng cho doanh nghiệp và người dùng.

Một khi được công bố rộng rãi ra công chúng, lỗ hổng 0-day trở thành lỗ hổng n-day.

**Cách phòng chống lỗ hổng Zero-day**

- Thường xuyên cập nhật phần mềm và hệ điều hành
- Triển khai giám sát bảo mật theo thời gian thực
- Triển khai hệ thống IDS và IPS
- Sử dụng phần mềm quét lỗ hổng bảo mật

**Các loại hình tấn công khác**

Ngoài ra, còn rất nhiều hình thức tấn công mạng khác như:

- Tấn công chuỗi cung ứng
- Tấn công Email
- Tấn công vào con người
- Tấn công nội bộ tổ chức

Mỗi hình thức tấn công đều có những đặc tính riêng. Và chúng ngày càng tiến hóa phức tạp, tinh vi đòi hỏi các cá nhân, tổ chức phải liên tục cảnh giác & cập nhật các công nghệ phòng chống mới.

**Các giải pháp hạn chế tấn công mạng**

Đối với cá nhân

- Bảo vệ mật khẩu cá nhân bằng cách: đặt mật khẩu phức tạp, bật tính năng bảo mật 2 lớp – xác nhận qua điện thoại,… Chi tiết tại: 3 kiểu Tấn công Password cơ bản & cách phòng chống
- Hạn chế truy cập vào các điểm Wifi công cộng
- Không sử dụng phần mềm bẻ khóa (crack)
- Luôn cập nhật phần mềm, hệ điều hành lên phiên bản mới nhất.
- Cẩn trọng khi duyệt Email, kiểm tra kỹ tên người gửi để phòng tránh lừa đảo.
- Tuyệt đối không tải các File hoặc nhấp vào đường link không rõ nguồn gốc.
- Hạn chế sử dụng các thiết bị ngoại vi (USB, ổ cứng) dùng chung.
- Sử dụng một phần mềm diệt Virus uy tín.

**Đối với tổ chức, doanh nghiệp**

- Xây dựng một chính sách bảo mật với các điều khoản rõ ràng, minh bạch
- Lựa chọn các phần mềm, đối tác một cách kỹ càng. Ưu tiên những bên có cam kết bảo mật và cam kết cập nhật bảo mật thường xuyên.
- Tuyệt đối không sử dụng các phần mềm Crack

- Luôn cập nhật phần mềm, Firmware lên phiên bản mới nhất.

- Sử dụng các dịch vụ lưu trữ đám mây uy tín cho mục đích lưu trữ.

- Đánh giá bảo mật & Xây dựng một chiến lược an ninh mạng tổng thể cho doanh nghiệp, bao gồm các thành phần: bảo mật Website, bảo mật hệ thống máy chủ, mạng nội bộ, hệ thống quan hệ khách hàng (CRM), bảo mật IoT, bảo mật hệ thống CNTT – vận hành…

- Tổ chức các buổi đào tạo, Training kiến thức sử dụng Internet an toàn cho nhân viên.

## 1.5. Các khía cạnh bảo mật mạng và mức độ bảo mật

### 1.5.1. Các khía cạnh bảo mật mạng

1) Các khía cạnh cần quan tâm khi phân tích bảo mật mạng

-Con người: Trong bảo mật mạng yếu tố con người cũng rất quan trọng. Khi nghiên cứu đến vấn đề bảo mật mạng cần quan tâm xem ai tham gia vào hệ thống mạng, họ có tránh nhiệm như thế nào. Ở mức độ vật lý khi một người không có thẩm quyền vào phòng máy họ có thể thực hiện một số hành vi phá hoại ở mức độ vật lý.

- Kiến trúc mạng: Kiến trúc mạng cũng là một vấn đề mà chúng ta cần phải quan tâm khi nghiên cứu, phân tích một hệ thống mạng. Chúng ta cần nghiên cứu hiện trạng mạng khi xây dựng và nâng cấp mạng đưa ra các kiểu kiến trúc mạng phù hợp với hiện trạng và cơ sở hạ tầng ở nơi mình đang định xây dựng....

- Phần cứng & phần mềm:

Mạng được thiết kế như thế nào. Nó bao gồm những phần cứng và phần mềm nào và tác dụng của chúng. Xây dựng một hệ thống phần cứng và phần mềm phù hợp với hệ thống mạng cũng là vấn đề cần quan tâm khi xây dựng hệ thống mạng. Xem xét tính tương thích của phần cứng và phần mềm với hệ thống và tính tương thích giữa chúng.

2) Các yếu tố cần được bảo vệ

+ Bảo đảm An toàn thông tin, dữ liệu.

+ Bảo vệ quyền riêng tư và thông tin cá nhân.

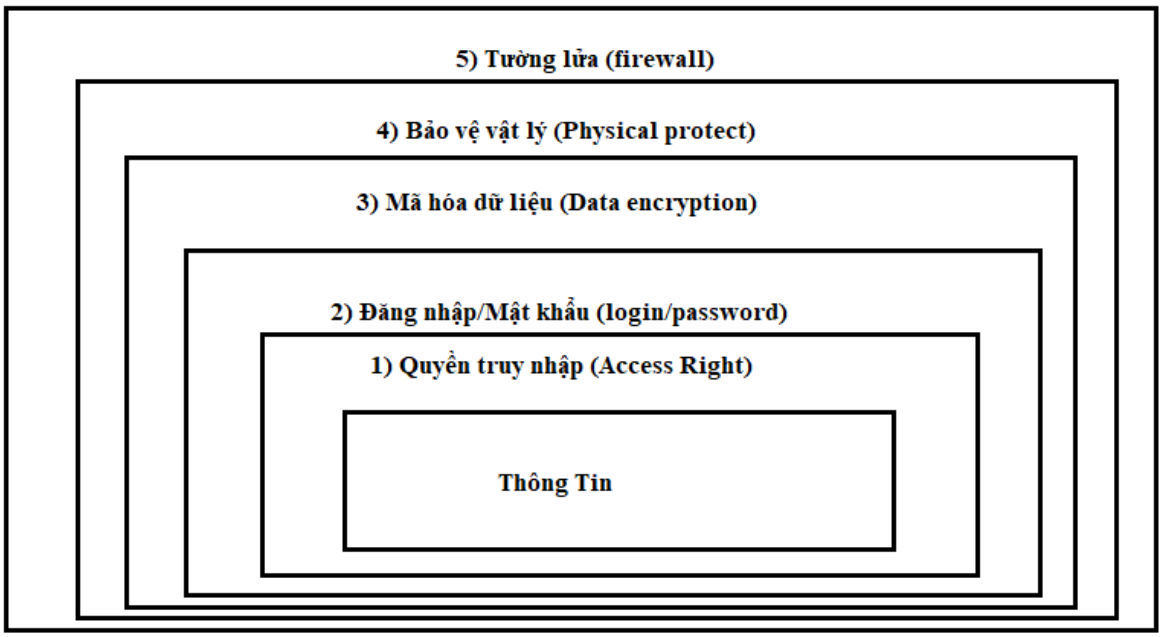
+ Mã hóa bảo đảm an toàn thông tin.

+ Bảo đảm an toàn hệ thống thông tin.

+ Bảo đảm an toàn hệ thống thông tin trọng yếu.

### 1.5.2 Mức độ an toàn bảo mật

Để đánh giá khả năng bảo mật mạng của một hệ thống người ta chia ra làm các mức độ an toàn:




Hình 1.14:Các mức độ bảo mật

1) Quyền truy nhập (Access Right)

Đây là lớp bảo vệ trong cùng nhằm kiểm soát các tài nguyên (ở đây là thông tin) của mạng và quyền hạn cho phép khai thác những gì trên tài nguyên đó. Ví dụ như nhà quản trị phân quyền cho người dùng như: chỉ đọc ( only read), chỉ ghi (only write), thực thi (execute)

2) Đăng nhập/Mật khẩu (login/password)

Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản, ít tốn kém và cũng rất hiệu quả. Khi người dùng muốn truy cập vào sử dụng các tài nguyên trên mạng thì phải đăng nhập tên và mật khẩu đã đăng ký. Người quản trị hệ thống có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy cập của những người sử dụng khác tùy theo thời gian và không gian

3) Mã hóa dữ liệu (Data encryption)

Mã hóa dữ liệu là quá trình chuyển đổi các dữ liệu (văn bản hay tài liệu gốc) thành các dữ liệu dưới dạng mật mã để bất cứ ai, ngoài người gửi và người nhận đều không đọc được.

4) Bảo vệ vật lý (Physical protect)

Đây là hình thức ngăn chặn nguy cơ truy nhập bất hợp pháp vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy, dùng hệ thống khóa trên máy tính hoặc cài đặt các hệ thống báo động khi có truy nhập vào hệ thống ...

5) Tường lửa (firewall)

Tường lửa là một cơ chế kiểm soát gói tin điển hình hoặc phòng thủ theo chu vi. Mục đích của tường lửa là để chặn lưu lượng truy cập từ bên ngoài, nhưng nó cũng có thể dùng để chặn lưu lượng từ bên trong. Tường lửa là cơ chế bảo vệ tuyến đầu chống lại những kẻ xâm nhập. Nó là một hệ thống được thiết kế để ngăn chặn truy cập trái phép vào hoặc từ một mạng riêng. Tường lửa có thể được thực hiện trong cả phần cứng và phần mềm, hoặc kết hợp cả hai.

## 1.6. Các chính sách và biện pháp bảo vệ an toàn cho mạng

### 1.6.1 Giải pháp bảo mật ứng dụng

1) Giải pháp tường lửa hệ thống ứng dụng Web (Web application firewall - WAF)

Lợi ích

Cho phép ngăn chặn các hành vi tấn công vào ứng dụng Web, liên tục giám sát hệ thống ứng dụng Web và cung cấp các cảnh báo nếu xuất hiện các lỗ hổng trên ứng dụng.

Tính năng

+ Quản lý lưu lượng web.

+ Bảo vệ ở tầng 7 (theo mô hình OSI)

+ Giám sát các giao thức HTTP/S

+ Bảo vệ các ứng dụng và dữ liệu trước các loại tấn công trái phép.

+Phân tích sâu các gói tin di chuyển trong các lưu lượng đi ra/ vào từ máy ch

dịch vụ Web.

2) Giải pháp chống giả mạo giao dịch (Fraud detection) Lợi ích

Ngăn chặn các hành vi giả mạo người dùng, chiếm đoạt và sử dụng các tài khoản thanh toán trên môi trường thanh toán điện tử, e-banking. Tính năng

+ Giám sát hành vi người dùng dịch vụ thanh toán điện tử, e-banking.

+ Chống đánh cắp định danh người dùng dựa trên nhiều thông tin: loại giao

dịch, số tiền giao dịch, thời gian làm việc, vị trí địa lý (theo địa chỉ IP), ..

+ Ngăn chặn hành lạm dụng trên hệ thống: truy cập trực tiếp vào các trang đặt hàng, sử dụng các biến môi trường đáng ngờ...

+ Ngăn chặn hành vi đáng ngờ trên hệ thống giao dịch trực tuyến như: số lần sử dụng thẻ thanh toán, thanh toán nhiều lần từ cùng địa chỉ IP...

### 1.6.2 Giải pháp bảo mật dữ liệu

1) Giải pháp giám sát an ninh hệ thống cơ sở dữ liệu

- Kiểm soát các thao tác lên CSDL, thiết lập các chính sách bảo vệ chặt chẽ.

- Ngăn chặn các hành vi bất thường từ quá trình tự học về các hoạt động bình thường của CSDL.

- Phát hiện và ngăn chặn các tấn công vào CSDL như một IPS chuyên dụng.

- Quản lý các tài khoản đặc quyền và quyền hạn của người dùng trên CSDL.

- Báo cáo hiệu năng hoạt động của CSDL như tải, các truy vấn, các đối tượng được truy xuất nhiều nhất, các đối tượng có vấn đề về response time ..

- Xác định và khuyến nghị cách thức xử lý các lỗ hổng an ninh, có khả năng đánh giá mức độ an ninh theo các tiêu chuẩn an ninh về CSDL.

2) Giải pháp mã hóa dữ liệu

Lợi ích

Bảo vệ các dữ liệu nhạy cảm bằng các hình thức mã hóa như: mã hóa thư mục, tập tin, ổ cứng ...

Tính năng

+ Thực thi mã hóa dữ liệu trên thiết bị đầu cuối (máy tính xách tay, smart phone, máy tính để bàn, ...)

+ Mã hóa dữ liệu trên ổ đĩa local, máy chủ mạng, ở cấp độ tập tin và thư mục.

### 1.6.3. Giải pháp bảo mật mạng

1) Giải pháp tường lửa đa năng UT

Lợi ích

Bảo vệ cổng hệ thống (gateway), ngăn chặn các rủi ro từ môi trường Internet.

Tính năng

+ Lọc web Chống xâm nhập (IPS) Chống DDoS Chống virus, spam. + Lọc các cổng dịch vụ Giám sát ứng dụng và người dùng

2) Giải pháp chống xâm nhập và chống tấn công từ chối dịch vụ (DDoS)

Lợi ích

Thiết bị chuyên dụng ngăn chặn hình thức tấn công DDoS.

Tính năng

+ Ngăn chặn các hình thức xâm nhập SSL offload.

+ Chống tấn công DdoS.

3) Giải pháp dò quét các lỗ hổng an ninh

Lợi ích

Xác định, giám sát và đưa ra phương án xử lý các lỗ hổng an ninh trên toàn hệ thống mạng, máy chủ, hệ điều hành, cơ sở dữ liệu và ứng dụng. Tính năng

+ Cung cấp báo cáo toàn diện về các lỗ hổng an ninh trên hệ thống

+ Đưa ra các báo tức thời khi hệ thống xuất hiện lỗ hổng bảo mật

+ Hỗ trợ người quản trị đưa ra quyết định về các chính sách và điều chỉnh bảo mật hệ thống chính xác, phù hợp và kịp thời

+ Tích hợp với các công cụ giám sát bảo vệ hệ thống như IDS/IPS, tường lửa ứng dụng web... tạo ra một hệ thống phòng thủ an ninh có chiều sâu và liên kết chặt chẽ giữa các thành phần bảo mật

4) Giải pháp phòng chống spam/ virus mức gateway

Lợi ích

Giải pháp chuyên dụng ngăn chặn các hình thức spam email, ngăn chặn virus.

Tính năng

+ SSL offload Lọc email spam Lọc email đính kèm virus

+ Cô lập các kết nối đến liên kết có mã độc

5) Giải pháp mã hóa và bảo mật đường truyền

Lợi ích

Giải pháp chuyên dụng bảo vệ kết nối giữa các site trong cùng một hệ thống, đặc biệt phù hợp với các doanh nghiệp có nhiều chi nhánh và yêu cầu bảo mật cao trên đường truyền.

Tính năng

+ Mã hóa từ mức layer 2 (theo mô hình OSI), hỗ trợ các giao thức Ethernet, Fibre Channel/FICON và SDH/SONET từ 20Mbps đến 10Gbps

+ Mã hóa cuộc gọi/ voice

+ Mã hóa đường truyền fax

6) Giải pháp giám sát và phân tích mã độc

Lợi ích

Xác định các loại mã độc đang hiện hữu trên hệ thống, tích hợp với các giải pháp mức gateway ngăn chặn mã độc xâm hại hệ thống.

Tính năng

+ Phát hiện và chống lại APTs và các tấn công có mục tiêu Zero-day malware và các khai thác lỗ hổng trên document.

+ Các hành vi tấn công mạng Email threats (phishing, spear-phishing): Bots, Trojans, Worms, Key Loggers and Crime ware.

+ Giám sát thời gian thực, phân tích sâu dựa trên giao diện điều khiển trực quan + Giám sát tập trung vào các nguy cơ có mức độ nghiêm trọng cao và các đối tượng có giá trị.

+ Cung cấp các thông tin về an ninh hệ thống, và đưa ra các biện pháp khắc phục.

### 1.6.4. Giải pháp bảo mật đầu cuối

1) Giải pháp giám sát truy cập

Lợi ích

Đảm bảo các quy định/ chính sách an ninh trên hệ thống được tuân thủ.

Tính năng

+ Đảm bảo các đầu cuối phải tuân thủ các chính sách trước khi truy cập tài nguyên hệ thống như: phải cập nhật bản vá mới nhất, phải cài đặt chương trình anti- virus theo quy định...

+ Tích hợp với các thành phần trên hệ thống cô lập các máy tính không tuân thủ chính sách, tự động sửa chữa hay áp đặt các chính sách lên các máy không tuân thủ

2) Giải pháp bảo mật đầu cuối

Lợi ích

Cho phép ngăn chặn các nguy cơ bảo mật có thể gây hại cho đầu cuối.

Tính năng

+ Chống thất thoát dữ liệu

+ Chống virus/ spyware/...

+ Lọc các liên kết web có hại

+ Chống tấn công trên đầu cuối (Hosted-IPS)

+Mã hóa các thông tin quan trọng Giám sát các ứng dụng cài đặt trên đầu cuối

3) Giải pháp giám sát truy cập

Lợi ích

Đảm bảo các quy định/ chính sách an ninh trên hệ thống được tuân thủ.

Tính năng

+ Đảm bảo các đầu cuối phải tuân thủ các chính sách trước khi truy cập tài nguyên hệ thống như: phải cập nhật bản vá mới nhất, phải cài đặt chương trình anti- virus theo quy định... + Tích hợp với các thành phần trên hệ thống cô lập các máy tính không tuân thủ chính sách, tự động sửa chữa hay áp đặt các chính sách lên các máy không tuân thủ,

4) Giải pháp mật khẩu sử dụng một lần (One-time password — OTP)

Lợi ích

Tăng cường bảo vệ truy cập của người dùng.

Tính năng

+ Mật khẩu phát sinh ngẫu nhau theo thời gian (30 giây, 60 giây, ...)

+ Tích hợp OTP vào hạ tầng CNTT khi truy cập máy chủ, thiết bị mạng, cơ sở dữ liệu, ứng dụng.

+ Hỗ trợ nhiều hình thức OTP khác nhau như gửi qua email, gửi qua SMS, sử dụng hardware token, software token.

### 1.6.5 Giải pháp quản lý bảo mật tập trung

1) Giải pháp phân tích sự kiện và cảnh báo an ninh

Lợi ích

Giám sát, phân tích và quản lý tập trung hệ thống nhật ký (log).

Tính năng

+ Thu thập log từ tất cả các thành phần hệ thống gồm: mạng, thiết bị bảo mật, máy chủ, hệ điều hành, ứng dụng, cơ sở dữ liệu.

+ Tự động tổng hợp và phân tích log trên toàn hệ thống Đưa ra các cảnh báo kịp thời cho người quản trị khi hệ thống có sự cố.

+ Liên kết các sự kiện từ nhiều nguồn log.

2) Giải pháp quản lý chính sách an ninh hệ thống

Lợi ích

Xây dựng, quản lý, giám sát các chính sách an ninh tổng thể trên hệ thống. Tính năng

+ Thu thập log từ tất cả các thành phần hệ thống gồm: mạng, thiết bị bảo mật, máy chủ, hệ điều hành, ứng dụng, cơ sở dữ liệu.

+ Tự động tổng hợp và phân tích log trên toàn hệ thống. Đưa ra các cảnh báo kịp thời cho người quản trị khi hệ thống có sự cố.

+ Liên kết các sự kiện từ nhiều nguồn log.

**Kết luận**

Chương này đã giới thiệu tổng quan về mạng máy tính và các vấn đề bảo mật mạng. Trong nội dung chương đã phân tích làm rõ các khái niệm về mạng máy tính, các phương pháp phân loại phổ biến hiện nay của mạng máy tính mà các nhà mạng đang khai thác, sử dụng, và phân tích một số hình thức tấn công mạng phổ biến hiện nay. Trong thời đại số, tin tặc có vô số cách để đánh cắp thông tin, và để bảo mật được mạng chúng ta phải nắm được các khía cạnh bảo mật và mức độ bảo mật mạng để từ đó lựa chọn ra được các giải pháp bảo mật phù hợp với hệ thống hạ tầng mạng của đơn vị mình.

# CHƯƠNG 2: CÁC HỆ THỐNG PHÁT HIỆN VÀ NGĂN CHẶN XÂM NHẬP MẠNG

## 2.1. Hệ thống phát hiện xâm nhập (Intrusion Detection Systems - IDS)

Hệ thống phát hiện xâm nhập là một hệ thống giám sát lưu lượng mạng nhằm phát hiện ra hiện tượng bất thường, các hoạt động trái phép xâm nhập vào hệ thống. Mục đích của IDS là giám sát các gói tin lưu thông trên mạng và phân tích các gói tin để phát hiện những dấu hiệu khả nghi cảnh báo cho nhà quản trị mạng kịp thời ngăn chặn đảm bảo an ninh mạng.

IDS cũng có thể phân biệt giữa những cuộc tấn công nội bộ (từ chính nhân viên hoặc khách hàng trong tổ chức) và tấn công bên ngoài (từ hacker). Trong một số trường hợp, IDS có thể phản ứng lại với các gói tin lưu thông bất thường/độc hại bằng cách chặn người dùng hoặc địa chỉ IP nguồn truy cập mạng.

### 2.1.1. Các chức năng của hệ thống phát hiện xâm nhập

Hệ thống phát hiện xâm nhập (IDS) thực hiện các chức năng cơ bản sau:

- Giám sát toàn bộ các gói tin lưu thông trên mạng.

- Phát hiện ngay lập tức khi có cuộc tấn công mạng xảy ra.

- Nhanh chóng triển khai biện pháp đối phó để ngăn chặn cuộc tấn công (hệ thống ngăn chặn xâm nhập)

- Gửi báo cáo cho quản trị viên hoặc nhóm bảo mật.

Mục đích của IDS là tạo ra một giao thức tự động để giám sát các cuộc tấn công mạng và thu hút sự tham gia của một nhóm các chuyên gia bảo mật trực tiếp, những người có thể phản ứng với nỗ lực vi phạm, xem phân tích kỹ thuật số về hoạt động và sau đó triển khai các giải pháp để cải thiện an ninh mạng. Hệ thống phát hiện xâm nhập được thiết kế để bảo vệ mọi thành phần của mạng bao gồm thiết bị, phần cứng và phần mềm trong trung tâm dữ liệu tại chỗ, máy chủ ảo hoặc nền tảng dựa trên đám mây. Nó tạo thành một vành đai kỹ thuật số bảo vệ an toàn cho mạng.

### 2.1.2. Vai trò của hệ thống phát hiện xâm nhập

- Kiểm tra lần nữa các điểm yếu của fire wall

- Nhận ra các cuộc tấn công mà firewall đã cho là hợp pháp (như cuộc tấn công vào webserver).

- Nhận ra được như là việc thử nhưng thất bại (bắt được việc scan port login...).

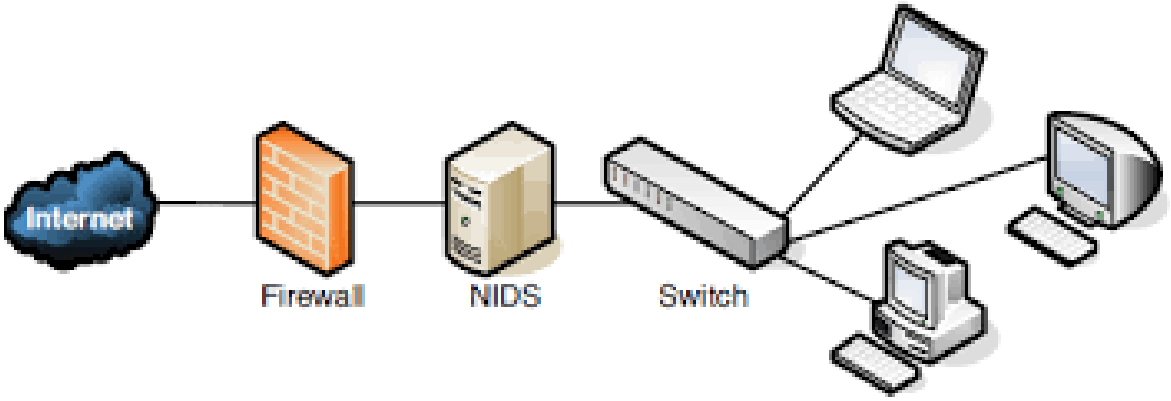
- Nhận ra các cuộc tấn công từ bên trong.

**2.1.3 Phân loại hệ thống phát hiện xâm nhập Hệ thống IDS được phân làm 2 loại cơ bản:**

- Hệ thống phát hiện xâm nhập mạng (Network-based IDS - NIDS): Là hệ thống giám sát tất các các lưu lượng đến và đi từ tất cả các thiết bị trong mạng.

- Hệ thống phát hiện xâm nhập máy chủ (Host-based IDS - HIDS): Là hệ thống theo dõi người dùng và xử lý các hoạt động trên các máy nội bộ để tìm dấu hiệu xâm nhập.

**1) Hệ thống phát hiện xâm nhập mạng (Network-based IDS - NIDS)**




Hình 2.1: Mô hình triển khai hệ thống NIDS

Hệ thống phát hiện xâm nhập mạng thường có hai thành phần logic: cảm biến và trạm quản lý. Thành phần Cảm biến nằm trên một phân đoạn mạng và nó giám sát phân đoạn mạng đó để biết lưu lượng truy cập đáng ngờ. Các trạm quản lý nhận các cảnh báo từ (các) cảm biến và hiển thị chúng cho người vận hành.

Các cảm biến thường là các hệ thống chuyên dụng chỉ tồn tại để giám sát mạng. Chúng có giao diện mạng ở chế độ quảng cáo, có nghĩa là chúng nhận được tất cả mạng lưu lượng truy cập, không chỉ dành cho địa chỉ IP nội mạng và chúng còn biết được địa chỉ IP của lưu lượng mạng truy cập để phân tích. Nếu chúng phát hiện điều gì đó có vẻ bất thường, chúng sẽ chuyển nó trở lại trạm phân tích. Trạm phân tích có thể hiển thị các cảnh báo hoặc thực hiện phân tích bổ sung. Một số màn hình là chỉ đơn giản là giao diện với công cụ quản lý mạng, nhưng một số các giao diện đồ họa người dùng tùy chỉnh, được thiết kế để giúp người vận hành phân tích vấn đề.

**- Ưu điểm:**

Hệ thống phát hiện xâm nhập mạng có thể phát hiện một số cuộc tấn công sử dụng mạng lưới. Chúng rất tốt để phát hiện các quyền truy cập trái phép hoặc một số loại truy cập vượt quá thẩm quyền.

Hệ thống phát hiện xâm nhập mạng không yêu cầu sửa đổi máy chủ hoặc máy chủ sản xuất. Đây là một lợi thế vì các máy chủ sản xuất thường xuyên hoạt động gần dung sai cho CPU, VO và dung lượng đĩa; cài đặt phần mềm bổ năng lực của hệ thống. sung có thể vượt quá

IDS không nằm trên con đường critcal cho bất kỳ dịch vụ hoặc quy trình sản xuất nào vì hệ thống phát hiện mạng không hoạt động như một bộ định tuyến hoặc thiết bị quan trọng khác. Lỗi hệ thống không ảnh hưởng đến hoạt động của mạng. Một lợi ích phụ của việc này là bạn ít có khả năng gặp phải sự tấn công từ bên trong mạng nội bộ; rủi ro đối với thao tác thực hiện trên hệ thống mạng thấp hơn so với máy chủ lưu trữ hệ thống.

Hệ thống phát hiện xâm nhập mạng có xu hướng khép kín hơn các hệ thống dựa trên máy chủ. Chúng chạy trên một hệ thống chuyên dụng dễ cài đặt; chỉ cần mở hộp thiết bị, làm một số cấu hình khắc phục và cắm nó vào mạng của bạn ở vị trí cho phép nó để giám sát lưu lượng truy cập nhạy cảm.

**- Nhược điểm**

Hệ thống phát hiện xâm nhập mạng chỉ kiểm tra lưu lượng mạng trên phân đoạn mà nó được kết nối trực tiếp, nhưng nó không thể phát hiện ra một cuộc tấn công đi qua phân đoạn mạng khác nhau.

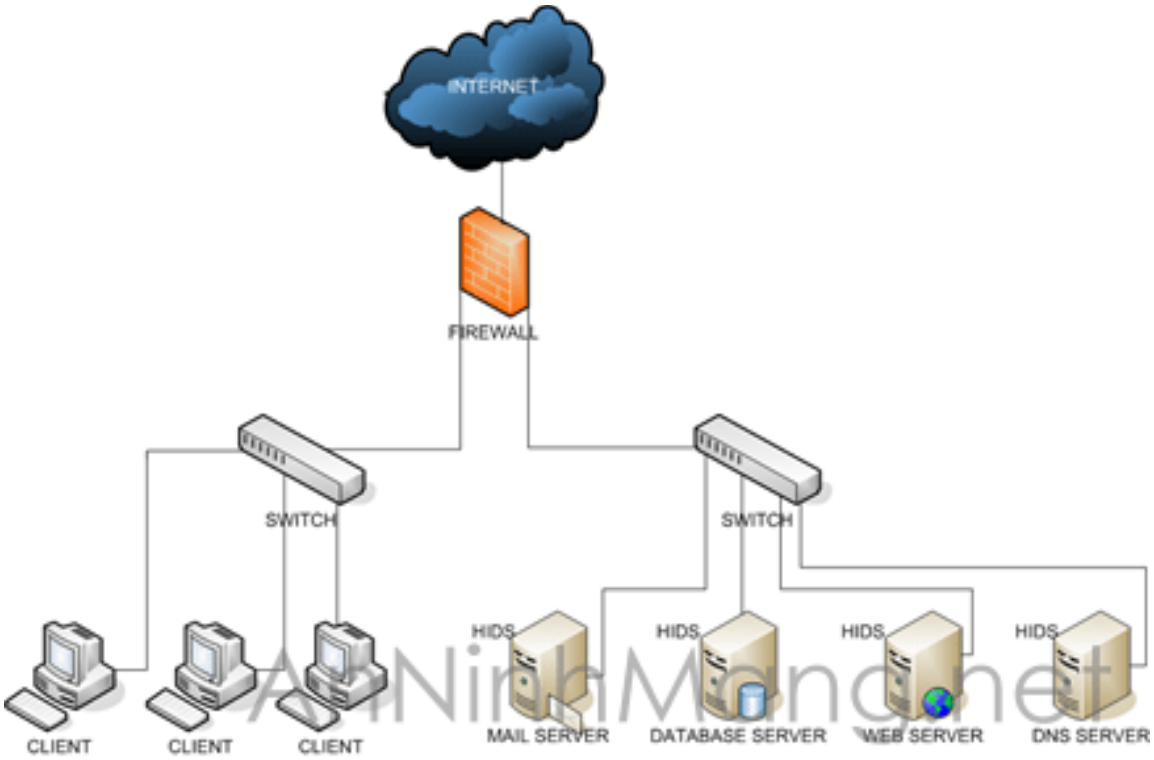
Hệ thống phát hiện xâm nhập mạng có xu hướng sử dụng phân tích chữ ký để đáp ứng các yêu cầu thực hiện. Điều này sẽ phát hiện các cuộc tấn công được lập trình phổ biến từ bên ngoài nhưng nó không đủ để phát hiện các mối đe dọa thông tin phức tạp hơn. Điều này yêu cầu khả năng kiểm tra môi trường mạnh mẽ hơn.

Hệ thống phát hiện xâm nhập mạng có thể cần giao tiếp khối lượng lớn dữ liệu được lưu trữ bên trong hệ thống trung tâm để phân tích. Đôi khi điều đó có nghĩa là bất kỳ gói tin nào được phân tích cũng tạo ra một lượng lớn hơn lưu lượng mạng thực tế. Nhiều hệ thống như vậy sử dụng tích cực quy trình giảm dữ liệu để giảm lượng lưu lượng truy cập được truyền thông. Họ cũng đẩy phần lớn quy trình ra quyết định được đưa vào chính cảm biến và sử dụng trạm trung tâm như một màn hình hiển thị trạng thái hoặc trung tâm liên lạc, thay vì để phân tích thực tế.

Các nhược điểm của điều này là nó cung cấp rất ít sự phối hợp giữa các cảm biến; bất kì đã cho cảm biến không biết rằng một cảm biến khác đã phát hiện một cuộc tấn công. Một hệ thống như vậy thông thường không thể phát hiện ra các cuộc tấn công hiệp đồng hoặc phức tạp

Hệ thống phát hiện xâm nhập mạng có thể gặp khó khăn trong việc xử lý các cuộc tấn công trong phạm vi mã hóa phiên họp. May mắn thay, có rất ít cuộc tấn công diễn ra trong một phiên lưu lượng truy cập, ngoại trừ các cuộc tấn công vào các máy chủ web yếu. Điều này sẽ trở nên nhiều hơn vấn đề khi các tổ chức chuyển đổi sang IPv6.

**2) Hệ thống phát hiện xâm nhập máy chủ (Host-based IDS - HIDS)**




Hình 2.2: Mô hình hệ thống HIDS

Hệ thống phát hiện xâm nhập máy chủ tìm kiếm các dấu hiệu xâm nhập vào hệ thống máy chủ cục bộ. Thường xuyên sử dụng cơ chế kiểm tra và ghi nhật ký của hệ thống máy chủ lưu trữ làm nguồn thông tin để phân tích. Họ tìm kiếm hoạt động bất thường được giới hạn trong máy chủ cục bộ chẳng hạn như đăng nhập, truy cập vượt giới hạn cho phép, báo cáo đặc quyền chưa được phê duyệt hoặc các thay đổi về đặc quyền hệ thống. Kiến trúc IDS thường sử dụng các công cụ dựa trên quy tắc để phân tích hoạt động; một ví dụ quy tắc như vậy có thể là, "đặc quyền siêu người dùng chỉ có thể đạt được thông qua chỉ huy." Do đó, các nỗ lực đăng nhập liên tiếp vào tài khoản gốc có thể được xem xét một cuộc tấn công.

**- Ưu điểm:**

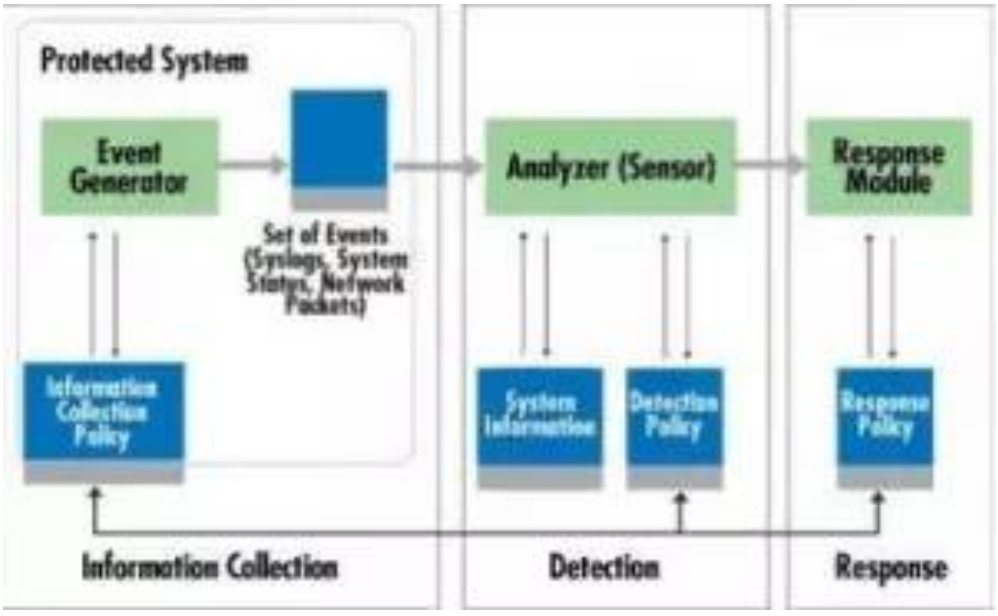
Hệ thống phát hiện xâm nhập máy chủ có thể là một công cụ cực kỳ mạnh mẽ để phân tích một cuộc tấn công có thể xảy ra. Đối với ví dụ, đôi khi nó có thể cho biết chính xác những gì kẻ tấn công đã làm, lệnh nào mà anh ta chạy, anh ta đã mở những tệp nào

và hệ thống nào gọi anh ta thực thi, thay vì chỉ là một cáo buộc rằng anh ta đã cố gắng thực hiện một lệnh nguy hiểm. Hệ thống phát hiện xâm nhập máy chủ thường cung cấp thông tin chi tiết và phù hợp hơn nhiều so với hệ thông phát hiện xâm nhập mạng. Hệ thống phát hiện xâm nhập máy chủ có khả năng phát hiện các truy cập trái phép chính xác hơn so với hệ thống phát hiện xâm nhập mạng. Điều này xảy ra do phạm vi lệnh được thực thi trên một máy chủ cụ thể tập trung hơn nhiều so với các loại lưu lượng truy cập qua mạng. Điều này tài sản có thể làm giảm sự phức tạp của các công cụ phân tích dựa trên máy chủ.

Hệ thống phát hiện xâm nhập máy chủ có thể được sử dụng trong môi trường nơi phát hiện xâm nhập rộng không cần thiết hoặc khi băng thông không có sẵn cho truyền thông từ cảm biến đến phân tích. Hệ thống phát hiện xâm nhập máy chủ có thể hoàn toàn độc lập. Điều này cũng cho phép hệ thống phát hiện xâm nhập máy chủ để chạy, trong một số trường hợp, từ phương tiện chỉ đọc; điều này ngăn cản kẻ tấn công vô hiệu hóa IDS.

Cuối cùng, hệ thống phát hiện xâm nhập máy chủ lưu trữ có thể ít rủi ro hơn khi định cấu hình với phản hồi hoạt động, chẳng hạn như chấm dứt một dịch vụ hoặc đăng xuất một người dùng vi phạm. Một hệ thống dựa trên máy chủ khó giả mạo hơn để hạn chế quyền truy cập từ các nguồn hợp pháp.

### 2.1.4. Các thành phần của hệ thống phát hiện xâm nhập




Hình 2.3: Các thành phần của IDS

Hệ thống phát hiện xâm nhập bao gồm các thành phần chính sau:

- Bộ sưu tập gói tin (information collection).

- Bộ phân tích xử lý gói tin (Detection).

- Bộ phận cảnh báo (response) nếu có truy cập bất thường nó sẽ gửi thông báo về cho quản trị viên. Trong ba thành phần trên thì bộ phân tích xử lý gói tin là quan trọng nhất và trong thành phần này thì bộ cảm biến (sensor) đóng vai trò quyết định.

-Bộ cảm biến được tích hợp với thành phần sưu tập dữ liệu và một bộ tạo sự kiện. Cách sưu tập này được xác định bởi chính sách tạo sự kiện. Bộ tạo sự kiện (hệ điều hành, mạng, ứng dụng) cung cấp một số chính sách thích hợp cho các sự kiện, có thể là một bản ghi các sự kiện của hệ thống hoặc các gói mạng.

-Vai trò của bộ cảm biến là dùng để lọc thông tin và loại bỏ dữ liệu không tương thích đạt được từ các sự kiện liên quan với hệ thống bảo vệ, vì vậy có thể phát hiện được các hành động nghi ngờ. Bộ phân tích sử dụng cơ sở dữ liệu chính sách phát hiện cho mục này. Ngoài ra còn có các thành phần: dấu hiệu tấn công, profile hành vi thông thường, các tham cấu hình, gồm có các chế độ truyền thông với module đáp trả. Bộ cảm biến cũng có cơ sở dữ liệu của riêng nó, bao gồm dữ liệu lưu về các xâm phạm phức tạp tiềm ẩn (tạo ra từ nhiều hành động khác nhau).

## 2.2. Hệ thống ngăn chặn xâm nhập (IPS)

### 2.2.1 Khái niệm

Hệ thống ngăn chặn xâm nhập (IPS - Intrusion Prevention System) là một hệ thống phát hiện xâm nhập ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động xâm nhập không mong muốn đối với hệ thống máy tính. Hệ thống ngăn chặn xâm nhập sử dụng tập luật tương tự như hệ thống phát hiện xâm nhập.

Hệ thống ngăn chặn xâm nhập (IPS) là hệ thống được phát triển mở rộng dựa trên khả năng của các hệ thống phát hiện xâm nhập (IDS), phục vụ mục đích cơ bản là giám sát lưu lượng mạng và hệ thống. Điều này làm cho IPS trở nên tiên tiến hơn các hệ thống IDS là IPS được đặt trực tiếp trên đường mạng vì vậy chúng có khả năng ngăn chặn các hoạt động độc hại đang xảy ra theo thời gian thực.

### 2.2.2. Chức năng của hệ thống ngăn chặn xâm nhập

Chức năng của hệ thống ngăn chặn xâm nhập là xác định các hoạt động truy cập trái phép, lưu giữ các thông tin này. Sau đó kết hợp với firewall để dừng ngay các hoạt động này và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên. Hệ thống ngăn chặn xâm nhập được xem là trường hợp mở rộng của hệ thống phát hiện xâm nhập, hai hệ thống này có đặc điểm và cách thức hoạt động tương đối giống nhau. Điểm khác biệt duy nhất là hệ thống ngăn chặn xâm nhập ngoài khả năng theo dõi, giám sát thì nó còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với

hệ thống. Hệ thống ngăn chặn xâm nhập sử dụng tập luật tương tự như hệ thống phát hiện xâm nhập.

Hệ thống ngăn chặn xâm nhập có các chức năng chính như sau:

- Theo dõi các hoạt động truy cập bất thường đối với hệ thống.

- Xác định ai đang tác động đến hệ thống và cách thức như thế nào, các hoạt động xâm nhập xảy ra tại vị trí nào trong cấu trúc mạng.

- Phối hợp với hệ thống firewall để ngăn chặn tức thời các hoạt động xâm nhập không mong muốn trên mạng.

- Tường thuật chi tiết về các hoạt động xâm nhập.

### 2.2.3. Phân loại hệ thống ngăn chặn xâm nhập

Hệ thống ngăn chặn xâm nhập được phân làm 2 loại chính sau:

1) Hệ thống ngăn chặn xâm nhập mạng (NIPS – Network-based Intrusion Prevention)

Hệ thống ngăn chặn xâm nhập mạng thường được triển khai trước hoặc sau firewall. Khi triển khai IPS trước firewall là có thể bảo vệ được toàn bộ hệ thống bên trong kể cả firewall, vùng DMZ. Có thể giảm thiểu nguy cơ bị tấn công từ chối dịch vụ đối với firewall. Khi triển khai IPS sau firewall có thể phòng tránh được một số kiểu tấn công thông qua khai thác điểm yếu trên các thiết bị di động sử dụng VPN để kết nối vào bên trong.

2) Hệ thống ngăn chặn xâm nhập máy chủ (HIPS – Host-based Intrusion Prevention)

Hệ thống ngăn chặn xâm nhập máy chủ thường được triển khai với mục đích phát hiện và ngăn chặn kịp thời các hoạt động thâm nhập trên các host. Để có thể ngăn chặn ngay các tấn công, HIPS sử dụng công nghệ tương tự như các giải pháp antivirus. Ngoài khả năng phát hiện ngăn ngừa các hoạt động thâm nhập, HIPS còn có khả năng phát hiện sự thay đổi các tập tin cấu hình.

## 2.3. Kết luận

Chương này trình bày về hệ thống phát hiện và ngăn chặn xâm nhập. Trước tình hình mất an toàn an ninh mạng ngày càng gia tăng đòi hỏi các hệ thống máy tính phải có một chiến lược phòng thủ theo chiều sâu nhiều lớp. Hệ thống IDS/IPS là một sự bo sung cần thiết cho các thiết bị Firewall, có chức năng phát hiện và cảnh báo trước các dấu hiệu tấn công lên hệ thống mạng, giúp cho người quản trị chủ động trong việc ngăn chặn các hành vi xâm nhập trái phép. Hệ thống IDS có thể phân làm 2 loại chính là NIDS và HIDS tùy theo đối tượng mà nó giám sát.

Một hệ thống IDS điển hình thường có 3 thành phần là: Cảm biến, bộ xử lý và giao diện, quá trình phát hiện tấn công theo 5 giai đoạn chính là: Giám sát, Phân tích, Liên lạc, Cảnh báo và Phản ứng. Tính năng chủ động phản ứng lại với các cuộc tấn công có thể bằng các hành động như: Ngắt phiên, ngắt dịch vụ hoặc khóa IP tấn công. Hiện tại đa số các hệ thống IDS phát hiện xâm nhập bằng kỹ thuật dựa trên dấu hiệu. Kỹ thuật này so sánh các dấu hiệu hiện tại với các mẫu tấn công đã có sẵn trong dữ liệu để đánh giá có tấn công hay không. Ưu điểm của phương pháp này là có thể hoạt động ngay lập tức, các cảnh báo đưa ra là chính xác, người quản trị có thể dễ dàng quản lý và chỉnh sửa tập các dấu hiệu.

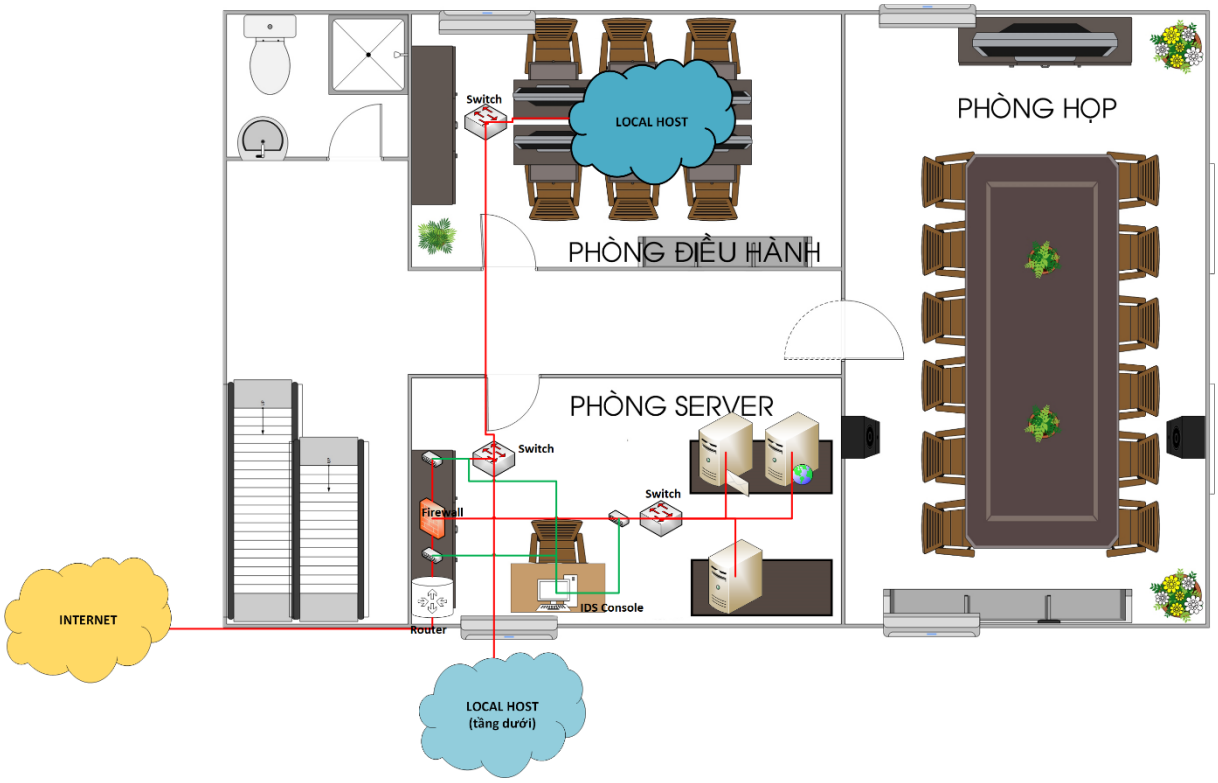
# CHƯƠNG 3:ỨNG DỤNG VÀ GIẢI PHÁP BẢO MẬT CHO MẠNG MÁY TÍNH CỦA CÔNG TY CMC

## 3.1. Mô hình ứng dụng và giải pháp an ninh mạng

Công ty CMC sở hữu trang web cmc.telecom và hệ thống server đặt ở lầu trên cùng của một tòa nhà 2 lầu. Công ty có một router kết nối với internet, sau router là firewall, sau firewall sẽ chia ra 2 đường truyền đi đến hệ thống máy server và đi đến hệ thống các thiết bị văn phòng trong mạng nội bộ.

Phương pháp an ninh mạng mà chúng ta sẽ sử dụng cho công ty là: Phát hiện và phòng chống xâm nhập mạng bằng Snort.

Cài đặt các bộ cảm biến IDS/IPS ở trước và sau firewall, cài trước firewall giúp chúng ta lọc được các gói tin độc hại. Tín hiệu của cảm biến sẽ được gửi về và tập hợp tại một máy tính điều khiển và phát ra cảnh báo cho nhân viên.




Hình 3.1 Sơ đồ thực tế cài đặt IDS vào hệ thống mạng

Các đường dẫn màu xanh là đường truyền tách ra từ đường truyền mạng bởi các thiết bị chia mạng (ở đây ta sử dụng network Tap). Đường truyền này dẫn các bản sao của gói tin từ internet ra vào hệ thống LAN của công ty đi qua cảm biến IDS, nếu có các gói tin bất thường sẽ IDS console sẽ phát ra cảnh báo.

## 3.2. Giải pháp triển khai hệ thống giám sát an toàn thông tin cho mạng.

### 3.2.1. Giới thiệu về Snort

Snort là hệ thống phát hiện xâm nhập mạng được Martin Roesch phát triển dưới mô hình mã nguồn mở. Snort ban đầu được xây dựng trên nền Unix nhưng sau đó phát triển sang các nền tảng khác. Snort được đánh giá rất cao về khả năng phát hiện xâm nhập. Snort có rất nhiều tính năng tốt. Với kiến trúc kiểu Module, người dùng có thể tụ tăng cường tính năng cho hệ thống Snort của mình.

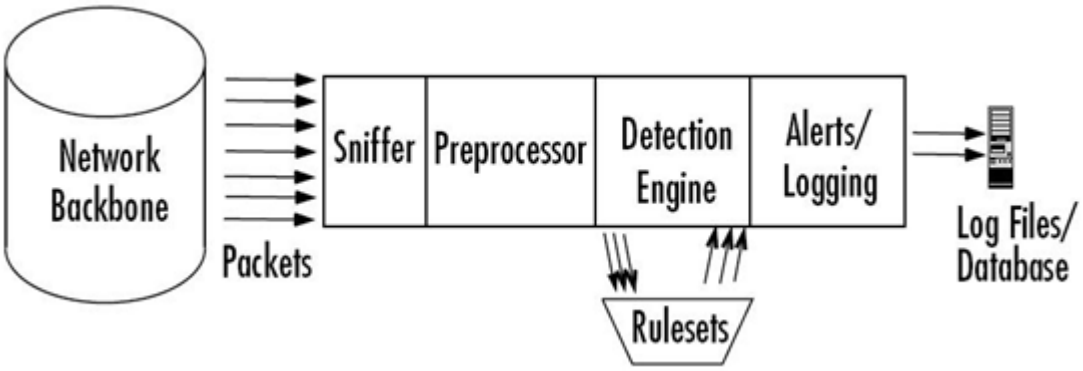
Snort chạy trên nhiều hệ thống như: Windows, Linux, OpenBSD, FreeBSD, Solaris...Snort ngoài việc hoạt động như một ứng dụng bắt gói tin thông thường, nó còn được cấu hình để chạy như một hệ thống phát hiện xâm nhập mạng.

### 3.2.2. Kiến trúc của snort

Snort bao gồm nhiều thành phần, với mỗi phần có một chức năng riêng.

Các phần chính đó là:

Môđun giải mã gói tin (Packet Decoder)
Môđun tiền xử lý (Preprocessors)
Môđun phát hiện (Detection Engine)
Môđun log và cảnh báo (Logging and Alerting System)
Môđun kết xuất thông tin (Output Module)
Kiến trúc của Snort được mô tả trong hình sau:




Hình 3.3. Kiến trúc và quy trình xử lý của Snort.

- Packet được đưa vào từ trục mạng chính.
- Packet được gửi thông qua Preprocessor để xác định xem nó có phải là packet hay không và có giữ nó lại hay không (preprocessor).
- Tiếp đến packet được sắp xếp theo theo loại, tùy theo việc có phát hiện được xâm nhập hay không mà gói tin có thể được bỏ qua để lưu thông tiếp hoặc được đưa vào Log và cảnh báo để xử lý.

• Cuối cùng nhiệm vụ của người quản trị là xác định xem làm gì với nó (ghi lại và lưu vào cơ sở dữ liệu).

### 3.2.3. Luật trong Snort

Cũng giống như virus, hầu hết các hoạt động tấn công hay xâm nhập đều có các dấu hiệu riêng. Các thông tin về các dấu hiệu này sẽ được sử dụng để tạo nên các luật cho Snort. Thông thường, các bẫy (honey pots) được tạo ra để tìm hiểu xem các kẻ tấn công làm gì cũng như các thông tin về công cụ và công nghệ chúng sử dụng. Và ngược lại, cũng có các cơ sở dữ liệu về các lỗ hổng bảo mật mà những kẻ tấn công muốn khai thác. Các dạng tấn công đã biết này được dùng như các dấu hiệu để phát hiện tấn công xâm nhập. Các dấu hiệu đó có thể xuất hiện trong phần header của các gói tin hoặc nằm trong phần nội dung của chúng. Hệ thống phát hiện của Snort hoạt động dựa trên các luật (rules) và các luật này lại được dựa trên các dấu hiệu nhận dạng tấn công. Các luật có thể được áp dụng cho tất cả các phần khác nhau của một gói tin dữ liệu.

Một luật có thể được sử dụng để tạo nên một thông điệp cảnh báo, log một thông điệp hay có thể bỏ qua một gói tin.

**Cấu trúc luật của Snort.**

Hãy xem xét một ví dụ đơn giản:

alert tcp 192.168.2.0/24 23 -> any any (content:”confidential”; msg: “Detected confidential”)

Ta thấy cấu trúc của một luật có dạng như sau:

| Rule Header | Rule Option |
|---|---|

Hình 3.4: Cấu trúc luật của Snort

***Diễn giải:***

Tất cả các Luật của Snort về logic đều gồm 2 phần: Phần header và phần Option.

Phần Header chứa thông tin về hành động mà luật đó sẽ thực hiện khi phát hiện ra có xâm nhập nằm trong gói tin và nó cũng chứa các tiêu chuẩn để áp dụng luật với gói tin đó.

Phần Option chứa một thông điệp cảnh báo và các thông tin về các phần của gói tin dùng để tạo nên cảnh báo. Phần Option chứa các tiêu chuẩn phụ thêm để đối sánh luật với gói tin. Một luật có thể phát hiện được một hay nhiều hoạt động thăm dò hay tấn công. Các luật thông minh có khả năng áp dụng cho nhiều dấu hiệu xâm nhập.

1) Phần tiêu đề (Header).

Dưới đây là cấu trúc chung của phần Header của một luật Snort:

| Action | Protocol | Address | Port | Direction | Address | Port |
|---|---|---|---|---|---|---|

Hình 3.5: Header luật của Snort

Như phần trên đã trình bày, Header của luật bao gồm nhiều phần. Sau đây, là chi tiết cụ thể của từng phần một.

Action:Là phần qui định loại hành động nào được thực thi khi các dấu hiệu của gói tin được nhận dạng chính xác bằng luật đó. Thông thường, các hành động tạo ra một cảnh báo hoặc log thông điệp hoặc kích hoạt một luật khác. Action chỉ ra hành động nào được thực hiện khi mà các điều kiện của luật được thoã mãn. Một hành động được thực hiện khi và chỉ khi tất cả các điều kiện đều phù hợp. Có 5 hành động đã được định nghĩa nhưng ta có thể tạo ra các hành động riêng tuỳ thuộc vào yêu cầu của mình. Đối với các phiên bản trước của Snort thì khi nhiều luật là phù hợp với một gói tin nào đó thì chỉ một luật được áp dụng. Sau khi áp dụng luật đầu tiên thì các luật tiếp theo sẽ không áp dụng cho gói tin ấy nữa. Nhưng đối với các phiên bản sau của Snort thì tất cả các luật sẽ được áp dụng gói tin đó.

Pass: Hành động này hướng dẫn Snort bỏ qua gói tin này. Hành động này đóng vai trò quan trọng trong việc tăng cường tốc độ hoạt động của Snort khi mà ta không muốn áp dụng các kiểm tra trên các gói tin nhất định. Ví dụ ta sử dụng các bẫy (đặt trên một máy nào đó) để nhử các hacker tấn công vào thì ta phải cho tất cả các gói tin đi đến được máy đó. Hoặc là dùng một máy quét để kiểm tra độ an toàn mạng của mình thì ta phải bỏ qua tất cả các gói tin đến từ máy kiểm tra đó.

Log: Hành động này dùng để log gói tin. Có thể log vào file hay vào cơ sở dữ liệu tuỳ thuộc vào nhu cầu của mình.

Alert: Gửi một thông điệp cảnh báo khi dấu hiệu xâm nhập được phát hiện. Có nhiều cách để gửi thông điệp như gửi ra file hoặc ra một Console. Tất nhiên là sau khi gửi thông điệp cảnh báo thì gói tin sẽ được log lại.

Activate: sử dụng để tạo ra một cảnh báo và kích hoạt một luật khác kiểm tra thêm các điều kiện của gói tin.

Dynamic: chỉ ra đây là luật được gọi bởi các luật khác có hành động là Activate.

***Protocols***

Là phần thứ hai của một luật có chức năng chỉ ra loại gói tin mà luật sẽ được áp dụng. Protocols qui định việc áp dụng luật cho các packet chỉ thuộc một giao thức cụ thể nào đó. Hiện tại Snort hiểu được các protocol sau:

- IP
- ICMP
- TCP
- UDP

Nếu là IP thì Snort sẽ kiểm tra header của lớp liên kết để xác định loại gói tin. Nếu bất kì giao thức nào khác được sử dụng thì Snort sử dụng header IP để xác định loại protocol. Protocol chỉ đóng vai trò trong việc chỉ rõ tiêu chuẩn trong phần header của luật. Phần option của luật có thể có các điều kiện không liên quan gì đến protocol.

***Address***

Là phần địa chỉ nguồn và địa chỉ đích. Các địa chỉ có thể là một máy đơn, nhiều máy hoặc của một mạng nào đó. Trong hai phần địa chỉ trên thì một sẽ là địa chỉ nguồn, một sẽ là địa chỉ đích và địa chỉ nào thuộc loại nào sẽ do phần Direction "->" qui định. Có hai phần địa chỉ trong một luật của Snort. Các địa chỉ này được dùng để kiểm tra nguồn sinh ra và đích đến của gói tin. Địa chỉ có thể là địa chỉ của một IP đơn hoặc là địa chỉ của một mạng. Ta có thể dùng từ any để áp dụng luật cho tất cả các địa chỉ.

Địa chỉ được viết ngay theo sau một dấu gạch chéo và số bit trong

subnet mask.Ví dụ như địa chỉ 192.168.2.0/24 thể hiện mạng lớp C 192.168.2.0 với 24 bit của subnet mask. Subnet mask 24 bit chính là 255.255.255.0. Ta biết rằng:

- Nếu subnet mask là 24 bit thì đó là mạng lớp C

- Nếu subnet mask là 16 bit thì đó là mạng lớp B
- Nếu subnet mask là 8 bit thì đó là mạng lớp A
- Nếu subnet mask là 32 bit thì đó là địa chỉ IP đơn.

Trong hai địa chỉ của một luật Snort thì có một địa chỉ là địa chỉ nguồn và địa chỉ còn lại là địa chỉ đích. Việc xác định đâu là địa chỉ nguồn, đâu là địa chỉ đích thì phụ thuộc vào phần hướng (direction).

Ví dụ như luật:

alert tcp any any -> 192.168.1.10/32 80 (msg: "TTL=100"; ttl: 100;)

Luật trên sẽ tạo ra một cảnh báo đối với tất cả các gói tin từ bất kì nguồn nào có TTL = 100 đi đến web server 192.168.1.10 tại cổng 80.

***Ngăn chặn địa chỉ hay loại trừ địa chỉ***

Snort cung cấp cho ta kĩ thuật để loại trừ địa chỉ bằng cách sử dụng dấu phủ định (dấu !). Dấu phủ định này đứng trước địa chỉ sẽ chỉ cho Snort không kiểm tra các gói tin đến từ hay đi tới địa chỉ đó. Ví dụ, luật sau sẽ áp dụng cho tất cả các gói tin ngoại trừ các gói có nguồn xuất phát từ mạng lớp C 192.168.2.0.

alert icmp![192.168.2.0/24] any

-> any any (msg: "Ping with TTL=100"; ttl: 100;)

***Danh sách địa chỉ***

Ta có thể định rõ ra danh sách các địa chỉ trong một luật của Snort. Ví dụ nếu bạn muốn áp dụng luật cho tất cả các gói tin trừ các gói xuất phát từ hai mạng lớp C 192.168.2.0 và 192.168.8.0 thì luật được viết như sau:

alert icmp![192.168.2.0/24, 192.168.8.0/24] any

-> any any (msg: "Ping with TTL=100"; ttl: 100;)

Hai dấu [] chỉ cần dùng khi có dấu ! đứng trước.

***Cổng (Port Number)***

Xác định các cổng nguồn và đích của một gói tin mà trên đó luật được áp dụng. Số hiệu cổng dùng để áp dụng luật cho các gói tin đến từ hoặc đi đến một cổng hay một phạm vi cổng cụ thể nào đó. Ví dụ ta có thể sử dụng số cổng nguồn là 23 để áp dụng luật cho tất cả các gói tin đến từ một server Telnet. Từ any cũng được dùng để đại diện cho tất cả các cổng. Chú ý là số hiệu cổng chỉ có ý nghĩa trong

các giao thức TCP và UDP thôi. Nếu protocol của luật là IP hay ICMP thì số hiệu cổng không đóng vai trò gì cả.

Ví dụ:

alert tcp 192.168.2.0/24 23 -> any any (content: “confidential”; msg:

”Detected confidential”;)

Số hiệu cổng chỉ hữu dụng khi ta muốn áp dụng một luật chỉ cho một loại gói tin dữ liệu cụ thể nào đó. Ví dụ như là một luật để chống hack cho web thì ta chỉ cần sử dụng cổng 80 để phát hiện tấn công.

2 )Qui tắc tùy chọn (Rule options)

Các tùy chọn quy tắc tạo thành trung tâm của công cụ phát hiện xâm nhập của Snort, kết hợp tính dễ sử dụng với sức mạnh và tính linh hoạt. Tất cả các tùy chọn quy tắc Snort được phân tách với nhau bằng dấu chấm phẩy ";" tính cách. Các từ khóa tùy chọn quy tắc được phân tách khỏi các đối số của chúng bằng ký tự dấu hai chấm "". Các từ khóa tùy chọn quy tắc có sẵn cho Snort:

• msg - in tin nhắn trong cảnh báo và nhật ký gói.

logto - ghi gói tin vào tên tệp do người dùng chỉ định thay vì tệp đầu ra tiêu chuẩn.

• ttl - kiểm tra giá trị trường TTL của tiêu đề IP.

tos - kiểm tra giá trị trường TOS của tiêu đề IP.

• id - kiểm tra trường ID phân đoạn của tiêu đề IP cho một giá trị cụ thể.

• ipoption - xem các trường tùy chọn IP để biết các mã cụ thể. fragbits - kiểm tra các bit phân mảnh của tiêu đề IP.

• dsize - kiểm tra kích thước tải trọng của gói với một giá trị.

• flags - kiểm tra cờ TCP cho các giá trị nhất định.

• seq - kiểm tra trường số thứ tự TCP cho một giá trị cụ thể.

• ack - kiểm tra trường xác nhận TCP cho một giá trị cụ thể.

• itype - kiểm tra trường loại ICMP với một giá trị cụ thể.

• icode - kiểm tra trường mã ICMP với một giá trị cụ thể. icmp_id - kiểm tra trường ID ICMP ECHO với một giá trị cụ thể.

• icmp_seq - kiểm tra số thứ tự ICMP ECHO với một giá trị cụ thể

• content - tìm kiếm một mẫu trong tải trọng của gó.i

• content - lists - tìm kiếm một tập hợp các mẫu trong tải trọng của gói.

• offset - công cụ sửa đổi cho tùy chọn nội dung, đặt offset để bắt đầu thử so khớp mẫu.

depth – công cụ sửa đổi cho tùy chọn nội dung, đặt độ sâu tìm kiếm tối đa cho lần thử đối sánh mẫu.

- Msg

Tùy chọn quy tắc tin nhắn báo cho bộ máy ghi nhật ký và cảnh báo tin nhắn sẽ in cùng với kết xuất gói tin hoặc cảnh báo. Nó là một chuỗi văn bản đơn giản sử dụng "\" làm ký tự thoát để chỉ ra một ký tự rời rạc có thể gây nhầm lẫn cho trình phân tích cú pháp quy tắc của Snort (chẳng hạn như ký tự dấu chấm phẩy ";").

- Logto

Tùy chọn logto yêu cầu Snort ghi lại tất cả các gói kích hoạt quy tắc này vào một tệp nhật ký đầu ra đặc biệt. Điều này đặc biệt tiện dụng để kết hợp dữ liệu từ những thứ như hoạt động NMAP, quét HTTP CGI, v.v. Cần lưu ý rằng tùy chọn này không hoạt động khi Snort ở chế độ ghi nhật ký nhị phân.

-TTL

Tùy chọn quy tắc này được sử dụng để đặt một giá trị thời gian tồn tại cụ thể để kiểm tra. Thử nghiệm nó thực hiện chỉ thành công trên một kết quả phù hợp chính xác. Từ khóa tùy chọn này được thiết kế để sử dụng trong việc phát hiện các nỗ lực theo dõi lộ trình.

- TOS

Từ khóa "tos" cho phép bạn kiểm tra trường TOS của tiêu đề IP để biết một giá trị cụ thể. Thử nghiệm nó thực hiện chỉ thành công trên một kết quả phù hợp chính xác.

- ID

Từ khóa tùy chọn này được sử dụng để kiểm tra đối sánh chính xác trong trường ID phân đoạn tiêu đề IP. Một số công cụ hack (và các chương trình khác) đặt trường này cho các mục đích đặc biệt khác nhau, ví dụ giá trị 31337 rất phổ biến với một số tin tặc. Điều này có thể chống lại họ bằng cách đưa ra một quy tắc đơn giản để kiểm tra điều này và một số "số hacker" khác.

- Ipoptions

Nếu các tùy chọn IP có trong một gói, tùy chọn này sẽ tìm kiếm một tùy chọn cụ thể đang được sử dụng, chẳng hạn như định tuyến nguồn. Các đối số hợp lệ cho tùy chọn này là:

rr - Ghi lại tuyến đường. eol - Cuối danh sách.

nop - Không có tùy chọn.

ts - Dấu thời gian. sec - tùy chọn bảo mật IP.

Isrr - Định tuyến nguồn lỏng lẻo.

ssrr - Định tuyến nguồn nghiêm ngặt.

satid - Mã định danh luồng.

Các tùy chọn IP được theo dõi thường xuyên nhất là định tuyển nguồn chặt chẽ và lỏng lẻo, không được sử dụng trong bất kỳ ứng dụng internet phổ biến nào. Chỉ một tùy chọn có thể được chỉ định cho mỗi quy tắc.

- Fragbits

Quy tắc này kiểm tra phân đoạn và các bit dành riêng trong tiêu đề IP. Có ba bit có thể được kiểm tra, bit dành riêng (RB), More Fragment (MF) bit và Don't Fragment (DF) bit. Các bit này có thể được kiểm tra bằng nhiều cách kết hợp. Sử dụng các giá trị sau để chỉ ra các bit cụ thể:

R-Reserved bit (RB): Bit dự trữ

D – Don’t Fragment (DF) bit: Nếu bit này được thiết lập thì gói tin không bị phân mảnh

M– More Fragments (MF) bit: nếu được thiết lập thì các thành phần khác của gói tin vẫn đang trên đường đi mà chưa tới đích. Nếu bit này mà không được thiết lập thì đây là phần cuối của gói tin.

Bạn cũng có thể sử dụng công cụ sửa đổi để chỉ ra tiêu chí đối sánh logic cho các bit được chỉ định:

+ - All flag, khớp trên các bit được chỉ định cộng với bất kỳ bit nào khác.

* - ANY flag, khớp nếu có bất kỳ bit nào được chỉ định được đặt.

! – NOT flag, khớp nếu các bit chỉ định không được đặt.

- Dsize

Tùy chọn dsize được sử dụng để kiểm tra kích thước tải trọng gói. Nó có thể được đặt thành bất kỳ giá trị nào, cộng với việc sử dụng các dấu hiệu lớn hơn / nhỏ hơn để biểu thị phạm vi và giới hạn. Ví dụ: nếu bạn biết rằng một dịch vụ nhất định có bộ đệm có kích thước nhất định, bạn có thể đặt tùy chọn này để theo dõi các lần cố tràn bộ đệm. Nó có thêm lợi thế là cách kiểm tra lỗi tràn bộ đệm nhanh hơn nhiều so với kiểm tra nội dung trọng tải.

- Nội dung (Content)

Từ khóa nội dung là một trong những tính năng quan trọng nhất của Snort. Nó cho phép người dùng thiết lập các quy tắc tìm kiếm nội dung cụ thể trong tải trọng gói và kích hoạt phản hồi dựa trên dữ liệu đó. Bất cứ khi nào khớp mẫu tùy chọn nội dung được thực hiện, hàm đối sánh mẫu Boyer-Moore được gọi và kiểm tra (khá mất thời gian về mặt tính toán) được thực hiện đối với nội dung gói. Nếu dữ liệu khớp chính xác với chuỗi dữ liệu trong hệ điều hành chứa ở bất kỳ đâu trong trọng tải của gói, thì kiểm tra sẽ thành công và phần còn lại của quy tắc kiểm tra tùy chọn được thực hiện. Lưu ý rằng thử nghiệm này phân biệt chữ hoa, chữ thường.

Dữ liệu tùy chọn cho từ khóa nội dung hơi phức tạp; nó có thể chứa hỗn hợp văn bản và dữ liệu nhị phân. Dữ liệu nhị phân thường được bao trong ký tự ống dẫn ("") và được biểu diễn dưới dạng mã bytecode. Bytecode biểu diễn dữ liệu nhị phân dưới dạng số thập phân và là một phương pháp viết tắt tốt để mô tả dữ liệu nhị phân phức tạp.

- Offset

Tùy chọn quy tắc bù đắp được sử dụng làm công cụ sửa đổi cho các quy tác sử dụng từ khóa tùy chọn nội dung. Từ khóa này sửa đổi vị trí tìm kiếm bắt đầu cho chức năng đối sánh mẫu từ đầu của trọng tải gói. Nó rất hữu ích cho những thứ như quy tắc phát hiện quét CGI trong đó chuỗi tìm kiếm nội dung không bao giờ được tìm thấy trong bốn byte đầu tiên của tải trọng. Cần cẩn thận chống lại việc đặt giá trị bù đắp quá "chặt chẽ" và có khả năng bị thiếu một cuộc tấn công! Không thể sử dụng từ khóa tùy chọn quy tắc này mà không chỉ định tùy chọn quy tắc nội dung.

- Depth

Độ sâu là một công cụ sửa đổi tùy chọn quy tắc nội dung khác. Điều này đặt độ sâu tìm kiếm tối đa cho chức năng đối sánh mẫu nội dung để tìm kiếm từ đầu vùng tìm kiếm của nó. Nó hữu ích để hạn chế chức năng đối sánh mẫu thực hiện các tìm kiếm không hiệu quả khi vùng tìm kiếm có thể có cho một tập hợp nội dung nhất định đã bị vượt quá. (Có nghĩa là, nếu bạn đang tìm kiếm "cgi-bin / phf" trong một

gói liên kết web, bạn có thể không cần phải lãng phí thời gian tìm kiếm trọng tải vượt quá 20 byte đầu tiên!)

- Nocase

Tùy chọn nocase được sử dụng để hủy kích hoạt phân biệt chữ hoa chữ thường trong quy tắc "nội dung". Nó được chỉ định một mình trong một quy tắc và bất kỳ ký tự ASCII nào được so sánh với tải trọng gói được coi như thể chúng là chữ hoa và chữ thường.

- Flag

Quy tắc này kiểm tra cờ TCP xem có khớp không. Thực tế có 8 biến cờ có sẵn

trong Snort:

F - FIN (LSB trong byte cờ TCP)

S-SYN

R-RST

P-PSH

A-ACK

U-URG

2 - Bit 2 dành riêng

1 - Bit 1 dành riêng (MSB trong byte cờ TCP)

Ngoài ra còn có các toán tử logic có thể được sử dụng để chỉ định tiêu chí phù hợp cho các cờ được chỉ định:

+ - ALL flag, khớp trên tất cả các cờ được chỉ định cộng với bất kỳ cờ nào

khác

* - ANY flag, phù hợp với bất kỳ cờ nào được chỉ định

! – NOT flag, khớp nếu các cờ được chỉ định không được đặt trong gói

Các bit dành riêng có thể được sử dụng để phát hiện hành vi bất thường, chẳng hạn như các nỗ lực lấy dấu vân tay ngăn xếp IP hoặc hoạt động đáng ngờ khác.

- Sep

Tùy chọn quy tắc này đề cập đến số thứ tự TCP. Về cơ bản, nó phát hiện xem gói có bộ số thứ tự tĩnh hay không.

- Ack

Từ khóa tùy chọn quy tắc ack đề cập đến trường xác nhận của tiêu đề TCP. Quy tắc này có một mục đích thực tế cho đến nay: phát hiện các ping TCP NMAP. Một ping TCP NMAP đặt trường này thành 0 và gửi một gói tin có cờ TCP ACK được đặt để xác định xem máy chủ mạng có đang hoạt động hay không.

- Itype

Quy tắc này kiểm tra giá trị của trường loại ICMP. Nó được đặt bằng giá trị số của trường này. Cần lưu ý rằng các giá trị có thể được đặt ngoài phạm vi để phát hiện các giá trị loại ICMP không hợp lệ đôi khi được sử dụng trong các cuộc tấn công từ chối dịch vụ và tràn ngập.

- Icode

Từ khóa tùy chọn quy tắc icode khá giống với quy tắc itype, chỉ cần đặt một giá trị số ở đây và Snort sẽ phát hiện bất kỳ lưu lượng nào sử dụng giá trị mã ICMP đó. Giá trị ngoài phạm vi cũng có thể được đặt để phát hiện lưu lượng truy cập đáng ngờ.

- Session

Từ khóa session là hoàn toàn mới kể từ phiên bản 1.3.1.1 và được sử dụng để trích xuất dữ liệu người dùng từ các phiên TCP. Nó cực kỳ hữu ích để xem những gì người dùng đang nhập trong telnet, rlogin, ftp hoặc thậm chí các phiên web. Có hai từ khóa đối số có sẵn cho tùy chọn quy tắc phiên, có thể in hoặc tất cả. Từ khóa có thể in chỉ in ra dữ liệu mà người dùng thường thấy hoặc có thể nhập. Tất cả từ khóa thay thế các ký tự không in được bằng các ký tự tương đương hệ thập lục phân của chúng. Hàm này có thể làm chậm Snort xuống đáng kể, vì vậy nó không nên được sử

dụng trong các trường hợp tải nặng và có lẽ phù hợp nhất cho các tệp nhật ký nhị phân (định dạng tcpdump) sau xử lý.

- Icmp_id

Tùy chọn icmp_id kiểm tra số ID ICMP của gói ICMP ECHO để tìm một giả trị cụ thể. Điều này rất hữu ích vì một số chương trình kênh bí mật sử dụng trường ICMP tĩnh khi chúng giao tiếp. Plugin đặc biệt này được phát triển để kích hoạt các quy tác phát hiện stacheldraht do Max Vision viết, nhưng nó chắc chắn hữu ích để phát hiện một số cuộc tấn công tiềm ẩn.

- Icmp_seq

Tùy chọn icmp_id kiểm tra trường trình tự ICMP của gói ICMP ECHO để tìm một giá trị cụ thể. Điều này rất hữu ích vì một số chương trình kênh bí mật sử dụng trường ICMP tĩnh khi chúng giao tiếp. Plugin đặc biệt này được phát triển để kích hoạt các quy tắc phát hiện stacheldraht do Max Vision viết, nhưng nó chắc chắn hữu ích để phát hiện một số cuộc tấn công tiềm ẩn.

- Rpc

Tùy chọn này xem xét các yêu cầu RPC và tự động giải mã ứng dụng, thủ tục và phiên bản chương trình, cho biết thành công khi cả ba biến được khớp. Định dạng của lệnh gọi quyền chọn là "ứng dụng, thủ tục, phiên bản". Các ký tự đại diện hợp lệ cho cả số thủ tục và phiên bản và được biểu thị bằng dấu ""

- Resp

Từ khóa tương ứng triển khai phản hồi linh hoạt (FlexResp) cho lưu lượng truy cập phù hợp với quy tắc Snort. Mã FlexResp cho phép Snort chủ động đóng các kết nối vi phạm. Các đối số sau hợp lệ cho mô-đun này:

•rst_snd - gửi các gói TCP-RST đến ổ cắm gửi.

• rst_rcv - gửi gói TCP-RST đến ổ cắm nhận. •rst_all - gửi gói TCP_RST theo cả hai hướng.

• icmp_net - gửi ICMP_NET_UNREACH cho người gửi. • icmp_host - gửi ICMP_HOST_UNREACH cho người gửi.

• icmp_port - gửi ICMP_PORT_UNREACH cho người gửi.

• icmp_all - gửi tất cả các gói ICMP trên cho người gửi.

Các tùy chọn này có thể được kết hợp để gửi nhiều phản hồi đến máy chủ đích. Nhiều đối số được phân tách bằng dấu phẩy.

- React

Từ khóa phản ứng dựa trên phản ứng linh hoạt (Flex Resp) triển khai phản ứng linh hoạt với lưu lượng truy cập phù hợp với quy tắc Snort. Phản ứng cơ bản là chặn các trang web thú vị mà người dùng muốn truy cập: New York Times, Slashdot hoặc một cái gì đó thực sự quan trọng - napster và các trang web khiêu dâm. Mã Flex Resp cho phép Snort chủ động đóng các kết nối vi phạm và / hoặc gửi thông báo hiển thị cho trình duyệt (cảnh báo sẽ sớm có công cụ sửa đổi). Thông báo có thể bao gồm nhận xét của riêng bạn. Các đối số sau đây (bổ ngữ cơ bản) hợp lệ cho tùy chọn này:

• Block - đóng kết nối và gửi thông báo hiển thị

Warn - gửi thông báo cảnh báo, hiển thị (sẽ sớm có)

Đối số cơ bản có thể được kết hợp với các đối số sau (bổ sung bổ sung):

• Msg - đưa văn bản tùy chọn tin nhắn vào thông báo hiển thị chặn

proxy: <port_nr> - sử dụng cổng proxy để gửi thông báo hiển thị (sẽ sớm có)

Nhiều đối số bổ sung được phân tách bằng dấu phẩy. Từ khóa react nên được

đặt ở vị trí cuối cùng trong danh sách tùy chọn. 3) Bộ tiền xử lý (Proprecessor)

- Tổng quan về bộ tiền xử lý

Các bộ tiền xử lý đã được giới thiệu trong phiên bản 1.5 của Snort. Chúng cho phép mở rộng chức năng của Snort bằng cách cho phép người dùng và lập trình viên thả các "plugin" mô-đun vào Snort khá dễ dàng. Mã tiền xử lý được chạy trước khi công cụ phát hiện được gọi, nhưng sau khi gói tin đã được giải mã. Gói tin có thể được sửa đổi hoặc phân tích theo cách "ngoài băng tần" thông qua cơ chế này.

Bộ tiền xử lý được tải và định cấu hình bằng từ khóa bộ tiền xử lý. Định dạng của chỉ thị tiền xử lý trong tệp quy tắc Snort.

- Các mô-đun tiền xử lý có sẵn

+ Minfrag

Bộ tiền xử lý minfrag kiểm tra các gói bị phân mảnh cho một ngưỡng kích thước được chỉ định. Khi các gói bị phân mảnh, nó thường do các bộ định tuyến giữa nguồn và đích gây ra. Nói chung, không có thiết bị mạng thương mại nào phân mảnh các gói có kích thước nhỏ hơn 512 byte, vì vậy chúng ta có thể sử dụng thực tế để cho phép giám sát lưu lượng đối với các đoạn nhỏ thường là dấu hiệu cho thấy ai đó đang cố gắng che giấu lưu lượng của họ đằng sau sự phân mảnh. này

+HTTP Decode

HTTP Decode được sử dụng để xử lý các chuỗi HTTP URI và chuyển đổi dữ liệu của chúng thành các chuỗi ASCII không bị xáo trộn. Điều này được thực hiện để đánh bại các trình quét URL web lẩn tránh và những kẻ tấn công thù địch có thể loại bỏ các chuỗi phân tích nội dung được sử dụng để kiểm tra lưu lượng truy cập HTTP để tìm hoạt động đáng ngờ. Mô-đun tiền xử lý lấy số cổng HTTP (phân tách bằng dấu cách) được chuẩn hóa làm đối số của nó (thường là 80 và 8080).

+ Máy dò quét cổng (Portscan Detector)

Bộ tiền xử lý Snort Portscan được phát triển bởi Patrick Mullen và (nhiều) thông tin khác có sẵn trên trang web của anh ấy.

Bộ tiền xử lý Snort Portscan làm gì:

Ghi nhật ký bắt đầu và kết thúc quét cổng từ một IP nguồn duy nhất vào cơ sở ghi nhật ký tiêu chuẩn.

Nếu một tệp nhật ký được chỉ định, hãy ghi nhật ký các IP và cổng đích được quét cũng như loại quét.

Quét cổng được định nghĩa là kết nối TCP cố gắng đến nhiều hơn cổng P trong T giây hoặc các gói UDP được gửi đến nhiều cổng P trong T giây. Các cổng có thể được trải rộng trên bất kỳ số lượng địa chỉ IP đích nào và tất cả có thể là cùng một cổng nếu trải rộng trên nhiều IP. Phiên bản này thực hiện quét đơn-> đơn và đơn nhiều cổng. Bản phát hành đầy đủ tiếp theo sẽ thực hiện quét các cổng phân tán (nhiều-> đơn hoặc nhiều-> nhiều). Một portcan cũng được định nghĩa là một gói "quét ấn", chẳng hạn như NULL, FIN, SYNFIN, XMAS, v.v. Điều này có nghĩa là từ scan

lib trong phân phối tiêu chuẩn của snort, bạn nên nhận xét phần dành cho các gói quét ẩn. Lợi ích là với mô-đun quét cổng, các cảnh báo này sẽ chỉ hiển thị một lần cho mỗi lần quét, thay vì một lần cho mỗi gói. Nếu bạn sử dụng tính năng ghi nhật ký bên ngoài, bạn có thể xem kỹ thuật và nhập tệp nhật ký.

Các đối số cho mô-đun này là:

• network to monitor - The network / CIDR để giám sát các lần quét cổng • number of ports - số cổng được truy cập trong khoảng thời gian phát hiện.

• detection period - số giây để đếm mà ngưỡng truy cập cổng được xem xét. • logdir / filename - thư mục / tên tệp để đặt cảnh báo. Cảnh báo cũng được ghi vào tệp cảnh báo chuẩn

- Cổng không quét (Portscan Ignorehosts)

Một mô-đun khác từ Patrick Mullen sửa đổi hoạt động của hệ thống phát hiện quét cổng. Nếu bạn có các máy chủ có xu hướng tắt máy dò quét cổng (chẳng hạn như máy chủ NTP, NFS và DNS), bạn có thể yêu cầu các máy chủ quét qua cổng TCP SYN và UDP từ các máy chủ nhất định. Các đối số của mô-đun này là danh sách các khối IP / CIDR cần được bỏ qua.

- Defrag

Mô-đun chống phân mảnh (từ Dragos Ruiu) cho phép Snort thực hiện chống phân mảnh IP hoàn toàn, khiến tin tặc khó khăn hơn khi chỉ đơn giản là phá vỡ khả năng phát hiện của hệ thống. Nó rất đơn giản trong cách sử dụng, chỉ yêu cầu thêm một chỉ thị tiền xử lý vào tệp cấu hình mà không có đối số. Tổng mô-đun này thay thế chức năng của mô-đun minfrag (tức là bạn không cần sử dụng minfrag nếu bạn đang sử dụng defrag).

4) Mô đun đầu ra (Output Modules)

Mô-đun đầu ra là mới kể từ phiên bản 1.6. Chúng cho phép Snort linh hoạt hơn nhiều trong việc định dạng và trình bày đầu ra cho người dùng. Các mô-đun đầu ra được chạy khi hệ thống con cảnh báo hoặc ghi nhật ký của Snort được gọi, sau bộ tiền xử lý và công cụ phát hiện. Định dạng của chỉ thị trong tệp quy tắc rất giống với định dạng của bộ tiền xử lý.

Nhiều plugin đầu ra có thể được chỉ định trong tệp cấu hình Snort. Khi nhiều plugin cùng loại (nhật ký, cảnh báo) được chỉ định, chúng được "xếp chồng lên nhau" và được gọi theo trình tự khi một sự kiện xảy ra. Như với các hệ thống ghi nhật ký và cảnh báo tiêu chuẩn, các plugin đầu ra gửi dữ liệu của chúng đến /var/log/snort theo mặc định hoặc đến thư mục do người dùng hướng dẫn (sử dụng chuyển đổi dòng lệnh "-1").

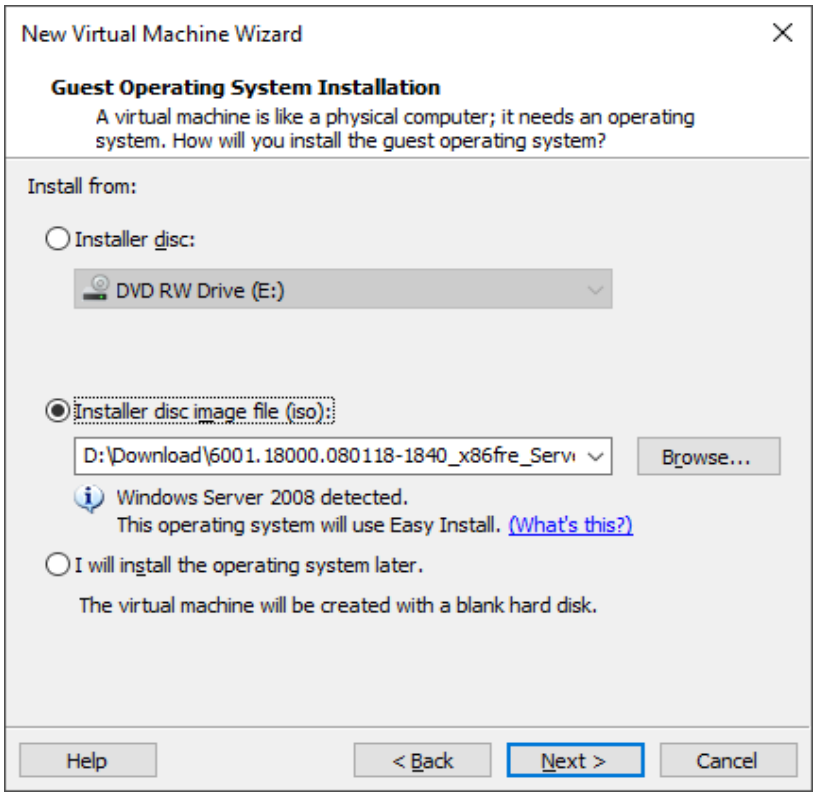
### 3.2.4 Cài đặt hệ thống

**Cài đặt máy ảo**

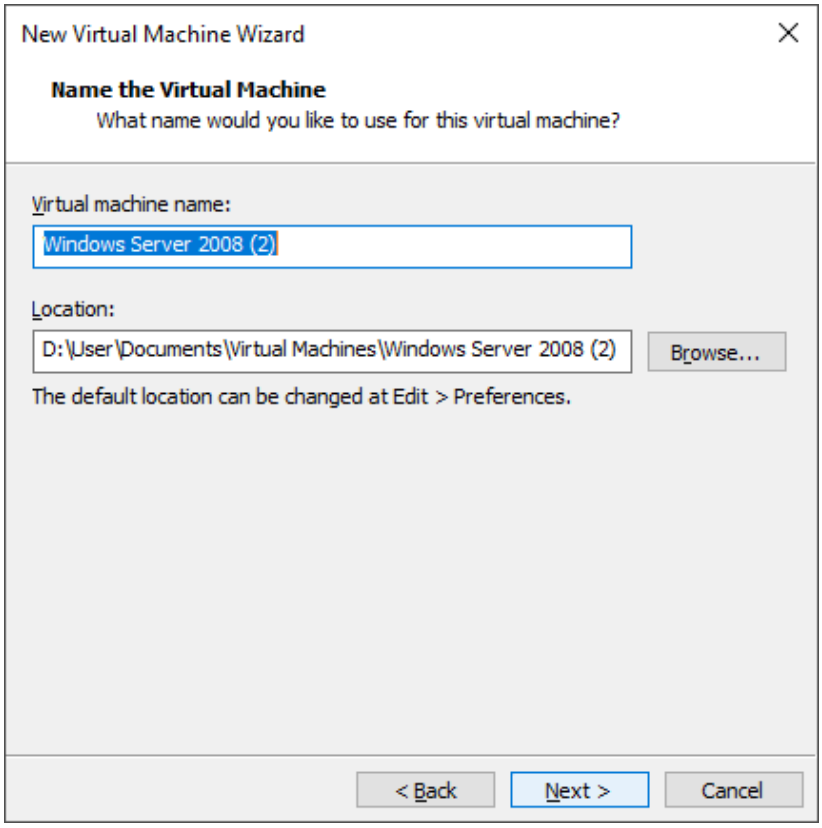
Bước 1: Khởi động Vmware Workstation.

Bước 2: Ctrl + N để mở trình tạo máy ảo mới -> Typical (recommended) -> Next

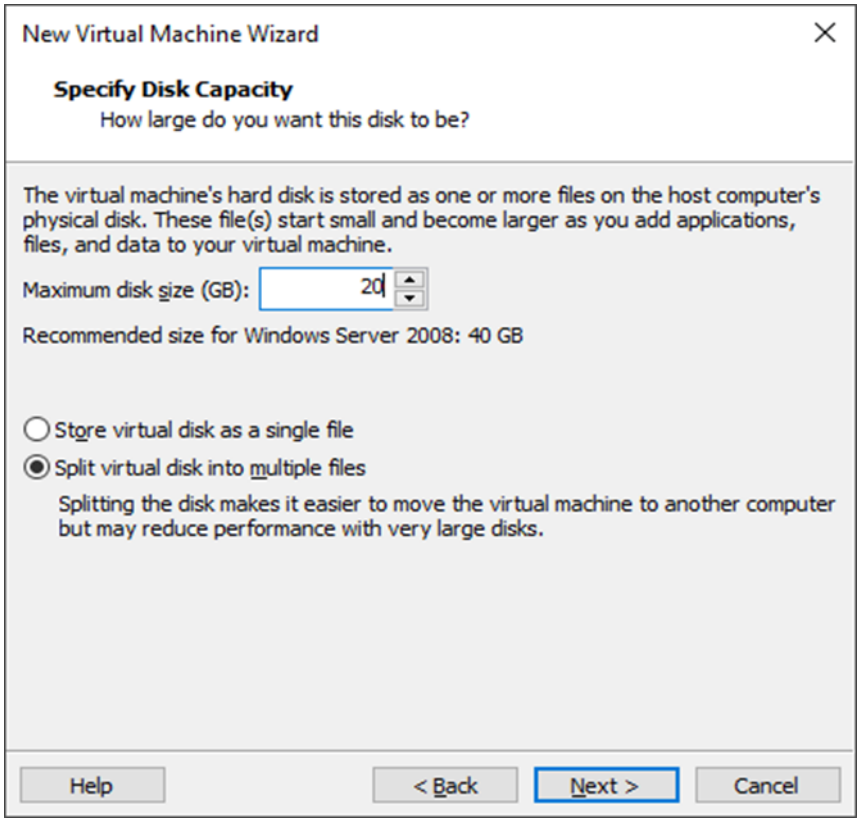
Bước 3: Installer disc_imge file (iso) -> Browse đến nơi lưu file iso hệ điều hành -> Next.



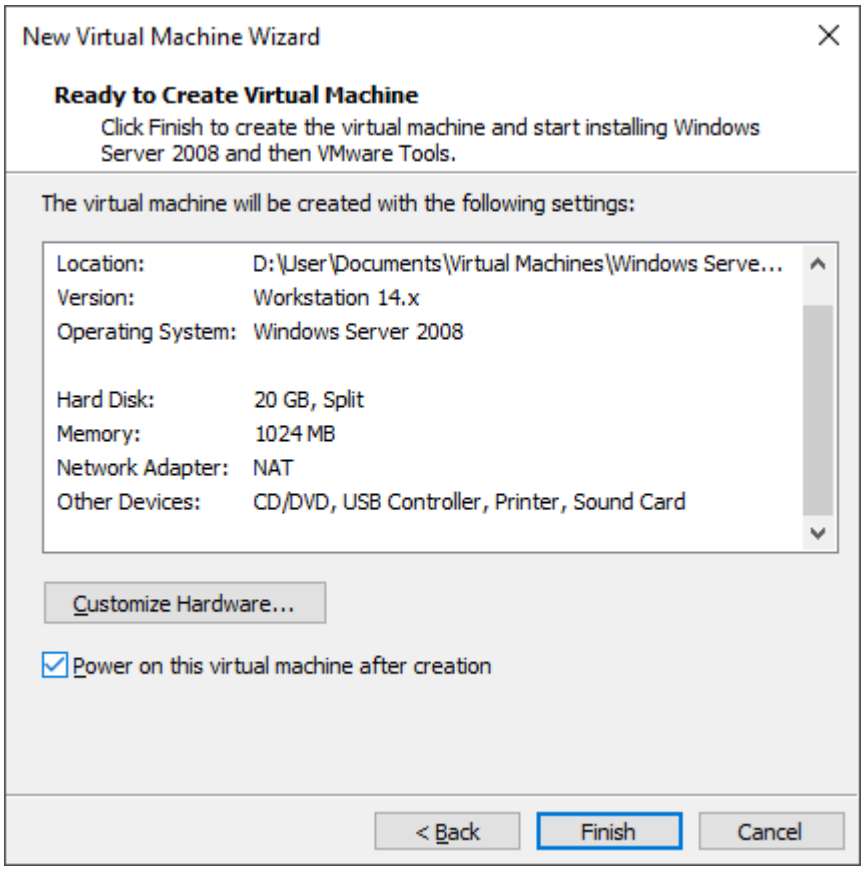

Bước 4: Đặt tên cho máy ảo và vị trí lưu trữ máy ảo.



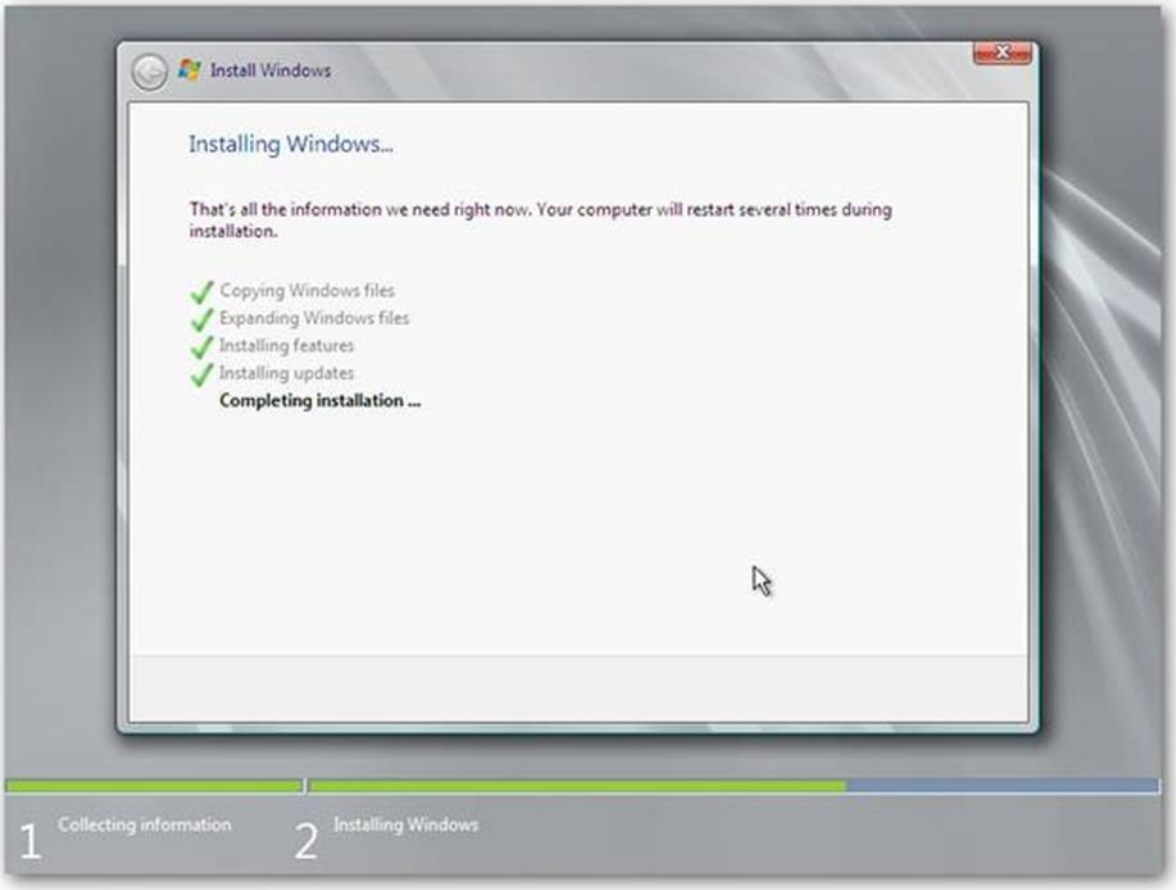
Bước 5: Phân vùng dung lượng ổ cứng cho máy ảo (để 20 GB là được) -> Next




Bước 6: Finish



Bước 7: Bước vào trình cài đặt windows, ta làm tương tự như khi cài đặt win máy thật



### 3.2.5. Cài đặt Snort trên Snort trên Windows Server 2008.

**Bước 1**: Cài đặt Snort

Link download: https://snort.org/downloads#snort-downloads

Download Snort_2_9_11_1_Installer.exe

Download snortrules-snapshot-29111.tar.gaz (Bắt buộc phải đăng ký tài khoản)

Double click vào file Snort_2_9_11_1_Installer và tiến hành cài đặt Snort vào ổ C:\

**Bước 2**: Giải nén file snortrules-snapshot-29111.tar

Sau đó copy toàn bộ thư mục giải nén được vào thư mục cài đặt snort (Mặc định C:\Snort), chọn Yes to All để dán đè.

**Bước 3**: Cấu hình Snort (Cài đặt notepad++ để đọc file)

Mở file C:\Snort\etc\snort.conf bằng Notepad++ để tiến hành chỉnh sửa file cấu hình từng bước như sau:

1. Sửa dòng: *ipvar HOME_NET any* thành *ipvar HOME_NET 192.168.92.128/24*
   * Dùng lệnh ipconfig trong cmd để kiểm tra ip của máy.

2.Sửa vị trí các thư mục rule (mặc định là c:\snort\) bằng cách:

Sửa 3 dòng : *var RULE_PATH ../rules*
*var SO_RULE_PATH ../so_rules*
*var PREPROC_RULE_PATH ../preproc_rules*

Thành :

*var RULE_PATH c:\snort\rules*
*var SO_RULE_PATH c:\snort\so_rules*
*var PREPROC_RULE_PATH c:\snort\preproc_rules*

*Hình 3.4 Sửa vị trí các thư mục rules*

3.Sửa dòng: *include classification.config*

*include reference.config*

Thành:

*include C:\Snort\etc\classification.config*

*include C:\Snort\etc\reference.config*

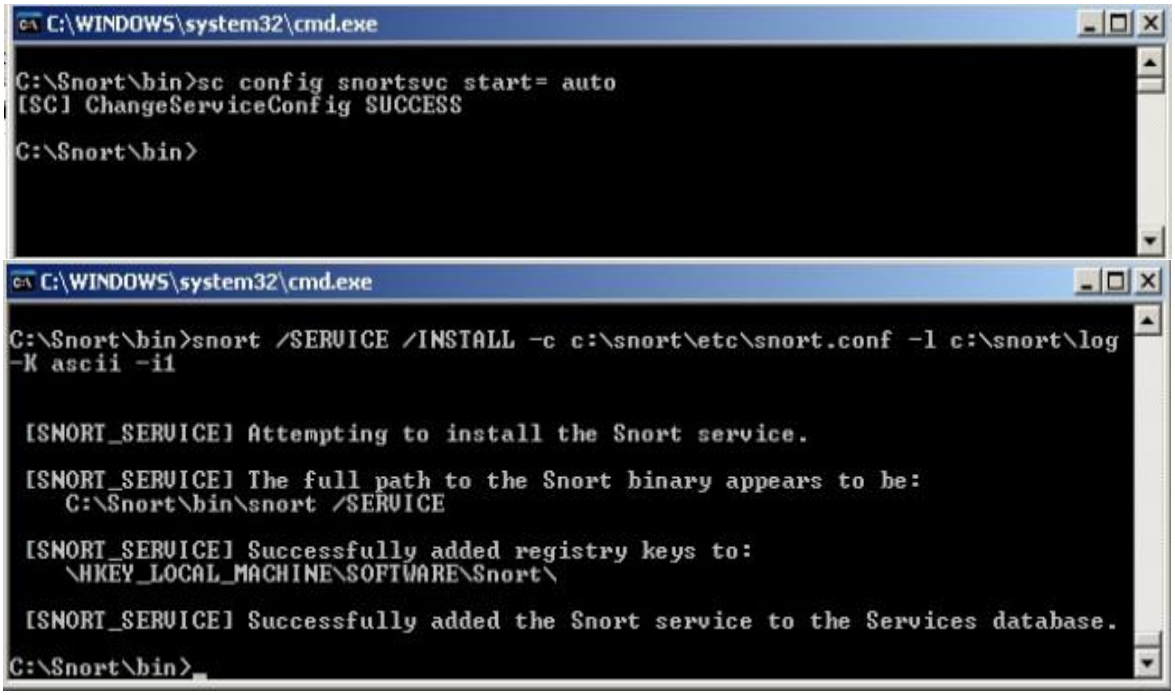
**Bước 4**.Chèn Dynamicpreprocessor

**Bước 5**.Thêm luật vào file config: include $RULE_PATH/<name>.rules

**+ Cài đặt Snort trong Service.**

Tại dấu nhắt lệnh gõ:

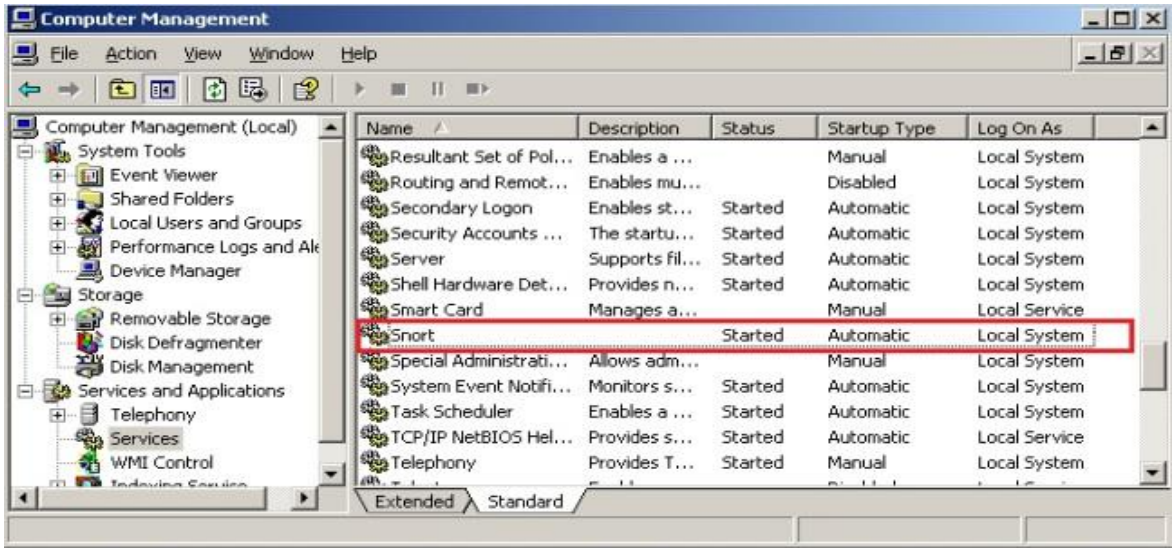
*Snort /SERVICE /INSTALL –c c:\snort\etc\snort.conf -l c:\snort\log –K ascii -i1*




Thực hiện tiếp lệnh: ***sc config snortsvc start= auto***

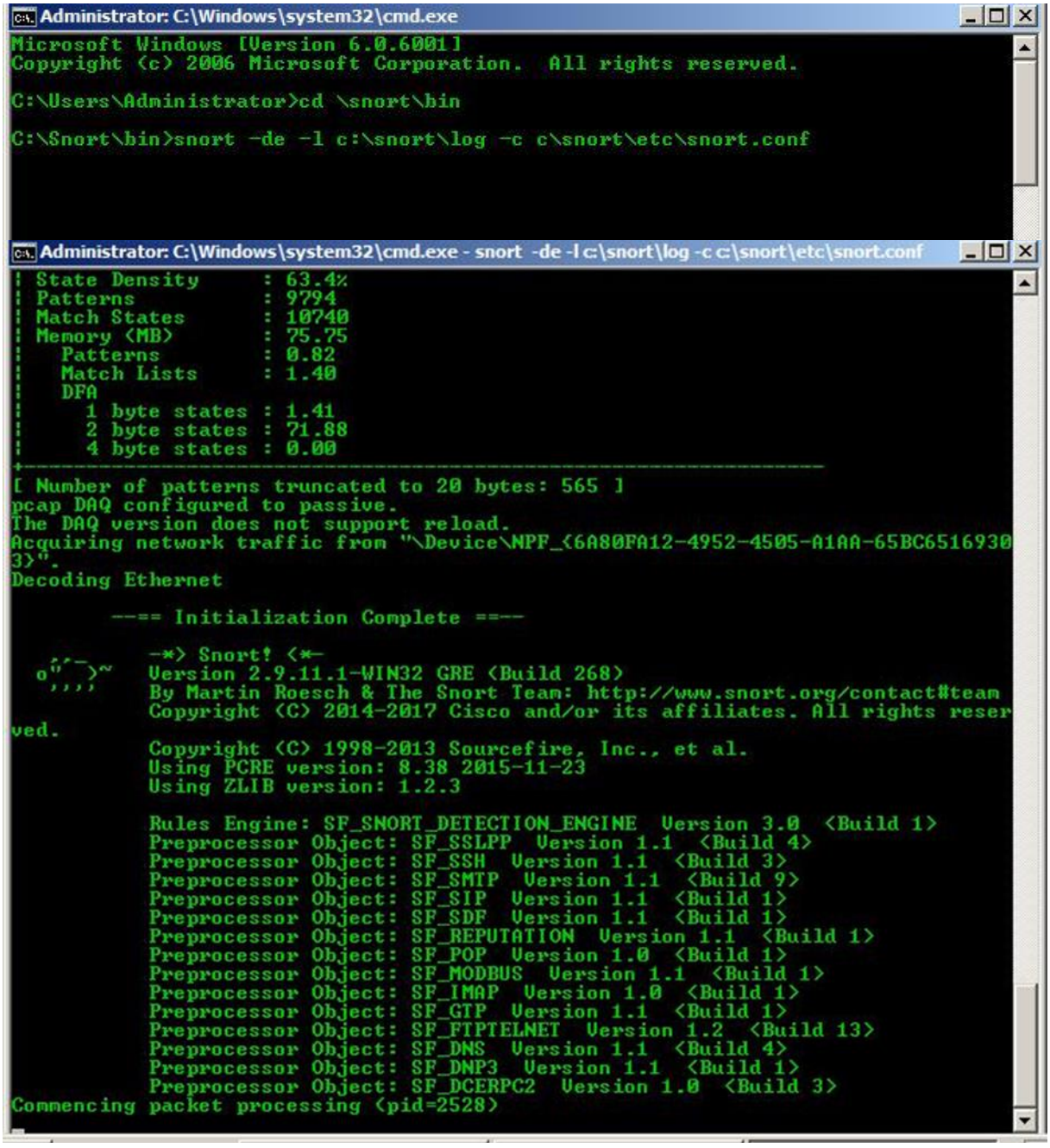
Khởi động lại Windows Server.

Sau khi khởi động lại Windows, vào Service để kiểm tra Snort được start thành công hay chưa



Bước 5: Chạy Snort ở chế độ Detect Intrusion (IDS): để phát hiện, ghi nhận và cảnh báo trên các loại traffic mạng:

Gõ lệnh: *snort –de –l c:\snort\log –c c:\snort\etc\snort.conf*




Hình 3.6:Hoàn tất khởi chạy Snort ở chế độ IDS

### 3.2.6.Mô phỏng quá trình sử lý của snort.

Vào file Local.rules theo đường dẫn C:\Snort\rules.

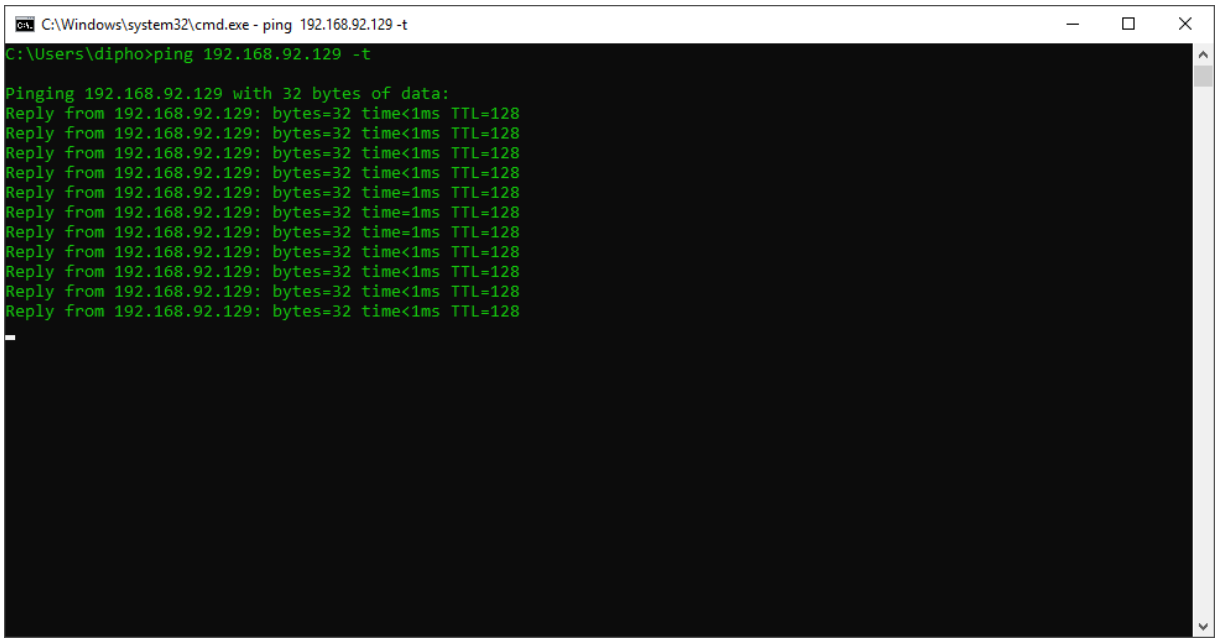
Trong file viết luật phát hiện ping với nội dung như sau:

*alert icmp any any -> $HOME_NET any (msg:"Canh bao co may dang ping"; sid:140791;)*

Sau đó lưu file lại theo đường dẫn cũ.

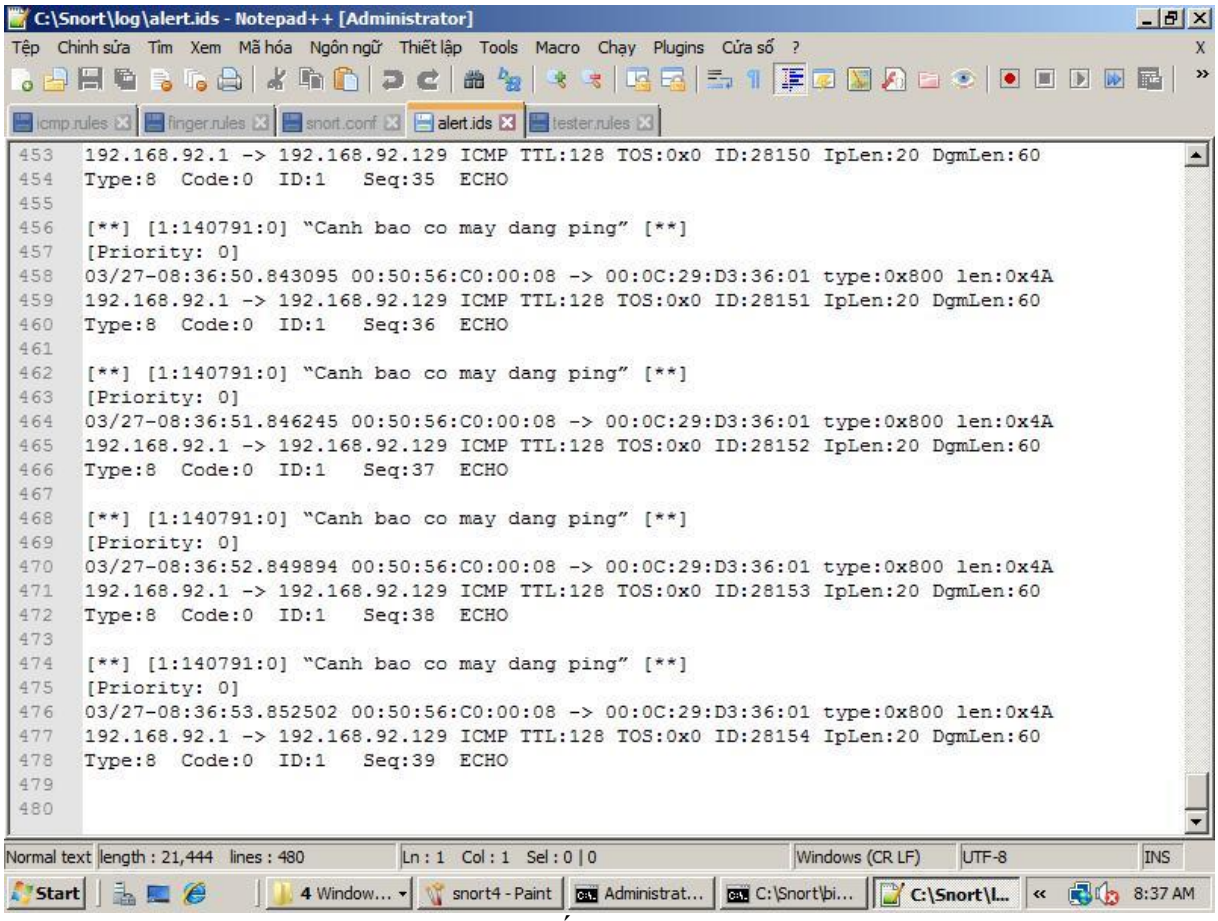
Tiếp theo ta vào máy tấn công tạo lệnh ping vào máy bị tấn công theo lệnh ping sau:Ping 192.168.92.129 -t

Kết quả ping trên máy bị tấn công như sau:




Hình 3.7 Máy attacker đang ping

Snort phát hiện ping và kiểm tra lại kết qua ở file alert.ids (C:\Snort\log)




Hình 3.8 Kết quả được ghi lại

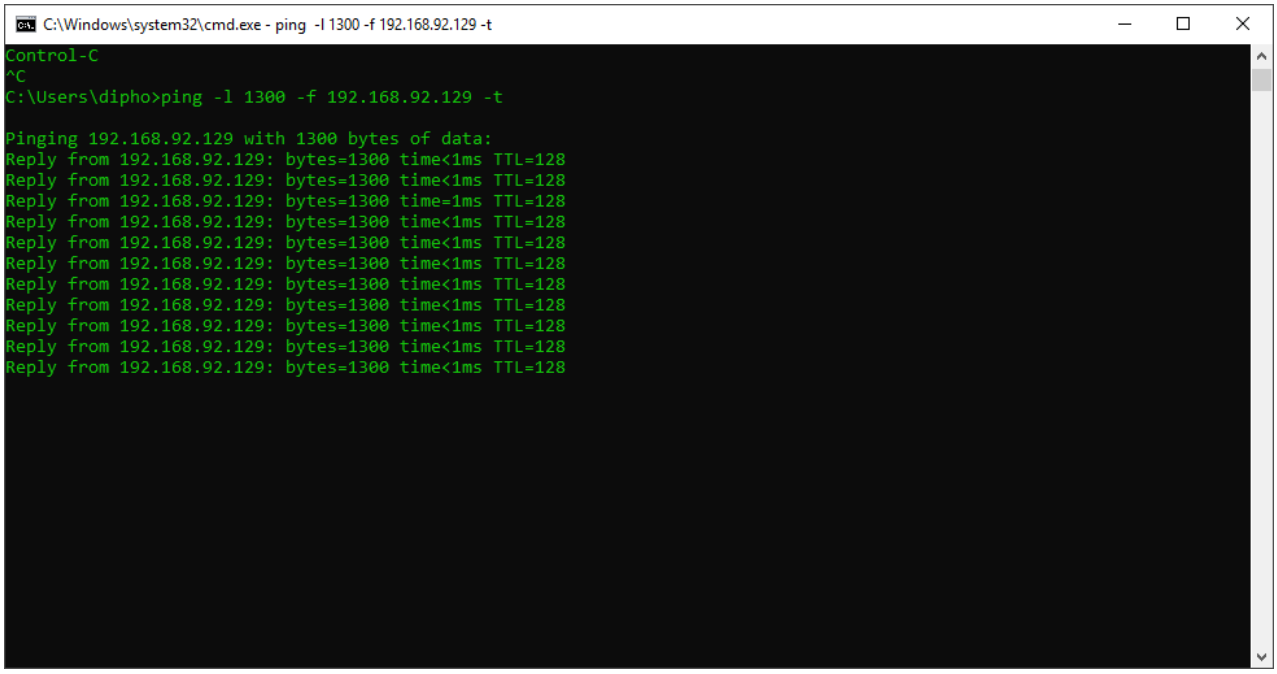
b.Tạo luật cảnh báo Ping có kích thước lớn.

Tạo file luật với lệnh:

alert icmp any any -> $HOME_NET any (msg: “Co Ping size lon”; dsize: > 1000; sid:2)

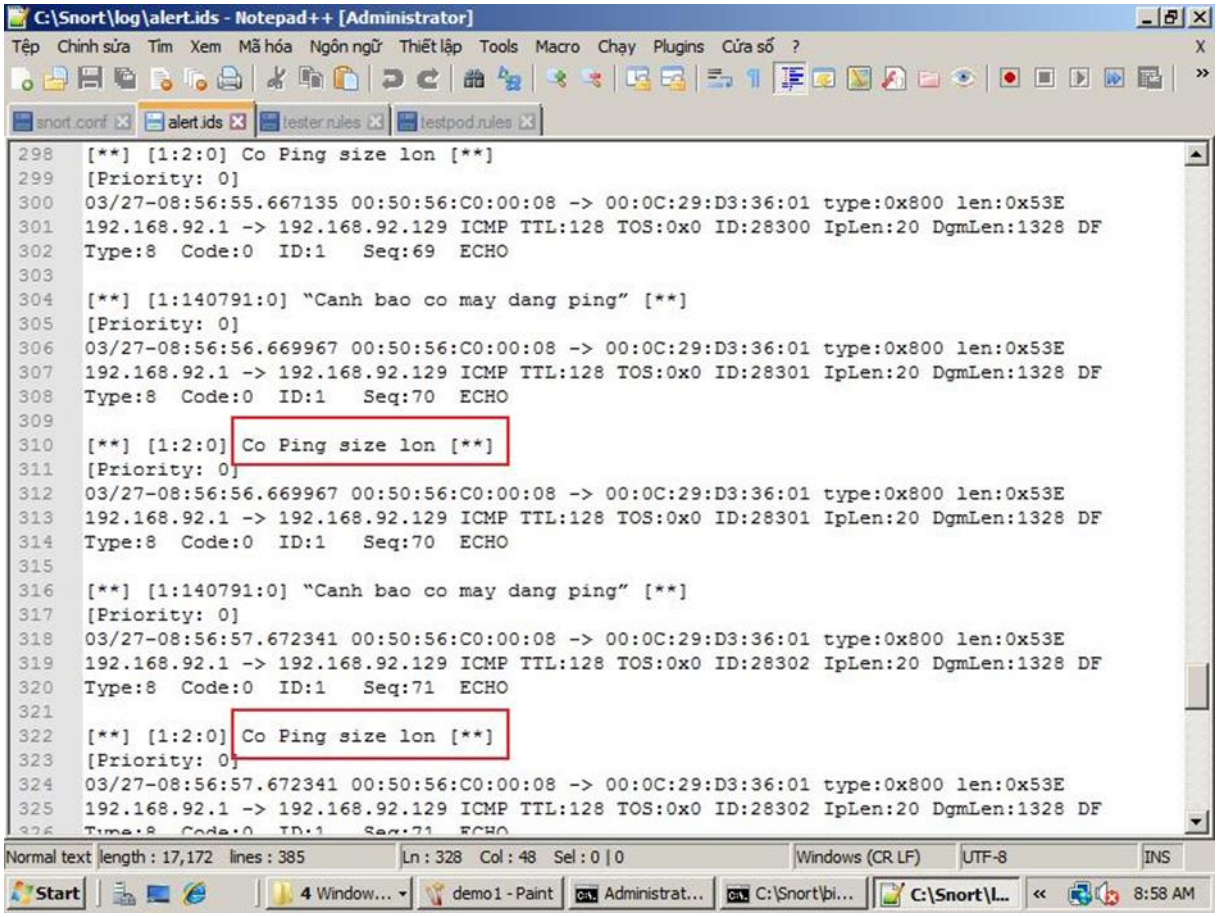
Thực hiện lệnh ping trên máy tấn công như sau:

ping –l 1300 –f 192.168.92.128 –t




Hình 3.9 Attacker đang ping gói 1300 byte tới Server

Kết quả hiển thị phát hiện trên snort




Hình 3.10:Kết quả hiển thị phát hiện phát hiện ping kích thước lớn trên snort.

## 3.3. Đề xuất quy trình đẩm bảo an toàn thông tin đối với người sử dụng mạng.

### 3.3.1. Đặt mật khẩu máy tính và ứng dụng

Đặt mật khẩu máy tính nhắm giúp người sử dụng bảo vệ được tài khoản Windows bằng mật khẩu. Nhất là các máy tính xách tay hoặc máy tính cá nhân nên khuyến khích người dùng đặt nhập mật khẩu mỗi lần bạn bật máy tính hoặc khi nó thoát khỏi chế độ ngủ đông hoặc màn hình ảo.

Mật khẩu tài khoản là một dòng lệnh phòng thủ hiệu quả đầu tiên, vì vậy nên khuyến cáo người dùng tránh sử dụng một mật khẩu thường xuyên hay mật khẩu dễ đoán. Khuyên người dùng nên chọn một mật khẩu dài, có những kí tự đặc biệt và tất nhiên phải khó để người khác đoán được.

Giải pháp bảo mật dữ liệu máy tính này được xem là cơ bản nhất, vì vậy cấp độ bảo mật cũng chỉ ở mức trung bình. Mật khẩu Windows có thể dễ dàng bị qua mặt hoặc tháo gỡ, vì thế khuyên người dùng không nên "gởi trọn niềm tin" vào nó nhé.

### 3.3.2. Sử dụng phầm mềm diệt virus

Một trong những cách bảo mật dữ liệu trên máy tính là sử dụng phần mềm diệt virus. Phần mềm độc hại (Malware) là phần mềm được thiết kế để thâm nhập hoặc gây hại cho dữ liệu máy tính mà không có sự đồng ý của bạn. Nó bao gồm virus máy tính, sâu, trojan, spyware, scareware và nhiều thứ khác nữa và có thể xuất hiện trên các trang web và email. Phần mềm độc hại là một vấn đề nghiêm trọng gây ảnh hưởng nhiều đến người sử dụng máy tính. Cách tốt nhất để tránh bị lây nhiễm là khuyến khích người người chạy một chương trình chống vi-rút tốt, chúng sẽ quét spyware định kỳ, cảnh báo khi người dùng nhấp chuột vào liên kết email hoặc trang web nguy hiểm. Điều này ít nhiều giúp người sử dụng tránh được những nguy cơ mất dữ liệu máy tính do phần mềm mã độc gây ra.

### 3.3.3. Cập nhật phần mềm thường xuyên

Cập nhật phần mềm có thể là một vấn đề gây phiền toái cho người sử dụng vì mất nhiều thời gian. Tuy nhiên chúng là một điều cần thiết, vì các bản cập nhật này chứa các bản vá bảo mật quan trọng, các bản vá lỗi ấy sẽ bảo vệ dữ liệu máy tính của bạn khỏi các mối đe dọa mới phát hiện gần nhất. Không cài đặt các cập nhật này có nghĩa là máy tính của bạn đang gặp nguy hiểm. Để đảm bảo rằng bạn sở hữu bản cập nhật bảo mật mới nhất từ hệ điều hành hãy bật hãy bật tính năng cập nhật tự động.

### 3.3.4. Mã hóa dữ liệu tối quan trọng

Mã hóa dữ liệu không chỉ dành cho những người chuyên sâu về công nghệ, người dùng bình thường cũng có thể mã hóa được. Các công cụ hiện đại sẽ giúp mọi người có thể mã hóa email và các thông tin khác một cách dễ dàng. Để tránh việc máy tính của bạn gặp rủi ro về việc mất thông tin, dữ liệu thì bạn có thể sử dụng một số phần mềm mã hóa dữ liệu máy tính như: AutoKrypt 11.09, TrueCrypt 7.1.

### 3.3.5. Bảo mật mạng không dây tại nhà ở hoặc nơi làm việc của người dùng

Khuyến cáo người dùng nên bảo mật mạng không dây tại nhà ở hoặc nơi làm việc bằng mật khẩu. Điều này ngăn ngừa các cá nhân bất hợp pháp chiếm quyền điều khiển mạng không dây của bạn. Ngay cả khi họ đang cố gắng truy cập Wi-Fi miễn phí, người dùng sẽ không muốn vô tình chia sẻ thông tin cá nhân với những người khác đang sử dụng mạng của mình mà không được sự cho phép. Mặt khác, những hacker giỏi họ có thể xâm nhập vào dữ liệu trên laptop của người dùng, vì thế để bảo mật dữ liệu máy tính yêu câu người dùng nâng cấp lớp bảo mật tại nhà ở hoặc nơi làm việc.

### 3.3.6. Bảo vệ máy tính khỏi những người sử dụng khác

Khuyến cáo người dùng hạn chế chia sẻ máy tính cho người khác, vì chúng ta không biết họ đã làm những gì với máy tính của mình. Nếu không máy tính của chúng ta có

thể bị cài những phần mềm độc hại, hay phần mềm theo dõi. Vì thế, khuyên người dùng chỉ giao máy tính cho những người thực sự tin tưởng.

### 3.3.7. Xóa hoàn toàn tập tin cần xóa

Xóa một tập tin trong Windows thực sự chỉ là di chuyển nó vào Recycle Bin. Dữ liệu của tệp tin vẫn còn trên ổ đĩa. Một tên trộm dữ liệu liên tục có thể sử dụng các tiện ích, công cụ để thu hồi thông tin đó. Vì thế, cần phải xóa các thư mục không cần thiết một cách triệt để.

### 3.3.8. Thiết lập các chính sách an toàn trên máy tính

Sử dụng tường lửa Windows, tắt dịch vụ Remote Desktop, CMD...

# KẾT LUẬN

Trong chương này đã tập trung đánh giá và phân tích hiện trạng mạng đang triển khai ở công ty CMC TELECOM. Dựa trên việc phân tích những điểm hạn chế từ đó đưa ra tính cấp thiết phải quy hoạch lại mạng máy tính của công ty. Trong phần nội dung quy hoạch mạng đã đưa ra mô hình quy hoạch và các giải pháp áp dụng vào mạng để đạt hiệu quả cao nhất. Tiếp theo trong chương đã trình bày về cấu trúc của Snort, nguyên lý hoạt động và quy tắc luật của Snort để có những kiến thức cơ bản áp dụng vào trong hệ thống.

Một trong những kết quả chính của chương là mô phỏng triển khai hệ thống phát hiện trên mô hình mạng quy hoạch. Qua kết quả mô phỏng nhận được cho thấy việc áp dụng phần mềm vào trong hệ thống là rất cần thiết, nó giúp cho người quản trị mạng kiểm soát được toàn bộ hệ thống mạng mà mình quản lý. Để bảo đảm an toàn mạng thì ngoài cơ sở hạ tầng mạng thì yếu tố con người cũng rất quan trọng, đóng vai trò quyết định đến kết quả thành công hay thất bại trong công tác bảo mật.

# TÀI LIỆU THAM KHẢO

[1.]Andrew R. Bakeer & Joel Esler (2007), Snort IDS and IPS Toolkit.Syngress Publishing, Inc.

[2.]The Snort Team (2012), Snort® User Manual 2.9.3, The Snort Project.

[3.]David Gullett (2012), Snort 2.9.3 and Snort Report 1.3.3 on Ubuntu

12.04 LTS Install Guide, Symmetrix Technologies.

[4.]VNCERT (2007), "Nghiên cứu xây dựng mô hình hệ thống quản lý An toàn Internet theo cấu trúc phân bổ", Hà Nội

[5.]Học viện kỹ thuật mật mã (2008), "Bộ giao thức TCP/IP", Học viện kỹ thuật mật mã, Hà Nội

[6.]https://www.snort.org

[7.]https://seclists.org/snort/

[8.]https://fossies.org/linux/snort/configure.in

[9.]https://www.academia.edu/4302986/Cai_d%E1%BA%B7t_Snort_Barnyard_BASE_tren_Cent_OS_5_2